ID: 356226
Sample Name: FAX-MESSAGE201636576736375362.hTMl
Cookbook: default.jbs
Time: 19:41:52
Date: 22/02/2021
Version: 31.0.0 Emerald

Table of Contents

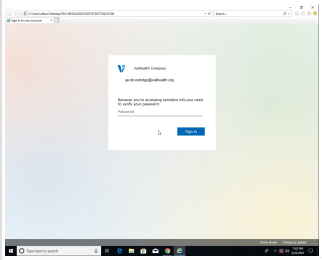
Analysis Report FAX-MESSAGE2016365767363753 62.hT…

Overview

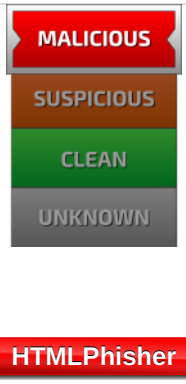
General Information

Sample Name:	FAX-MESSAGE201636576736375362.hTMl
Analysis ID:	356226
MD5:	9c0f59a8ec93478..
SHA1:	f35fc0edde9dbe0..
SHA256:	59c6ccf88f60e92…

Most interesting Screenshot:



Detection



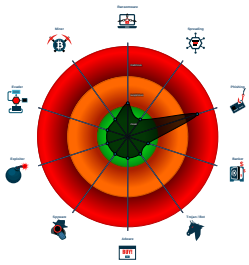
HTMLPhisher

Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Phishing site detected (based on fav…
- Yara detected HtmlPhish_10
- HTML title does not match URL
- IP address seen in connection with o…
- JA3 SSL client fingerprint seen in co…
- None HTTPS page querying sensitiv…

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 6260 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6312 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6260 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

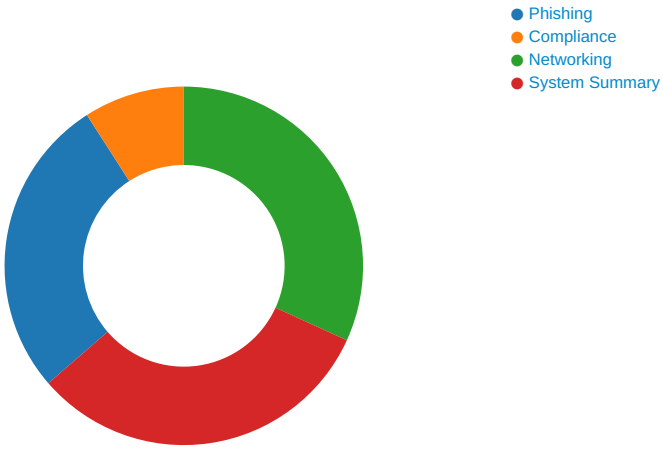
Initial Sample

Source	Rule	Description	Author	Strings
FAX-MESSAGE201636576736375362.hTMl	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	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

Compliance:

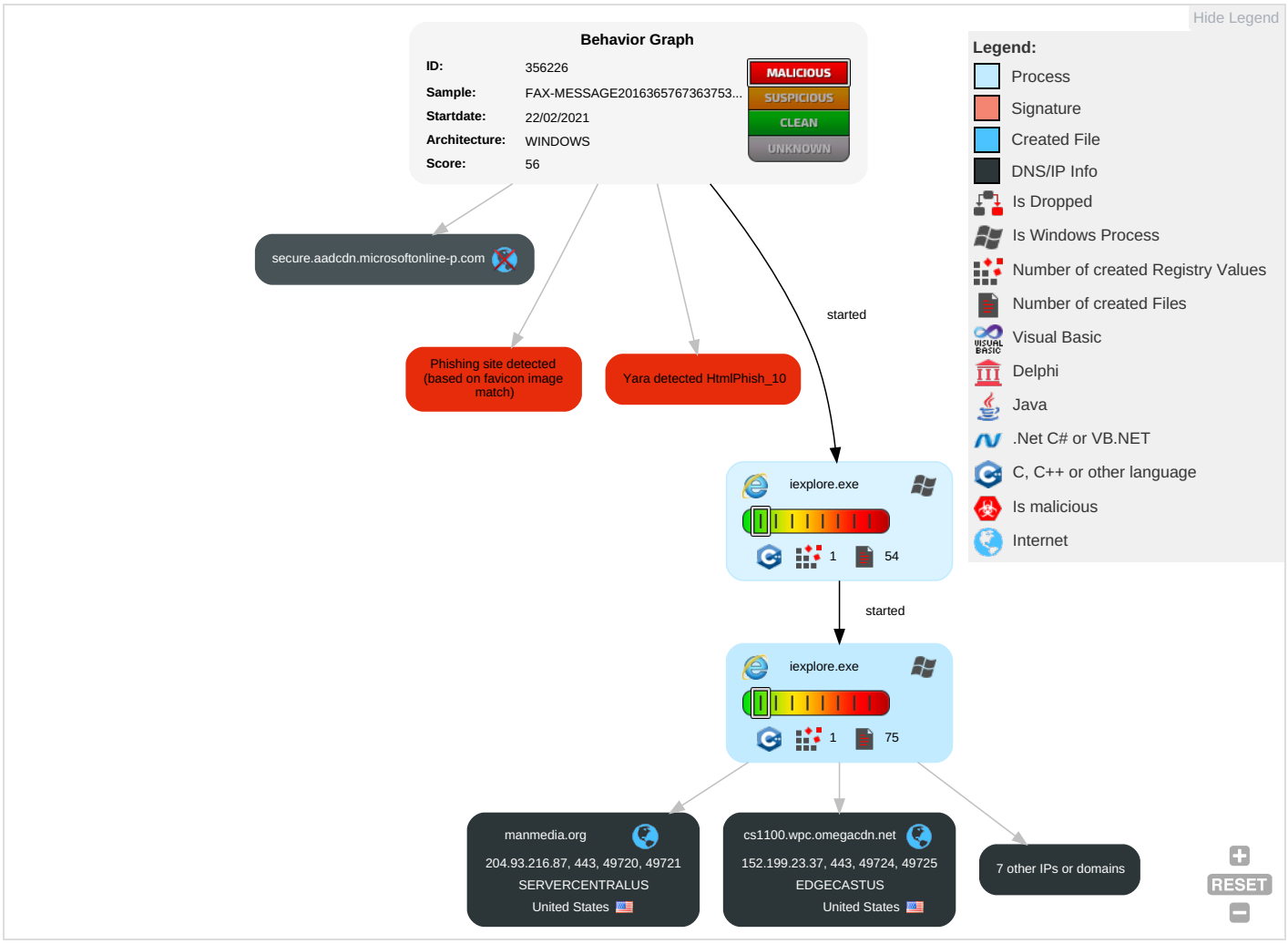
Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

