ID: 363829
Sample Name: Paid561571.htm
Cookbook: default.jbs
Time: 13:32:47
Date: 05/03/2021
Version: 31.0.0 Emerald

Table of Contents

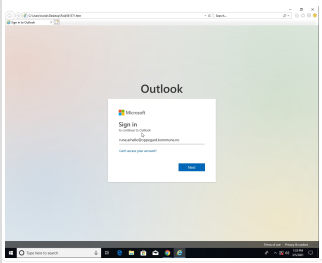
Analysis Report Paid561571.htm

Overview

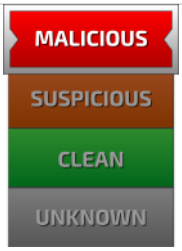
General Information

Sample Name:	Paid561571.htm
Analysis ID:	363829
MD5:	34b0610fb39400c.
SHA1:	b63e46c20b06f21.
SHA256:	6f49afc966c3172..
Infos:	

Most interesting Screenshot:



Detection



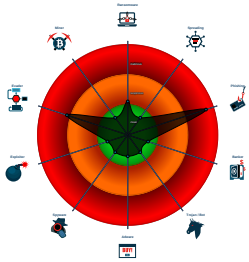
HTMLPhisher

Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Phishing site detected (based on fav…
- Yara detected HtmlPhish_10
- Yara detected obfuscated html page
- Obfuscated HTML file found
- Phishing site detected (based on log…
- HTML title does not match URL
- IP address seen in connection with o…
- Invalid 'forgot password' link found
- JA3 SSL client fingerprint seen in co…
- None HTTPS page querying sensitiv…

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 6016 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 4260 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6016 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

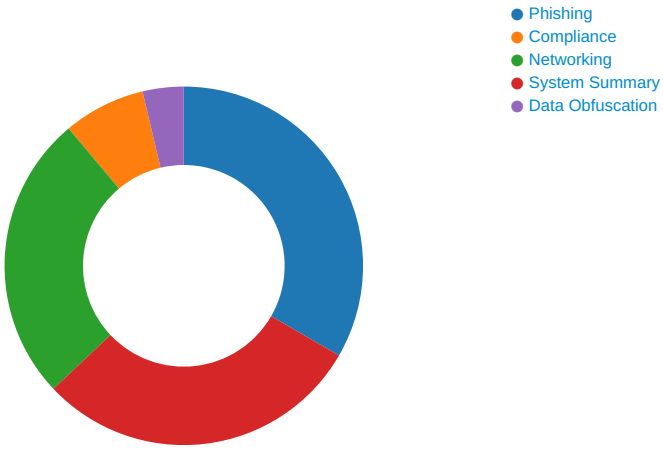
Initial Sample

Source	Rule	Description	Author	Strings
Paid561571.htm	JoeSecurity_Obshtml	Yara detected obfuscated html page	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 HtmlPhish_10

Yara detected obfuscated html page

Phishing site detected (based on logo template match)

Compliance:

Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

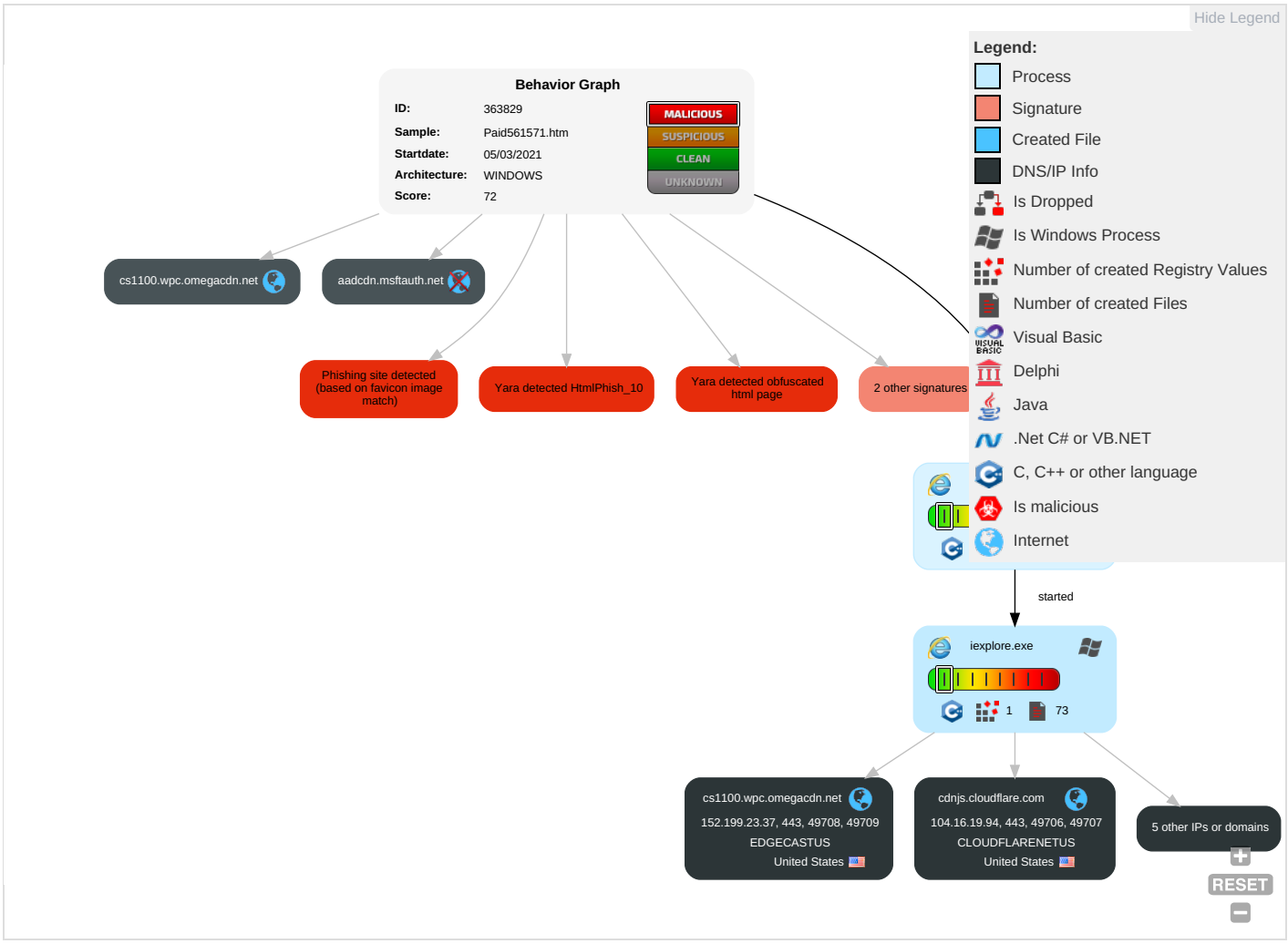
Data Obfuscation:

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

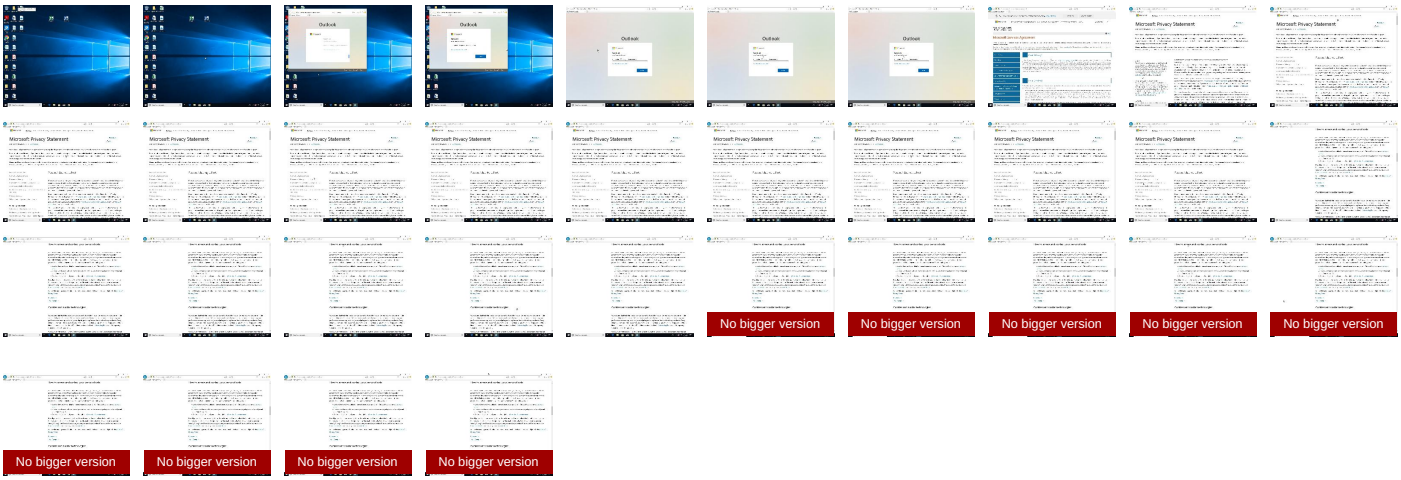
Behavior Graph

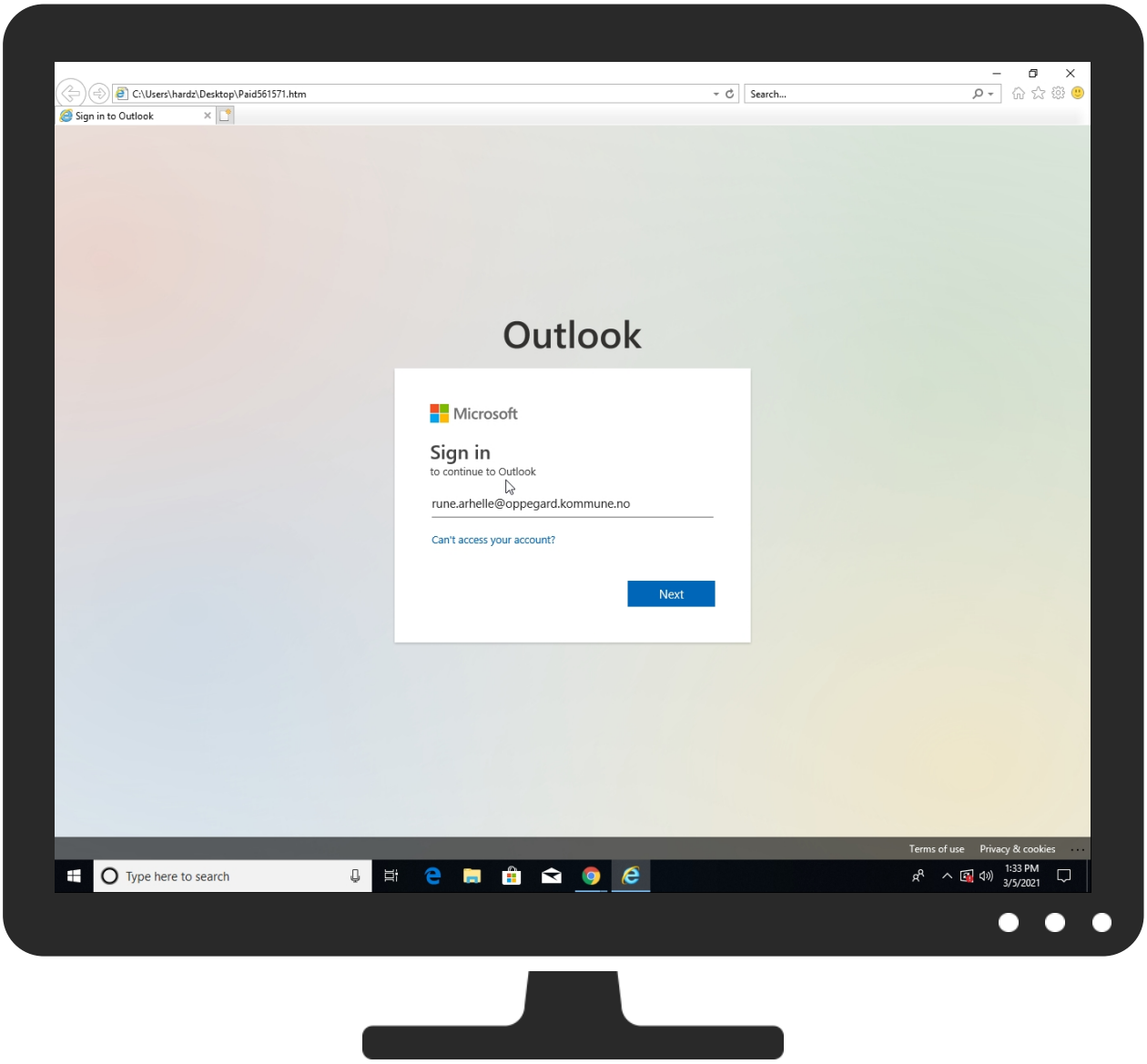


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

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
assets.onestore.ms	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://www.youradchoices.ca/fr	0%	URL Reputation	safe	
http://https://www.youradchoices.ca/fr	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://www.youradchoices.ca/fr	0%	URL Reputation	safe	
http://https://www.youradchoices.ca/fr	0%	URL Reputation	safe	
http://https://privacy.micros	0%	URL Reputation	safe	
http://https://privacy.micros	0%	URL Reputation	safe	
http://https://privacy.micros	0%	URL Reputation	safe	
http://https://privacy.micros	0%	URL Reputation	safe	
http://https://www.youradchoices.ca	0%	URL Reputation	safe	
http://https://www.youradchoices.ca	0%	URL Reputation	safe	
http://https://www.youradchoices.ca	0%	URL Reputation	safe	
http://https://www.youradchoices.ca	0%	URL Reputation	safe	
http://www.mpegla.com).	0%	Avira URL Cloud	safe	
http://https://www.skype.com).	0%	Avira URL Cloud	safe	
http://https://www.microsoft./Desktop/Paid561571.htm	0%	Avira URL Cloud	safe	
http://fontello.comiconsRegulariconsiconsVersion	0%	URL Reputation	safe	
http://fontello.comiconsRegulariconsiconsVersion	0%	URL Reputation	safe	
http://fontello.comiconsRegulariconsiconsVersion	0%	URL Reputation	safe	
http://fontello.comiconsRegulariconsiconsVersion	0%	URL Reputation	safe	
http://https://www.microsoft.	0%	URL Reputation	safe	
http://https://www.microsoft.	0%	URL Reputation	safe	
http://https://www.microsoft.	0%	URL Reputation	safe	
http://https://www.microsoft.	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	104.16.19.94	true	false		high
code.jquery.com	unknown	unknown	false		high
aadcdn.msftauth.net	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
assets.onestore.ms	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
ajax.aspnetcdn.com	unknown	unknown	false		high