Mitre Att&ck Matrix

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

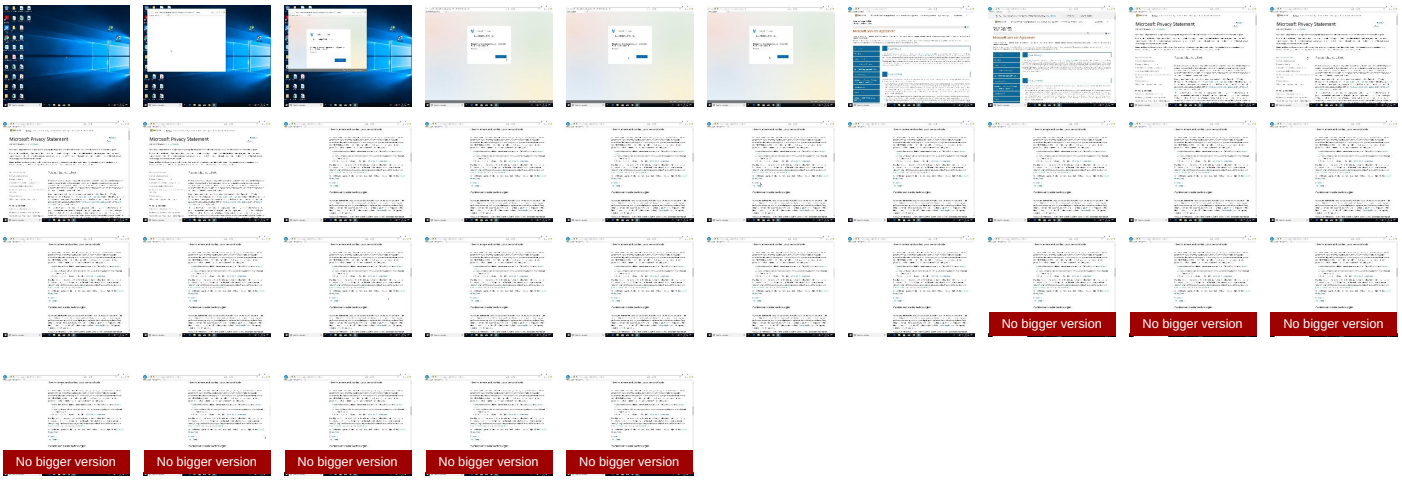
Behavior Graph

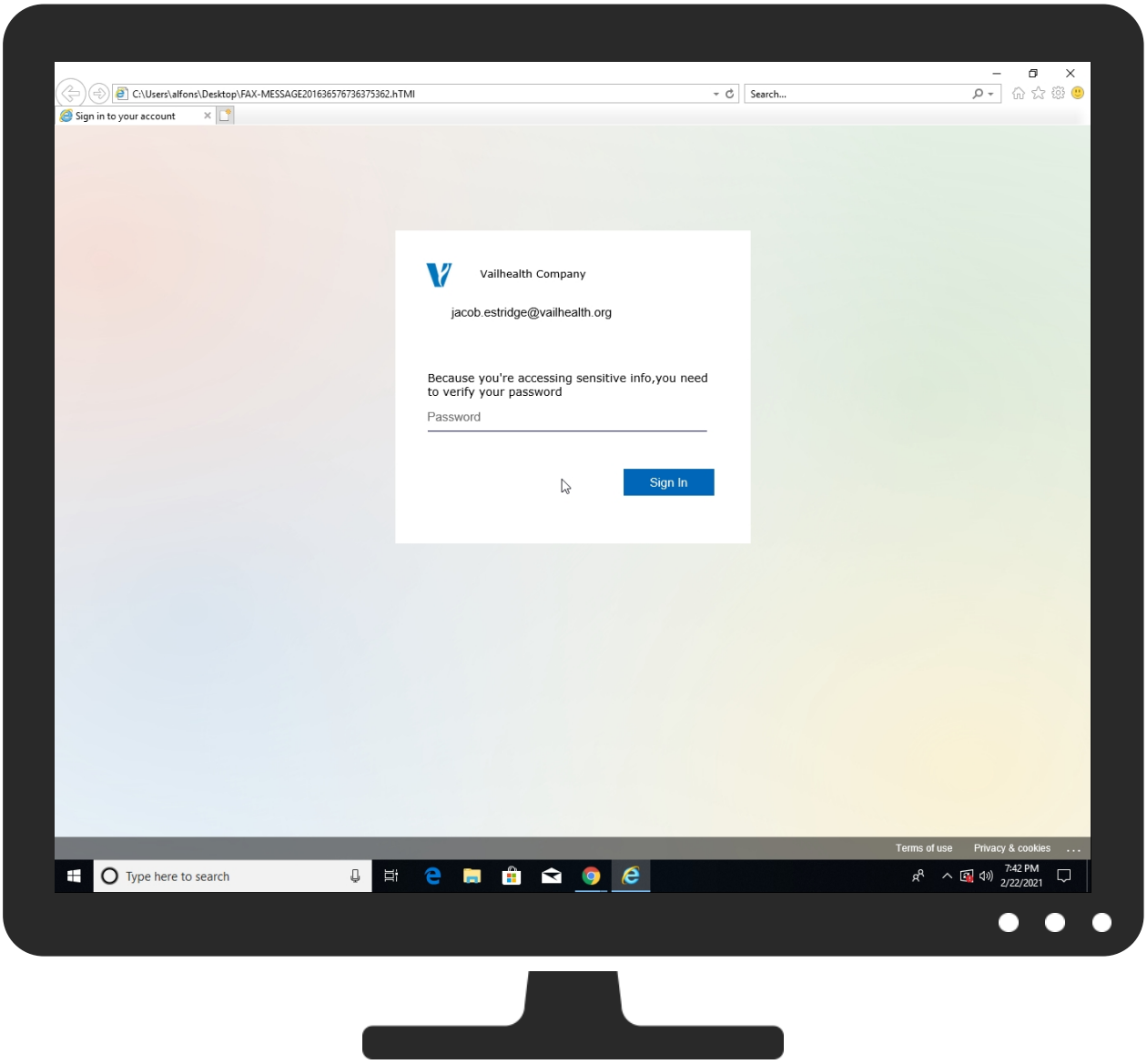


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

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
manmedia.org	0%	Virustotal		Browse
secure.aadcdn.microsoftonline-p.com	0%	Virustotal		Browse
aadcdn.msftauth.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://aadcdn.msftauthimg.net/dbd5a2dd-xs-ly6aik51q1xmokwuzg7cgil517bv-ngigbudd-ua/logintenantbrand	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/backgrounds/2_bc3d32a696895f78c19df6c717586a5d.s	0%	Avira URL Cloud	safe	
http://https://www.microsoft.s/Desktop/FAX-MESSAGE201636576736375362.hTMl	0%	Avira URL Cloud	safe	
http://https://www.youradchoices.ca/fr	0%	URL Reputation	safe	
http://https://www.youradchoices.ca/fr	0%	URL Reputation	safe	
http://https://www.youradchoices.ca/fr	0%	URL Reputation	safe	
http://https://tuicura.com/offic/next2.php	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauthimg.net/dbd5a2dd-2ivja-xubozxczt8hkuyvxiwoa4vmtaxu-16djdwpc4/logintenantbrand	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauthimg.net/dbd5a2dd-mg0l7zcxfhbgphoiomweiqgq-z4rxnrzczncff4igy/logintenantbrandi	0%	Avira URL Cloud	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://secure.aadcdn.microsoftonline-p.com/dbd5a2dd-mg0l7zcxfhbgphoiomweiqgq-z4rxnrzczncff4igy/logi	0%	Avira URL Cloud	safe	
http://https://privacy.m	0%	Avira URL Cloud	safe	
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.8576.13/content/images/favicon_a_eupayfgghqiai7	0%	Avira URL Cloud	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://manmedia.org/offic/n.page/style.css	0%	Avira URL Cloud	safe	
http://https://manmedia.org/offic/n.page/actions.js	0%	Avira URL Cloud	safe	
http://https://secure.aadcdn.microsoftonline-p.com/dbd5a2dd-pd-rbmzbvqe7c-fjbigunke9t2gf5jszgqrgsatxfkk/log	0%	Avira URL Cloud	safe	
http://www.mpegla.com).	0%	Avira URL Cloud	safe	
http://https://www.skype.com).	0%	Avira URL Cloud	safe	
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.8576.13/content/cdnbundles/converged.v2.login.m	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauthimg.net/dbd5a2dd-pd-rbmzbvqe7c-fjbigunke9t2gf5jszgqrgsatxfkk/logintenantbrand	0%	Avira URL Cloud	safe	
http://https://manmedia.org/offic/n.page/jqueryLib.js	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauthimg.net/dbd5a2dd-pglwtvfgjxd-jsxdxcu-ixstqem6dnqipplqonbe8ro/logintenantbrand	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://https://aadcdn.msftauthimg.net/dbd5a2dd-uhsmbqxf0i-fc4inz9zgqi96xh-agvghl3xbkxk-y7c/logintenantbrand	0%	Avira URL Cloud	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://secure.aadcdn.microsoftonline-p.com/dbd5a2dd-daldttgld72orokijcgtjn9zgk-dhdwrgaphu-0dqka/log	0%	Avira URL Cloud	safe	
http://https://tuicura.com/offic/nexxt.php	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauthimg.net/dbd5a2dd-bo8shd6svfocawg-d1lkuqyily-ch6cw-n5c0rmtwbq/logintenantbrand	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cs1100.wpc.omegacdn.net	152.199.23.37	true	false	• 0%, Virustotal, Browse	unknown
cdnjs.cloudflare.com	104.16.18.94	true	false		high
manmedia.org	204.93.216.87	true	false	• 0%, Virustotal, Browse	unknown
stackpath.bootstrapcdn.com	unknown	unknown	false		high
secure.aadcdn.microsoftonline-p.com	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
code.jquery.com	unknown	unknown	false		high
aadcdn.msftauth.net	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
assets.onestore.ms	unknown	unknown	false		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ajax.aspnetcdn.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
file:///C:/Users/user/Desktop/FAX-MESSAGE201636576736375362.hTMl	true		low

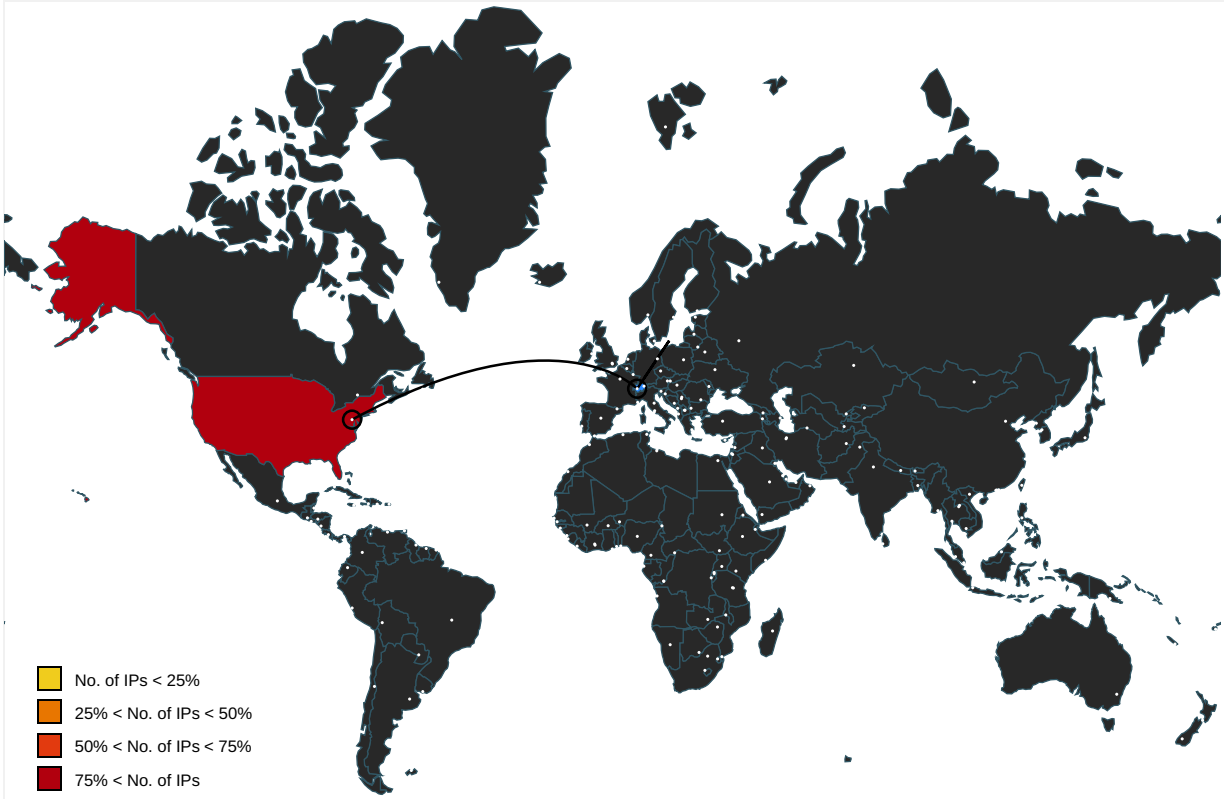
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://aka.ms/useterms	servicesagreement[1].htm.2.dr	false		high
http://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://aadcdn.msftauthimg.net/dbd5a2dd-xs-ly6aik51q1xmokwuzg7cgil517bv-ngigbudd-ua/logintenantbrand	style[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.1.0/js/bootstrap.min.js	FAX-MESSAGE201636576736375362.hTMl	false		high
http://https://www.optimizely.com/legal/opt-out/	privacystatement[1].htm.2.dr	false		high
http://https://aadcdn.msftauth.net/ests/2.1/content/images/backgrounds/2_bc3d32a696895f78c19df6c717586a5d.s	style[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.microsoft.s/Desktop/FAX-MESSAGE201636576736375362.hTMl	{2D14E88D-7589-11EB-90E5-ECF4BB570DC9}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.youradchoices.ca/fr	privacystatement[1].htm.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.microsoftonline.com/common/oauth2/authorize?client_id=4345a7b9-9a63-4910-a426-35363201	actions[1].js.2.dr	false		high
http://https://code.jquery.com/jquery-3.3.1.slim.min.js	FAX-MESSAGE201636576736375362.hTMl	false		high
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://tuicura.com/offic/next2.php	FAX-MESSAGE201636576736375362.hTMl	false	• Avira URL Cloud: safe	unknown
http://https://www.xbox.com/en-US/Legal/CodeOfConduct	servicesagreement[1].htm.2.dr	false		high
http://https://aadcdn.msftauthimg.net/dbd5a2dd-2ivja-xubozxczt8hkuyvxiwoa4vmtaxu-16djdwpc4/logintenantbrand	style[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
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://aadcdn.msftauthimg.net/dbd5a2dd-mg0l7zcxfhbgphoiomweiqgq-z4rxnrzczncff4igy/logintenantbrandi	style[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/twbs/bootstrap/graphs/contributors)	bootstrap.min[1].js.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
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	{2D14E88D-7589-11EB-90E5-ECF4BB570DC9}.dat.1.dr	false	• 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://https://secure.aadcdn.microsoftonline-p.com/dbd5a2dd-mg0l7zcxfhbgphoiomweiqgq-z4rxnrzczncff4igy/logi	style[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
http://logo.clearbit.com/	FAX-MESSAGE201636576736375362.hTMl	false		high
http://https://privacy.m	{2D14E88D-7589-11EB-90E5-ECF4BB570DC9}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://opensource.org/licenses/MIT).	popper.min[1].js.2.dr	false		high
http://www.mpegla.com	servicesagreement[1].htm.2.dr	false		high
http://https://secure.aadcdn.microsoftonline-p.com/ests/2.1.8576.13/content/images/favicon_a_eupayfgghqiai7	FAX-MESSAGE201636576736375362.hTMl	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.youradchoices.ca	privacystatement[1].htm.2.dr	false	• 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://manmedia.org/offic/n.page/style.css	FAX-MESSAGE201636576736375362.hTMl	false	• Avira URL Cloud: safe	unknown
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://manmedia.org/offic/n.page/actions.js	FAX-MESSAGE201636576736375362.hTMl	false	• Avira URL Cloud: safe	unknown
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://https://my.navyfederal.org/NFOAA_Auth/resources/img/css/img-billboard-BG.svg);	style[1].css.2.dr	false		high
http://https://secure.aadcdn.microsoftonline-p.com/dbd5a2dd-pd-rbmzbvqe7c-fjbigunke9t2gf5jszgqrgsatxfkk/log	style[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
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://secure.aadcdn.microsoftonline-p.com/ests/2.1.8576.13/content/cdnbundles/converged.v2.login.m	FAX-MESSAGE201636576736375362.hTMl	false	• Avira URL Cloud: safe	unknown
http://https://www.clicktale.net/disable.html	privacystatement[1].htm.2.dr	false		high
http://https://aadcdn.msftauthimg.net/dbd5a2dd-pd-rbmzbvqe7c-fjbigunke9t2gf5jszgqrgsatxfkk/logintenantbrand	style[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://getbootstrap.com/)	bootstrap.min[1].js.2.dr	false		high
http://https://manmedia.org/offic/n.page/jqueryLib.js	FAX-MESSAGE201636576736375362.hTMl	false	• Avira URL Cloud: safe	unknown
http://https://aadcdn.msftauthimg.net/dbd5a2dd-pglwtvfgjxd-jsxdxcu-ixstqem6dnqipplqonbe8ro/logintenantbrand	style[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.skype.com/go/allrates	servicesagreement[1].htm.2.dr	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.14.0/umd/popper.min.js	FAX-MESSAGE201636576736375362.hTMl	false		high
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	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://aadcdn.msftauthimg.net/dbd5a2dd-uhsmbqxf0i-fc4inz9zgqi96xh-agvghl3xbkxk-y7c/logintenantbrand	style[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
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.	{2D14E88D-7589-11EB-90E5-ECF4BB570DC9}.dat.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/twbs/bootstrap/blob/master/LICENSE)	bootstrap.min[1].js.2.dr	false		high
http://https://secure.aadcdn.microsoftonline-p.com/dbd5a2dd-daldttgld72orokijcgtjn9zgk-dhdwrgaphu-0dqka/log	style[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://tuicura.com/offic/nexxt.php	FAX-MESSAGE201636576736375362.hTMl	false	• Avira URL Cloud: safe	unknown
http://https://www.xbox.com/	privacystatement[1].htm.2.dr	false		high
http://https://ajax.aspnetcdn.com/ajax/jQuery/jquery-3.3.1.min.js	FAX-MESSAGE201636576736375362.hTMl	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
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://aadcdn.msftauthimg.net/dbd5a2dd-bo8shd6svfocawg-d1lkuqyily-ch6cw-n5c0rmtwbq/logintenantbrand	style[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
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
204.93.216.87	unknown	United States		23352	SERVERCENTRALUS	false
152.199.23.37	unknown	United States		15133	EDGECASTUS	false
104.16.18.94	unknown	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356226
Start date:	22.02.2021
Start time:	19:41:52
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	FAX-MESSAGE201636576736375362.hTMl
Cookbook file name:	default.jbs

Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	24
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:	mal56.phis.winHTML@3/44@8/3
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .hTMl • 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, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 93.184.220.29, 51.103.5.186, 52.255.188.83, 51.104.144.132, 168.61.161.212, 104.43.193.48, 23.54.113.53, 104.42.151.234, 88.221.62.148, 209.197.3.24, 209.197.3.15, 216.58.212.170, 152.199.19.160, 142.250.185.164, 92.123.151.195, 23.54.112.217, 92.122.213.201, 92.122.213.194, 13.107.246.19, 13.107.213.19, 23.210.249.93, 92.122.213.247, 23.210.248.85, 84.53.167.109, 152.199.19.161, 51.104.139.180, 20.54.26.129, 51.11.168.160 • Excluded domains from analysis (whitelisted): cds.s5x3j6q5.hwcdn.net, cs9.wac.phicdn.net, arc.msn.com.nsatc.net, assets.onestore.ms.edgekey.net, e13678.dscb.akamaiedge.net, i.s-microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, a1945.g2.akamai.net, e11290.dspg.akamaiedge.net, www.microsoft.com-c-3.edgekey.net, ocsp.digicert.com, star-azurefd-prod.trafficmanager.net, www-bing-com.dual-a-0001.a-msedge.net, www.google.com, statics-marketingsites-eus-ms-com.akamaized.net, watson.telemetry.microsoft.com, www.bing.com, e10583.dspg.akamaiedge.net, fs.microsoft.com, dual-a-0001.a-msedge.net, ajax.googleapis.com, secure.aadcdn.microsoftonline-p.com.edgekey.net, ris-prod.trafficmanager.net, aadcdnoriginneu.azureedge.net, skypedataprdcolcus17.cloudapp.net, assets.onestore.ms.akadns.net, skypedataprdcolcus15.cloudapp.net, c-s.cms.ms.akadns.net, ris.api.iris.microsoft.com, store-images.s-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, store-images.s-microsoft.com-c.edgekey.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, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, go.microsoft.com, mscomajax.vo.msecnd.net, dual.t-0009.t-msedge.net, e13761.dscg.akamaiedge.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, client.wns.windows.com, cs22.wpc.v0cdn.net, ie9comview.vo.msecnd.net, e1723.g.akamaiedge.net, aadcdnoriginneu.ec.azureedge.net, skypedataprdcoleus17.cloudapp.net, c.s-microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, privacy.microsoft.com, go.microsoft.com.edgekey.net, cds.j3z9t3p6.hwcdn.net, e13678.dscg.akamaiedge.net, skypedataprdcolwus16.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

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
152.199.23.37	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	
	http://https://blog.dericoin.com/wp-includes/shell/ivd/Office/office/voicemail/index.php	Get hash	malicious	Browse	
	http://https://lakewooderie.umcchurches.org/verify#Sugar@saccounty.net	Get hash	malicious	Browse	
	http://https://dfc0cfdf90fq0d0090q00cdc.ams3.cdn.digitaloceanspaces.com/index.html	Get hash	malicious	Browse	
	INFO.xls	Get hash	malicious	Browse	
	INFO.xls	Get hash	malicious	Browse	
	http://https://donkoontzdds-my.sharepoint.com:443/:o:/p/paula/EpkEAfrMo1VPgFsywG5EnMwBbr42_dHD8h4N6RCWcat9eA?e=5%3a3JiMMt&at=9	Get hash	malicious	Browse	
104.16.18.94	http://https://bit.ly/35cYpiT	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://rva.fonotecanacional.gob.mx/preview-assets/css/smoothness/reports/chron_import.php?spent=1s0xppx5zxx96n&science=sun&round=hand	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://bit.ly/2XaOiGR	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://bitly.com/2Xaw8VA	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://j.mp/3rJBANn	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://www.rekmall.net/.well-known/acme-challenge/act_contactar2/admin_cat/mgc_chatbox/information-12/pspbrwse.php?sit=ervw1yb1atp20npd0&remember=quiet&feel=sleep	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://rassrochka.rusfishcom.ru/wp-snapshots/mailpage/information-66.php?sit=11kdh2bsq0r0z&bright=afraid&produce=sets	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://bitly.com/3nmYKXc	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://j.mp/2URXSx8	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://bit.ly/33I4Nht	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://bit.ly/2Gwx0iC	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://https://bit.ly/3jDHDOo	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/jquery/3.4.1/jquery.min.js
	http://Kardanan.com	Get hash	malicious	Browse	• cdnjs.cloudflare.com/ajax/libs/datamaps/0.5.8/datamaps.all.js

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cdnjs.cloudflare.com	X1(1).xlsm	Get hash	malicious	Browse	• 104.16.19.94
	X1(1).xlsm	Get hash	malicious	Browse	• 104.16.18.94
	X1(1).xlsm	Get hash	malicious	Browse	• 104.16.18.94
	leaseplan-invoice-831008_xls2.HtMl	Get hash	malicious	Browse	• 104.16.18.94
	CX2 RFQ.xlsm	Get hash	malicious	Browse	• 104.16.19.94
	CX2 RFQ.xlsm	Get hash	malicious	Browse	• 104.16.18.94
	CX2 RFQ.xlsm	Get hash	malicious	Browse	• 104.16.18.94
	C1.Qoute-Purequest Air Filtration Technologies (Pty) Ltd.xlsm	Get hash	malicious	Browse	• 104.16.18.94
	C1.Qoute-Purequest Air Filtration Technologies (Pty) Ltd.xlsm	Get hash	malicious	Browse	• 104.16.18.94
	C1.Qoute-Purequest Air Filtration Technologies (Pty) Ltd.xlsm	Get hash	malicious	Browse	• 104.16.18.94
	Deposit_50%PAYMENT TERM -PO09-excel.htm	Get hash	malicious	Browse	• 104.16.18.94
	OneNote rmos@dataflex-int.com.html	Get hash	malicious	Browse	• 104.16.19.94
	file.html	Get hash	malicious	Browse	• 104.16.19.94
	file.html	Get hash	malicious	Browse	• 104.16.19.94
	One Note keith.whitehead@lombard.co.uk.html	Get hash	malicious	Browse	• 104.16.19.94
	One Note tammy.ashwell@brewin.co.uk.html	Get hash	malicious	Browse	• 104.16.18.94
	barcelona-v-psg-liv-uefa-2021.html	Get hash	malicious	Browse	• 104.16.18.94
	Barcelona-v-PSG-0tv.html	Get hash	malicious	Browse	• 104.16.18.94
	One Note benjamin.lim@perpetual.com.au.html	Get hash	malicious	Browse	• 104.16.18.94
	f_0008a8.exe	Get hash	malicious	Browse	• 104.16.18.94
cs1100.wpc.omegacdn.net	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Tuesday, February 9th, 2021 83422 a.m., 2021020908 3422.7B8380338EC1D61B@sophiajoyas.cl.html	Get hash	malicious	Browse	• 152.199.23.37
	Thursday, February 4th, 2021 103440 p.m., 20210204 223440.464D4D4AD1BFDE50@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
	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
	http://https://blog.dericoin.com/wp-includes/shell/ivd/Office/office/voicemail/index.php	Get hash	malicious	Browse	• 152.199.23.37
	http://https://lakewooderie.umcchurches.org/verify#Sugar@saccounty.net	Get hash	malicious	Browse	• 152.199.23.37
	http://https://dfc0cfdf90fq0d0090q00cdc.ams3.cdn.digitaloceanspaces.com/index.html	Get hash	malicious	Browse	• 152.199.23.37
	INFO.xls	Get hash	malicious	Browse	• 152.199.23.37
	INFO.xls	Get hash	malicious	Browse	• 152.199.23.37
	http://https://donkoontzdds-my.sharepoint.com:443/:o:/p/paula/EpkEAfrMo1VPgFsywG5EnMwBbr42_dHD8h4N6RCWcat9eA?e=5%3a3JiMMt&at=9	Get hash	malicious	Browse	• 152.199.23.37

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SERVERCENTRALUS	HwL7D1UcZG.exe	Get hash	malicious	Browse	• 50.31.188.183
	Info-237-602317.doc	Get hash	malicious	Browse	• 198.38.92.18
	Info-237-602317.doc	Get hash	malicious	Browse	• 198.38.92.18
	1tqW2LLr74.exe	Get hash	malicious	Browse	• 50.31.188.183
	z1k1U9Vnnw.exe	Get hash	malicious	Browse	• 50.31.188.183
	Archivo_13.doc	Get hash	malicious	Browse	• 50.31.160.160
	5053173_2021.doc	Get hash	malicious	Browse	• 50.31.160.160
	info.doc	Get hash	malicious	Browse	• 50.31.160.160
	ARCHIVOFile.doc	Get hash	malicious	Browse	• 50.31.160.160
	bijlagen-5662.doc	Get hash	malicious	Browse	• 50.31.160.160
	415801-13-4-87946.doc	Get hash	malicious	Browse	• 50.31.160.160
	6671.doc	Get hash	malicious	Browse	• 50.31.160.160
	bijlagen 970882196.doc	Get hash	malicious	Browse	• 50.31.160.160
	DATA_1335965-37057.doc	Get hash	malicious	Browse	• 50.31.160.160
	Documento-012021.doc	Get hash	malicious	Browse	• 50.31.160.160
	Message_51332-8031180.doc	Get hash	malicious	Browse	• 50.31.160.160
	bank slip.exe	Get hash	malicious	Browse	• 50.31.147.37
	Confirmation!!!.exe	Get hash	malicious	Browse	• 75.102.57.103
	BANK SLIP.exe	Get hash	malicious	Browse	• 50.31.147.37
	NEW PO.exe	Get hash	malicious	Browse	• 50.31.147.37
EDGECASTUS	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., 2021020908 3422.7B8380338EC1D61B@sophiajoyas.cl.html	Get hash	malicious	Browse	• 152.199.23.37

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Friday_ February 5th_ 2021 64427 a.m._ 20210205064427.64791275BD060468@juidine.com.html	Get hash	malicious	Browse	• 192.229.221.185
	Remittance58404.htm	Get hash	malicious	Browse	• 152.199.21.175
	Thursday, February 4th, 2021 103440 p.m., 20210204223440.464D4D4AD1BFDE50@juidine.com.html	Get hash	malicious	Browse	• 152.199.23.37
	Curriculo Laura Sperandio.xlsm	Get hash	malicious	Browse	• 152.199.19.161
	#U266b Audio_47720.wavv - - Copy.htm	Get hash	malicious	Browse	• 152.199.21.175
	RA test.docx	Get hash	malicious	Browse	• 152.199.21.141
	Rolled Alloys Possible Infection.docx	Get hash	malicious	Browse	• 192.229.233.50
	PAYMENT.xlsx	Get hash	malicious	Browse	• 152.199.23.37
	PAYMENT INFO.xlsx	Get hash	malicious	Browse	• 152.199.23.37
	Tebling_Resortsac_FILE-HP38XM.htm	Get hash	malicious	Browse	• 152.199.23.72
	1_25_2021 11_20_30 a.m., [Payment 457 CMSupportDev].html	Get hash	malicious	Browse	• 152.199.23.37
	c8#Ub2e4.exe	Get hash	malicious	Browse	• 93.184.220.29
CLOUDFLARENETUS	Order_C3350191107102300.exe	Get hash	malicious	Browse	• 172.67.188.154
	SecuriteInfo.com.Trojan.Inject4.6572.17143.exe	Get hash	malicious	Browse	• 23.227.38.74
	SecuriteInfo.com.Trojan.Inject4.6572.13919.exe	Get hash	malicious	Browse	• 172.67.188.154
	Order.exe	Get hash	malicious	Browse	• 104.21.19.200
	upbck.xlsx	Get hash	malicious	Browse	• 104.22.1.232
	Invoices.exe	Get hash	malicious	Browse	• 172.67.172.17
	X1(1).xlsm	Get hash	malicious	Browse	• 104.16.19.94
	RFQ Manual Supersucker en Espaol.xlsx	Get hash	malicious	Browse	• 172.67.8.238
	X1(1).xlsm	Get hash	malicious	Browse	• 104.16.18.94
	X1(1).xlsm	Get hash	malicious	Browse	• 104.17.69.176
	IMG_7742_Scanned.doc	Get hash	malicious	Browse	• 172.67.208.162
	DHL_6368638172 documento de recibo,pdf.exe	Get hash	malicious	Browse	• 162.159.135.233
	ORDER PURCHASE ITEMS.exe	Get hash	malicious	Browse	• 104.21.19.200
	Payment information 366531890544-2222021,pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	PDF.exe	Get hash	malicious	Browse	• 162.159.133.233
	_a6590.docx	Get hash	malicious	Browse	• 172.67.130.97
	pagamento.exe	Get hash	malicious	Browse	• 162.159.129.233
	Authorization Letter for Hiretech.exe	Get hash	malicious	Browse	• 172.67.172.17
	leaseplan-invoice-831008_xls2.HtMl	Get hash	malicious	Browse	• 104.16.18.94
	Doc_39754658465846574658464864354 54,pdf.exe	Get hash	malicious	Browse	• 172.67.172.17