Contacted URLs

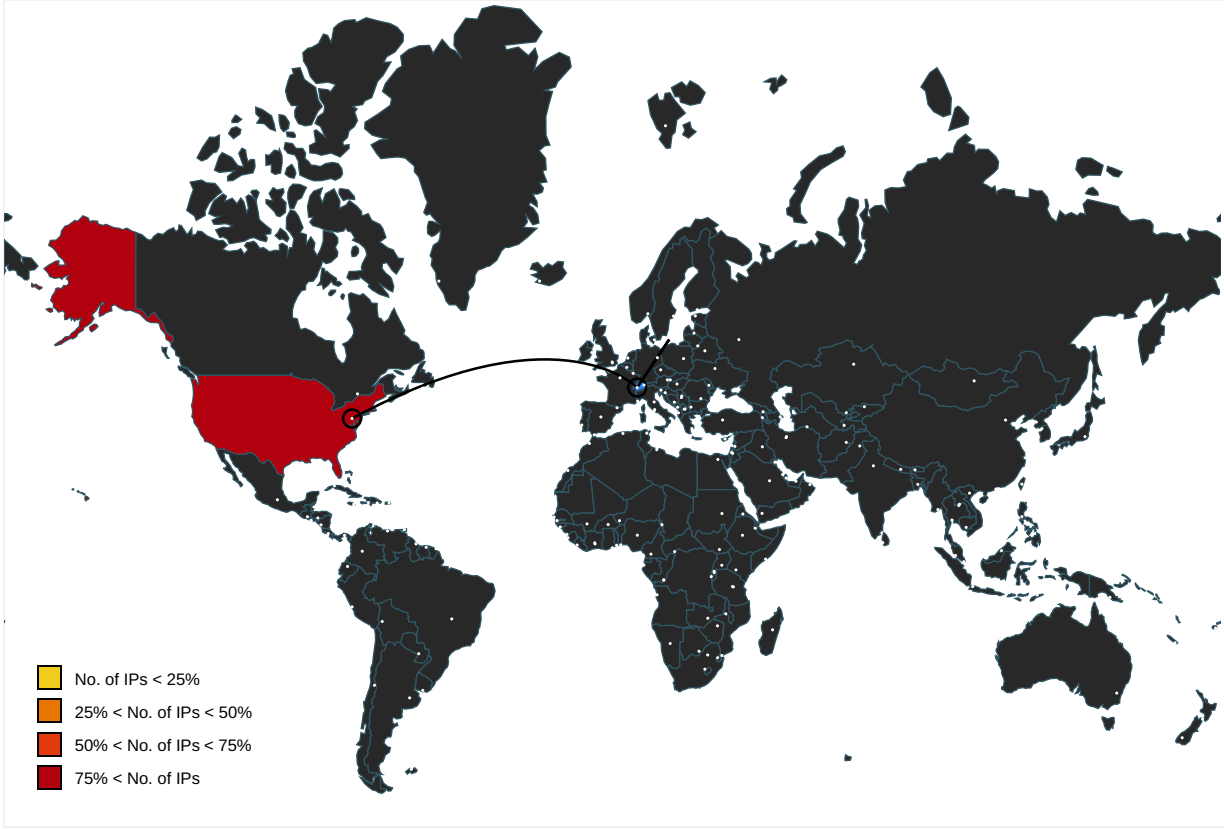
Name	Malicious	Antivirus Detection	Reputation
file:///C:/Users/user/Desktop/Paid561571.htm	true		low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://aka.ms/useterms	servicesagreement[1].htm.2.dr	false		high
http://fontawesome.io	font-awesome[1].css.2.dr	false		high
http://https://aka.ms/redeemrewards	servicesagreement[1].htm.2.dr	false		high
http://https://signin.kissmetrics.com/privacy/#controls	privacystatement[1].htm.2.dr	false		high
http://https://login.skype.com/login	privacystatement[1].htm.2.dr	false		high
http://https://www.acuityads.com/opt-out/	privacystatement[1].htm.2.dr	false		high
http://https://www.skype.com/go/ustax	servicesagreement[1].htm.2.dr	false		high
http://https://www.optimizely.com/legal/opt-out/	privacystatement[1].htm.2.dr	false		high
http://https://www.youradchoices.ca/fr	privacystatement[1].htm.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.adr.org	servicesagreement[1].htm.2.dr	false		high
http://https://www.xbox.com/en-US/Legal/CodeOfConduct)	servicesagreement[1].htm.2.dr	false		high
http://www.asp.net/ajaxlibrary/CDN.ashx.	privacystatement[1].htm.2.dr	false		high
http://https://www.xbox.com/en-US/Legal/CodeOfConduct	servicesagreement[1].htm.2.dr	false		high
http://https://aka.ms/taxservice	servicesagreement[1].htm.2.dr	false		high
http://https://www.privacyshield.gov/welcome	privacystatement[1].htm.2.dr	false		high
http://https://ondemand.webtrends.com/support/optout.asp	privacystatement[1].htm.2.dr	false		high
http://https://www.skype.com/go/legal.broadcast	servicesagreement[1].htm.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://skype.com/go/myaccount	servicesagreement[1].htm.2.dr	false		high
http://https://www.skype.com	servicesagreement[1].htm.2.dr	false		high
http://https://www.appsflyer.com/optout	privacystatement[1].htm.2.dr	false		high
http://https://privacy.micros	{6E400DE5-7DFA-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.appnexus.com/	privacystatement[1].htm.2.dr	false		high
http://https://aka.ms/redeemrewards).	servicesagreement[1].htm.2.dr	false		high
http://www.mpegla.com	servicesagreement[1].htm.2.dr	false		high
http://https://www.youradchoices.ca	privacystatement[1].htm.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://priv-policy.imrworldwide.com/priv/browser/us/en/optout.html	privacystatement[1].htm.2.dr	false		high
http://github.com/requirejs/almond/LICENSE	17-f90ef1[1].js.2.dr	false		high
http://https://www.youronlinechoices.com/	privacystatement[1].htm.2.dr	false		high
http://https://mixer.com/contact	servicesagreement[1].htm.2.dr	false		high
http://https://www.here.com/)	privacystatement[1].htm.2.dr	false		high
http://https://www.skype.com/go/store.reactivate.credit	servicesagreement[1].htm.2.dr	false		high
http://https://www.aboutads.info/	privacystatement[1].htm.2.dr	false		high
http://https://www.adjust.com/opt-out/	privacystatement[1].htm.2.dr	false		high
http://https://www.xbox.com/managedatacollection	privacystatement[1].htm.2.dr	false		high
http://https://www.xbox.com/legal/codeofconduct	privacystatement[1].htm.2.dr	false		high
http://https://www.xbox.com/xbox-game-studios)	servicesagreement[1].htm.2.dr	false		high
http://https://developer.yahoo.com/flurry/end-user-opt-out/	privacystatement[1].htm.2.dr	false		high
http://fontello.com	icons[1].eot.2.dr	false		high
http://www.mpegla.com).	servicesagreement[1].htm.2.dr	false	• Avira URL Cloud: safe	low
http://https://aka.ms/kinectprivacy/	privacystatement[1].htm.2.dr	false		high
http://https://www.skype.com).	servicesagreement[1].htm.2.dr	false	• Avira URL Cloud: safe	low
http://https://www.xbox.com	privacystatement[1].htm.2.dr	false		high
http://https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protectio	privacystatement[1].htm.2.dr	false		high
http://https://www.clicktale.net/disable.html	privacystatement[1].htm.2.dr	false		high
http://fontawesome.io/license	font-awesome[1].css.2.dr	false		high
http://https://www.skype.com/go/allrates	servicesagreement[1].htm.2.dr	false		high
http://https://www.microsoft./Desktop/Paid561571.htm	{6E400DE5-7DFA-11EB-90E4-ECF4BB862DED}.dat.1.dr	true	• Avira URL Cloud: safe	unknown
http://https://www.xbox.com/xbox-game-studios	servicesagreement[1].htm.2.dr	false		high
http://fontello.comiconsRegulariconsiconsVersion	icons[1].eot.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://support.xbox.com/help/family-online-safety/online-safety/manage-online-safety-and-privacy-se	privacystatement[1].htm.2.dr	false		high
http://https://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager.html	privacystatement[1].htm.2.dr	false		high
http://https://www.skype.com/go/legal	servicesagreement[1].htm.2.dr	false		high
http://https://mixer.com/about/tos	servicesagreement[1].htm.2.dr	false		high
http://https://www.microsoft.	{6E400DE5-7DFA-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.xbox.com/	privacystatement[1].htm.2.dr	false		high
http://https://github.com/h5bp/html5-boilerplate/blob/master/src/css/main.css	app[1].css.2.dr	false		high
http://https://www.linkedin.com/legal/privacy-policy	privacystatement[1].htm.2.dr	false		high
http://https://aka.ms/DPA	privacystatement[1].htm.2.dr	false		high
http://https://support.xbox.com/help/friends-social-activity/community/use-safety-settings	privacystatement[1].htm.2.dr	false		high
http://https://www.xbox.com/Legal/ThirdPartyDataSharing	privacystatement[1].htm.2.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
152.199.23.37	cs1100.wpc.omegacdn.net	United States		15133	EDGECASTUS	false
104.16.19.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	363829
Start date:	05.03.2021
Start time:	13:32:47
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Paid561571.htm
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:	26
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:	mal72.phis.evad.winHTM@3/44@6/2

Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .htm • Browsing link: https://www.microsoft.com/en-US/servicesagreement/ • Browsing link: https://privacy.microsoft.com/en-US/privacystatement
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.42.151.234, 104.108.39.131, 209.197.3.24, 104.43.139.144, 104.43.193.48, 13.64.90.137, 13.88.21.125, 23.211.5.92, 92.122.213.200, 92.122.213.219, 184.30.25.170, 152.199.19.160, 13.107.246.19, 13.107.213.19, 92.122.213.247, 92.122.213.194, 104.108.38.107, 152.199.19.161, 184.30.24.56, 20.82.209.183, 168.61.161.212, 20.54.26.129, 51.11.168.160 • Excluded domains from analysis (whitelisted): cds.s5x3j6q5.hwcdn.net, standard.t-0009.t-msedge.net, assets.onestore.ms.edgekey.net, arc.msn.com.nsatc.net, e13678.dscb.akamaiedge.net, i.s-microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, e11290.dspg.akamaiedge.net, www.microsoft.com-c-3.edgekey.net, star-azurefd-prod.trafficmanager.net, watson.telemetry.microsoft.com, a1778.g2.akamai.net, e10583.dspg.akamaiedge.net, fs.microsoft.com, db3p-ris-pf-prod-atm.trafficmanager.net, ris-prod.trafficmanager.net, aadcdnoriginneu.azureedge.net, skypedataprdcolcus17.cloudapp.net, skypedataprdcolcus16.cloudapp.net, statics-marketingsites-wcus-ms-com.akamaized.net, assets.onestore.ms.akadns.net, skypedataprdcolcus15.cloudapp.net, c-s.cms.ms.akadns.net, ris.api.iris.microsoft.com, t-0009.t-msedge.net, blobcollector.events.data.trafficmanager.net, c.s-microsoft.com-c.edgekey.net, privacy.microsoft.com.edgekey.net, cs9.wpc.v0cdn.net, i.s-microsoft.com, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net, iecvlist.microsoft.com, go.microsoft.com, mscomajax.vo.msecnd.net, dual.t-0009.t-msedge.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, cs22.wpc.v0cdn.net, ie9comview.vo.msecnd.net, e1723.g.akamaiedge.net, aadcdnoriginneu.ec.azureedge.net, c.s-microsoft.com, privacy.microsoft.com, go.microsoft.com.edgekey.net, Edge-Prod-FRAr3.ctrl.t-0009.t-msedge.net, e13678.dscg.akamaiedge.net, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net, www.microsoft.com, e13678.dspb.akamaiedge.net, wcpstatic.microsoft.com • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

No simulations

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
152.199.23.37	Remittance0434.htm	Get hash	malicious	Browse	
	remit726498.htm	Get hash	malicious	Browse	
	Payment.html	Get hash	malicious	Browse	
	Remittance advice.htm	Get hash	malicious	Browse	
	moog_invoice_Wednesday 02242021._xslx.hTML	Get hash	malicious	Browse	
	FAX-MESSAGE201636576736375362.hTMl	Get hash	malicious	Browse	
	Thursday, February 11th, 2021, 20210211033346.3BD4A181171AEBE1@gotasdeamor.cl.htm	Get hash	malicious	Browse	
	February Payroll.xls.htm	Get hash	malicious	Browse	
	Tuesday, February 9th, 2021 83422 a.m., 20210209083422.7B8380338EC1D61B@sophiajoyas.cl.html	Get hash	malicious	Browse	
	Thursday, February 4th, 2021 103440 p.m., 20210204223440.464D4D4AD1BFDE50@juidine.com.html	Get hash	malicious	Browse	
	PAYMENT.xlsx	Get hash	malicious	Browse	
	PAYMENT INFO.xlsx	Get hash	malicious	Browse	
	1_25_2021 11_20_30 a.m., [Payment 457 CMSupportDev].html	Get hash	malicious	Browse	
	20202237F.html	Get hash	malicious	Browse	
	Notice_Admin_Johnstoncompanies_8578.htm	Get hash	malicious	Browse	
	1.html	Get hash	malicious	Browse	
	http://https://r0qp15r0b1rq05rrpbqbrpq5.s3-eu-west-1.amazonaws.com/Ap3dX.html#joetorre@gmail.com	Get hash	malicious	Browse	
	http://https://app.box.com/s/cwvx197f4b14m7rxw8vlqc08jwv0c5og	Get hash	malicious	Browse	
	http://message.mydopweb.com	Get hash	malicious	Browse	
	http://https://r0qp15r0b1rq05rrpbqbrpq5.s3-eu-west-1.amazonaws.com/Ap3dX.html#orderadmin@roku.com	Get hash	malicious	Browse	
104.16.19.94	http://https://bit.ly/3hDDoTm	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://ninjutsu.4ryu.com/.well-known/pki-validation/zombaiogw_1_1/print_recipe.php?living=ytpr1h11zw0qw0&south=difference&slide=during	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://surl.me/vy4l	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://u15974653.ct.sendgrid.net/ls/click?upn=sKo8P2XHLOhqpgLcALrpHsAMymMPQ9pJ-2BnCP9l5luXmX2tau-2FkmeQME9D69RU7ffQBYwWBrDSW94kS5u6ig5BmkhgBhgQJfm-2BsLwvjPlmdPdsXD4ILOaqVNEwgY7GAZQPkafmgyIOS5FU-2B6124ooi1O-2FMB47qUlmVhTTnK6qV5fGlsBAy7itOSHfP1wikhvsiyeK_Y89n8cg5DiKkjVvtw-2FYSjk3JbqBqCNqd4QE5c0z9p4IJ6aN66chjxOUHcribC2kbrQ6ua83fMfn3Hnb3TofbErA9L2X-2BpZpbvzOnYxCl6WSRvjbd6cnTXhRnH1-2Btzg-2FEpNckJ170lMbhRvVxgpvwWV6rRyYLwNDxpt3lm1lgyNi-2B-2B86Pp03BP8O3y-2Bw2BSUYNj8fK3irR9dYwZuWCkvZJ3fJURjdr0uD0itVZut-2BhVs-3D	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/font-awesome/4.1.0/fonts/fontawesome-webfont.eot?

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://j.mp/38NwiZZ	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://lokalny-biznes.eu/modules/mod_simplefileuploadv1.3/elements/reactivation/indextest.php?youll=enwht11p10sc0&picture=call&please=gave	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://pinpoint-insights.com/interx/tracker?op=click&id=107b4.3e3b&url=https%3A%2F%2Fpinpoint-insights.com%2Finterx%2Funsubscribe%3Fid%3D107b4.3e3b%26type%3Dnormal&_hC=D7C07475	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/flickity/1.0.0/flickity.min.css
	http://https://pinpoint-insights.com/interx/tracker?op=click&id=107b4.3e3b&url=https%3A%2F%2Fpinpoint-insights.com%2Finterx%2Funsubscribe%3Fid%3D107b4.3e3b%26type%3Dnormal&_hC=D7C07475	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/flickity/1.0.0/flickity.min.css

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cdnjs.cloudflare.com	Remittance0434.htm	Get hash	malicious	Browse	• 104.16.18.94
	Invoice 76221 Secured_Pdf_brianc@johnstoncompanies.com.html	Get hash	malicious	Browse	• 104.16.18.94
	INV#45567.html	Get hash	malicious	Browse	• 104.16.18.94
	holla.htm	Get hash	malicious	Browse	• 104.16.18.94
	wzdu53.exe	Get hash	malicious	Browse	• 104.16.18.94
	wzdu53.exe	Get hash	malicious	Browse	• 104.16.19.94
	remit726498.htm	Get hash	malicious	Browse	• 104.16.18.94
	ARMI Contractors RFQ.xlsx	Get hash	malicious	Browse	• 104.16.18.94
	ARMI Contractors RFQ.xlsx	Get hash	malicious	Browse	• 104.16.18.94
	DTN Basis AWS Basis Main (1).xlsm	Get hash	malicious	Browse	• 104.16.18.94
	DTN Basis AWS Basis Main (1).xlsm	Get hash	malicious	Browse	• 104.16.18.94
	DTN Basis AWS Basis Main (1).xlsm	Get hash	malicious	Browse	• 104.16.18.94
	#Ud83d#Udcde..... dianna.graves@claremontmckenna.edu.html	Get hash	malicious	Browse	• 104.16.18.94
	Sprint Note nicla.dipalma@brewin.co.uk 113816 AM .html	Get hash	malicious	Browse	• 104.16.19.94
	DTN Basis AWS Basis Main.xlsm	Get hash	malicious	Browse	• 104.16.19.94
	RFQ.xlsx	Get hash	malicious	Browse	• 104.16.18.94
	RFQ.xlsx	Get hash	malicious	Browse	• 104.16.18.94
	DTN Basis AWS Basis Main.xlsm	Get hash	malicious	Browse	• 104.16.19.94
	Sprint Note tod.friedman@americansignaturefurniture.com 81454 AM .html	Get hash	malicious	Browse	• 104.16.19.94
	Outllook_Membership_Update.html	Get hash	malicious	Browse	• 104.16.19.94
cs1100.wpc.omegacdn.net	Remittance0434.htm	Get hash	malicious	Browse	• 152.199.23.37
	remit726498.htm	Get hash	malicious	Browse	• 152.199.23.37
	Payment.html	Get hash	malicious	Browse	• 152.199.23.37
	Remittance advice.htm	Get hash	malicious	Browse	• 152.199.23.37
	moog_invoice_Wednesday 02242021._xslx.hTML	Get hash	malicious	Browse	• 152.199.23.37
	FAX-MESSAGE201636576736375362.hTMl	Get hash	malicious	Browse	• 152.199.23.37
	Thursday, February 11th, 2021, 20210211033346.3BD4A181171AEBE1@gotasdeamor.cl.htm	Get hash	malicious	Browse	• 152.199.23.37
	February Payroll.xls.htm	Get hash	malicious	Browse	• 152.199.23.37
	Tuesday, February 9th, 2021 83422 a.m., 20210209083422.7B8380338EC1D61B@sophiajoyas.cl.html	Get hash	malicious	Browse	• 152.199.23.37
	Thursday, February 4th, 2021 103440 p.m., 20210204223440.464D4D4AD1BFDE50@juidine.com.html	Get hash	malicious	Browse	• 152.199.23.37
	PAYMENT.xlsx	Get hash	malicious	Browse	• 152.199.23.37
	PAYMENT INFO.xlsx	Get hash	malicious	Browse	• 152.199.23.37
	1_25_2021 11_20_30 a.m., [Payment 457 CMSupportDev].html	Get hash	malicious	Browse	• 152.199.23.37
	20202237F.html	Get hash	malicious	Browse	• 152.199.23.37
	Notice_Admin_Johnstoncompanies_8578.htm	Get hash	malicious	Browse	• 152.199.23.37
	1.html	Get hash	malicious	Browse	• 152.199.23.37
	http://https://r0qp15r0b1rq05rrpbqbrpq5.s3-eu-west-1.amazonaws.com/Ap3dX.html#joetorre@gmail.com	Get hash	malicious	Browse	• 152.199.23.37

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://app.box.com/s/cwvx197f4b14m7rxw8vlqc08jwv0c5og	Get hash	malicious	Browse	• 152.199.23.37
	http://message.mydopweb.com	Get hash	malicious	Browse	• 152.199.23.37
	http://https://r0qp15r0b1rq05rrpbqbrpq5.s3-eu-west-1.amazonaws.com/Ap3dX.html#orderadmin@roku.com	Get hash	malicious	Browse	• 152.199.23.37

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
EDGECASTUS	Remittance0434.htm	Get hash	malicious	Browse	• 152.199.23.37
	603e0ffd2eeb9.tar.dll	Get hash	malicious	Browse	• 192.229.221.206
	remit726498.htm	Get hash	malicious	Browse	• 152.199.23.37
	#Ud83d#Udd04nick.ulycz- domesticandgeneral.com OKeep.htm	Get hash	malicious	Browse	• 152.199.23.72
	Gewinncode-32532404.docm	Get hash	malicious	Browse	• 152.199.21.141
	2021-02-18 Fivoor - Overleg - Kwartaaloverleg.docx	Get hash	malicious	Browse	• 152.199.21.175
	Xeros from condor.htm	Get hash	malicious	Browse	• 93.184.220.70
	Payment.html	Get hash	malicious	Browse	• 152.199.23.37
	Remittance advice.htm	Get hash	malicious	Browse	• 152.199.23.37
	moog_invoice_Wednesday 02242021._xslx.hTML	Get hash	malicious	Browse	• 152.199.23.37
	FAX-MESSAGE201636576736375362.hTMl	Get hash	malicious	Browse	• 152.199.23.37
	Z4fYo3NwC0.exe	Get hash	malicious	Browse	• 93.184.220.29
	602b97e0b415b.png.dll	Get hash	malicious	Browse	• 192.229.221.215
	Thursday, February 11th, 2021, 20210211033346.3BD4A181171AEBE1@gotasdeamor.cl.htm	Get hash	malicious	Browse	• 152.199.23.37
	Tuesday, February 9th, 2021 8%3A1%3A54 a.m., _20210209080154.8E45EAA12FF8DC21@sophiajoyas.cl_.html	Get hash	malicious	Browse	• 192.229.221.185
	Farie PO.doc	Get hash	malicious	Browse	• 192.229.221.185
	5DktGbEvIA.apk	Get hash	malicious	Browse	• 68.232.34.193
	February Payroll.xls.htm	Get hash	malicious	Browse	• 152.199.23.37
	Tuesday, February 9th, 2021 83422 a.m., 20210209083422.7B8380338EC1D61B@sophiajoyas.cl.html	Get hash	malicious	Browse	• 152.199.23.37
	Friday_ February 5th_ 2021 64427 a.m._ 20210205064427.64791275BD060468@juidine.com.html	Get hash	malicious	Browse	• 192.229.221.185
CLOUDFLARENETUS	COAU7229898130.xlsx	Get hash	malicious	Browse	• 104.16.16.194
	QO-QC201909Rev1.xlsx	Get hash	malicious	Browse	• 23.227.38.74
	New Order.doc	Get hash	malicious	Browse	• 172.67.219.133
	PO_701_36_01_27.doc	Get hash	malicious	Browse	• 172.67.208.139
	tGb2s1rgMG.exe	Get hash	malicious	Browse	• 1.1.1.1
	March 4, 2021, 055038 PM.HTM	Get hash	malicious	Browse	• 104.18.10.207
	44260.8523962963.dll	Get hash	malicious	Browse	• 104.20.184.68
	xfe.dll	Get hash	malicious	Browse	• 104.20.185.68
	pago de documento de pedido.exe	Get hash	malicious	Browse	• 162.159.133.233
	N0ir32BDve.dll	Get hash	malicious	Browse	• 104.20.184.68
	flashInstaller.dmg	Get hash	malicious	Browse	• 104.21.21.95
	Overdue-Debt-2127683982-03042021.xls	Get hash	malicious	Browse	• 172.67.166.253
	Overdue-Debt-2127683982-03042021.xls	Get hash	malicious	Browse	• 172.67.166.253
	Datos factura.doc	Get hash	malicious	Browse	• 104.21.10.120
	FileZilla_3.50.0_win64-setup.exe	Get hash	malicious	Browse	• 162.159.200.1
	SecuriteInfo.com.Heur.26922.xls	Get hash	malicious	Browse	• 104.21.75.26
	SecuriteInfo.com.Heur.26922.xls	Get hash	malicious	Browse	• 172.67.166.253
	SecuriteInfo.com.Heur.20362.xls	Get hash	malicious	Browse	• 172.67.166.253
	Overdue-Debt-772042115-03042021.xls	Get hash	malicious	Browse	• 104.21.75.26
	SecuriteInfo.com.Heur.20362.xls	Get hash	malicious	Browse	• 104.21.75.26

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	44260.8523962963.dll	Get hash	malicious	Browse	• 104.16.19.94 • 152.199.23.37
	xfe.dll	Get hash	malicious	Browse	• 104.16.19.94 • 152.199.23.37
	March 4, 2021, 071116 AM.HTM	Get hash	malicious	Browse	• 104.16.19.94 • 152.199.23.37

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SWIFT_XV5.exe	Get hash	malicious	Browse	• 104.16.19.94 • 152.199.23.37
	Sample_Item.exe	Get hash	malicious	Browse	• 104.16.19.94 • 152.199.23.37
	N0ir32BDve.dll	Get hash	malicious	Browse	• 104.16.19.94 • 152.199.23.37
	remmittance859405__.htm	Get hash	malicious	Browse	• 104.16.19.94 • 152.199.23.37
	SecuriteInfo.com.generic.ml.4293.dll	Get hash	malicious	Browse	• 104.16.19.94 • 152.199.23.37
	7.attach.dll	Get hash	malicious	Browse	• 104.16.19.94 • 152.199.23.37
	Static.dll	Get hash	malicious	Browse	• 104.16.19.94 • 152.199.23.37
	Static.dll	Get hash	malicious	Browse	• 104.16.19.94 • 152.199.23.37
	b2een4.exe	Get hash	malicious	Browse	• 104.16.19.94 • 152.199.23.37
	RemittanceAdvice-000010434.htm	Get hash	malicious	Browse	• 104.16.19.94 • 152.199.23.37
	audio_shanti.ramesh@cae.com_file.htm	Get hash	malicious	Browse	• 104.16.19.94 • 152.199.23.37
	DF2jAD8YEb.dll	Get hash	malicious	Browse	• 104.16.19.94 • 152.199.23.37
	msals.dll	Get hash	malicious	Browse	• 104.16.19.94 • 152.199.23.37
	maxe.exe	Get hash	malicious	Browse	• 104.16.19.94 • 152.199.23.37
	Waybill.html	Get hash	malicious	Browse	• 104.16.19.94 • 152.199.23.37
	mon103.dll	Get hash	malicious	Browse	• 104.16.19.94 • 152.199.23.37
	Remittance0434.htm	Get hash	malicious	Browse	• 104.16.19.94 • 152.199.23.37
37f463bf4616ecd445d4a1937da06e19	midterm_problem1.exe	Get hash	malicious	Browse	• 152.199.23.37
	midterm_problem1.exe	Get hash	malicious	Browse	• 152.199.23.37
	PDC_156280_5635_ALF.xlsx	Get hash	malicious	Browse	• 152.199.23.37
	equinitiTicket#51347303511505986.htm	Get hash	malicious	Browse	• 152.199.23.37
	condiz_03.21.doc	Get hash	malicious	Browse	• 152.199.23.37
	pago de documento de pedido.exe	Get hash	malicious	Browse	• 152.199.23.37
	remmittance859405__.htm	Get hash	malicious	Browse	• 152.199.23.37
	SecuriteInfo.com.Variant.Midie.79660.31247.exe	Get hash	malicious	Browse	• 152.199.23.37
	WinRAR_1845561462.exe	Get hash	malicious	Browse	• 152.199.23.37
	annualreport.xlsx	Get hash	malicious	Browse	• 152.199.23.37
	Weekly Vacancy Status Report.xlsm	Get hash	malicious	Browse	• 152.199.23.37
	Order MR-B. 04 03 21.exe	Get hash	malicious	Browse	• 152.199.23.37
	RemittanceAdvice-000010434.htm	Get hash	malicious	Browse	• 152.199.23.37
	Weekly Vacancy Status Report.xlsm	Get hash	malicious	Browse	• 152.199.23.37
	audio_shanti.ramesh@cae.com_file.htm	Get hash	malicious	Browse	• 152.199.23.37
	Weekly Vacancy Status Report.xlsm	Get hash	malicious	Browse	• 152.199.23.37
	PaymentConfirmation_9QE1-NSSB8U-CHF3.htm	Get hash	malicious	Browse	• 152.199.23.37
	Document (2).exe	Get hash	malicious	Browse	• 152.199.23.37
	SecuriteInfo.com.__vbaHresultCheckObj.5571.exe	Get hash	malicious	Browse	• 152.199.23.37
	Waybill.html	Get hash	malicious	Browse	• 152.199.23.37

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{6E400DE3-7DFA-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	33368

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{6E400DE3-7DFA-11EB-90E4-ECF4BB862DED}.dat	
Entropy (8bit):	1.8736066976027632
Encrypted:	false
SSDEEP:	96:ryZVZs2INW+Mt+aPf+7S1WM+TUde+1X0+Vde+mnt+yS+m3:ryZVZs2INWzt5fiFMwTHttrS3
MD5:	97763BD2282AAFC03BE426915FBAC9AC
SHA1:	6E55EBA3139F5AF8A1C458FF45EAE5E4617E2EFD
SHA-256:	373E23BD7939B9360A64D74388EA8052065B3656F4335C91600D7A3214CEFAA2
SHA-512:	3857FAF6B1F6E891B0EB8E44ADE97C1CC591843B396C7A2DE66C20A914FE19AACE74898FDB1802E41F49FC46E01A67C82BBCC118DB1A245F58F7A3FE6B2A0995
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\{6E400DE5-7DFA-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	53776
Entropy (8bit):	2.2680724973768234
Encrypted:	false
SSDEEP:	192:r5ZOQG6pkAjx2NWhM1TXY6fJYNNgfJcNMfs3Nn8H4IuWkw2q+IsOu4TL2:rvLR6Cgk6to6fJygfJnUpQ40krqdsn4e
MD5:	21ED7C45BF907F86ABCFEF95C80E3E0F
SHA1:	104B567A3E780FD6C6AB10B4875400F11C27939D
SHA-256:	6B9A32B77B90254D79BC230F0BFACCB8CF5680935C2B59EC7A073AB962B65E1C
SHA-512:	E58FF23A844C38C779B239A671AA072DAADE9A654B6F18A0CC8DE9D7ADB0E71622BF1D6C1E16E51C5972CF3FA898B88FD5FD766EB4B55396A9E8DFF699F8EED
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\{6E400DE6-7DFA-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5656222631305714
Encrypted:	false
SSDEEP:	48:IwhGcprsGwpa6G4pQuGrapbSHGQpKRG7HpRtTGIpG:rXZEQ66gBSxAATLA
MD5:	59EE728F1E296D8876881C22D9F71001
SHA1:	4D5521B72FFA9348854482EBBE7EDA17C345BE5E
SHA-256:	7B9C8E9ADAA72B4CA48E5BB2164CF73E27A88F797BA781186791A6B094B66098
SHA-512:	F47B78D1BF275B09C5B55FEF829D24D627A3CC9520886CF15D7953D4B7CAC17A79752B44A836EA1F02781E918DF93A61CDE8054D17FF2A29AA8A1578FE43D32
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	35788
Entropy (8bit):	3.039048300693387
Encrypted:	false
SSDEEP:	48:OAnAKASAtgyyyyyyyyyyyyyLADuAGQQQQQRAFAMAMAGgyyyyyyyyyyyyy+A07A9s:iQQQQQUQQQQQt
MD5:	4024F18293EA8605C23348DE4B2B575E
SHA1:	89B8D07FC56B5348A6E500ABA947A331C1A2068A
SHA-256:	67B6FCB65F211F0C8FCBEF2EAEACC4DFECCDFA3D308B8D5DFC18B1889EA51BC2

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat

SHA-512:	C6EA8DC4BD71818FF36B008FC6A44522755E4CE25D25151D00E5252D6BD63F11664EE9A51121F5BA6DC61533313065182AC7C9459A38DAD1CB43AEE725D7435
Malicious:	false
Reputation:	low
Preview:	%.h.t.t.p.s.:././.w.w.w...m.i.c.r.o.s.o.f.t...c.o.m./.f.a.v.i.c.o.n...i.c.o.~(................h(......(....................(....................................."P.."""""""""""""""""""""""""""""""""" """""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...33333333333333333333333 3333333"""""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...3 333333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""" """""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""""""" ...33333333333 33333333333333333333"""""""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Print[1].png

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	476
Entropy (8bit):	7.35124642782842
Encrypted:	false
SSDEEP:	12:6v/78/8QCeKXzjl5V6VQTdwbtsxET1SDQi7N:sNfF6VYd6tf1SdN
MD5:	B8E8859FCD4E43D51233559C17A3C7BD
SHA1:	F0CA023F26A84761995FA0BF6935DE6A3B8AE6F8
SHA-256:	DC15A37B4015D0DECF639006E4F9002E742DDBFD7C669EC0AE469057F238B78D
SHA-512:	3605E4C4FE22E6E05553F89D34CFE8B3E5CA72FBDADCCD8B279835A0ECEFCD10B1BF2AD1ACCEEB168EE369E23A8AD205720FBF33A184188A7F23AEA7B0F2 005
Malicious:	false
Reputation:	moderate, very likely benign file
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/Print.png?version=03620f3a-5d1e-5a73-a117-a2f71eee437d
Preview:	.PNG........IHDR................a....sRGB.........gAMA......a.....IDAT8O.S;..A.........M6.4....@.47....^I..<."&..W..Y...Y...........m...E.<..$..n...j..kL&......}.j.......)@......r..Q....]. .+.w...f3.R)...2^...ddO.^..Ud.BE..*D..h...!........h..p..t...9.........1.."tD.......y.h.AQ.{."...J.D.U....c.b.i.h.t:..$&q..J..n.+9.r..B..F...e..`<...oS....Z-.H....NG...Jl..D.Z..@!...s<....m.'Ll..vc.?..~..v.n.9.; .m.5..K.A ......z=../>...M....r9..~...*..go.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\ellipsis_635a63d500a92a0b8497cdc58d0f66b1[1].svg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	900
Entropy (8bit):	3.8081778439799248
Encrypted:	false
SSDEEP:	24:t4CvnAVRHf1QqCSzGUdiHTVtpRduf1QqCWbVHTVeUV0Uv6f1QqCWbVHTVeUV0UFl:fn+1QqC4GuiHFXS1QqCWRHQ3V1QqCWRV
MD5:	635A63D500A92A0B8497CDC58D0F66B1
SHA1:	A32EBA4B4D139E8DA52C5801A13C1EE222B2B882
SHA-256:	61D7CCC5D2C41BF86BE6CEFB0063405067849BA64E9F219F60596EF09A54A942
SHA-512:	EFFE15E105FC5FA853E76917B533AAE6C75EBA9A256049FB5EAB88BBF319D63A4CE4AE3743A09D6A5F474B01649D6EDC5C8BCCC61B8CA9EA9E5C39E7AE724 C16
Malicious:	false
Reputation:	moderate, very likely benign file
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/images/ellipsis_635a63d500a92a0b8497cdc58d0f66b1.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16" viewBox="0 0 16 16"><title>assets</title><path d="M1.143,6.857a1.107,1.107,0,0,1,.446.089,1.164,1 .164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.107,1.107,0,0,1-.446.089A1.107,1.107,0,0,1,.7,9.054a1.164,1.164,0,0,1-.607-.607,1.161, 1.161,0,0,1,0-.893A1.164,1.164,0,0,1,.7,6.946a1.107,1.107,0,0,1,.446-.089M8,6.857a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893 ,1.164,1.164,0,0,1-.607.607,1.161,1.161,0,0,1-.893,0,1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893,1.164,1.164,0,0,1,.607-.607A1.107,1.107,0,0,1,8,6.857m 6.857,0a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.161,1.161,0,0,1-.893,0,1.164,1.164,0,0,1-.607- .607,1.161,1.161,0,0,1,0-.893,1.164,1.164,0,0,1,.607-.607A1.107,1.107,0,0,1,14.857,6.857Z"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\favicon[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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\favicon[1].ico

Reputation:	high, very likely benign file
IE Cache URL:	http://https://www.microsoft.com/favicon.ico?v2

Preview:

.............h(..f...HH..........(..00......h....6.. ....=..............@.........(....A..(...................(....................................."P..."""""""""""""""""""""""""""""""""""""" ...3
33333333333333333333333333333"" ...333333333333333333333333333333"" ...333333333333333333333333333333""""
"""""""""""""""""""""""""""""""""""" ...333333333333333333333333333333"" ...333333333333333333333333333333"" ...33333333333
3333333333333333333"" ...333333333333333333333333333333"" ...333333333333333333333333333333""
""""""""" ...333333333333333333333333333333"" ...333333333333333333333333333333"" ...33333333333333333333
333333333"" ...333333333333333333333333333333""""""""""""""""""""""""""""""""""

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\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:	high, very likely benign file
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/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\0W10PBUV\mwfmdl2-v3.54[1].woff

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 26288, version 0.0
Category:	downloaded
Size (bytes):	26288
Entropy (8bit):	7.984195877171481
Encrypted:	false
SSDEEP:	768:56JqQaQphRbTHiKNF5z/02h5KpJW3pPOA8Y9g/:gdTTH5XKpJWdH1W/
MD5:	D0263DC03BE4C393A90BDA733C57D6DB
SHA1:	8A032B6DEAB53A33234C735133B48518F8643B92
SHA-256:	22B4DF5C33045B645CAFA45B04685F4752E471A2E933BFF5BF14324D87DEEE12
SHA-512:	9511BEF269AE0797ADDF4CD6F2FEC4AD0C4A4E06B3E5BF6138C7678A203022AC4818C7D446D154594504C947DA3061030E82472D2708149C0709B1A070FDD0E
Malicious:	false
Reputation:	moderate, very likely benign file
IE Cache URL:	http://https://www.microsoft.com/mwf/_h/v3.54/mwf.app/fonts/mwfmdl2-v3.54.woff

Preview:

wOFF......f........D.......................OS/2...X...H...`JM.FVDMX............^.qcmap............*.9cvt ...4... ...*....fpgm...T.......Y...gasp...D...........glyf...P..U5.......head..]....2...6..
.Chhea..]........$$...hmtx..]..........ye'loca..^...........Gmaxp..`.... ... ./..name..`....8....]..Rpost..f........ .Q.wprep..f$........x...x.c`.Pf......:....Q.B3_dHc..`e.bdb... .`@..`......./9.|...
V...)00...-.Wx...S......._..m.m.m.m.m;e..y.~.......<p..a.0t.&...a.pa.0B.1..F...Q.ha.0F.3.....q.xa.0A.0L.&...I.da.0E.2L....i.ta.0C.1..f...Y.la.0G.3.....y.|a..@X0,.....E.ba.DX2,....e
.ra..BX1..V...U.ja..FX3.....u.za..A.0l.6...M.fa.E.2l....m.va..C.1..v...].na..G.3......}.~a.p@80......C.a..pD82.....c.q..pB81..N...S.i..pF83.....s.y..pA.0\.....K.e..pE.2\....k.u..pC.1..n...[.
m..pG.3......{.}...@x0<.....G.c...Dx2<....g.s...Bx1..^...W.k...Fx3.....w.{...A.0|.>...O.g...E.2|....o.w...C.1..~..._.o..08........?..0$........x...mL.U.............9.x.`[...&BF@X...V.h.Z..h.
.....`n....[..U