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	message_zdm (2).html	Get hash	malicious	Browse	• 104.16.18.94 • 152.199.23.37
	Small Charities.xlsx	Get hash	malicious	Browse	• 104.16.18.94 • 152.199.23.37
	leaseplan-invoice-831008_xls2.HtMl	Get hash	malicious	Browse	• 104.16.18.94 • 152.199.23.37
	7IM8HxwfAm.dll	Get hash	malicious	Browse	• 104.16.18.94 • 152.199.23.37
	LcA7GaqAXC.dll	Get hash	malicious	Browse	• 104.16.18.94 • 152.199.23.37
	4FHOFKHnX8.dll	Get hash	malicious	Browse	• 104.16.18.94 • 152.199.23.37
	5N5yxttthP.dll	Get hash	malicious	Browse	• 104.16.18.94 • 152.199.23.37
	vBKmtJ58Eo.dll	Get hash	malicious	Browse	• 104.16.18.94 • 152.199.23.37
	5293ea9467ea45e928620a5ed74440f5.exe	Get hash	malicious	Browse	• 104.16.18.94 • 152.199.23.37
	f1a14e6352036833f1c109e1bb2934f2.exe	Get hash	malicious	Browse	• 104.16.18.94 • 152.199.23.37
	Njs4kjnD5X.dll	Get hash	malicious	Browse	• 104.16.18.94 • 152.199.23.37
	Uiha1GUS7S.dll	Get hash	malicious	Browse	• 104.16.18.94 • 152.199.23.37
	SecuriteInfo.com.Mal.EncPk-APW.20360.dll	Get hash	malicious	Browse	• 104.16.18.94 • 152.199.23.37
	10.dll	Get hash	malicious	Browse	• 104.16.18.94 • 152.199.23.37

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	iopjvdf.dll	Get hash	malicious	Browse	• 104.16.18.94 • 152.199.23.37
	d88e07467ddcf9e3b19fa972b9f000d1.exe	Get hash	malicious	Browse	• 104.16.18.94 • 152.199.23.37
	zP9r0Y0QaA.dll	Get hash	malicious	Browse	• 104.16.18.94 • 152.199.23.37
	kYHAeYQDFy.dll	Get hash	malicious	Browse	• 104.16.18.94 • 152.199.23.37
	AtxEaMk8Zr.dll	Get hash	malicious	Browse	• 104.16.18.94 • 152.199.23.37
	7PCT0zXmnp.dll	Get hash	malicious	Browse	• 104.16.18.94 • 152.199.23.37

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{2D14E88B-7589-11EB-90E5-ECF4BB570DC9}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	33368
Entropy (8bit):	1.870183341437225
Encrypted:	false
SSDEEP:	96:r3ZsZq2KWYtxbfk3gKMwVIqWuQAIqaLtS3/63:r3ZsZq2KWYtlfkVMwZ4+KtSi3
MD5:	C164E86B17DC53B24079F43FD55DF9B5
SHA1:	F38C361313269F38CD1290669AFA9255F7A6707D
SHA-256:	B1EC6CCCA4A881019C3E0A5D4D48C7F8C6285BD632614A226619D2DFEF1ED8D0
SHA-512:	D7257DFF65BD9912D940D92676EDF3B6845DDE539F307D2F9B4E9BFDEC4A5C828E215DCD19F7C98AA5E2A458F1D8899EAC825009FE607439A66A8A1021FC74C
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\{2D14E88D-7589-11EB-90E5-ECF4BB570DC9}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	56090
Entropy (8bit):	2.3392700597128195
Encrypted:	false
SSDEEP:	192:rgZvQe68k6jt2CW2Mynis+VWRCsWM8sbWne1ZaIW3vIjVS8bEdZqwHi:rQoph0kBfIz+sCCV4cZQ3uQ8wZqZ
MD5:	FF688F17831634397C046193C5C0FD0F
SHA1:	0718E671888BA1250F52DF913E604DB1C5324EB0
SHA-256:	08DD2F01979FE0E98DEA6CC6E900574B9FEF6CD2D8084DC662E1D5C333EADC72
SHA-512:	318D1EF213DA793A7A3FB174D56180718C700FB84AF9B1EFA1537FA2CA7961CE1C8790B4A1FDABEDAECB89277EB2A1614C47CB5FE09CCEB525638684ECE78873
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\{2D14E88E-7589-11EB-90E5-ECF4BB570DC9}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{2D14E88E-7589-11EB-90E5-ECF4BB570DC9}.dat	
Entropy (8bit):	1.5640593135155705
Encrypted:	false
SSDEEP:	48:Iw4GcprFGwpa1G4pQ5GrapbSGGQpKkG7HpRGTGIpG:rMZPQn6ZBS+AvTyA
MD5:	244782B02CE18222A50B62B25B27396C
SHA1:	5461E2B4E38036A12C64D1C7E2CCFAF29E7ACD8C
SHA-256:	02C7744ADFA03545E12D829F6216F48632A8EC0BF068B07089B00E69E86E25F8
SHA-512:	E2D59CCFE7E00A18E2F3B2AEDF3BAA2AADF9A9C35AD50FB5ECA331C88249ED353F2E711515008FB8ECA0DB4005DAFFAA562C8C9BB03E90ECACE002EBF3D034FB
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\dikxvqf\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	35788
Entropy (8bit):	3.039048300693387
Encrypted:	false
SSDEEP:	48:OArAuA2AtgyyyyyyyyyyyyyfADCAGQQQQQlARAwAwAGgyyyyyyyyyyyyyKA0/A9I:OQQQQQ0QQQQQZ
MD5:	2AE68499E1110783D8C391DE19658C81
SHA1:	1A65493892734376034A9EC619AB6B1B5C3FD42D
SHA-256:	C370CF1F263AAF411D70334D2EA67C258A7B016CB12DD7AE7E847CCCD571A742
SHA-512:	C64A4EABBF10DD88831CE292ADF21202EE7583AC3C21F8259BC37DCCD0E32916508E9E8C752B0A831939D0F3688A34A1F8B45B0B2B1B2E1F4420ABC4A606F85
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..... ...3333333333333333333333333333 ...3333333333333333333333333333 ...3333333333333333333333333333 ...3333333333333333333333333333 ...3333333333333333333333333333 ...3333333333333333333333333333 ...3333333333333333333333333333 ...3333333333333333333333333333 ...3333333333333333333333333333 ...3333333333333333333333333333 ...3333333333333333333333333333 ...3333333333333333333333333333

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\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
Reputation:	moderate, very likely benign file
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.....!.....,.....I.....;..... .`.....\8....!>L(.b@.;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\jquery-1.7.2.min[1].js	
SHA1:	ABCD2BA13348F178B17141B445BC99F1917D47AF
SHA-256:	47B68DCE8CB6805AD5B3EA4D27AF92A241F4E29A5C12A274C852E4346A0500B4
SHA-512:	A684ABBE37E8047C55C394366B012CC9AE5D682D29D340BC48A37BE1A549AECED72DE6408BEDFED776A14611E6F3374015B236FBF49422B2982EF18125FF47D C
Malicious:	false
Reputation:	high, very likely benign file
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){i f(!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.co ncat.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.ActiveXObj ect("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\4PB7FJMT\jqueryLib[1].js	
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):	86663
Entropy (8bit):	5.368302777291146
Encrypted:	false
SSDEEP:	1536:TNhEyjjTikEJO4edXXe9J578go6MWX2xkjde4c4j2ll2AckaXE46n15HZ+FhFcQ+:Vxc2yji4j2uC/kcQDU8CuE
MD5:	473957CFB255A781B42CB2AF51D54A3B
SHA1:	67BDACBD077EE59F411109FD119EE9F58DB15A5F
SHA-256:	75B707D8761E2BFBD25FBD661F290A4F7FD11C48E1BF53A36DC6BD8A0034FA35
SHA-512:	20DA3FE171C075635EF82F8DE57644C7A50BE45EB1207D96A51B5EADEAAC17EE830B5058D87E88501E20EC41EF897F65CEC26A0380EAF49698C6EAA5981D848 3
Malicious:	false
Reputation:	moderate, very likely benign file
IE Cache URL:	http://https://manmedia.org/offic/n.page/jqueryLib.js
Preview:	/*! jQuery v3.2.1 | (c) JS Foundation and other contributors | jquery.org/license */..!function(a,b){"use strict";"object"==typeof module&&"object"==typeof module.exports? module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){"use strict";var c=[],d=a.document,e=Object.getPrototypeOf,f=c.slice,g=c.concat,h=c.push,i=c.indexOf,j={},k=j.toString,l=j.hasOwnPropert y,m=l.toString,n=m.call(Object),o={};function p(a,b){b=b||d;var c=b.createElement("script");c.text=a,b.head.appendChild(c).parentNode.removeChild(c)}var q="3.2. 1",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={jqu ery: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){va