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\override[1].css

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	1531
Entropy (8bit):	4.797455242405607
Encrypted:	false
SSDEEP:	24:Udf0F+MOu2UOqD3426TKgR2Yyk9696TkMYqdfskeEkeGk/ksuF9qaSm9qags:Ud8FYqTj36TKgR2Yyk9696TkMYO0keEW
MD5:	A570448F8E33150F5737B9A57B6D889A
SHA1:	860949A95B7598B394AA255FE06F530C3DA24E4E
SHA-256:	0BD288D5397A69EAD391875B422BF2CBDCC4F795D64AA2F780AFF45768D78248
SHA-512:	217F971A8012DE8FE170B4A20821A52FA198447FA582B82CF221F4D73E902C7E3AA1022CB0B209B6679C2EAE0F10469A149F510A6C2132C987F46214B1E2BBBC
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\override[1].css	
Reputation:	high, very likely benign file
IE Cache URL:	http://https://statics-marketingsites-wcus-ms-com.akamaized.net/statics/override.css?c=7
Preview:	a.c-call-to-action:hover, button.c-call-to-action:hover{box-shadow:none!important}a.c-call-to-action:hover span, button.c-call-to-action:hover span{left:0!important}...c-call-to-action:not(.glyph-play):after { right: 0!important;} a.c-call-to-action:focus,button.c-call-to-action:focus{box-shadow:none!important}a.c-call-to-action:focus span,button.c-call-to-action:focus span{left:0!important;box-shadow:none!important}...theme-dark .c-me .msame_Header_name {color: #f2f2f2;}...pmg-page-wrapper .uhf div, .pmg-page-wrapper .uhf button, .pmg-page-wrapper .uhf a, .pmg-page-wrapper .uhf span, .pmg-page-wrapper .uhf p, .pmg-page-wrapper .uhf input {font-family: Segoe UI, SegoeUI,Helvetica Neue,Helvetica,Arial,sans-serif !important;}..@media (min-width: 540px) {.pmg-page-wrapper .uhf .c-uhfh-alert span, .pmg-page-wrapper .uhf #uhf-g-nav span, .pmg-page-wrapper .uhf .c-uhfh-actions span, .pmg-page-wrapper .uhf li, .pmg-page-wrapper .uhf button, .pmg-page-wrapper .uhf a, .pmg-page-wrapper .uhf #meC

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\print-icon[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	173
Entropy (8bit):	5.970149697517944
Encrypted:	false
SSDEEP:	3:yionv//thPl9vtt+NTl0qRthwkBDsTBZtqmA73Fs+rQx33npdtnoypZh9Dicl2up:6v/lhPmNp0WnDspBAzqPnpdiyTh9Fp
MD5:	023F5AC6E0114AF1F781BE5D3C956385
SHA1:	C166284B8541F1DE32DC5C4DEC635C296BF85C98
SHA-256:	75D637BF6B6DFF2525095D0BE7E0C90F012BB118C2EF19099AFDCBC630ADFC79
SHA-512:	DAFA49056E3D3014DB392410685CC05773C09938E2E700657727928EDCFF8EA2D7C769D377539C52DA70321B94F4E8F045F565EC51BC2B701D95BB3213CC220
Malicious:	false
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/print-icon.png?version=60ebb5de-511c-db20-3795-563c739c5e12
Preview:	.PNG.....IHDR.....h6....tEXtSoftware.Adobe ImageReadyq.e<...OIDATx.b...?..0222`..jX..a5...D0.50.....k.....:...X=....'..(..I.....K..... .....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\script[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	30250
Entropy (8bit):	5.330396235509644
Encrypted:	false
SSDEEP:	384:ekorlyUMfQ8sW5hXDiWiQRKKwoOdo/r4nqdRy/dRyWhtyFhtyYKQys05DU7BS5ha:0olDi2RKQOOwqjE2l/3FJ1C/n+NYiKq
MD5:	79493518F253F3F74970CF43C8A3FEEE
SHA1:	E0CC16264EA44A55C17766A5E0F0F4DB7DD8AAF2
SHA-256:	BD041981B6512D6DA32A6AE752EFE67DD0BA22FACFA9A534B0F5B08651B7852A
SHA-512:	D204999F215BA5A837391AD447F3A26461439EF4FBBF39CEC22CE970F7F86EC908FD3CF4C0500F6A529FCDF5C0707214896ECACC15FB0B04259E7EBEFF749D5
Malicious:	false
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSScripts/script.jsx?k=8c27a4b8-356f-dd50-ddb2-9e2c834bf9c4
Preview:	function ShowSelectedComponentKeyPress(n,t){if(window.event.keyCode==13)return ShowSelectedComponent(n,t),!1}function SetRightSideNavigationMenuHeight(){$("[id^=dvModuleGroup_]").hide();window.location.search.toLowerCase().indexOf("bookmarkid")!=-1&&SelectBookMark();window.location.search.toLowerCase().indexOf("componentid")!=-1&&LoadSelectedInternalLink();$(".div_side_comp").length>0&&$(".div_content").css("min-height",$(".div_side_comp").height()-27)}function ShowSelectedComponent(n,t){var i=$("#"+t).attr("data-parentModule");return i!=undefined&&i!=null&&($("[data-parentmodule="+i+"]").show(),$("#"+i+" [id$=_LongDescription]").length>0?(document.getElementById(i+"_LongDescription").style.display="block",document.getElementById(i+"_ShortDescription").style.display="none",ShowText($("#"+i+".learnMoreLabel"),"long")):ShowText($("#"+i+".learnMoreLabel"),"long"),DisplayTopNavigation(i)),$("html, body").animate({scrollTop:$("#"+t).offset().top-1},800),!1}function ShowToolTip(){var n,i,t;w

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\style[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	137436
Entropy (8bit):	5.360850019087837
Encrypted:	false
SSDEEP:	1536:+Fk5W00zHVaAgrBmeZCstBwB/BxBf9e969j9S9h919g9Z9C9f9g9Z9e979Q9t9Vp:+Fk5W003MC/
MD5:	D0519383C16A2B2D2879BFBF15845F0C
SHA1:	B2FBBC365B2CA853B1CBEAAA0F10BB05148ED9AA
SHA-256:	046BA9FDD7992751785036A03AB6EDD3052465C23C2BAD1ADC80905DC6AA39A9
SHA-512:	2DB8E6E4AD75F756D0B70071EC49EA4FF54360AFDAAC007C0FFD5ACF575961E661DD275329347210AD71206885A50DA2E58F12CE84E6C7A3BC3D5EDD81E3B5BE
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\style[1].css	
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSStyles/style.csx?k=3c9ade18-bc6a-b6bd-84c3-fc69aaaa7520_899796fc-1ab6-ed87-096b-4f10b915033c_e8d8727e-02f3-1a80-54c3-f87750a8c4de_6e5b2ac7-688a-4a18-9695-a31e8139fa0f_b3dad3e4-0853-1041-fa46-2e9d6598a584_fc29d27f-7342-9cf3-c2b5-a04f30605f03_28863b11-6a1b-a28c-4aab-c36e3deb3375_907fa087-b443-3de8-613e-b445338dad1f_a66bb9d1-7095-dfc6-5a12-849441da475c_1b0ca1a3-6da9-0dbf-9932-198c9f68caeb_ef11258b-15d1-8dab-81d5-8d18bc3234bc_11339d5d-cf04-22ad-4987-06a506090313_50edf96d-7437-c38c-ad33-ebe81b170501_8031d0e3-4981-8dbc-2504-bbd5121027b7_3f0c3b77-e132-00a5-3afc-9a2f141e9eae_aebeacd9-6349-54aa-9608-cb67eadc2d17_0cdb912f-7479-061d-e4f3-bea46f10a753_343d1ae8-c6c4-87d3-af9d-4720b6ea8f34_a905814f-2c84-2cd4-839e-5634cc0cc383_190a3885-bf35-9fab-6806-86ce81df76f6_05c744db-5e3d-bcfb-75b0-441b9afb179b_8beffb66-d700-2891-2c8d-02e40c7ac557_b1fe3f15-7512-0a8f-a55b-b316245621b5_f9c8eff0-3e34-2c33-6c0d-1fa7c5077eec
Preview:	@font-face{font-family:'wf_segoe-ui_light';src:url('//c.s-microsoft.com/static/fonts/segoe-ui/west-european/light/latest.eot');src:local("Segoe UI Light"),local("Segoe WP Light"),url('//c.s-microsoft.com/static/fonts/segoe-ui/west-european/light/latest.eot?#iefix') format('embedded-opentype'),url('//c.s-microsoft.com/static/fonts/segoe-ui/west-european/light/latest.woff') format('woff'),url('//c.s-microsoft.com/static/fonts/segoe-ui/west-european/light/latest.ttf') format('truetype'),url('//c.s-microsoft.com/static/fonts/segoe-ui/west-european/light/latest.svg#web') format('svg');font-weight:normal;font-style:normal}@font-face{font-family:'wf_segoe-ui_normal';src:url('//c.s-microsoft.com/static/fonts/segoe-ui/west-european/normal/latest.eot');src:local("Segoe UI"),local("Segoe"),local("Segoe WP"),url('//c.s-microsoft.com/static/fonts/segoe-ui/west-european/normal/latest.eot?#iefix') format('embedded-opentype'),url('//c.s-microsoft.com/static/fonts/segoe-ui/west-european/normal/latest.w

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\2_bc3d32a696895f78c19df6c717586a5d[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1864
Entropy (8bit):	5.222032823730197
Encrypted:	false
SSDEEP:	48:yvswNIBLBpJawmMH44log6gw/MHm7pJroog6gwkMH9Xog6gwdMHdqdyqog7C:ykfXYx+odPcs9B
MD5:	BC3D32A696895F78C19DF6C717586A5D
SHA1:	9191CB156A30A3ED79C44C0A16C95159E8FF689D
SHA-256:	0E88B6FCBB8591EDFD28184FA70A04B6DD3AF8A14367C628EDD7CABA32E58C68
SHA-512:	8D4F38907F3423A86D90575772B292680F7970527D2090FC005F9B096CC81D3F279D59AD76EAFCA30C3D4BBAF2276BBAA753E2A46A149424CF6F1C319DED5A6
Malicious:	false
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/images/backgrounds/2_bc3d32a696895f78c19df6c717586a5d.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="1920" height="1080" fill="none"><g opacity=".2" clip-path="url(#E)"><path d="M1466.4 1795.2c950.37 0 1720.8-627.52 1720.8-1401.6S2416.77-1008 1466.4-1008-254.4-380.482-254.4 393.6s770.428 1401.6 1720.8 1401.6z" fill="url(#A)"/><path d="M394.2 1815.6c746.58 0 1351.8-493.2 1351.8-1101.6S1140.78-387.6 394.2-387.6-957.6 105.603-957.6 714-352.38 1815.6 394.2 1815.6z" fill="url(#B)"/><path d="M1548.6 1885.2c631.92 0 1144.2-417.45 1144.2-932.4S2180.52 20.4 1548.6 20.4 404.4 437.85 404.4 952.8s512.276 932.4 1144.2 932.4z" fill="url(#C)"/><path d="M265.8 1215.6c690.246 0 1249.8-455.595 1249.8-1017.6S956.046-819.6 265.8-819.6-984-364.005-984 198-424.445 1215.6 265.8 1215.6z" fill="url(#D)"/></g><defs><radialGradient id="A" cx="0" cy="0" r="1" gradientUnits="userSpaceOnUse" gradientTransform="translate(1466.4 393.6) rotate(90) scale(1401.6 1720.8)"><stop stop-color="#107c10"/><stop offset="1" stop-color="#c4c4c4" stop-opacity="0"/></radialGradient><r

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\53_8b36337037cff88c3df203bb73d58e41[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 342 x 72, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	5139
Entropy (8bit):	7.865234009830226
Encrypted:	false
SSDEEP:	96:oX2DsRVNYc82nTGTirCPqKO1gDPFjDiwK3aM5yO/bUlVV6JKo5N9jIMw7RLW1ZHb:ofRgc82nTprQsgDNDP7QgVVoH9+kMK9
MD5:	8B36337037CFF88C3DF203BB73D58E41
SHA1:	1ADA36FA207B8B96B2A5F55078BFE2A97ACEAD0E
SHA-256:	E4E1E65871749D18AEA150643C07E0AAB2057DA057C6C57EC1C3C43580E1C898
SHA-512:	97D8CC97C4577631D8D58C0D9276EE55E4B80128080220F77E01E45385C20FE55D208122A8DFA5DADCB87543B1BC291B98DBBA44E8A2BA90D17C638C15D487
Malicious:	false
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/images/applogos/53_8b36337037cff88c3df203bb73d58e41.png
Preview:	.PNG.....IHDR...V...H.....tEXtSoftware.Adobe ImageReadyq.e<...%iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c148 79.164036, 2019/08/13-01:06:57 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmp:CreatorTool="Adobe Photoshop 21.0 (Macintosh)" xmpMM:InstanceID="xmp.iid:DB120779422011EA9888910153D3A5E6" xmpMM:DocumentID="xmp.did:DB12077A422011EA9888910153D3A5E6"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:DB120777422011EA9888910153D3A5E6" stRef:documentID="xmp.did:DB120778422011EA9888910153D3A5E6"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>P.WI....IDATx..]]l.....(.5.K0P..0...E.qT..J X)F.(5X....J.}(m.R5.Q...RUEUPU~.....qp@.b.....L...k.m"0....."c.3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\arrow_left_a9cc2824ef3517b6c4160dcf8ff7d410[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	513
Entropy (8bit):	4.720499940334011
Encrypted:	false
SSDEEP:	12:t4BdU/uRqv6DLfBHKFWJCDLfBSU1pRXIFl+MJ4bADc:t4TU/uRff0EcfIU1XXU+t2c
MD5:	A9CC2824EF3517B6C4160DCF8FF7D410
SHA1:	8DB9AEBAD84CA6E4225BFDD2458FF3821CC4F064
SHA-256:	34F9DB946E89F031A80DFCA7B16B2B686469C9886441261AE70A44DA1DFA2D58

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\arrow_left_a9cc2824ef3517b6c4160dcf8ff7d410[1].svg	
SHA-512:	AA3DDAB0A1CFF9533F9A668ABA4FB5E3D75ED9F8AFF8A1CAA4C29F9126D85FF4529E82712C0119D2E81035D1CE1CC491FF9473384D211317D4D00E0E234AD9F
Malicious:	false
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/images/arrow_left_a9cc2824ef3517b6c4160dcf8ff7d410.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="24" height="24" viewBox="0 0 24 24"><title>assets</title><path d="M18,11.578v.844H7.617l3.921,3.928-.594.594L6,12l4.944-4.944.594.594L7.617,11.578Z" fill="#404040"/><path d="M10.944,7.056l.594.594L7.617,11.578H18v.844H7.617l3.921,3.928-.594.594L6,12l4.944-4.944m0-.141-.071.07L5.929,11.929,5.858,12l.071.071,4.944,4.944.071.07.071-.07.594-.595.071-.07-.071-.071L7.858,12.522H18.1V11.478H7.858l3.751-3.757.071-.071-.071-.07-.594-.595-.071-.07Z" fill="#404040"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\ellipsis_grey_2b5d393db04a5e6e1f739cb266e65b4c[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	915
Entropy (8bit):	3.8525277758130154
Encrypted:	false
SSDEEP:	24:t4CvnAVRfFArf1QqCSzGUdiHTVtpRduf1QqCWbVHTVeUV0Uv6f1QqCWbVHTVeUVx:fn1r1QqC4GuiHFXS1QqCWRHQ3V1QqCWz
MD5:	2B5D393DB04A5E6E1F739CB266E65B4C
SHA1:	6A435DF5CAC3D58CCAD655FE022CCF3DD4B9B721
SHA-256:	16C3F6531D0FA5B4D16E82ABF066233B2A9F284C068C663699313C09F5E8D6E6
SHA-512:	3A692635EE8EBD7B15930E78D9E7E808E48C7ED3ED79003B8CA6F9290FA0E2B0FA3573409001489C00FB41D5710E75D17C3C4D65D26F9665849FB7406562A406
Malicious:	false
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/images/ellipsis_grey_2b5d393db04a5e6e1f739cb266e65b4c.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16" viewBox="0 0 16 16"><title>assets</title><path fill="#777777" d="M1.143,6.857a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.107,1.107,0,0,1-.446.089A1.107,1.107,0,0,1,.7,9.054a1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893A1.164,1.164,0,0,1,.7,6.946a1.107,1.107,0,0,1,.446-.089M8,6.857a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.107,1.107,0,0,1-.446.089,1.107,1.107,0,0,1-.446-.089,1.164,1.164,0,0,1-.607-.607A1.107,1.107,0,0,1,8,6.857m6.857,0a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.107,1.107,0,0,1-.446.089,1.107,1.107,0,0,1-.446-.089,1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893,1.164,1.164,0,0,1,.607-.607A1.107,1.107,0,0,1,14.857,6.857Z"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\icons[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), icons family
Category:	downloaded
Size (bytes):	4388
Entropy (8bit):	5.568378803379191
Encrypted:	false
SSDEEP:	96:2WZx42qACoApC6do8MPOGiN4mER38GTDfO/fv:1x42qAHAo6VMPi6mcTy
MD5:	77E1987DF3A0274C5A51E3C55CEE7C98
SHA1:	9B0FE96AF141AB09183F386F65BC627B8C396460
SHA-256:	EF04649D4D068673CF0FA47EF4C45C8BE291E703F4EC5FC0E507F17839120AA2
SHA-512:	B1E0CFB515FF2298799BA54574899D27B1FC043F66CC4E9591C504F88273B98697B99ED25955DB84986B39ED9F51864611833DC88064B14C29ADC020FBF6E295
Malicious:	false
IE Cache URL:	http://https://assets.onestore.ms/cdnfiles/external/oneui/oneui1.16.2/dist/fonts/icons/icons.eot?
Preview:	$.....LP.....G.....i.c.o.n.s.....R.e.g.u.l.a.r.....V.e.r.s.i.o.n. .1...0.....i.c.o.n.s..... OS/2@.Mn...(...Vcmap.1.....Jglyf.....dhead.9.....6hhea.$.....$hmtx@.....loca". h...L...Bmaxp.3.`..... name.....post{NK..... .....G..._.<.....|.....|..... .T.....D.I...H.D.I.....PfEd.@.....D.....(.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\latest[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Segoe UI Light family
Category:	downloaded
Size (bytes):	28315
Entropy (8bit):	7.9724193003797
Encrypted:	false
SSDEEP:	384:+R0Z7+bHAtrQ1yBFbgqLct7rJhhPLLkHsrvSzaJu4mI3n5o+MmKCxDg6iT7jdVye:+uNUAtE3phPLLFTiMu+pxCjHyGEQ9zL
MD5:	17DFE73CB9C64527F7248B0A24DB317D
SHA1:	345198B9239FCDAF038FB2D3A919E4724037DBAA
SHA-256:	AD75FB92B2EBCE6C37640F03E1AB96A752F388BCE60C877ADE4780B13839E8C4
SHA-512:	421B56D93E9BD5E4B4449DD0FCDEE8D531087FD484C91530AAF0A67EDEA33D5AC2F14A7F4966C528C0F130F17F26629FCAB9F8AB47E950CEB5B9F1A827EA0728
Malicious:	false
IE Cache URL:	http://https://i.s-microsoft.com/fonts/segoe-ui/west-european/light/latest.eot?