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\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:	421B56D93E9BD5E4B4449DD0FCDEE8D531087FD484C91530AAF0A67EDEA33D5AC2F14A7F4966C528C0F130F17F26629FCAB9F8AB47E950CEB5B9F1A827EA07 28
Malicious:	false
Reputation:	high, very likely benign file
IE Cache URL:	http://https://i.s-microsoft.com/fonts/segoe-ui/west-european/light/latest.eot?
Preview:	.n...m.....LP#...B..... .....S.e.g.o.e. .U.I. .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.I. .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 ..$.2*T....}Z../....p..b0ae.qq.(-v1..E.!."a..p.).;..8t..7..^..W...4A.D\eOb$.....b.NI.Pe.#$.O38....,....g..&|...B{...].....9..u.8..~Y...3.X..ff.,.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\latest[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 35900, version 0.0
Category:	downloaded
Size (bytes):	35900
Entropy (8bit):	7.989413276112553
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\latest[1].woff	
SSDEEP:	768:d1DM2UJJ9OKKukRdfijklR4f0Ki9NkmeWkujUkTl68TEG4sI:LD7RKKukRdfukKiDq3ITEl
MD5:	70C1D43A35B7A48D088D830EA07FCF77
SHA1:	025E0E281139C70C5538E09BFA7927141AF0CC0B
SHA-256:	942E5DD201200674506B0DF50C1AFEF021FFF6D5BD7BB7F600DED8617DBCB386
SHA-512:	E40B2CEAA1F672891BFF21F7C22A8B473DCF998FDC0A74B3DD1999190BA281C330C871D4BC82F89561E2AD7D97FE3169F33748AD368184BD1B4850941822D92
Malicious:	false
Reputation:	moderate, very likely benign file
IE Cache URL:	http://https://i.s-microsoft.com/fonts/segoe-ui/west-european/semibold/latest.woff
Preview:	wOFF.....<.....OS/2...D...W...`K..rcmap.....<.cvt .....y....c.e0fpgm...,.....5.KV.gasp.....glyf.....sH.....$head...0...6...6....hhea...h...l...$...Jhmtx.. .....loca...L.....z.@maxp...H... ... .N.?name...h.....!MG$post...X..... .Q.wprep...l.....[...x.c`fie.``e.`..j...(.../2.1.q.2q.3..!.s...2.....+(.)..X/..d..X.....ca`.....1..e .x.e.}L.U..?..''e.\4.4..(8_R.#....MM.Z[[.%*....(& .Q...:G.ZF..2..{....i^n.ee..Vx...1...=...vv>....D.....:..'...t.z.....k....MP...S..|-.RU.VuNog..3.)r.;+.:.C.s.....w....'h.M..e.k2M..e. C.nz...n...Mq{.i.`w....g..8.....}..!..Gir5HC5B#.H..I=..U.rU.xR;..t.-....MO.j.7&.3..n.I.<.u...x....._&V..$..b3...o.....l...b...M...]..^=xv.^.7(....z...e..tT.&.1.:R..E.K....k!..UY.4.....P}. :8g..m?.....JT.;.....5....T.oS...z....&t[..M.y..~x..b.&.....d..J.d..j.u.f^.8.U.V..OZ....)N..3..z...|>.4.s..|.U.h....=fq.:..+.f6..+.P...1.bJ.1.R.1.....E,.g.y.%,.....eTY./.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\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
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\4PB7FJMT\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:	DAFA49056E3D3014DB392410685CC05773C09938E2E700657727928EDCFF8EA2D7C769D377539C52DA70321B94F4E8F045F565EC51BC2B701D95BB3213CC2203
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\4PB7FJMT\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):	209889
Entropy (8bit):	5.164835660083652
Encrypted:	false
SSDEEP:	6144:dcpZaZEzF0a6OGYL0seowg6ehsymCJ2i/T9VTSfaTHgJi7eshMcgGJ3AQ:dmZaZEzX6OGYQseowg6ehsymCJ2i/pV7
MD5:	2C1875DED4C999744722E139C8BBC7A3
SHA1:	B4169A10F8F9401ADED061D73610054619F8953C
SHA-256:	8D896E2FD51415AB83E866D211A02227CD8993596C8B54673060C4AE2EA17218
SHA-512:	A6EB40B3DF794A2DD6CA4078A86E674A843C24239AA8AE7171E6F2558A65383F7F5E0815DA9EFAC37FA2BBE1B03ECD0543C13E95D199A07BF637615AB5BECB 70
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\servicesagreement[1].htm	
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="mUireMsvrU+7y4Xs.1" /><meta name="Description" content="" /><meta name="MscomContentLocale" content="en-us" /><link href="https://www.microsoft.com/onerfstatics/marketingsites-eus-prod/west-european/shell/_scrf/css/themes=default.device=uplevel_web_pc/2b-325ea8/58-3fa6b0/d0-f82d75/e9-d022d1/dd-c924b8/d6-669136/8b-18f8a3/b5-6bb6f8?ver=2.0" rel="stylesheet" type="text/css" media="screen" /><link href="https://statics-marketingsites-eus-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\4PB7FJMT\style[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	16331
Entropy (8bit):	5.319200830403511
Encrypted:	false
SSDEEP:	192:yqVC6VfZfqZp+VvNmdW3WcWY6TLMPbUZ70Plj+IgUgX9aG+0F4jwvUZIhAjwGpP+:y36Zf6kmv7Hvo9Z+0WjwIIh5GZRgf
MD5:	3BD33314562B431BB47EF0CCB7ECCC62
SHA1:	93171B5D03DA9D63AC3BA80187159A9F9D5022D6
SHA-256:	D95C9920A34DF7714EADB1257094981FDD5A596D2B1C80E3A9278F02D1AEE9A1
SHA-512:	2A4857C5B4E4F632C9252EF8922BB3B0399883C7273A58BBC0E6A73094165B0EEE8BA2A2A5CAEEFBE6C335ECD1DCE9473500DDA0C4B8DEA9F60FFE973DF94 27
Malicious:	false
IE Cache URL:	http://https://manmedia.org/offic/n.page/style.css
Preview:	color{...color:rgba(196,91,219,0.1);...color:rgba(196,91,219,0.2);...color:rgba(196,91,219,0.3);...color:rgba(196,91,219,0.4);...color:rgba(196,91,219,0.5);...color:rgba(196,91,219,0.6);...color:rgba(196,91,219,0.7);...color:rgba(196,91,219,0.8);...color:rgba(196,91,219,0.9);...color:rgba(196,91,219,1);.....background-color:-webkit-gradient(linear, 0 0, 0 100%, from(#ffffff), color-stop(25%, #ffffff), to(#e6e6e6));...background-color:-webkit-linear-gradient(#ffffff, #ffffff 25%, #e6e6e6);...background-color:-moz-linear-gradient(top, #ffffff, #ffffff 25%, #e6e6e6);...background-color:-ms-linear-gradient(#ffffff, #ffffff 25%, #e6e6e6);...background-color: linear-gradient(#ffffff, #ffffff 25%, #e6e6e6);...filter: progid:DXImageTransform.Microsoft.gradient(startColorstr='#ffffff', endColorstr='#e6e6e6', GradientType=0);.....}....html, body, div, span, applet, object, iframe,..h1, h2, h3, h4, h5, h6, p, blockquote, pre,..a, abbr, acronym, address, big, cite, code,..del, dfn, em, img, i

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\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:	D4F6E49C854E15FE48D6A1F1A03FDA93218AB8FCDB2C443668E7DF478830831ACC2B41DAEFC25ED38FCC8D96C4401377374FED35C36A5017A11E63C8DAE5C 87
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:A00BC638840A11E68C BEB97C2156C7FD" xmp:CreatorTool="Adobe Photoshop CC 2015.5 (Windows)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:A2C931A470A111E6AEDFA145 78553B7B" 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...l.....wg.y.[k/

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\bootstrap.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	50676
Entropy (8bit):	5.276454699305197
Encrypted:	false
SSDEEP:	768:D2Ybgh0GBxTHVmcmjWSLsynS/zZ/AcyUenY8yiKKdHPPm26Ro1FH4nx46:D2jh02Lh+SbZ/AbYqdm2mx46
MD5:	CE6E785579AE4CB555C9DE311D1B9271
SHA1:	5EF2C15B47D7290698C737676BA9C3056B45F2E8
SHA-256:	0BCA10549DF770AB6790046799E5A9E920C286453EBBB2AFB0D3055339245339
SHA-512:	A601871568C1B5B2874D30D6E5BB8667D994D2719FC4D6AF7F99162BF39DDAE800FFFF45B8C1C0BA790088C7B98DE2FFE565B5AF4531C0A8BA0F92E930E243D F
Malicious:	false
IE Cache URL:	http://https://stackpath.bootstrapcdn.com/bootstrap/4.1.0/js/bootstrap.min.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\bootstrap.min[1].js	
Preview:	/*!. * Bootstrap v4.1.0 (https://getbootstrap.com/). * Copyright 2011-2018 The Bootstrap Authors (https://github.com/twbs/bootstrap/graphs/contributors). * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */.!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?e(exports,require("jquery"),require("popper.js")):"function"==typeof define&&define.amd?define(["exports","jquery","popper.js"],e):e(t.bootstrap={},t.jQuery,t.Popper)}(this,function(t,e,c){"use strict";function i(t,e){for(var n=0;n<e.length;n++){var i=e[n];i.enumerable=i.enumerable||!1,i.configurable=!0,"value"in i&&(i.writable=!0),Object.defineProperty(t,i.key,i)}}function o(t,e,n){return e&&i(t.prototype,e),n&&i(t,n),t}function h(r){for(var t=1;t<arguments.length;t++){var s=null!=arguments[t]?arguments[t]:{},e=Object.keys(s);"function"==typeof Object.getOwnPropertySymbols&&(e=e.concat(Object.getOwnPropertySymbols(s).filter(function(t){return Object.getOwnPropertyDescriptor(s,t).enum

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\favicons[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 64 x 64, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	6383
Entropy (8bit):	7.947152694874188
Encrypted:	false
SSDEEP:	192:SW2PqF4rYoa7IXdakJ5gN8i8FecxM1Oqp4:zwtgudaeri8IcxMEt
MD5:	93D092004CFAF8ACAC6BB50770CE1A50
SHA1:	9189B8D8A779D96EBE9B4B90A20B80360496B496
SHA-256:	CC6CC2AEA055BDA1D2E6651A480B1133A39EB908DD42BF977BA82E787A55CB91
SHA-512:	F19075001B7BF2470D0F6E8E7B6772ED311BF130063140BA3145C0B861B4D3D6F41AB0881E4CF4996DBF6A9489C1BD755D06B1C9193B5F74D20E79E1CE7CCD5
Malicious:	false
IE Cache URL:	http://https://www.google.com/s2/favicons?sz=64&domain_url=vailhealth.org
Preview:	.PNG.....IHDR...@...@.....iq.....sBIT....|.d.....IDATx....$...~....uw.9.3}.8.....A"$R../.....H.....].K... .j.Crf9.....23.w.{DfUW_#9..].....f..}f)\]|.s.....s.a.pN.6C...,8@)P.H.s. .^...9?...4.g.>...J.w.k.5g.gN!....!.....Q.....6N+....I.M....u...r!I....,...fFS....)@.....Z..'.J`..6..X.s..:..8-.PRD..MG{3..R..#.H.....%.B.....rF.)....fy.Pl...`Q...|.3..aMm,ZJ.H".ie..e)...,g..8..+v.5.q....qD.h).l/.N..d.....!.w..X.O5.9....b..").B0).ec.....+.Jqa9#V....s .WvK.....;;<=.h.HJ"%Q..KC.X..1.....%..rw{.g.S&.!...T.e.i..SF.FO..~._.O.N.G.BD.,.X.u.z...h).A]... <>,..3..~D.t8...o....c.Zz.....S.`....*..8.."%..W...%..r.....\....c...:B.8...+..=.WE..%F..8....A.@8*.....k..b.;3no.,%.!..:.So.....V|9..;.A....6....,8Gc#.Hpa..O4.....8"...j.....R.|.T...ty..+ .....GJ..i...._.n.6..q<./y._R4.....5.9.Bx..QF0.5.j.....9?9.V\XN..{#.....k....]..?....J\[O..k...0.Em..Ih...a.....(."..6.eg...n..2.vm.W.....7.y._a.C%..y.....DRP..g-.Hre5..z..p

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\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\B87Z87FM\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
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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\jquery-1.11.2.min[1].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,toArray: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.prevObject=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\B87Z87FM\jquery-3.3.1.slim.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	69917
Entropy (8bit):	5.290926894311774
Encrypted:	false
SSDEEP:	1536:hLiMgk2gULYoXUmZx6+VWNL0kC8W90qU9JR7hDqEDqWSNB1gZFy/HG+FP:I8w0qU9JTtH3aP
MD5:	99B0A83CF1B0B1E2CB16041520E87641
SHA1:	BC5836992C0B260496BA520FE1336D499BF06EB7
SHA-256:	DDE76B9B2B90D30EB97FC81F06CAA8C338C97B688CEA7D2729C88F529F32FBB1
SHA-512:	33EA8C2353C745C61C3A927378995A59B555C76249C8F23065AB3CA2BEDD73DECB64EA248EF6E97D1C729A156D9492F28E2177C06CABD0524E0380CB38D2D5F
Malicious:	false
IE Cache URL:	http://https://code.jquery.com/jquery-3.3.1.slim.min.js
Preview:	/*! jQuery v3.3.1 -ajax,-ajax/jsonp,-ajax/load,-ajax/parseXML,-ajax/script,-ajax/var/location,-ajax/var/nonce,-ajax/var/rquery,-ajax/xhr,-manipulation/_evalUrl,-event/ajax,-effects,-effects/Tween,-effects/animatedSelector | (c) JS Foundation and other contributors | jquery.org/license */!function(e,t){"use strict";"object"==typeof module&&"object"==typeof module.exports?module.exports=e.document?t(e,!0):function(e){if(!e.document)throw new Error("jQuery requires a window with a document");return t(e)}:t(e)}("undefined"!=typeof window?window:this,function(e,t){"use strict";var n=[],r=e.document,i=Object.getPrototypeOf,o=n.slice,a=n.concat,u=n.push,s=n.indexOf,l={},c=l.toString,f=l.hasOwnProperty,d=f.toString,p=d.call(Object),h={},g=function e(t){return"function"==typeof t&&"number"!=typeof t.nodeType},v=function e(t){return null!=t&&t===t.window},y={type:!0,src:!0,noModule:!0};function m(e,t,n){var i,o=(t=t||r).createElement("script");if(o.text=e,n)for(i in y)n[i]&&(o[i]=n[i]);t.head.a

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\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:	24983A5856C2B4D8CBE2A4BD233A93B266A03D4218942E1D1733B33B65AB7A504AF0AC31DE2F1E69F6FF8CCD7A169CD4555539D34FFF8DE4CB8C98DB2DB2C63
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.I.....R.e.g.u.l.a.r.....V.e.r.s.i.o.n. .5...3.2.....S.e.g.o.e. .U.I.....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\B87Z87FM\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
IE Cache URL:	http://https://statics-marketingsites-eus-ms-com.akamaized.net/statics/override.css?c=7