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\latest[1].eot	
Preview:	.n...m.....LP#...B..... .....S.e.g.o.e. .U.l. .L.i.g.h.t.....R.e.g.u.l.a.r.....V.e.r.s.i.o.n. .5...3.2.....S.e.g.o.e. .U.l. .L.i.g.h.t.....K..e..66.....U.D.-.. iu...4P\..GLFM..C?.;..-...~|...P..\.(..)RI.....>.>..CE..SsV.jPR...H.....].R..&.n.hT.....x.....q .....wA[....F.....c."....Zed..>.?...`..3...B..W....R....F.j....v..'?.5.k^.....+..a...).. _].x.#QSi.....|<t....k.;..Hv1.G...L$.9....5.t.:...V.Y.....\|.@....B.....P`..2.Z.0....2`.FR.MF8.x....GP0..$:.....PYm.22..."S."1.*j[=.=.mR.*.....j....&.4...k..].1@..y$....."y..C..g7..k.B*. ..V..F\...G.m.jK ...O....b.Qlo...!.N.V....t.[..p.N..~@1d...YX.."....R_i.4.$j.P..U....u9...<..6..4%.....9`.....S...N.Y..L..B$2\.E.vhe...n..h..5..Z..K?.H..S...2..=R..x.....EX.2.....$.".... It8..z.+.h ..$.2*T....}Z../....p..b0ae.qq.(-v1..E.!.l".a..p.).;..8t..7..^..W...4A.D\eOb$.....b.NI.Pe.#$.O38....,....g..&|...B{...].....9..u.8..~Y...3.X..ff.,.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\latest[2].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Segoe UI Semibold family
Category:	downloaded
Size (bytes):	30643
Entropy (8bit):	7.976822258863597
Encrypted:	false
SSDEEP:	768:UOtV1asJ9G0dAdnVrKX/HkVJRPvkgxYZ4Zoe:bLasJ9G0u0fk/RnkgxGof
MD5:	E812BA8B7E2A657F2B70CFACE93C7682
SHA1:	2F02CDDBB483F9B11BBBE74C3CA917A4C345FBAD
SHA-256:	3330C1DEAC468874238DD0C6BF902179A8731EDA8A208C7D01DAC0AB1EAE1BC9
SHA-512:	354B2DB12BC1D67F26F94352B0B663DAD64C46C107454FC19CFEA01C54BB09340BC26C06DE1B96FF826F5287CE246A6317722BAE41B72B63BA86FDAF844BA94 E
Malicious:	false
IE Cache URL:	http://https://i.s-microsoft.com/fonts/segoe-ui/west-european/semibold/latest.eot?
Preview:	.w...v.....X.....LP#...B..... .....".S.e.g.o.e. .U.l. .S.e.m.i.b.o.l.d.....R.e.g.u.l.a.r.....V.e.r.s.i.o.n. .5...3.2...".S.e.g.o.e. .U.l. .S.e.m.i.b.o.l.d.....H .P..lb.7^.....U.D.-..iu...:4P\..GLFM.Y.#?.;..-...~}_).z{.rmD.1".$.....{.t.....=...!cK...%.~.....g.....j.9S....6. .n..V.]pz...e.....#X...=,.p.F..6&.VR...k$~J..n....7.....K.8..T.....x..J.....#.J .XaQ.Q%_{3..xr.... 0Dm...k..Ep.....>..?Pk!KB..C...Q.q..1=6<,.S.F.&B..J.....ya2b."S.....6.2.....H.....*..09A...Tb/.&.d..#.E.:.E.(..I5.M..444d.1.....K..l...l.O..VBb...:..:b..Mh.'= 4.d/..o.k.mMm.....bx..!..S.@E.....>@:..k.JCas..7."..uG3hR.h..w..8W>.4.....pX....J..a....}.Y.....(>H^=.`=.mg*.!.....w'....J.<.ob..3A .../.....5%.'....XS0a.....I.Ia....a...=..g..... {V1+.."_)7$2 O..!bb.=..|.s.1..2qm..#.O.....+E(I..1....EgQ.....E)R.m.?.8.q...J.G.@!f..n.F.r#..(..2p.?.9.8..?.d]..s..0.9.f..A...r.iq....x.g.aO....S.....R0i..BT.yl.".<k...:&Ja.\.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\picker_account_aad_9de70d1c5191d1852a0d5aac28b44a6c[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	756
Entropy (8bit):	4.879179443781471
Encrypted:	false
SSDEEP:	12:t4pb8WsQKvkBWSfYcW3ffBfYfomQO1a7aajR2F1hgWSnuCNSganii7v/NPujARqj:t4pb8WvKMTfY3ffBfYfomQO1eXjR2oug
MD5:	9DE70D1C5191D1852A0D5AAC28B44A6C
SHA1:	F4F64F5CBDBE6D1115C10A7F9CCB8828E6B67CAE
SHA-256:	5D3357BD875B7335ACE42E8EE3A64578E4253BED1A4E279109DE403EEDAE3A69
SHA-512:	CAC13FC2FE30E10772008F2AFF70FCA031EA9918E1F8C5C8B91CB9E79463383183406EFAADF89360DE3A08573FCDF2716C14DA6411E24B7E260B96AF84F0076
Malicious:	false
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/images/picker_account_aad_9de70d1c5191d1852a0d5aac28b44a6c.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="48" height="48" viewBox="0 0 48 48"><title>assets</title><circle cx="24" cy="24" r="24" fill="#e6e6e6"/><path d=" M34,35V14a2.938,2.938,0,0,0-3-3H27V8l2-1L27.948,5.638,24,8,20.07,5.648,19,7l2,1v3H17a2.938,2.938,0,0,0-3,3V35a2.938,2.938,0,0,0,3,3H31A2.938,2.938,0,0 ,0,34,35Zm-3,1H17a.979.979,0,0,0,1-1-1V14a.979.979,0,0,1,1-1h6V10h2v3h6a.979.979,0,0,1,1,1V35A.979.979,0,0,1,31,36Z" fill="#404040"/><path d="M26.766,25 .42a4.432,4.432,0,1,0-5.533,0A6.237,6.237,0,0,0,17.765,31h1.653a4.582,4.582,0,1,1,9.165,0h1.653A6.237,6.237,0,0,0,26.766,25.42Zm-5.546-3.435A2.779,2.779,0,1,1,2 4,24.765,2.783,2.783,0,0,1,21.221,21.985Z" fill="#404040"/><rect x="21" y="14" width="6" height="2" rx="1" ry="1" fill="#404040"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\picker_account_add_56e73414003cdb676008ff7857343074[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	222
Entropy (8bit):	5.004415423297573
Encrypted:	false
SSDEEP:	3:tIsqDmJS4RKb5zMc7XpCN+bJMacvRxyJAgR/QvfqhcDQKG2TcVER+HLZqWTboZUq:tI9mc4slztdbC/yXADQKDTcVEqLwDZsc
MD5:	56E73414003CDB676008FF7857343074
SHA1:	9ED7A58CD0E81E9689AC8C6D548A47D0185E0FDC
SHA-256:	749F85621D92A5B31B2A377A8C385A36D48A83327DAD9A8A8DA93CD831B8C9A2
SHA-512:	FAD0071AC2DFA23989BFBC7D3850415F3C340A74A54D3D8D797AFCCD6A301513BBC769DF4E5148605BE1E23A8750973EB80726F3CC959A2A457B0EC09AE14F 7
Malicious:	false
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/images/picker_account_add_56e73414003cdb676008ff7857343074.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="48" height="48" viewBox="0 0 48 48"><title>assets</title><circle cx="24" cy="24" r="24" fill="#e6e6e6"/><path d=" M25,23H36v2H25V36H23V25H12V23H23V12h2Z" fill="#404040"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\picker_more_7568a43cf440757c55d2e7f51557ae1f[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	899
Entropy (8bit):	3.8260330857236338
Encrypted:	false
SSDEEP:	24:t4CvnAVROLgCWbVHTVSRUyL3Fe09gCWbVHTVeUVh10UsSgCWbVHTVeUVh10Usb7:fncCWRH0JL3FECWRHQA10rCWRHQA10F
MD5:	7568A43CF440757C55D2E7F51557AE1F
SHA1:	55C22CA98B5CDCED134F6E24205C288845312A2D
SHA-256:	B7FCD37EAAFE3F08647ED072D5289EADFFF6C660A26CDEF31532B3FCFB4A0BB2
SHA-512:	F01DA2804594C3C78C0694FD6CC49B667663DA95AE7367EE3F0F5112B9957A3220389AAE4A5B750BCB3BC4F1092EA614266A4BFFD7E0FE16232E1CB57606E90
Malicious:	false
IE Cache URL:	http://https://aadcdn.msftauth.net/ests/2.1/content/images/picker_more_7568a43cf440757c55d2e7f51557ae1f.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16" viewBox="0 0 16 16"><title>assets</title><path d="M9.143,1.143a1.107,1.107,0,0,1-.089.446,1.164,1.164,0,0,1-.607.607,1.161,1.161,0,0,1-.893,0,1.164,1.164,0,0,1-.607-.607,1.107,1.107,0,0,1-.089-.446A1.107,1.107,0,0,1,6.946.7,1.164,1.164,0,0,1,7.554.089a1.161,1.161,0,0,1,.893,0A1.164,1.164,0,0,1,9.054.7a1.107,1.107,0,0,1,.089.446M9.143,8a1.107,1.107,0,0,1-.089.446,1.164,1.164,0,0,1-.607.607,1.161,1.161,0,0,1-.893,0,1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893,1.164,1.164,0,0,1,.607-.607,1.161,1.161,0,0,1,.893,0,1.164,1.164,0,0,1,.607.607A1.107,1.107,0,0,1,9.143,8m0,6.857a1.107,1.107,0,0,1-.089.446,1.164,1.164,0,0,1-.607.607,1.161,1.161,0,0,1-.893,0,1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893,1.164,1.164,0,0,1,.607-.607,1.161,1.161,0,0,1,.893,0,1.164,1.164,0,0,1,.607.607A1.107,1.107,0,0,1,9.143,14.857Z"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\17-f90ef1[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	134136
Entropy (8bit):	5.224428921008954
Encrypted:	false
SSDEEP:	3072:1f/HuFVppxvIeq0i9d1EwgXA95Ki5DCE4t:1f/Hu/FIhRwt
MD5:	D567746F6D3BABF05ACF7A63730AC2CB
SHA1:	DDB8B9E24115D9653C432C1C2A3C57E0F881AFEB
SHA-256:	F4DF01A10175F31D0620AE8AA24854DF0D8DCB0C752E8465376B2ED3DEF62DE0
SHA-512:	3F9F18CD40F4CDCDA4F55174AC02766F4F511A61797296D59F1F216E2A51FC9068981E0C41C998ECB05053495BD7971FEA56A032F5438438A224CCA1A33F7189
Malicious:	false
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-wcus-prod/shell/_scrf/js/themes=default/54-af9f9f/c0-247156/de-099401/e1-a50eee/e7-954872/d8-97d509/f0-251fe2/46-be1318/77-04a268/11-240c7b/63-077520/a4-34de62/bb-d7480b/db-bc0148/dc-7e9864/6d-c07ea1/29-1ec5a9/f6-aa5278/cd-23d3b0/6d-1e7ed0/b7-cadaa7/c4-898cf2/ca-40b7b0/4e-ee3a55/3e-f5c39b/c3-6454d7/f9-7592d3/92-10345d/79-499886/7e-cda2d3/69-13871c/e5-08f1c0/e0-3c9860/91-97a04f/1f-100dea/33-abe4df/17-f90ef1?ver=2.0&iife=1
Preview:	(function(){/**. * @license almond 0.3.3 Copyright jQuery Foundation and other contributors.. * Released under MIT license, http://github.com/requirejs/almond/LICENSE. */ .var requirejs,require,define,__extends;(function(n){function r(n,t){return w.call(n,t)}function s(n,t){var o,s,f,e,h,p,c,b,r,l,w,k,u=t&&t.split("/"),a=i.map,y=a&&a["*"]||{};if(n){ for(n=n.split("/"),h=n.length-1,i.nodeIdCompat&&v.test(n[h])&&(n[h]=n[h].replace(v,"")),n[0].charAt(0)==="."&&u&&(k=u.slice(0,u.length-1),n=k.concat(n)),r=0;r<n.length;r++)if(w=n[r],w==="."")n.splice(r,1),r=1;else if(w===".."){if(r===0||r===1&&n[2]===".."||n[r-1]==="..")continue;else r>0&&(n.splice(r-1,2),r-=2);n=n.join("/")}if((u||y)&&a){ for(o=n.split("/"),r=o.length;r>0;r-=1){if(s=o.slice(0,r).join("/"),u)for(l=u.length;l>0;l-=1)if(f=a[u.slice(0,l).join("/")],f&&(f=f[s],f)){e=f;p=r;break}if(e)break;!c&&y&&y[s]&&(c=y[s],b=r)}!e&&c&&(e=c,p=b);e&&(o.splice(0,p,e),n=o.join("/"))}return n}function y(t,i){return function(){var r=b.call(arguments,0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\RE1Mu3b[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 216 x 46, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	4054
Entropy (8bit):	7.797012573497454
Encrypted:	false
SSDEEP:	48:zICvnyRHJ3BRZPcSPQ72N2xoiR4fTJX/rj4sFNMkk5/p1k2lPUmbm39o4aL7V9XH:10nvE724xoiRQJPrjpLKSFl9oX31Z1d
MD5:	9F14C20150A003D7CE4DE57C298F0FBA
SHA1:	DAA53CF17CC45878A1B153F3C3BF47DC9669D78F
SHA-256:	112FEC798B78AA02E102A724B5CB1990C0F909BC1D8B7B1FA256EAB41BBC0960
SHA-512:	D4F6E49C854E15FE48D6A1F1A03FDA93218AB8FCDB2C443668E7DF478830831ACC2B41DAEFC25ED38FCC8D96C4401377374FED35C36A5017A11E63C8DAE5C87
Malicious:	false
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE1Mu3b?ver=5c31
Preview:	.PNG.....IHDR.....J.....tEXtSoftware.Adobe ImageReadyq.e<...(iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c132 79.159284, 2016/04/19-13:13:40 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:DocumentID="xmp.did:A00BC639840A11E68CBEB97C2156C7FD" xmpMM:InstanceID="xmp.iid:A00BC638840A11E68CBEB97C2156C7FD" xmp:CreatorTool="Adobe Photoshop CC 2015.5 (Windows)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:A2C931A470A111E6AEDFA14578553B7B" stRef:documentID="xmp.did:A2C931A570A111E6AEDFA14578553B7B"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>.....DIDATx..\..UU.>.7..3....h.L..& j2...h.@..".....`U.....R"..Dq.&.BJR 1.4`$.200...I.....wg.y.[k/

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\app[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	262641
Entropy (8bit):	4.9463902181496096
Encrypted:	false
SSDEEP:	3072:u+Vd0pBbqPLYoyjFkxD2hAYwJb8ILm731Ss:u+Vd0DePLYoyjFkxD2hAYwJbZLM31Ss
MD5:	7C593B06759DB6D01614729D206738D6
SHA1:	0D4F76D10944933B8DDECFFE9691081439A77A3C
SHA-256:	F7D9FB0479DE843CF3FB0B78FC56BBB9E30BF0A238C6F79D9209FA8B22EFB574
SHA-512:	EF91B610CF17A17AAFB48984B4403EF175EB86096E3F12E23AE8D4C7C96EF60ED14DA3F69721E095CD2ACE3F0A06190186D000992823814BB906F7FB3576C2C1
Malicious:	false
IE Cache URL:	http://https://assets.onestore.ms/cdnfiles/external/oneui/oneui1.16.2/dist/css/app.css
Preview:	@font-face {. font-family: "wf_segoe-ui_normal";. src: url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.eot");. src: url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.eot?#iefix") format("embedded-opentype"), url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.woff") format("woff"), url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.ttf") format("truetype"), url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.svg#web") format("svg");. font-weight: normal;. font-style: normal; }..@font-face {. font-family: "wf_segoe-ui_light";. src: url("//i.s-microsoft.com/fonts/segoe-ui/west-european/light/latest.eot");. src: url("//i.s-microsoft.com/fonts/segoe-ui/west-european/light/latest.eot?#iefix") format("embedded-opentype"), url("//i.s-microsoft.com/fonts/segoe-ui/west-european/light/latest.woff") format("woff"), url("//i.s-microsoft.com/fonts/segoe-ui/west-european/light/latest.ttf") format("truetype

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\favicon[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
IE Cache URL:	http://https://www.microsoft.com/favicon.ico
Preview:	.............h(..f...HH...........(..00......h....6.. ....=..............@..........(....A..(....................(.....................................""P..."""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333"""""""""""""""""""""""""""""""" ...3333333333333333333333333333333""""""""""""""""""""""""""""""""