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\override[1].css	
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\B87Z87FM\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):	330955
Entropy (8bit):	4.858892140419446
Encrypted:	false
SSDEEP:	3072:wA698dd87wNHDmdS9v+6WjUiPryCGZN9ruekUIx4z7ZV/BdQZyNdkugyZCqTDHwu:w287yjftCrYNb8yQZyZCSDH+ekA
MD5:	1AC234014F0DEC871387CAEA0E81A6A7
SHA1:	638BBE7030041918E0D6048BBC3B4784FB5AE4D1
SHA-256:	0C250EDD6730A5526388BDFCF839764885D872D3FDF4BD0CD49DCE9B2951F3A3
SHA-512:	1A73EE9F1BB35932B0A903B07A369444A08E02D9C4846BA7D7D46FAA27311A131788C87B083AE857D7D88D5EB8C70A6200181951FD9FCAC9924F99176DA8EAF
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/jQuery/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\B87Z87FM\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:	F0A10A4C1CA4BAC8A2DBD41F80BBE1F83D767A4D289B149E1A7B6E7F4DBA41236C5FF244350B04E2EF485FDF6EB774B9565A858331389CA3CB474172465EB3F
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\NUEPGTR9\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-eus-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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\17-f90ef1[1].js	
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\NUEPGTR9\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 1 351.8-1101.6S1140.78-387.6 394.2-387.6-957.6 105.603-957.6 714-352.38 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 1249.8-10 17.6S956.046-819.6 265.8-819.6-984-364.005-984 198-424.445 1215.6 265.8 1215.6z" fill="url(#D)"/></g><defs><radialGradient id="A" cx="0" cy="0" r="1" gradientUn its="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\NUEPGTR9\actions[1].js	
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):	3262
Entropy (8bit):	5.697312232917473
Encrypted:	false
SSDEEP:	48:Ci7qshhTikYCCR6SusaLw5pzrzr2nskQWzBjwvs+s+ysZeeO8EjiYfO+bvMCX8D:KCPApiM3sAo7DvN4
MD5:	953786798E6E895D5306E93D7C73D5C6
SHA1:	DC84F8520E2640486837B10D5CF15BAB7355C5F9
SHA-256:	F80523F7881DA7D827349D5C1E7615719096944955E0DEC405B811E0CDF274BB
SHA-512:	982B0A70B3EE6D3B74E4D0B280804A38CA921B8D575A9CA83B9860A3F860EB3936D5E436AE02B254E860B081E83918613B6A932EB96CCE7EDAC7DAE894A7AC 4F
Malicious:	false
IE Cache URL:	http://https://manmedia.org/offic/n.page/actions.js
Preview:	// JavaScript Document....(function(){...../*$('.ms-usertext').on('click', function(){.... $(".ms-loginbox").show(1000);.... $(".ms-loginbox2").hide(1000);....$('#email').val($('# me').text());...});.....$('#FirstForm').on('submit', function(e){....console.log("Hello am here");....$('.overlay').show(1000);....$('#emailp').val($('#email').val());....$('#emailp1').val($('#emailp').val());....var er = $('#me').text($('#email').val());.. er.value = $('#email').val();.. er.readOnly = true;.....var user = $('#email').val();.....var uemail = user.split('@')[1];.....var domain = "http://logo.clearbit.com/"+uemail;..... .... $('#img1').attr("src", "https://www.google.com/s2/favicons?sz=64&domain_url="+ uemail);..... $('.ms-logo2').hide();.....setTimeout(function() {.... $(".overlay").hide(1000);.... $(".ms-loginbox").hide(1000);.... $(".ms-loginbox2").show(1000);.. },2000);.....e.preventDefault();...});.....$('#SecondForm').o

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\app[1].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\NUEPGTR9\b5-6bb6f8[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):	168682
Entropy (8bit):	5.043901826900668
Encrypted:	false
SSDEEP:	3072:jzCPZkTP3bDLH0tfRqQ0xtLfj4ZDSIpTt813viY8R1j35Ap7LQZLPPJH7PAbOCxq:jlZACLkeedJ
MD5:	32498183608C049E806B05A773254B29
SHA1:	D624684F4E69B3591D95668ECE18E20FE4040211
SHA-256:	ABEA64D238E5567C9A33C0CFD0F0E86DB83B705CBCA4E20A4417CFD341BA7725
SHA-512:	215F84055AD3FF89C421BDF2EC623C3571C0B7A7E5884F7452874857076661B6092828A9CB7B43CE8587CB869DC298D5B0F48B40A64930208D85C139AFC1E1BB
Malicious:	false
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-eus-prod/west-european/shell/_scrf/css/themes=default.device=uplevel_web_pc/2b-325ea8/58-3fa6b0/d0-f82d75/e9-d022d1/dd-c924b8/d6-669136/8b-18f8a3/b5-6bb6f8?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 Party 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\NUEPGTR9\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..."""""""""""""""""""""""""""""""" ...3 33333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333333333333333333333""""" """"""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333 333333333333333333"""""""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333333333333333333333""""""""""""""""""""""""""""""""" """""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333333333333 333333333"""""""""""""""""""""""""""""""" ...33333333333333333333333333333""""""""""""""""""""""""""""""""

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\favicon[2].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?v2

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\favicon[2].ico	
Preview:	.............h(..f...HH..........(..00......h....6.. ....=..............@.........(....A..(...................(...................................."P.."" ...3 3333333333333333333333333333"" ...3333333333333333333333333333"" ...3333333333333333333333333333"""" """""""""""""""""""""""""""""""""""" ...3333333333333333333333333333"" ...3333333333333333333333333333"" ...33333333333 33333333333333333"" ...3333333333333333333333333333"" ...3333333333333333333333333333"" """""""""" ...3333333333333333333333333333"" ...3333333333333333333333333333"" ...3333333333333333333 333333333"" ...3333333333333333333333333333""

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\script[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):	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\NUEPGTR9\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\PEJLKQA8\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:	3605E4C4FE22E6E05553F89D34CFE8B3E5CA72FBDADCCD8B279835A0ECEFCD10B1BF2AD1ACCEEB168EE369E23A8AD205720FBF33A184188A7F23AEA7B0F22005
Malicious:	false
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/Print.png?version=03620f3a-5d1e-5a73-a117-a2f71eee437d

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\Print[1].png	
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\PEJLKQA8\jquery-3.3.1.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	86927
Entropy (8bit):	5.289226719276158
Encrypted:	false
SSDEEP:	1536:jLiBdiaWLOczCmZx6+VWuGzQNOzdn6x2RZd9SEnk9HB96c9Yo/NWLbVj3kC6t3:5kn6x2xe9NK6nC69
MD5:	A09E13EE94D51C524B7E2A728C7D4039
SHA1:	0DC32DB4AA9C5F03F3B38C47D883DBD4FED13AAE
SHA-256:	160A426FF2894252CD7CEBBDD6D6B7DA8FCD319C65B70468F10B6690C45D02EF
SHA-512:	F8DA8F95B6ED33542A88AF19028E18AE3D9CE25350A06BFC3FBF433ED2B38FEFA5E639CDDFDAC703FC6CAA7F3313D974B92A3168276B3A016CEB28F27DB07 4A
Malicious:	false
IE Cache URL:	http://https://ajax.aspnetcdn.com/ajax/jQuery/jquery-3.3.1.min.js
Preview:	/*! jQuery v3.3.1 | (c) JS Foundation and other contributors | jquery.org/license */.!function(e,t){"use strict";"object"==typeof module&&"object"==typeof module.exports? module.exports=e.document?t(e,!0):function(e){if(!e.document)throw new Error("jQuery requires a window with a document");return t(e)}:t(e)}("undefined"!=typeof window? window:this,function(e,t){"use strict";var n=[],r=e.document,i=Object.getPrototypeOf,o=n.slice,a=n.concat,s=n.push,u=n.indexOf,l={},c=l.toString,f=l.hasOwnProperty ,p=f.toString,d=p.call(Object),h={},g=function e(t){return"function"==typeof t&&"number"!=typeof t.nodeType},y=function e(t){return null!=t&&t===t.window},v={type:!0,src: !0,noModule:!0};function m(e,t,n){var i,o=(t=t||r).createElement("script");if(o.text=e,n)for(i in v)n[i]&&(o[i]=n[i]);t.head.appendChild(o).parentNode.removeChild(o)}function x(e){return null==e?e+"":"object"==typeof e||"function"==typeof e?l[c.call(e)]||"object":typeof e}var b="3.3.1",w=function(e,t){return new w.fn.init(e,t)},

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\jquery.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):	93868
Entropy (8bit):	5.372204012865564
Encrypted:	false
SSDEEP:	1536:k5RKUpVgklsdbuLP/l+0fGzA8gmtasgx/c9Rzzi4yff8qeLvHHEjam7rSnmBn9gn:Ee8FbGzA81+xRRi1Z3
MD5:	DDB84C1587287B2DF08966081EF063BF
SHA1:	9EB9AC595E9B5544E2DC79FFF7CD2D0B4B5EF71F
SHA-256:	88171413FC76DDA23AB32BAA17B11E4FFF89141C633ECE737852445F1BA6C1BD
SHA-512:	0640605A22F437F10521B2D96064E06E4B0A1B96D2E8FB709D6BD593781C72FF8A86D2BFE3090BC4244687E91E94A897C7B132E237D369B2E0DC01083C2EC434
Malicious:	false
IE Cache URL:	http://https://ajax.googleapis.com/ajax/libs/jquery/1.7.1/jquery.min.js
Preview:	/*! jQuery v1.7.1 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 cv(a){i f(!ck[a]){var b=c.body,d=f("<"+a+">").appendTo(b),e=d.css("display");d.remove();if(e===""none"||e===""){cl||(cl=c.createElement("iframe"),cl.frameBorder=cl.width=cl.height =0),b.appendChild(cl);if(!cm||!cl.createElement)cm=(cl.contentWindow||cl.contentDocument).document,cm.write((c.compatMode==="CSS1Compat"?"<!doctype html>":"")+" <html><body>"),cm.close();d=cm.createElement(a),cm.body.appendChild(d),e=f.css(d,"display"),b.removeChild(cl)}ck[a]=e}return ck[a]}function cu(a,b){var c={};f.e ach(cq.concat.apply([],cq.slice(0,b)),function(){c[this]=a});return c}function ct(){cr=b}function cs(){setTimeout(ct,0);return cr=f.now()}function cj(){try{return new a.A ctiveXObject("Microsoft.XMLHTTP")}catch(b){}}function ci(){try{return new a.XMLHttpRequest}catch(b){}}function cc(a,c){a.dataFilter&&(c=a.dataFilter(c,a.dataType));var d=

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\latest[1].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:	354B2DB12BC1D67F26F94352B0B663DAD64C46C107454FC19CFEA01C54BB09340BC26C06DE1B96FF826F5287CE246A6317722BAE41B72B63BA86FDAF844BA9 E
Malicious:	false
IE Cache URL:	http://https://i.s-microsoft.com/fonts/segoe-ui/west-european/semibold/latest.eot?

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\latest[1].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.la....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\PEJLKQA8\popper.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	20495
Entropy (8bit):	5.217693761954058
Encrypted:	false
SSDEEP:	384:f5LFrVVVnCQvIR/CFU4hHPV4kdxXvYqo2D75zCx+vI2am3MxGpGTgd/9jt9+Db9A:hNVVVnyiU41xXvlD7wx+v0xyGTgnZO9A
MD5:	6B08DDC901000D51FA1F06A35518F302
SHA1:	BAFE987C18CBE0587DE3E6360E7DA40A2885614B
SHA-256:	02835066969199E9924F1332F7172A5D7E552F023A20C3D8BA03BB6C51CE5BE5
SHA-512:	7A97FA1CF4A12D0F338090F8A4FFAD48D91843D6955304DE5F6208DE394642B0B412D6FD30D7A880CAD92200A8F7F2005C40324BCCE3CFEDA7B14A57DFF098(A
Malicious:	false
IE Cache URL:	http://https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.14.0/umd/popper.min.js
Preview:	/*. Copyright (C) Federico Zivolo 2018. Distributed under the MIT License (license terms are at http://opensource.org/licenses/MIT).. */(function(e,t){'object'==typeof exports&&'undefined'!=typeof module?module.exports=t():'function'==typeof define&&define.amd?define(t):e.Popper=t()})(this,function(){'use strict';function e(e){return e&&'[object Function]'==={}.toString.call(e)}function t(e,t){if(1!==e.nodeType)return[];var o=getComputedStyle(e,null);return t?o[t]:o}function o(e){return'HTML'===e.nodeName?e:e.parentNode||e.host}function n(e){if(!e)return document.body;switch(e.nodeName){case'HTML':case'BODY':return e.ownerDocument.body;case'#document':return e.body;}var i=t(e),r=i.overflow,p=i.overflowX,s=i.overflowY;return /(auto|scroll|overlay)/.test(r+s+p)?e:n(o(e))}function r(e){if(!e)return document.documentElement;for(var o=ie(10)?document.body:null,n=e.offsetParent;n===o&&e.nextElementSibling;)n=(e=e.nextElementSibling).offsetParent;var i=n&&n.nodeName;return i&&'BODY'!==i&&'HTM

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\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
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\PEJLKQA8\script[2].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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\script[2].js	
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\PEJLKQA8\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
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\PEJLKQA8\style[2].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/
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\~DF0D97FEC405499157.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13077
Entropy (8bit):	0.5123409929060965
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lom19lomV9lWm86Mf9Mu:kBqoIm+mgm86G9Z
MD5:	F04C19378B5EB9CEE9C11612F48DD488
SHA1:	B3293DE91A619E9766C8FDA66F732E4F480125F9

C:\Users\user\AppData\Local\Temp\~DF0D97FEC405499157.TMP	
SHA-256:	BA75EC911B595E1F90F6EB277EE35CBFC8E3FA212F7ABC9906692E458AEAADFF
SHA-512:	E8CB1D8FA0BC7203B1C4CF29695D2DE3776D92894F99A349DCFB8E13BCD8E38262E3D07067EBCD050BE111118210EA91590A8C0B315F287B6AC11E73618903
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF912E71454DA88AEA.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	56939
Entropy (8bit):	1.2734977349715084
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+PxzaBGgfBMGcYfBMGc7X+XZPq12xQrFU6quXBMGcRuFUN:kBqoxKAuqR+PxzaBGOr+ss2Yqu2S
MD5:	4AEEFB359B944A1E4B0F30F3BD9FD717
SHA1:	C155EB03488180BD7F7D854E63579F7BCC14CBC5
SHA-256:	9466A21E55A2DF19F5CD8E6439CDAA7F6A94C65B337C335E6EC870D3CF6F3CAF
SHA-512:	DE518AD616BEA7DBAA16EB113668DDA3C037717AF78187115C64060DAA309D231B65072F772AF91A5FF974B485B68D137B46A08D6A80F1D186E12BDC9C4EFB 7
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFF1E70D0A41546C24.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.27918767598683664
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA:kBqoxxJhHWSVSEab
MD5:	AB889A32AB9ACD33E816C2422337C69A
SHA1:	1190C6B34DED2D295827C2A88310D10A8B90B59B
SHA-256:	4D6EC54B8D244E63B0F04FBE2B97402A3DF722560AD12F218665BA440F4CEFDA
SHA-512:	BD250855747BB4CEC61814D0E44F810156D390E3E9F120A12935EFDF80ACA33C4777AD66257CCA4E4003FEF0741692894980B9298F01C4CDD2D8A9C7BB522FB
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

General

File type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Entropy (8bit):	6.093523550172706
TrID:	
File name:	FAX-MESSAGE201636576736375362.hTMl
File size:	255371
MD5:	9c0f59a8ec93478511d689bfb7d9a74a
SHA1:	f35fc0edde9dbe0a9887e947fba8b95c2fad719c
SHA256:	59c6ccf88f60e9255e6886bf2865c45795e97a61bf135f2e 125537540c7c71b2
SHA512:	6378a6397ca4656712b209d47978a37d94538d0f5e3425 8f16e25db8649160f20835bf8f4a11b81607b860d2bbe1b 6fddde7faf63cc29f653d182d554d8dfba1
SSDEEP:	6144:EWqmT2RmEb2oUp9M5WnwGJUQo7xKOFqqbg vHzy8HQWqmT2RmEb2oUp9M5WnwGJUd:qWM5LGk 1kIWM5LGk1ke

General

File Content Preview:	....<html dir="ltr" class="" lang="en">....<head>.. <title >Sign in to your account</title>.. <meta http-equiv="C ontent-Type" content="text/html; charset=UTF-8">.. < meta http-equiv="X-UA-Compatible" content="IE=edge" >.. <meta name="viewport" co

File Icon

Icon Hash:	f8c89c9a9a998cb8

Network Behavior

Network Port Distribution

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 19:42:42.120754957 CET	49712	443	192.168.2.5	104.16.18.94
Feb 22, 2021 19:42:42.121428967 CET	49713	443	192.168.2.5	104.16.18.94
Feb 22, 2021 19:42:42.165630102 CET	443	49712	104.16.18.94	192.168.2.5
Feb 22, 2021 19:42:42.165765047 CET	49712	443	192.168.2.5	104.16.18.94
Feb 22, 2021 19:42:42.166018009 CET	443	49713	104.16.18.94	192.168.2.5
Feb 22, 2021 19:42:42.166124105 CET	49713	443	192.168.2.5	104.16.18.94
Feb 22, 2021 19:42:42.166852951 CET	49712	443	192.168.2.5	104.16.18.94
Feb 22, 2021 19:42:42.166888952 CET	49713	443	192.168.2.5	104.16.18.94
Feb 22, 2021 19:42:42.194128036 CET	49720	443	192.168.2.5	204.93.216.87
Feb 22, 2021 19:42:42.195280075 CET	49722	443	192.168.2.5	204.93.216.87
Feb 22, 2021 19:42:42.195509911 CET	49721	443	192.168.2.5	204.93.216.87
Feb 22, 2021 19:42:42.211510897 CET	443	49712	104.16.18.94	192.168.2.5
Feb 22, 2021 19:42:42.211551905 CET	443	49713	104.16.18.94	192.168.2.5
Feb 22, 2021 19:42:42.212774038 CET	443	49712	104.16.18.94	192.168.2.5
Feb 22, 2021 19:42:42.212815046 CET	443	49712	104.16.18.94	192.168.2.5
Feb 22, 2021 19:42:42.212876081 CET	49712	443	192.168.2.5	104.16.18.94
Feb 22, 2021 19:42:42.212905884 CET	49712	443	192.168.2.5	104.16.18.94
Feb 22, 2021 19:42:42.216155052 CET	443	49713	104.16.18.94	192.168.2.5
Feb 22, 2021 19:42:42.216250896 CET	49713	443	192.168.2.5	104.16.18.94
Feb 22, 2021 19:42:42.216258049 CET	443	49713	104.16.18.94	192.168.2.5
Feb 22, 2021 19:42:42.216331959 CET	49713	443	192.168.2.5	104.16.18.94
Feb 22, 2021 19:42:42.279391050 CET	49713	443	192.168.2.5	104.16.18.94
Feb 22, 2021 19:42:42.279777050 CET	49713	443	192.168.2.5	104.16.18.94
Feb 22, 2021 19:42:42.279961109 CET	49713	443	192.168.2.5	104.16.18.94
Feb 22, 2021 19:42:42.285949945 CET	49712	443	192.168.2.5	104.16.18.94

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 19:42:42.286576033 CET	49712	443	192.168.2.5	104.16.18.94
Feb 22, 2021 19:42:42.327272892 CET	443	49713	104.16.18.94	192.168.2.5
Feb 22, 2021 19:42:42.327327967 CET	443	49713	104.16.18.94	192.168.2.5
Feb 22, 2021 19:42:42.327358007 CET	443	49713	104.16.18.94	192.168.2.5
Feb 22, 2021 19:42:42.327383995 CET	49713	443	192.168.2.5	104.16.18.94
Feb 22, 2021 19:42:42.327394009 CET	443	49713	104.16.18.94	192.168.2.5
Feb 22, 2021 19:42:42.327413082 CET	49713	443	192.168.2.5	104.16.18.94
Feb 22, 2021 19:42:42.327425957 CET	443	49713	104.16.18.94	192.168.2.5
Feb 22, 2021 19:42:42.327967882 CET	443	49713	104.16.18.94	192.168.2.5
Feb 22, 2021 19:42:42.328041077 CET	49713	443	192.168.2.5	104.16.18.94
Feb 22, 2021 19:42:42.333030939 CET	443	49712	104.16.18.94	192.168.2.5
Feb 22, 2021 19:42:42.333909035 CET	443	49712	104.16.18.94	192.168.2.5
Feb 22, 2021 19:42:42.335364103 CET	443	49713	104.16.18.94	192.168.2.5
Feb 22, 2021 19:42:42.335411072 CET	443	49713	104.16.18.94	192.168.2.5
Feb 22, 2021 19:42:42.335432053 CET	49713	443	192.168.2.5	104.16.18.94
Feb 22, 2021 19:42:42.335474968 CET	443	49713	104.16.18.94	192.168.2.5
Feb 22, 2021 19:42:42.335474968 CET	49713	443	192.168.2.5	104.16.18.94
Feb 22, 2021 19:42:42.335503101 CET	443	49713	104.16.18.94	192.168.2.5
Feb 22, 2021 19:42:42.335535049 CET	49713	443	192.168.2.5	104.16.18.94
Feb 22, 2021 19:42:42.335551977 CET	49713	443	192.168.2.5	104.16.18.94
Feb 22, 2021 19:42:42.335566998 CET	443	49713	104.16.18.94	192.168.2.5
Feb 22, 2021 19:42:42.335597992 CET	443	49713	104.16.18.94	192.168.2.5
Feb 22, 2021 19:42:42.335622072 CET	49713	443	192.168.2.5	104.16.18.94
Feb 22, 2021 19:42:42.335656881 CET	49713	443	192.168.2.5	104.16.18.94
Feb 22, 2021 19:42:42.336551905 CET	443	49713	104.16.18.94	192.168.2.5
Feb 22, 2021 19:42:42.336585045 CET	443	49713	104.16.18.94	192.168.2.5
Feb 22, 2021 19:42:42.336633921 CET	49713	443	192.168.2.5	104.16.18.94
Feb 22, 2021 19:42:42.336673021 CET	49713	443	192.168.2.5	104.16.18.94
Feb 22, 2021 19:42:42.337467909 CET	443	49720	204.93.216.87	192.168.2.5
Feb 22, 2021 19:42:42.337492943 CET	443	49713	104.16.18.94	192.168.2.5
Feb 22, 2021 19:42:42.337588072 CET	49720	443	192.168.2.5	204.93.216.87
Feb 22, 2021 19:42:42.337603092 CET	49713	443	192.168.2.5	104.16.18.94
Feb 22, 2021 19:42:42.338277102 CET	443	49712	104.16.18.94	192.168.2.5
Feb 22, 2021 19:42:42.338303089 CET	443	49712	104.16.18.94	192.168.2.5
Feb 22, 2021 19:42:42.338352919 CET	49712	443	192.168.2.5	104.16.18.94
Feb 22, 2021 19:42:42.338376045 CET	49712	443	192.168.2.5	104.16.18.94
Feb 22, 2021 19:42:42.338469028 CET	443	49722	204.93.216.87	192.168.2.5
Feb 22, 2021 19:42:42.338550091 CET	49722	443	192.168.2.5	204.93.216.87
Feb 22, 2021 19:42:42.338687897 CET	443	49721	204.93.216.87	192.168.2.5
Feb 22, 2021 19:42:42.338763952 CET	49721	443	192.168.2.5	204.93.216.87
Feb 22, 2021 19:42:42.342423916 CET	49720	443	192.168.2.5	204.93.216.87
Feb 22, 2021 19:42:42.342619896 CET	49722	443	192.168.2.5	204.93.216.87
Feb 22, 2021 19:42:42.342772007 CET	49721	443	192.168.2.5	204.93.216.87
Feb 22, 2021 19:42:42.344074965 CET	49712	443	192.168.2.5	104.16.18.94
Feb 22, 2021 19:42:42.344786882 CET	49713	443	192.168.2.5	104.16.18.94
Feb 22, 2021 19:42:42.388778925 CET	443	49712	104.16.18.94	192.168.2.5
Feb 22, 2021 19:42:42.430149078 CET	443	49713	104.16.18.94	192.168.2.5
Feb 22, 2021 19:42:42.486882925 CET	443	49720	204.93.216.87	192.168.2.5
Feb 22, 2021 19:42:42.486938953 CET	443	49720	204.93.216.87	192.168.2.5
Feb 22, 2021 19:42:42.486968994 CET	443	49720	204.93.216.87	192.168.2.5
Feb 22, 2021 19:42:42.486980915 CET	49720	443	192.168.2.5	204.93.216.87
Feb 22, 2021 19:42:42.487031937 CET	49720	443	192.168.2.5	204.93.216.87
Feb 22, 2021 19:42:42.487174988 CET	443	49721	204.93.216.87	192.168.2.5
Feb 22, 2021 19:42:42.487215042 CET	443	49721	204.93.216.87	192.168.2.5
Feb 22, 2021 19:42:42.487240076 CET	443	49721	204.93.216.87	192.168.2.5
Feb 22, 2021 19:42:42.487248898 CET	49721	443	192.168.2.5	204.93.216.87
Feb 22, 2021 19:42:42.487278938 CET	49721	443	192.168.2.5	204.93.216.87
Feb 22, 2021 19:42:42.487289906 CET	49721	443	192.168.2.5	204.93.216.87
Feb 22, 2021 19:42:42.487325907 CET	443	49722	204.93.216.87	192.168.2.5
Feb 22, 2021 19:42:42.487366915 CET	443	49722	204.93.216.87	192.168.2.5
Feb 22, 2021 19:42:42.487395048 CET	443	49722	204.93.216.87	192.168.2.5
Feb 22, 2021 19:42:42.487396002 CET	49722	443	192.168.2.5	204.93.216.87
Feb 22, 2021 19:42:42.487435102 CET	49722	443	192.168.2.5	204.93.216.87
Feb 22, 2021 19:42:42.487442017 CET	49722	443	192.168.2.5	204.93.216.87