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\jquery-1.7.2.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	94840
Entropy (8bit):	5.372946098601679
Encrypted:	false
SSDEEP:	1536:8YRKUfAjtledhTmtaFyQHGvCXsedOgRc9izzr4yff8teLvHHEjam7W5X3yzSiLnM:VUb6GvCu09s2o2skAieW
MD5:	B8D64D0BC142B3F670CC0611B0AEBCAE
SHA1:	ABCD2BA13348F178B17141B445BC99F1917D47AF
SHA-256:	47B68DCE8CB6805AD5B3EA4D27AF92A241F4E29A5C12A274C852E4346A0500B4
SHA-512:	A684ABBE37E8047C55C394366B012CC9AE5D682D29D340BC48A37BE1A549AECED72DE6408BEDFED776A14611E6F3374015B236FBF49422B2982EF18125FF47DC
Malicious:	false
IE Cache URL:	http://https://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.7.2.min.js
Preview:	/*! jQuery v1.7.2 jquery.com | jquery.org/license */.(function(a,b){function cy(a){return f.isWindow(a)?a:a.nodeType===9?a.defaultView||a.parentWindow:!1}function cu(a){if(!cj[a]){var b=c.body,d=f("<"+a+">").appendTo(b),e=d.css("display");d.remove();if(e==="none"||e===""){ck||(ck=c.createElement("iframe"),ck.frameBorder=ck.width=ck.height=0),b.appendChild(ck);if(!cl||!ck.createElement)cl=(ck.contentWindow||ck.contentDocument).document,cl.write((f.support.boxModel?"<!doctype html>":"")+"<html><body>"),cl.close();d=cl.createElement(a),cl.body.appendChild(d),e=f.css(d,"display"),b.removeChild(ck)}cj[a]=e}return cj[a]}function ct(a,b){var c={};f.each(cp.concat.apply([],cp.slice(0,b)),function(){c[this]=a});return c}function cs(){cq=b}function cr(){setTimeout(cs,0);return cq=f.now()}function ci(){try{return new a.ActiveXObject("Microsoft.XMLHTTP")}catch(b){}}function ch(){try{return new a.XMLHttpRequest}catch(b){}}function cb(a,c){a.dataFilter&&(c=a.dataFilter(c,a.dataType));var d=a.dataTyp

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\jquery-3.1.1.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\jquery-3.1.1.min[1].js	
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\Microsoft\Windows\INetCache\IE\PSUEOSZZ\shell.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	82190
Entropy (8bit):	5.036904170769404
Encrypted:	false
SSDEEP:	1536:tJzwN0CbUTqI34/9w6/Qua+1IGEbjBko230WBYT:vyA
MD5:	1F9995AB937AC429A73364B4390FF6E8
SHA1:	81998DCC6407CEB5CEF236AD52B9F2A3A9528D3B
SHA-256:	49E5166F40D8586714F86E08AB76A977199DF979357147A0E81980A804151C2A
SHA-512:	6669AE352FF46DB734BB8F973D1C0527C3A5EC4119D534AAE4C33F29EFF970168ED5FE200A05D4E1B6A2EC0E090E2207549B926317D489DC7664B0D9C208546
Malicious:	false
IE Cache URL:	http://https://assets.onestore.ms/cdnfiles/onestorerolling-1510-19009/shell/v3/scss/shell.min.css
Preview:	@charset "UTF-8";@font-face{font-family:'wf_segoe-ui_normal';src:local("Segoe UI");src:url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.eot");src:url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.eot?#iefix") format("embedded-opentype"),url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.woff") format("woff"),url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.ttf") format("truetype"),url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.svg#web") format("svg");font-weight:normal;font-style:normal}@font-face{font-family:'wf_segoe-ui_semilight';src:url("//i.s-microsoft.com/fonts/segoe-ui/west-european/semilight/latest.eot");src:url("//i.s-microsoft.com/fonts/segoe-ui/west-european/semilight/latest.eot?#iefix") format("embedded-opentype"),url("//i.s-microsoft.com/fonts/segoe-ui/west-european/semilight/latest.woff") format("woff"),url("//i.s-microsoft.com/fonts/segoe-ui/west-european/semilight/latest.ttf")

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\wcp-consent[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	255440
Entropy (8bit):	6.051861579501256
Encrypted:	false
SSDEEP:	6144:PIgagvUI0iDsW9Whsredo7NjIZjIZP0aNWgF9Dyjzh:PIgaHI0iIUedo7NjIZjIZP0o74t
MD5:	38B769522DD0E4C2998C9034A54E174E
SHA1:	D95EF070878D50342B045DCF9ABD3FF4CCA0AAF3
SHA-256:	208EDBED32B2ADAC9446DF83CAA4A093A261492BA6B8B3BCFE6A75EFB8B70294
SHA-512:	F0A10A4C1CA4BAC8A2DBD41F80BBE1F83D767A4D289B149E1A7B6E7F4DBA41236C5FF244350B04E2EF485FDF6EB774B9565A858331389CA3CB474172465EB3EF
Malicious:	false
IE Cache URL:	http://https://wcpstatic.microsoft.com/mscc/lib/v2/wcp-consent.js
Preview:	var WcpConsent=function(e){var a={};function i(n){if(a[n])return a[n].exports;var o=a[n]={i:n,l:!1,exports:{}};return e[n].call(o.exports,o,o.exports,i),o.l=!0,o.exports}return i.m=e,i.c=a,i.d=function(e,a,n){i.o(e,a)||Object.defineProperty(e,a,{enumerable:!0,get:n})},i.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},i.t=function(e,a){if(1&a&&(e=i(e)),8&a)return e;if(4&a&&"object"==typeof e&&e&&e.__esModule)return e;var n=Object.create(null);if(i.r(n),Object.defineProperty(n,"default",{enumerable:!0,value:e}),2&a&&"string"!=typeof e)for(var o in e)i.d(n,o,function(a){return e[a]}.bind(null,o));return n},i.n=function(e){var a=e&&e.__esModule?function(){return e.default}:function(){return e};return i.d(a,"a",a),a},i.o=function(e,a){return Object.prototype.hasOwnProperty.call(e,a)},i.p="",i(i.s=1)}([function(e,a,i){window,e.exports=function(e){var a={};function i(n)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\64-460736[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	168761

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\64-460736[1].css	
Entropy (8bit):	5.043970134287402
Encrypted:	false
SSDEEP:	3072:jzCPZkTP3bDLH0tfRqQ0xtLfj4ZDSIpTt813viY8R1j35Ap7LQZLPPJH7PAbOCxa:jlZAMLkeetd
MD5:	FA8CBCA2432D7B92BB2F0523082D7C02
SHA1:	E079A2337832ABCA75CF9B9E67D7969EDCA36DA1
SHA-256:	4B5DA91CCC0A5063F5096201B50587B3F8EC68AE799F13CEF8571BA936F2CA39
SHA-512:	0215FCED4E18CDF2CC4F7CFB23897EF60E8CF562E12FBD56B925A4E2F7BA00A775236B07E26D3B9FAA12D6916507FE16E82F2FDD2911BC1D2D8B3EBF521FA0 88
Malicious:	false
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-wcus-prod/west-european/shell/_scrf/css/themes=default.device=uplevel_web_pc/4d-9e2636/56-1c4656/c9-48785f/2c-a9a6a4/40-11102f/10-4f9f5d/7d-35b35c/64-460736?ver=2.0
Preview:	@charset "UTF-8";./*! | Copyright 2017 Microsoft Corporation | This software is based on or incorporates material from the files listed below (collectively, "Third Party Code"). Microsoft is not the original author of the Third Party Code. The original copyright notice and the license under which Microsoft received Third Party Code are set forth below together with the full text of such license. Such notices and license are provided solely for your information. Microsoft, not the third party, licenses this Third P arty Code to you under the terms in which you received the Microsoft software or the services, unless Microsoft clearly states that such Microsoft terms do NOT apply for a particular Third Party Code. Unless applicable law gives you more rights, Microsoft reserves all other rights not expressly granted under such agreement(s), whether by implication, estoppel or otherwise.*/./*! normalize.css v3.0.3 | MIT License | github.com/necolas/normalize.css */.body{margin:0}.context-uh

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\arrow_px_up[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 7 x 9
Category:	downloaded
Size (bytes):	829
Entropy (8bit):	0.6055646407132698
Encrypted:	false
SSDEEP:	3:CKY1q/rylAxrt/laIFBYEQvyIFle:sGFaIFBYfvDfe
MD5:	95B65C94F57061E15ECC8304D3E578D5
SHA1:	A7483D668A780949FDA842F39877A3C08D0FC51C
SHA-256:	BDA2D6EB8E72B3DBCA5EEF086178033F8A2BB3481180B2C63295FCF23843D960
SHA-512:	B17552D90D0038531A5F4E78DA553F9109346CB25851F38996BFAB54906A898DE848FEFFD31E8D0BF0A32D956513CA7ED72D2F4C3AE47922C6F9D370584288EF
Malicious:	false
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/arrow_px_up.gif?version=27f11222-771f-bb95-a744-f0b962f89b91
Preview:	GIF89a.....3..... ....!.....,..... ..... .`.....\8....!>L(.b@.;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\font-awesome[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	troff or preprocessor input, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	37414
Entropy (8bit):	4.82325822639402
Encrypted:	false
SSDEEP:	768:mmMtI+A4CSIDqvnI+YTBrFPvVrJjhiRAiiEL:mXtI+A4GDUI+Y9rpVljhiIEL
MD5:	C495654869785BC3DF60216616814AD1
SHA1:	0140952C64E3F2B74EF64E050F2FE86EAB6624C8
SHA-256:	36E0A7E08BEE65774168528938072C536437669C1B7458AC77976EC788E4439C
SHA-512:	E40F27C1D30E5AB4B3DB47C3B2373381489D50147C9623D853E5B299364FD65998F46E8E73B1E566FD79E97AA7B20354CD3C8C79F15372C147FED9C913FFB106
Malicious:	false
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.css
Preview:	/*!. * Font Awesome 4.7.0 by @davegandy - http://fontawesome.io - @fontawesome. * License - http://fontawesome.io/license (Font: SIL OFL 1.1, CSS: MIT License). */./* FONT PATH. * ---------- */.@font-face {. font-family: 'FontAwesome';. src: url('../fonts/fontawesome-webfont.eot?v=4.7.0');. src: url('../fonts/fontawesome-webfont.eot?#iefix&v=4.7.0') format('embedded-opentype'), url('../fonts/fontawesome-webfont.woff2?v=4.7.0') format('woff2'), url('../fonts/fontawesome-webfont.woff?v=4.7.0') format('woff'), url('../fonts/fontawesome-webfont.ttf?v=4.7.0') format('truetype'), url('../fonts/fontawesome-webfont.svg?v=4.7.0#fontawesomeregular') format('svg');. font-weight: normal;. font-style: normal;.}..fa {. display: inline-block;. font: normal normal normal 14px/1 FontAwesome;. font-size: inherit;. text-rendering: auto;. -webkit-font-smoothing: antialiased;. -moz-osx-font-smoothing: grayscale;.}./* makes the font 33% larger relative to the icon container */..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\jquery-1.11.2.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	95931
Entropy (8bit):	5.394232486761965
Encrypted:	false
SSDEEP:	1536:5P1vk7i6GUHdXXeyQazBu+4HhiO2AEeLNFoqqhJ7SerN5sVI6xcBgPv7E+nzms9d:A4Ud4qhJvNPqcB47MfWWca98HrB

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\jquery-1.11.2.min[1].js	
MD5:	5790EAD7AD3BA27397AEDFA3D263B867
SHA1:	8130544C215FE5D1EC081D83461BF4A711E74882
SHA-256:	2ECD295D295BEC062CEDEBE177E54B9D6B19FC0A841DC5C178C654C9CCFF09C0
SHA-512:	781ACEDC99DE4CE8D53D9B43A158C645EAB1B23DFDFD6B57B3C442B11ACC4A344E0D5B0067D4B78BB173ABBDED75FB91C410F2B5A58F71D438AA6266D048 98A
Malicious:	false
IE Cache URL:	http://https://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.11.2.min.js
Preview:	/*! jQuery v1.11.2 | (c) 2005, 2014 jQuery Foundation, Inc. | 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=c.slice,e=c.concat,f=c.push,g=c.indexOf,h={},i=h.toString,j=h.hasOwnProperty,k={},l="1.11.2",m=function(a,b){return new m.fn.init(a,b)},n=/^ [\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,o=/^-ms-/,p=/-([\da-z])/gi,q=function(a,b){return b.toUpperCase()};m.fn=m.prototype={jquery:l,constructor:m,selector:"",length:0,toArra y:function(){return d.call(this)},get:function(a){return null!=a?0>a?this[a+this.length]:this[a]:d.call(this)},pushStack:function(a){var b=m.merge(this.constructor(),a);return b.pr evObject=this,b.context=this.context,b},each:function(a,b){return m.each(this,a,b)},map:function(a){return this.pushStack(m.map(this,function(b,c){ret

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\latest[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Segoe UI family
Category:	downloaded
Size (bytes):	35047
Entropy (8bit):	7.975792390307888
Encrypted:	false
SSDEEP:	768:I6ibzTDpOGuAJ63YB9eSzDtQEspfAzyNyuBmOfAJYCM:/iPMYJ4GEAZoTyglcM
MD5:	CAD76E4816AF6890C9BFD02A6D1EA899
SHA1:	9EDC91541C31034FCE0D83AABBAAD4C314CD3D33
SHA-256:	D5794223D1A062E5DBE6C34C1994C8CE3792B24AFD5218D0644CB1F53DA4BE58
SHA-512:	24983A5856C2B4D8CBE2A4BD233A93B266A03D4218942E1D1733B33B65AB7A504AF0AC31DE2F1E69F6FF8CCD7A169CD4555539D34FFF8DE4CB8C98DB2DB2C 63
Malicious:	false
IE Cache URL:	http://https://i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.eot?
Preview:	...=.....LP#...B..... .....S.e.g.o.e. .U.l.....R.e.g.u.l.a.r.....V.e.r.s.i.o.n. .5...3.2.....S.e.g.o.e. .U.l.....RV.z..;~.....U.D.-..iu...N4P\..GLFM .Y.?.;..-...~~....Ox.M..".$.._.....g..sC*2..4W.....9AGc.[a..*.rCl,..@..U_..L...e..Ru.J.-.f..3.....S`.A.....K<;...n.Y...rli.....([...W...5k.....^K.G...U.@....2H..B.)N0w.....C..9..... ....#.l2,4..6y.3$b....K.wx...l.$E..?3.8.c...,x..t.wa.O....4.c...!..+.<EM...2T.>\..]4.A.H.;..G.....W.:.?...Z".....e....8....84.L,.)0..y.Xdd.Pa.@.&.o(.I.q.yF...[.y.m(D...(....T.....,A.;q.... .w.$..C..a.. .Y.O?{..0...'1.;C.,.....W..Q-..'.5tD@9..U...E4e.&_...S.Y...\)b.s.rIR.....%..R..KU O..{.0(.....^Q\^!.et...Kf%..K...}.1...S.{.....3p..]...|Y...w..|JeS$..k.....>(8 .ZlV..N.). c...Z.K.\..q.....'S.j.....9...._..E.#s*'#.....[.....DJ^.L7../1...+U.qG.....-..MM..q....L..c...^...:e....<h..:..`.jz..fb.Ha.....k.....e\)g..\."..M

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\privacystatement[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	330860
Entropy (8bit):	4.858123109445773
Encrypted:	false
SSDEEP:	3072:/f698Kd87wNHDmdS9v+6WjUiPryCGZN9ruekUIx4z7ZV/BdQZyNdkugyZCqTDHwr:/G87yjftCrYNb8yQZyZCSDH+ekB
MD5:	7D298A557FC6016EB069B53C999FE042
SHA1:	C09DF82F2B1EF87809293B0484F7537C1A5B9652
SHA-256:	9B43F0B0D31F95E74C12F71DAB742F5D9DB0E7FFE2AFA47CB77C25C1F1B43DDB
SHA-512:	CD699544FA93ED351E5B34AD397393DBD5CD6BB5B04EE6BC2FBAA87A1FEEF20CEB040E4E3902A7EB43580F52D37742278F2AA62DE2193C597CEAB818304A58 50
Malicious:	false
Preview:	.<!DOCTYPE html ><html xmlns:mscom="http://schemas.microsoft.com/CMSvNext" xmlns:md="http://schemas.microsoft.com/mscom-data" lang="en-us" xmlns="http ://www.w3.org/1999/xhtml"><head><meta http-equiv="X-UA-Compatible" content="IE=edge" /><meta charset="utf-8" /><meta name="viewport" content="width=device- width, initial-scale=1.0" /><link rel="shortcut icon" href="https://www.microsoft.com/favicon.ico?v2" /><script type="text/javascript" src="https://ajax.aspnetcdn.com/ajax/jQu ery/jquery-1.11.2.min.js">.....// Third party scripts and code linked to or referenced from this website are licensed to you by the parties that own such code, not by Microsoft. See ASP.NET Ajax CDN Terms of Use - http://www.asp.net/ajaxlibrary/CDN.ashx... </script><script type="text/javascript" language="javascript">/*<![CDATA[*/if($(document).bind("mobileinit",function(){$.mobile.autoInitializePage=!1}),navigator.userAgent.match(/IEMobile\/10\.0/)){var msViewportStyle=document.createElement ("style");msViewpo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\script[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	121249
Entropy (8bit):	5.258860505507024
Encrypted:	false
SSDEEP:	1536:+JXd+YOlaYOyguxH6GdXJKjZtQ3EBJ0PYmwYmEZeQ8Wt2Db7ACu8J8lvC7CQBgAc:ed+YOlaYOyguxHbdX2nX5PaCfey
MD5:	B110D87662D257F657ABCCEF7AF5CD09
SHA1:	FD7519D842B6344448E6F1D69DFFA5F896FAE4A6