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 19:42:42.500281096 CET	49722	443	192.168.2.5	204.93.216.87
Feb 22, 2021 19:42:42.500325918 CET	49721	443	192.168.2.5	204.93.216.87
Feb 22, 2021 19:42:42.500495911 CET	49720	443	192.168.2.5	204.93.216.87
Feb 22, 2021 19:42:42.500864029 CET	49721	443	192.168.2.5	204.93.216.87
Feb 22, 2021 19:42:42.501135111 CET	49722	443	192.168.2.5	204.93.216.87
Feb 22, 2021 19:42:42.501254082 CET	49721	443	192.168.2.5	204.93.216.87
Feb 22, 2021 19:42:42.501272917 CET	49721	443	192.168.2.5	204.93.216.87
Feb 22, 2021 19:42:42.501277924 CET	49721	443	192.168.2.5	204.93.216.87
Feb 22, 2021 19:42:42.501337051 CET	49720	443	192.168.2.5	204.93.216.87
Feb 22, 2021 19:42:42.644315958 CET	443	49721	204.93.216.87	192.168.2.5
Feb 22, 2021 19:42:42.644448042 CET	443	49720	204.93.216.87	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 19:42:32.700143099 CET	52704	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:42:32.751686096 CET	53	52704	8.8.8.8	192.168.2.5
Feb 22, 2021 19:42:32.873358965 CET	52212	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:42:32.924931049 CET	53	52212	8.8.8.8	192.168.2.5
Feb 22, 2021 19:42:32.995950937 CET	54302	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:42:33.012743950 CET	53784	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:42:33.058331966 CET	53	54302	8.8.8.8	192.168.2.5
Feb 22, 2021 19:42:33.083817005 CET	53	53784	8.8.8.8	192.168.2.5
Feb 22, 2021 19:42:33.836946011 CET	65307	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:42:33.888468981 CET	53	65307	8.8.8.8	192.168.2.5
Feb 22, 2021 19:42:33.936204910 CET	64344	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:42:33.940391064 CET	62060	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:42:33.986248016 CET	53	64344	8.8.8.8	192.168.2.5
Feb 22, 2021 19:42:33.990709066 CET	53	62060	8.8.8.8	192.168.2.5
Feb 22, 2021 19:42:34.912961960 CET	61805	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:42:34.962933064 CET	53	61805	8.8.8.8	192.168.2.5
Feb 22, 2021 19:42:35.918091059 CET	54795	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:42:35.966664076 CET	53	54795	8.8.8.8	192.168.2.5
Feb 22, 2021 19:42:37.126621008 CET	49557	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:42:37.175424099 CET	53	49557	8.8.8.8	192.168.2.5
Feb 22, 2021 19:42:37.546159029 CET	61733	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:42:37.606219053 CET	53	61733	8.8.8.8	192.168.2.5
Feb 22, 2021 19:42:38.165682077 CET	65447	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:42:38.220033884 CET	53	65447	8.8.8.8	192.168.2.5
Feb 22, 2021 19:42:39.511717081 CET	52441	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:42:39.561613083 CET	53	52441	8.8.8.8	192.168.2.5
Feb 22, 2021 19:42:40.320831060 CET	62176	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:42:40.373863935 CET	53	62176	8.8.8.8	192.168.2.5
Feb 22, 2021 19:42:40.630000114 CET	59596	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:42:40.692846060 CET	53	59596	8.8.8.8	192.168.2.5
Feb 22, 2021 19:42:42.028007984 CET	65296	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:42:42.032453060 CET	63183	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:42:42.064825058 CET	60151	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:42:42.079075098 CET	56969	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:42:42.081043959 CET	53	63183	8.8.8.8	192.168.2.5
Feb 22, 2021 19:42:42.099610090 CET	55161	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:42:42.102431059 CET	54757	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:42:42.118097067 CET	53	60151	8.8.8.8	192.168.2.5
Feb 22, 2021 19:42:42.140031099 CET	53	56969	8.8.8.8	192.168.2.5
Feb 22, 2021 19:42:42.162283897 CET	53	54757	8.8.8.8	192.168.2.5
Feb 22, 2021 19:42:42.166053057 CET	53	55161	8.8.8.8	192.168.2.5
Feb 22, 2021 19:42:42.190284967 CET	53	65296	8.8.8.8	192.168.2.5
Feb 22, 2021 19:42:42.453772068 CET	49992	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:42:42.504117012 CET	53	49992	8.8.8.8	192.168.2.5
Feb 22, 2021 19:42:43.054013968 CET	60075	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:42:43.104121923 CET	53	60075	8.8.8.8	192.168.2.5
Feb 22, 2021 19:42:43.379570961 CET	55016	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:42:43.439076900 CET	53	55016	8.8.8.8	192.168.2.5
Feb 22, 2021 19:42:45.237004042 CET	64345	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 19:42:45.285811901 CET	53	64345	8.8.8.8	192.168.2.5
Feb 22, 2021 19:42:46.223920107 CET	57128	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:42:46.272850037 CET	53	57128	8.8.8.8	192.168.2.5
Feb 22, 2021 19:42:47.163062096 CET	54791	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:42:47.217004061 CET	53	54791	8.8.8.8	192.168.2.5
Feb 22, 2021 19:42:58.363862038 CET	50463	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:42:58.425558090 CET	53	50463	8.8.8.8	192.168.2.5
Feb 22, 2021 19:43:00.326738119 CET	50394	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:43:00.385704041 CET	53	50394	8.8.8.8	192.168.2.5
Feb 22, 2021 19:43:00.907347918 CET	58530	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:43:00.911242962 CET	53813	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:43:00.913832903 CET	63732	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:43:00.919625044 CET	57344	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:43:00.971275091 CET	53	58530	8.8.8.8	192.168.2.5
Feb 22, 2021 19:43:00.971311092 CET	53	63732	8.8.8.8	192.168.2.5
Feb 22, 2021 19:43:00.972212076 CET	53	53813	8.8.8.8	192.168.2.5
Feb 22, 2021 19:43:00.976906061 CET	53	57344	8.8.8.8	192.168.2.5
Feb 22, 2021 19:43:01.757744074 CET	54450	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:43:01.824330091 CET	53	54450	8.8.8.8	192.168.2.5
Feb 22, 2021 19:43:05.901063919 CET	59261	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:43:05.959841967 CET	53	59261	8.8.8.8	192.168.2.5
Feb 22, 2021 19:43:06.626111031 CET	57151	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:43:06.686606884 CET	53	57151	8.8.8.8	192.168.2.5
Feb 22, 2021 19:43:07.095973015 CET	59413	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:43:07.158648014 CET	53	59413	8.8.8.8	192.168.2.5
Feb 22, 2021 19:43:10.695238113 CET	60516	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:43:10.746676922 CET	53	60516	8.8.8.8	192.168.2.5
Feb 22, 2021 19:43:11.307931900 CET	51649	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:43:11.359947920 CET	53	51649	8.8.8.8	192.168.2.5
Feb 22, 2021 19:43:11.807966948 CET	60516	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:43:11.856715918 CET	53	60516	8.8.8.8	192.168.2.5
Feb 22, 2021 19:43:12.314518929 CET	51649	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:43:12.366180897 CET	53	51649	8.8.8.8	192.168.2.5
Feb 22, 2021 19:43:12.815783978 CET	60516	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:43:12.864737988 CET	53	60516	8.8.8.8	192.168.2.5
Feb 22, 2021 19:43:13.333830118 CET	51649	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:43:13.386872053 CET	53	51649	8.8.8.8	192.168.2.5
Feb 22, 2021 19:43:14.815207958 CET	60516	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:43:14.863894939 CET	53	60516	8.8.8.8	192.168.2.5
Feb 22, 2021 19:43:15.345506907 CET	51649	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:43:15.397375107 CET	53	51649	8.8.8.8	192.168.2.5
Feb 22, 2021 19:43:16.838984966 CET	65086	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:43:16.891166925 CET	53	65086	8.8.8.8	192.168.2.5
Feb 22, 2021 19:43:18.830656052 CET	60516	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:43:18.879324913 CET	53	60516	8.8.8.8	192.168.2.5
Feb 22, 2021 19:43:19.361643076 CET	51649	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:43:19.415884018 CET	53	51649	8.8.8.8	192.168.2.5
Feb 22, 2021 19:43:28.904625893 CET	56432	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:43:28.966559887 CET	53	56432	8.8.8.8	192.168.2.5
Feb 22, 2021 19:43:35.668194056 CET	52929	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:43:35.716905117 CET	53	52929	8.8.8.8	192.168.2.5
Feb 22, 2021 19:43:42.345645905 CET	64317	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:43:42.407318115 CET	53	64317	8.8.8.8	192.168.2.5
Feb 22, 2021 19:43:59.338802099 CET	61004	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:43:59.409931898 CET	53	61004	8.8.8.8	192.168.2.5
Feb 22, 2021 19:44:15.218272924 CET	56895	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:44:15.270029068 CET	53	56895	8.8.8.8	192.168.2.5
Feb 22, 2021 19:44:15.657108068 CET	62372	53	192.168.2.5	8.8.8.8
Feb 22, 2021 19:44:15.733612061 CET	53	62372	8.8.8.8	192.168.2.5

DNS Queries

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

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 22, 2021 19:42:42.028007984 CET	192.168.2.5	8.8.8.8	0x4dcc	Standard query (0)	manmedia.org	A (IP address)	IN (0x0001)
Feb 22, 2021 19:42:42.032453060 CET	192.168.2.5	8.8.8.8	0x96c3	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Feb 22, 2021 19:42:42.064825058 CET	192.168.2.5	8.8.8.8	0xd960	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Feb 22, 2021 19:42:42.079075098 CET	192.168.2.5	8.8.8.8	0x9220	Standard query (0)	stackpath.bootstrapcdn.com	A (IP address)	IN (0x0001)
Feb 22, 2021 19:42:42.099610090 CET	192.168.2.5	8.8.8.8	0xfeae	Standard query (0)	ajax.aspnetcdn.com	A (IP address)	IN (0x0001)
Feb 22, 2021 19:42:43.054013968 CET	192.168.2.5	8.8.8.8	0x6bd2	Standard query (0)	aadcdn.msftauth.net	A (IP address)	IN (0x0001)
Feb 22, 2021 19:42:58.363862038 CET	192.168.2.5	8.8.8.8	0xd5d2	Standard query (0)	secure.aadcdn.microsoftonline-p.com	A (IP address)	IN (0x0001)
Feb 22, 2021 19:43:06.626111031 CET	192.168.2.5	8.8.8.8	0xfa55	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
Feb 22, 2021 19:42:42.081043959 CET	8.8.8.8	192.168.2.5	0x96c3	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 19:42:42.118097067 CET	8.8.8.8	192.168.2.5	0xd960	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Feb 22, 2021 19:42:42.118097067 CET	8.8.8.8	192.168.2.5	0xd960	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Feb 22, 2021 19:42:42.140031099 CET	8.8.8.8	192.168.2.5	0x9220	No error (0)	stackpath.bootstrapcdn.com	cds.j3z9t3p6.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 19:42:42.166053057 CET	8.8.8.8	192.168.2.5	0xfeae	No error (0)	ajax.aspnetcdn.com	mscomajax.vo.msecnd.net		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 19:42:42.190284967 CET	8.8.8.8	192.168.2.5	0x4dcc	No error (0)	manmedia.org		204.93.216.87	A (IP address)	IN (0x0001)
Feb 22, 2021 19:42:43.104121923 CET	8.8.8.8	192.168.2.5	0x6bd2	No error (0)	aadcdn.msftauth.net	aadcdnoriginneu.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 19:42:43.104121923 CET	8.8.8.8	192.168.2.5	0x6bd2	No error (0)	cs1100.wpc.omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)
Feb 22, 2021 19:42:58.425558090 CET	8.8.8.8	192.168.2.5	0xd5d2	No error (0)	secure.aadcdn.microsoftonline-p.com	secure.aadcdn.microsoftonline-p.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 19:43:00.971311092 CET	8.8.8.8	192.168.2.5	0x4f2c	No error (0)	consentdeliveryfd.azurefd.net	star-azurefd-prod.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 19:43:06.686606884 CET	8.8.8.8	192.168.2.5	0xfa55	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
Feb 22, 2021 19:42:42.212815046 CET	104.16.18.94	443	192.168.2.5	49712	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	Thu Oct 21 01:59:59 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 22, 2021 19:42:42.216258049 CET	104.16.18.94	443	192.168.2.5	49713	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		
Feb 22, 2021 19:42:43.339541912 CET	152.199.23.37	443	192.168.2.5	49724	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		
Feb 22, 2021 19:42:43.340235949 CET	152.199.23.37	443	192.168.2.5	49725	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		

Code Manipulations

Statistics

Behavior

● iexplore.exe
● iexplore.exe

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 6260 Parent PID: 792

General

Start time:	19:42:39
Start date:	22/02/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff690ff0000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 6312 Parent PID: 6260

General

Start time:	19:42:40

Start date:	22/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6260 CREDAT:17410 /prefetch:2
Imagebase:	0x250000
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