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\script[1].js	
SHA-256:	65E82E7414D88BC864191400084C24DA27052E7A61F9F3C1F1EFDFEE433D558C
SHA-512:	EF429EE8701D0748DE81CEE25D15C9674487691ACA8982F6D43DA519E1CDFD5082D9DE5A71D1FB457250828433856BAB4A2CE7E035152FE9C16224FA433D35D
Malicious:	false
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSScripts/script.jsx?k=0502864a-b6ef-2f14-9f8e-267004d3a4e0_c5ea3348-55af-729a-2641-14f0312bacf3_742bd11f-3d7c-9955-3df5-f02b66689699_cb9d43d2-fbae-5b5c-827f-72166d6b87fc_49488e0d-6ae2-5101-c995-f4d56443b1d8_7dea7b90-4334-c043-b252-9f132d19ee19_38aa9ffb-ddb5-75be-6536-a58628f435f5_e3e65a0a-c133-43e7-571d-2293e03f85e6_4ca0e9dc-a4de-17ba-f0de-d1d346cb99e2_06310cd8-41c6-3b11-4645-b4884789ed70_5c27e8aa-9347-969e-39ac-37a4de428a8d_d6872b5a-5310-a73c-7cb3-227a3213a1c5_be92d794-4118-193f-9871-58b72092a5ac_64c742e2-b29c-b6c1-fdd9-accf33ec40bd_cf2ceca9-3467-a5b3-d095-68958eee6d4c_cec39dd8-f1d3-56f1-abfc-a7db34ff7b46_ec5fa2c9-3950-ff57-a5c3-1fa77e0db190_d19f9592-65df-bcc9-e30e-439b875c3381_76a3d06f-f11f-77ef-9bfd-6227ba750200_5e1caa45-461c-3b04-f88b-8cd50af16db5_c2dceda8-20b4-7d3f-13b6-9cac67d7df17_914fa41b-cc86-d3b0-4e15-2fdfa357bcc7_40c6c884-da6e-7c2c-081f-4a7dfe7c7245_ae79ba96-1a9d-debd-a5b1-f3067213b9b8
Preview:	function getQueryValue(n,t){var r=new RegExp("[\\?&]"+t+"=([^&#]*)","gi"),i=r.exec(n);return i==null?"":decodeURIComponent(i[1].replace(/\+/g," "))}function getStore(n){var t="ClosestStore.asmx",r,i;$(".store-geo[data-GeoStoreLocalServiceURL]").length&&(t=$(".store-geo").first().attr("data-GeoStoreLocalServiceURL"));i="POST";typeof n!="undefined"&&(r={latitude:JSON.stringify(n.coords.latitude),longitude:JSON.stringify(n.coords.longitude)},t=t+"ClientGeo",i="GET");$.ajax({url:t,type:i,timeout:5e3,data:r,contentType:"application/json; charset=UTF-8",dataType:"json",error:function(){$(".store-geo").remove();$(".store-editorial").fadeIn(1e3)},success:function(n){if(typeof n!="undefined"&&typeof n.d!="undefined"&&typeof n.d.City!="undefined"&&n.d.City!=""&&n.d.StoreUrl!="undefined"&&n.d.StoreUrl!=""){var t=$(".store-geo:first").text();$(".store-geo a").html(t+" "+n.d.City);$(".store-geo a").attr("href",n.d.StoreUrl);$(".store-editorial").remove();$(".store-geo").fadeIn(1e3)}else $(".store-g

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\script[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	50466
Entropy (8bit):	5.403327253117392
Encrypted:	false
SSDEEP:	768:3Vs4A3c/bSKCzUm4D19h3j9UIAyjYXQgyjYXEoygRRsRnMtoafRnvdMIKebqH:h6c/bSKCzUm4DDh3j+9XQ4XE+BZdMIK9
MD5:	633B23CA8A850C508C146635DB4239F5
SHA1:	CF78DA53BD7561F3ACB33710016ECBF60E9F0204
SHA-256:	DAA1677D2640BE8A77F6C69EEE3911D2F8CF81DAA7BB604800A2D63A8F130C95
SHA-512:	82D4887AB9BB6A449FB0E5B6DEF80215B5F9E51058DCB1B8B7CD583A880F93428C3FB75B37C0E9481843203A4878FEF32424B5CD2EBCDD811D92604A1C1BCAB
Malicious:	false
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSScripts/script.jsx?k=1a053411-4f63-d069-d3b8-11d5d720eeb4
Preview:	function ShowSelectedComponentKeyPress(n,t){if(window.event.keyCode==13)return ShowSelectedComponent(n,t),!1}function ShowHighLight(n){var t=$("#div"+n).height();$.browser.msie&&parseInt($.browser.version,10)==7?$("#div"+n+" > .highlight").css({width:"0",height:"0","background-color":"white",float:"left","border-top":Math.round(t/2+.3)+"px solid white","border-right":"0.75em solid "+$("#div"+n).css("background-color"),"border-bottom":Math.round(t/2+.3)+"px solid white"}):$("#div"+n+" > .highlight").css({width:"0",height:"0","background-color":"white",float:"left","border-top":t/2+.3+"px solid white","border-right":"0.75em solid "+$("#div"+n).css("background-color"),"border-bottom":t/2+.3+"px solid white"})}function SetRightSideNavigationMenuHeight(){$("[id^=dvModuleGroup_]").hide();window.location.search.toLowerCase().indexOf("bookmarkid")!=-1&&SelectBookMark();window.location.search.toLowerCase().indexOf("componentid")!=-1&&LoadSelectedInternalLink();$(".div_side_comp").length>0&&$(".

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\servicesagreement[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	211739
Entropy (8bit):	5.164859489347292
Encrypted:	false
SSDEEP:	6144:kzpZaZEzF0a6OGYL0seowg6ehsymCJ2i/T9VTSfaTHgJi7eshMcgGJ3Ha:kdZaZEzX6OGYQseowg6ehsymCJ2i/pVI
MD5:	EE61A55C95AD614195CF1F9895769AC7
SHA1:	26379BA99926A285448AD5EEC347607B296C9187
SHA-256:	289DB1761B502922A40555CB684EA96144AC5DC6D9FA204604C20AA10F22DDB3
SHA-512:	DEEA6CF2EB999E6AD1B38619148F0C0912BFE5D852D08660827679F466C41C31D60BE8ED1672BDC781FA9991D470470E6C437098C02363847BEB0F31DFF7C59
Malicious:	false
Preview:	.<!DOCTYPE html ><html xmlns:mscom="http://schemas.microsoft.com/CMSvNext" xmlns:md="http://schemas.microsoft.com/mscom-data" lang="en-us" xmlns="http://www.w3.org/1999/xhtml"><head><meta name="viewport" content="initial-scale=1.0, width=device-width" /><meta http-equiv="X-UA-Compatible" content="IE=edge" /><title>Microsoft Services Agreement</title><meta name="Title" content="Microsoft Services Agreement" /><meta name="CorrelationVector" content="4SnQ9vHYfkqocHjk.1" /><meta name="Description" content="" /><meta name="MscomContentLocale" content="en-us" /><link href="https://www.microsoft.com/onerfstatics/marketingsites-wcus-prod/west-european/shell/_scrf/css/themes=default.device=uplevel_web_pc/4d-9e2636/56-1c4656/c9-48785f/2c-a9a6a4/40-11102f/10-4f9f5d/7d-35b35c/64-460736?ver=2.0" rel="stylesheet" type="text/css" media="screen" /><link href="https://statics-marketingsites-wcus-ms-com.akamaized.net/statics/override.css?c=7" rel="stylesheet" type="text/css" media="screen" /><link rel

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\style[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	836
Entropy (8bit):	4.940950417710206
Encrypted:	false
SSDEEP:	24:Cn5ZoK2kNMCJZ4ZVaeao1DphsILHJNM2WXgEXgf0Xgm:u5dxJZ4+BWIIPLQ73/

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\style[1].css	
MD5:	2AC383F4677A1036C8EA4289F99A31E3
SHA1:	E65967B9273029CDDD5A5F8DF9E61DACF89CF11C
SHA-256:	2206A95E6BAC7C185CC54638EBF0B0089CBC27FF729B45AC63C968CFE4991AA4
SHA-512:	9E61D4E2B42A1BC776C5649ECD2E32A1CE1ACEDA929E8C013D20BE95D12B7B56864FD588D6117E6410988331F85E21815E2E135030F49BEA2A244F872570DBE
Malicious:	false
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSStyles/style.csx?k=4627136a-bd68-db6e-30c9-37cf96c98eee
Preview:	body .grid,.body-open .grid,.grid h3,.grid .h3,.grid .header-small,.grid strong,.grid .body-tight-2,.grid h1,.grid .h1,.grid .header-large,.grid .caption{font-family:"Segoe UI"}.grid{max-width:1600px !important}.c-uhfh-actions,.c-uhfh-gcontainer-st .all-ms-nav,.glyph-global-nav-button{display:none !important}.shell-header-wrapper,.shell-footer-wrapper,.shell-category-nav,.shell-notification .shell-notification-grid-row{max-width:1180px !important}.PsTitle{font-family:Segoe UI,sans-serif;margin-right:.3em !important;font-size:2em;display:inline-block;vertical-align:top;margin-left:-.02em}.childModule{margin-left:8% !important}.CollectingYourInfoRightNav{display:none}html[dir=rtl] .m-r-md{margin-right:0;margin-left:10px}html[dir=rtl] .m-l-md{margin-left:0;margin-right:10px}html[dir=rtl] .m-r-bl{margin-right:0;margin-left:40px}

C:\Users\user\AppData\Local\Temp\~DF1F4FC221F135EB7E.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.3370277143757601
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laAThVo/:kBqoxxJhHWSVSEabS
MD5:	A49F5173D61F6EA73F343ED1511E20C8
SHA1:	DA8BFA3A43B0E52588A763F4423A39D1C9102959
SHA-256:	7CBBB043FBF31929770A3CAFDA4A3065050CF096AE8DFCF31F03679407FE0868
SHA-512:	1BAA5745186BF422EF905578450FB0E41D58F1A0734F9022D8E5F4B7420CB33DEE628139FD840609DDAC4527A39301D3D61EF92CA8EC7BFCA5FCC4753A52A38
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFE0206310410160BF.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13077
Entropy (8bit):	0.511499866701377
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lolDF9lolJ9lWlAOGaV5OGyIemGyZGyowf5wf2:kBqoIlSlMlAOGG5OGyIDGyZGyowf5wf2
MD5:	628E5FEF95544E3001AB3333988E1EB0
SHA1:	CF0E579D34DC390B5E173337175098A0543BF564
SHA-256:	8E60A65017DA90310C607FEEA602E6F265DEEDF376542286CA0C79846F5D3D3C
SHA-512:	7EDC2A2EBAD13C631606F31C2134DB5C4CA4F556F8D3480E966A6B2ECE3A7AC466CB6697795850CC447157AC06271FF277AF3A1CF3EF08C6F4A810C4B99153
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFF60A6E91562499B3.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	56873
Entropy (8bit):	0.8738602810221622
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+2wqDwHQPjzftjzLBYjzftjzLB/QscGIgNo4JUN:kBqoxKAuqR+2wqDwH6fJMfJN9cGFo4J
MD5:	E30C17ABA7A771765B989AED7C1B265F
SHA1:	04D1293589F952494417366C22204A227B45B848
SHA-256:	F699118AC0E3C85D85F8237AA7AD08F776E7F15778FB96DF2424D3BE18DDC121
SHA-512:	A17C59B1241C17C7914E4BFDBC030ACCFA002DDF0DD04B7E14E1D52BC6478933711C98ED5224A2E5AC50AB637118C243A5EEFCA185676F6847102008566E8F B
Malicious:	false

C:\Users\user\AppData\Local\Temp\~DFF60A6E91562499B3.TMP	
Preview:	.............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

General

File type:	HTML document, ASCII text, with very long lines, with no line terminators
Entropy (8bit):	3.2853032451299216
TrID:	
File name:	Paid561571.htm
File size:	345831
MD5:	34b0610fb39400c8e26a062f15c82b7e
SHA1:	b63e46c20b06f2111aeb4c986f02bbee0e5de15e
SHA256:	6f49afc966c3172c1fdf6be50d268a58dac5f837559b7753ab5ae74997442103
SHA512:	a80e3638be5f824f465f20887afadd57e333873f3d01c6698a4ea032a55d89a71ed60d7ae7db18c4af2959e60d4a9c946b5149784febf64f2d5b15b6d39ea5e7
SSDEEP:	1536:psdE0PWs2pKueZz8ZQlvv3XL9Fn9B9L40:s
File Content Preview:	<script type='text/javascript'>document.write(unescape('%3C%21%44%4F%43%54%59%50%45%20%68%74%6D%6C%3E%0D%0A%3C%68%74%6D%6C%20%64%69%72%3D%22%6C%74%72%22%20%6C%61%6E%67%3D%22%65%6E%22%3E%0D%0A%20%20%20%20%3C%6D%65%74%61%20%63%68%61%72%73%65%74%3D%22%75%74%

File Icon

Icon Hash:	f8c89c9a9a998cb8

Network Behavior

Network Port Distribution

Total Packets: 103

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 5, 2021 13:33:34.120831966 CET	49706	443	192.168.2.3	104.16.19.94
Mar 5, 2021 13:33:34.120836020 CET	49707	443	192.168.2.3	104.16.19.94
Mar 5, 2021 13:33:34.169342995 CET	443	49707	104.16.19.94	192.168.2.3
Mar 5, 2021 13:33:34.169487000 CET	49707	443	192.168.2.3	104.16.19.94
Mar 5, 2021 13:33:34.169820070 CET	443	49706	104.16.19.94	192.168.2.3
Mar 5, 2021 13:33:34.169919014 CET	49706	443	192.168.2.3	104.16.19.94
Mar 5, 2021 13:33:34.174242020 CET	49707	443	192.168.2.3	104.16.19.94
Mar 5, 2021 13:33:34.175865889 CET	49706	443	192.168.2.3	104.16.19.94
Mar 5, 2021 13:33:34.222717047 CET	443	49707	104.16.19.94	192.168.2.3
Mar 5, 2021 13:33:34.227119923 CET	443	49706	104.16.19.94	192.168.2.3
Mar 5, 2021 13:33:34.227165937 CET	443	49706	104.16.19.94	192.168.2.3
Mar 5, 2021 13:33:34.227204084 CET	443	49706	104.16.19.94	192.168.2.3
Mar 5, 2021 13:33:34.227303982 CET	49706	443	192.168.2.3	104.16.19.94
Mar 5, 2021 13:33:34.227361917 CET	49706	443	192.168.2.3	104.16.19.94
Mar 5, 2021 13:33:34.228060961 CET	443	49707	104.16.19.94	192.168.2.3
Mar 5, 2021 13:33:34.228099108 CET	443	49707	104.16.19.94	192.168.2.3
Mar 5, 2021 13:33:34.228121996 CET	49707	443	192.168.2.3	104.16.19.94
Mar 5, 2021 13:33:34.228149891 CET	49707	443	192.168.2.3	104.16.19.94
Mar 5, 2021 13:33:34.290031910 CET	49706	443	192.168.2.3	104.16.19.94
Mar 5, 2021 13:33:34.292073965 CET	49707	443	192.168.2.3	104.16.19.94
Mar 5, 2021 13:33:34.297123909 CET	49706	443	192.168.2.3	104.16.19.94
Mar 5, 2021 13:33:34.297506094 CET	49706	443	192.168.2.3	104.16.19.94
Mar 5, 2021 13:33:34.297636032 CET	49707	443	192.168.2.3	104.16.19.94
Mar 5, 2021 13:33:34.339059114 CET	443	49706	104.16.19.94	192.168.2.3
Mar 5, 2021 13:33:34.339265108 CET	443	49706	104.16.19.94	192.168.2.3
Mar 5, 2021 13:33:34.339309931 CET	443	49706	104.16.19.94	192.168.2.3
Mar 5, 2021 13:33:34.339420080 CET	49706	443	192.168.2.3	104.16.19.94
Mar 5, 2021 13:33:34.339473009 CET	49706	443	192.168.2.3	104.16.19.94
Mar 5, 2021 13:33:34.340522051 CET	443	49707	104.16.19.94	192.168.2.3
Mar 5, 2021 13:33:34.340709925 CET	443	49707	104.16.19.94	192.168.2.3
Mar 5, 2021 13:33:34.340735912 CET	443	49707	104.16.19.94	192.168.2.3
Mar 5, 2021 13:33:34.340786934 CET	49707	443	192.168.2.3	104.16.19.94
Mar 5, 2021 13:33:34.340809107 CET	49707	443	192.168.2.3	104.16.19.94
Mar 5, 2021 13:33:34.341048002 CET	49706	443	192.168.2.3	104.16.19.94
Mar 5, 2021 13:33:34.342097044 CET	49707	443	192.168.2.3	104.16.19.94
Mar 5, 2021 13:33:34.345884085 CET	443	49706	104.16.19.94	192.168.2.3
Mar 5, 2021 13:33:34.345912933 CET	443	49707	104.16.19.94	192.168.2.3
Mar 5, 2021 13:33:34.345940113 CET	443	49706	104.16.19.94	192.168.2.3
Mar 5, 2021 13:33:34.346009016 CET	49706	443	192.168.2.3	104.16.19.94
Mar 5, 2021 13:33:34.346776009 CET	443	49707	104.16.19.94	192.168.2.3
Mar 5, 2021 13:33:34.346847057 CET	49707	443	192.168.2.3	104.16.19.94
Mar 5, 2021 13:33:34.353100061 CET	443	49706	104.16.19.94	192.168.2.3
Mar 5, 2021 13:33:34.353127956 CET	443	49706	104.16.19.94	192.168.2.3
Mar 5, 2021 13:33:34.353174925 CET	443	49706	104.16.19.94	192.168.2.3
Mar 5, 2021 13:33:34.353205919 CET	443	49706	104.16.19.94	192.168.2.3
Mar 5, 2021 13:33:34.353236914 CET	49706	443	192.168.2.3	104.16.19.94
Mar 5, 2021 13:33:34.353245020 CET	443	49706	104.16.19.94	192.168.2.3
Mar 5, 2021 13:33:34.353271008 CET	49706	443	192.168.2.3	104.16.19.94
Mar 5, 2021 13:33:34.353276014 CET	49706	443	192.168.2.3	104.16.19.94
Mar 5, 2021 13:33:34.353280067 CET	49706	443	192.168.2.3	104.16.19.94
Mar 5, 2021 13:33:34.353283882 CET	443	49706	104.16.19.94	192.168.2.3
Mar 5, 2021 13:33:34.353297949 CET	49706	443	192.168.2.3	104.16.19.94
Mar 5, 2021 13:33:34.353343010 CET	49706	443	192.168.2.3	104.16.19.94
Mar 5, 2021 13:33:34.354188919 CET	443	49706	104.16.19.94	192.168.2.3
Mar 5, 2021 13:33:34.354219913 CET	443	49706	104.16.19.94	192.168.2.3
Mar 5, 2021 13:33:34.354260921 CET	49706	443	192.168.2.3	104.16.19.94
Mar 5, 2021 13:33:34.354289055 CET	49706	443	192.168.2.3	104.16.19.94
Mar 5, 2021 13:33:34.354847908 CET	443	49706	104.16.19.94	192.168.2.3
Mar 5, 2021 13:33:34.354918003 CET	49706	443	192.168.2.3	104.16.19.94
Mar 5, 2021 13:33:34.430080891 CET	443	49706	104.16.19.94	192.168.2.3
Mar 5, 2021 13:33:34.431090117 CET	443	49707	104.16.19.94	192.168.2.3
Mar 5, 2021 13:33:34.902720928 CET	49708	443	192.168.2.3	152.199.23.37
Mar 5, 2021 13:33:34.903301954 CET	49709	443	192.168.2.3	152.199.23.37
Mar 5, 2021 13:33:34.903558016 CET	49710	443	192.168.2.3	152.199.23.37

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 5, 2021 13:33:34.903675079 CET	49711	443	192.168.2.3	152.199.23.37
Mar 5, 2021 13:33:34.903896093 CET	49712	443	192.168.2.3	152.199.23.37
Mar 5, 2021 13:33:34.904436111 CET	49713	443	192.168.2.3	152.199.23.37
Mar 5, 2021 13:33:34.940742970 CET	443	49708	152.199.23.37	192.168.2.3
Mar 5, 2021 13:33:34.940828085 CET	49708	443	192.168.2.3	152.199.23.37
Mar 5, 2021 13:33:34.941056967 CET	443	49709	152.199.23.37	192.168.2.3
Mar 5, 2021 13:33:34.941119909 CET	49709	443	192.168.2.3	152.199.23.37
Mar 5, 2021 13:33:34.941370964 CET	443	49710	152.199.23.37	192.168.2.3
Mar 5, 2021 13:33:34.941423893 CET	443	49711	152.199.23.37	192.168.2.3
Mar 5, 2021 13:33:34.941442966 CET	49710	443	192.168.2.3	152.199.23.37
Mar 5, 2021 13:33:34.941545963 CET	49711	443	192.168.2.3	152.199.23.37
Mar 5, 2021 13:33:34.941663980 CET	443	49712	152.199.23.37	192.168.2.3
Mar 5, 2021 13:33:34.941771984 CET	49712	443	192.168.2.3	152.199.23.37
Mar 5, 2021 13:33:34.941930056 CET	49708	443	192.168.2.3	152.199.23.37
Mar 5, 2021 13:33:34.942280054 CET	443	49713	152.199.23.37	192.168.2.3
Mar 5, 2021 13:33:34.942373991 CET	49713	443	192.168.2.3	152.199.23.37
Mar 5, 2021 13:33:34.942910910 CET	49712	443	192.168.2.3	152.199.23.37
Mar 5, 2021 13:33:34.943463087 CET	49713	443	192.168.2.3	152.199.23.37
Mar 5, 2021 13:33:34.944071054 CET	49709	443	192.168.2.3	152.199.23.37
Mar 5, 2021 13:33:34.944617033 CET	49710	443	192.168.2.3	152.199.23.37
Mar 5, 2021 13:33:34.945250034 CET	49711	443	192.168.2.3	152.199.23.37
Mar 5, 2021 13:33:34.979650974 CET	443	49708	152.199.23.37	192.168.2.3
Mar 5, 2021 13:33:34.980659008 CET	443	49708	152.199.23.37	192.168.2.3
Mar 5, 2021 13:33:34.980707884 CET	443	49708	152.199.23.37	192.168.2.3
Mar 5, 2021 13:33:34.980745077 CET	443	49708	152.199.23.37	192.168.2.3
Mar 5, 2021 13:33:34.980748892 CET	49708	443	192.168.2.3	152.199.23.37
Mar 5, 2021 13:33:34.980768919 CET	49708	443	192.168.2.3	152.199.23.37
Mar 5, 2021 13:33:34.980772972 CET	443	49708	152.199.23.37	192.168.2.3
Mar 5, 2021 13:33:34.980792046 CET	49708	443	192.168.2.3	152.199.23.37
Mar 5, 2021 13:33:34.980799913 CET	443	49712	152.199.23.37	192.168.2.3
Mar 5, 2021 13:33:34.980824947 CET	49708	443	192.168.2.3	152.199.23.37
Mar 5, 2021 13:33:34.981245041 CET	443	49713	152.199.23.37	192.168.2.3
Mar 5, 2021 13:33:34.981837034 CET	443	49712	152.199.23.37	192.168.2.3
Mar 5, 2021 13:33:34.981875896 CET	443	49712	152.199.23.37	192.168.2.3
Mar 5, 2021 13:33:34.981923103 CET	443	49712	152.199.23.37	192.168.2.3
Mar 5, 2021 13:33:34.981952906 CET	443	49712	152.199.23.37	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 5, 2021 13:33:25.753874063 CET	64938	53	192.168.2.3	8.8.8.8
Mar 5, 2021 13:33:25.799927950 CET	53	64938	8.8.8.8	192.168.2.3
Mar 5, 2021 13:33:32.758287907 CET	60152	53	192.168.2.3	8.8.8.8
Mar 5, 2021 13:33:32.809266090 CET	53	60152	8.8.8.8	192.168.2.3
Mar 5, 2021 13:33:34.064307928 CET	57544	53	192.168.2.3	8.8.8.8
Mar 5, 2021 13:33:34.110126972 CET	53	57544	8.8.8.8	192.168.2.3
Mar 5, 2021 13:33:34.749773026 CET	55984	53	192.168.2.3	8.8.8.8
Mar 5, 2021 13:33:34.811003923 CET	53	55984	8.8.8.8	192.168.2.3
Mar 5, 2021 13:33:34.912435055 CET	64185	53	192.168.2.3	8.8.8.8
Mar 5, 2021 13:33:34.961241961 CET	53	64185	8.8.8.8	192.168.2.3
Mar 5, 2021 13:33:36.045650005 CET	65110	53	192.168.2.3	8.8.8.8
Mar 5, 2021 13:33:36.094325066 CET	53	65110	8.8.8.8	192.168.2.3
Mar 5, 2021 13:33:37.035125017 CET	58361	53	192.168.2.3	8.8.8.8
Mar 5, 2021 13:33:37.082550049 CET	53	58361	8.8.8.8	192.168.2.3
Mar 5, 2021 13:33:48.202728033 CET	63492	53	192.168.2.3	8.8.8.8
Mar 5, 2021 13:33:48.248437881 CET	53	63492	8.8.8.8	192.168.2.3
Mar 5, 2021 13:33:50.164554119 CET	60831	53	192.168.2.3	8.8.8.8
Mar 5, 2021 13:33:50.213462114 CET	53	60831	8.8.8.8	192.168.2.3
Mar 5, 2021 13:33:50.413544893 CET	60100	53	192.168.2.3	8.8.8.8
Mar 5, 2021 13:33:50.463351965 CET	53	60100	8.8.8.8	192.168.2.3
Mar 5, 2021 13:33:52.278075933 CET	53195	53	192.168.2.3	8.8.8.8
Mar 5, 2021 13:33:52.326467991 CET	53	53195	8.8.8.8	192.168.2.3
Mar 5, 2021 13:33:52.890130997 CET	50141	53	192.168.2.3	8.8.8.8
Mar 5, 2021 13:33:52.893707991 CET	53023	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 5, 2021 13:33:52.900439024 CET	49563	53	192.168.2.3	8.8.8.8
Mar 5, 2021 13:33:52.902162075 CET	51352	53	192.168.2.3	8.8.8.8
Mar 5, 2021 13:33:52.911966085 CET	59349	53	192.168.2.3	8.8.8.8
Mar 5, 2021 13:33:52.940737963 CET	53	50141	8.8.8.8	192.168.2.3
Mar 5, 2021 13:33:52.950987101 CET	53	53023	8.8.8.8	192.168.2.3
Mar 5, 2021 13:33:52.956326962 CET	53	49563	8.8.8.8	192.168.2.3
Mar 5, 2021 13:33:52.961492062 CET	53	51352	8.8.8.8	192.168.2.3
Mar 5, 2021 13:33:52.964148998 CET	53	59349	8.8.8.8	192.168.2.3
Mar 5, 2021 13:33:55.380856037 CET	57084	53	192.168.2.3	8.8.8.8
Mar 5, 2021 13:33:55.432066917 CET	53	57084	8.8.8.8	192.168.2.3
Mar 5, 2021 13:33:55.732086897 CET	58823	53	192.168.2.3	8.8.8.8
Mar 5, 2021 13:33:55.777808905 CET	53	58823	8.8.8.8	192.168.2.3
Mar 5, 2021 13:33:55.938761950 CET	57568	53	192.168.2.3	8.8.8.8
Mar 5, 2021 13:33:55.999516964 CET	53	57568	8.8.8.8	192.168.2.3
Mar 5, 2021 13:33:56.378648043 CET	50540	53	192.168.2.3	8.8.8.8
Mar 5, 2021 13:33:56.426701069 CET	53	50540	8.8.8.8	192.168.2.3
Mar 5, 2021 13:34:01.058068991 CET	54366	53	192.168.2.3	8.8.8.8
Mar 5, 2021 13:34:01.107064962 CET	53	54366	8.8.8.8	192.168.2.3
Mar 5, 2021 13:34:02.747386932 CET	53034	53	192.168.2.3	8.8.8.8
Mar 5, 2021 13:34:02.794343948 CET	53	53034	8.8.8.8	192.168.2.3
Mar 5, 2021 13:34:03.394486904 CET	57762	53	192.168.2.3	8.8.8.8
Mar 5, 2021 13:34:03.443569899 CET	53	57762	8.8.8.8	192.168.2.3
Mar 5, 2021 13:34:03.757812023 CET	53034	53	192.168.2.3	8.8.8.8
Mar 5, 2021 13:34:03.804188013 CET	53	53034	8.8.8.8	192.168.2.3
Mar 5, 2021 13:34:04.398243904 CET	57762	53	192.168.2.3	8.8.8.8
Mar 5, 2021 13:34:04.445283890 CET	53	57762	8.8.8.8	192.168.2.3
Mar 5, 2021 13:34:04.774904013 CET	53034	53	192.168.2.3	8.8.8.8
Mar 5, 2021 13:34:04.822372913 CET	53	53034	8.8.8.8	192.168.2.3
Mar 5, 2021 13:34:05.049129009 CET	55435	53	192.168.2.3	8.8.8.8
Mar 5, 2021 13:34:05.105515957 CET	53	55435	8.8.8.8	192.168.2.3
Mar 5, 2021 13:34:05.581114054 CET	57762	53	192.168.2.3	8.8.8.8
Mar 5, 2021 13:34:05.627609968 CET	53	57762	8.8.8.8	192.168.2.3
Mar 5, 2021 13:34:06.740950108 CET	50713	53	192.168.2.3	8.8.8.8
Mar 5, 2021 13:34:06.788402081 CET	53034	53	192.168.2.3	8.8.8.8
Mar 5, 2021 13:34:06.791548967 CET	53	50713	8.8.8.8	192.168.2.3
Mar 5, 2021 13:34:06.834481001 CET	53	53034	8.8.8.8	192.168.2.3
Mar 5, 2021 13:34:06.956602097 CET	56132	53	192.168.2.3	8.8.8.8
Mar 5, 2021 13:34:07.007204056 CET	53	56132	8.8.8.8	192.168.2.3
Mar 5, 2021 13:34:07.569554090 CET	57762	53	192.168.2.3	8.8.8.8
Mar 5, 2021 13:34:07.615866899 CET	53	57762	8.8.8.8	192.168.2.3
Mar 5, 2021 13:34:08.528765917 CET	58987	53	192.168.2.3	8.8.8.8
Mar 5, 2021 13:34:08.586783886 CET	53	58987	8.8.8.8	192.168.2.3
Mar 5, 2021 13:34:09.704741001 CET	56579	53	192.168.2.3	8.8.8.8
Mar 5, 2021 13:34:09.750963926 CET	53	56579	8.8.8.8	192.168.2.3
Mar 5, 2021 13:34:10.804393053 CET	53034	53	192.168.2.3	8.8.8.8
Mar 5, 2021 13:34:10.850717068 CET	53	53034	8.8.8.8	192.168.2.3
Mar 5, 2021 13:34:10.976608992 CET	60633	53	192.168.2.3	8.8.8.8
Mar 5, 2021 13:34:11.022742033 CET	53	60633	8.8.8.8	192.168.2.3
Mar 5, 2021 13:34:11.585439920 CET	57762	53	192.168.2.3	8.8.8.8
Mar 5, 2021 13:34:11.633579969 CET	53	57762	8.8.8.8	192.168.2.3
Mar 5, 2021 13:34:13.252573967 CET	61292	53	192.168.2.3	8.8.8.8
Mar 5, 2021 13:34:13.301217079 CET	53	61292	8.8.8.8	192.168.2.3
Mar 5, 2021 13:34:17.241662979 CET	63619	53	192.168.2.3	8.8.8.8
Mar 5, 2021 13:34:17.288996935 CET	53	63619	8.8.8.8	192.168.2.3
Mar 5, 2021 13:34:19.050249100 CET	64938	53	192.168.2.3	8.8.8.8
Mar 5, 2021 13:34:19.096375942 CET	53	64938	8.8.8.8	192.168.2.3
Mar 5, 2021 13:34:20.403048992 CET	61946	53	192.168.2.3	8.8.8.8
Mar 5, 2021 13:34:20.453608036 CET	53	61946	8.8.8.8	192.168.2.3
Mar 5, 2021 13:34:21.821317911 CET	64910	53	192.168.2.3	8.8.8.8
Mar 5, 2021 13:34:21.871584892 CET	53	64910	8.8.8.8	192.168.2.3
Mar 5, 2021 13:34:27.264529943 CET	52123	53	192.168.2.3	8.8.8.8
Mar 5, 2021 13:34:27.313613892 CET	53	52123	8.8.8.8	192.168.2.3
Mar 5, 2021 13:34:28.375503063 CET	56130	53	192.168.2.3	8.8.8.8
Mar 5, 2021 13:34:28.422605991 CET	53	56130	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 5, 2021 13:34:33.353888988 CET	56338	53	192.168.2.3	8.8.8.8
Mar 5, 2021 13:34:33.408948898 CET	53	56338	8.8.8.8	192.168.2.3
Mar 5, 2021 13:34:44.510734081 CET	59420	53	192.168.2.3	8.8.8.8
Mar 5, 2021 13:34:44.559777975 CET	53	59420	8.8.8.8	192.168.2.3
Mar 5, 2021 13:34:49.102823019 CET	58784	53	192.168.2.3	8.8.8.8
Mar 5, 2021 13:34:49.150603056 CET	53	58784	8.8.8.8	192.168.2.3
Mar 5, 2021 13:35:20.794872999 CET	63978	53	192.168.2.3	8.8.8.8
Mar 5, 2021 13:35:20.843646049 CET	53	63978	8.8.8.8	192.168.2.3
Mar 5, 2021 13:35:22.414436102 CET	62938	53	192.168.2.3	8.8.8.8
Mar 5, 2021 13:35:22.461411953 CET	53	62938	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 5, 2021 13:33:34.064307928 CET	192.168.2.3	8.8.8.8	0xc6b2	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Mar 5, 2021 13:33:34.749773026 CET	192.168.2.3	8.8.8.8	0xc899	Standard query (0)	aadcdn.msftauth.net	A (IP address)	IN (0x0001)
Mar 5, 2021 13:33:34.912435055 CET	192.168.2.3	8.8.8.8	0x1713	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Mar 5, 2021 13:33:50.413544893 CET	192.168.2.3	8.8.8.8	0x82e1	Standard query (0)	aadcdn.msftauth.net	A (IP address)	IN (0x0001)
Mar 5, 2021 13:33:52.900439024 CET	192.168.2.3	8.8.8.8	0xf457	Standard query (0)	ajax.aspnetcdn.com	A (IP address)	IN (0x0001)
Mar 5, 2021 13:33:55.938761950 CET	192.168.2.3	8.8.8.8	0x739c	Standard query (0)	assets.onestore.ms	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 5, 2021 13:33:34.110126972 CET	8.8.8.8	192.168.2.3	0xc6b2	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Mar 5, 2021 13:33:34.110126972 CET	8.8.8.8	192.168.2.3	0xc6b2	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Mar 5, 2021 13:33:34.811003923 CET	8.8.8.8	192.168.2.3	0xc899	No error (0)	aadcdn.msftauth.net	aadcdnoriginneu.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Mar 5, 2021 13:33:34.811003923 CET	8.8.8.8	192.168.2.3	0xc899	No error (0)	cs1100.wpc.omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)
Mar 5, 2021 13:33:34.961241961 CET	8.8.8.8	192.168.2.3	0x1713	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Mar 5, 2021 13:33:50.463351965 CET	8.8.8.8	192.168.2.3	0x82e1	No error (0)	aadcdn.msftauth.net	aadcdnoriginneu.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Mar 5, 2021 13:33:50.463351965 CET	8.8.8.8	192.168.2.3	0x82e1	No error (0)	cs1100.wpc.omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)
Mar 5, 2021 13:33:52.956326962 CET	8.8.8.8	192.168.2.3	0xf457	No error (0)	ajax.aspnetcdn.com	mscomajax.vo.msecnd.net		CNAME (Canonical name)	IN (0x0001)
Mar 5, 2021 13:33:52.961492062 CET	8.8.8.8	192.168.2.3	0x5767	No error (0)	consentdeliveryfd.azurefd.net	star-azurefd-prod.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Mar 5, 2021 13:33:55.999516964 CET	8.8.8.8	192.168.2.3	0x739c	No error (0)	assets.onestore.ms	assets.onestore.ms.akadns.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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 5, 2021 13:33:34.227204084 CET	104.16.19.94	443	192.168.2.3	49706	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 5, 2021 13:33:34.228099108 CET	104.16.19.94	443	192.168.2.3	49707	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 5, 2021 13:33:34.980745077 CET	152.199.23.37	443	192.168.2.3	49708	CN=aadcdn.msftauth.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	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 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 5, 2021 13:33:34.981923103 CET	152.199.23.37	443	192.168.2.3	49712	CN=aadcdn.msftauth.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	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 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 5, 2021 13:33:34.982255936 CET	152.199.23.37	443	192.168.2.3	49713	CN=aadcdn.msftauth.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	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 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 5, 2021 13:33:34.982934952 CET	152.199.23.37	443	192.168.2.3	49709	CN=aadcdn.msftauth.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	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 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 5, 2021 13:33:34.983650923 CET	152.199.23.37	443	192.168.2.3	49710	CN=aadcdn.msftauth.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	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 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 5, 2021 13:33:34.985937119 CET	152.199.23.37	443	192.168.2.3	49711	CN=aadcdn.msftauth.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	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 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 5, 2021 13:33:50.547442913 CET	152.199.23.37	443	192.168.2.3	49720	CN=aadcdn.msftauth.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	Thu Jul 09 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jul 09 14:00:00 CEST 2021 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					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		

Code Manipulations

Statistics

Behavior

- iexplore.exe
- iexplore.exe

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 6016 Parent PID: 792

General

Start time:	13:33:31
Start date:	05/03/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff67dc30000
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	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 4260 Parent PID: 6016

General

Start time:	13:33:32
Start date:	05/03/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6016 CREDAT:17410 /prefetch:2
Imagebase:	0x1240000
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	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly