

ID: 403292
Cookbook: browseurl.jbs
Time: 01:24:04
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report http://covid19-immunization-learning-program-2021.ca 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Sigma Overview 4
Signature Overview 4
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
Contacted URLs 9
URLs from Memory and Binaries 9
Contacted IPs 12
Public 12
Private 12
General Information 12
Simulations 14
Behavior and APIs 14
Joe Sandbox View / Context 14
IPs 14
Domains 14
ASN 15
JA3 Fingerprints 15
Dropped Files 15
Created / dropped Files 15
Static File Info 48
No static file info 48
Network Behavior 48
Network Port Distribution 48
TCP Packets 48
UDP Packets 50
DNS Queries 52
DNS Answers 53
HTTP Request Dependency Graph 54
HTTP Packets 55
HTTPS Packets 55
Code Manipulations 64
Statistics 65
Behavior 65
System Behavior 65
Analysis Process: iexplore.exe PID: 3008 Parent PID: 792 65

Copyright Joe Security LLC 2021

General 65
File Activities 65
Registry Activities 65
Analysis Process: iexplore.exe PID: 4800 Parent PID: 3008 66
General 66
File Activities 66
Registry Activities 66
Analysis Process: iexplore.exe PID: 4744 Parent PID: 3008 66
General 66
File Activities 66
Disassembly 67

Copyright Joe Security LLC 2021

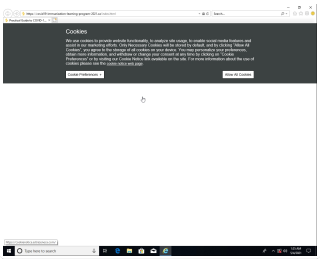
Analysis Report http://covid19-immunization-learning-p…

Overview

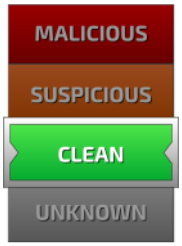
General Information

Sample URL:	http://covid19-immunization-learning-program-2021.ca
Analysis ID:	403292
Infos:	

Most interesting Screenshot:



Detection

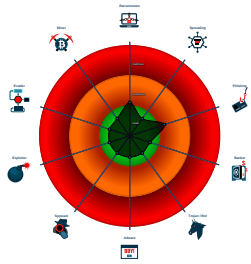


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

Found iframes

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 3008 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 4800 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3008 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 4744 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3008 CREDAT:17418 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

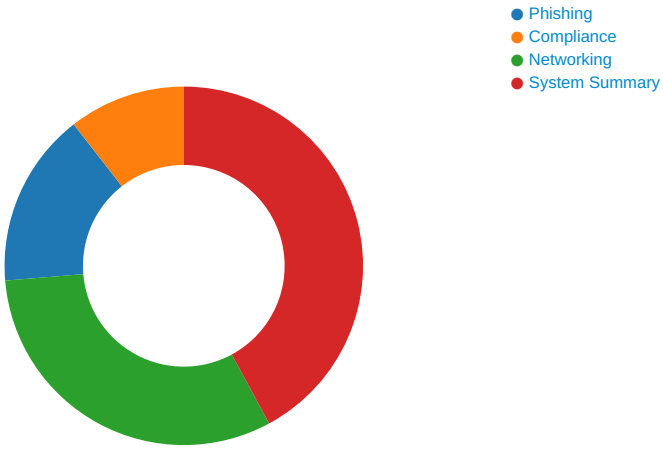
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

Copyright Joe Security LLC 2021



Click to jump to signature section

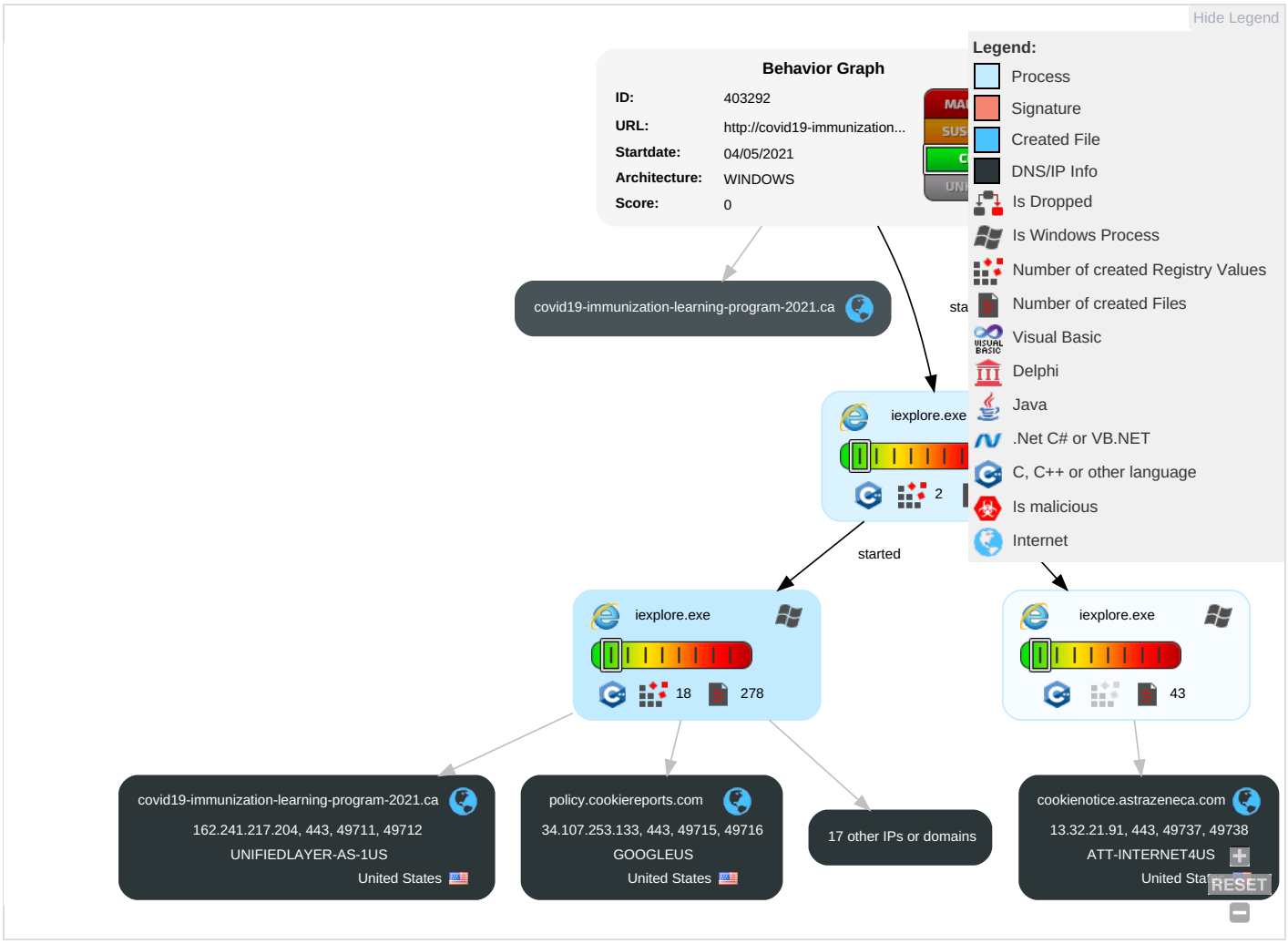
There are no malicious signatures, click here to show all signatures.

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
Drive-by Compromise 1	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
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 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
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 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM Card Swap	

Behavior Graph

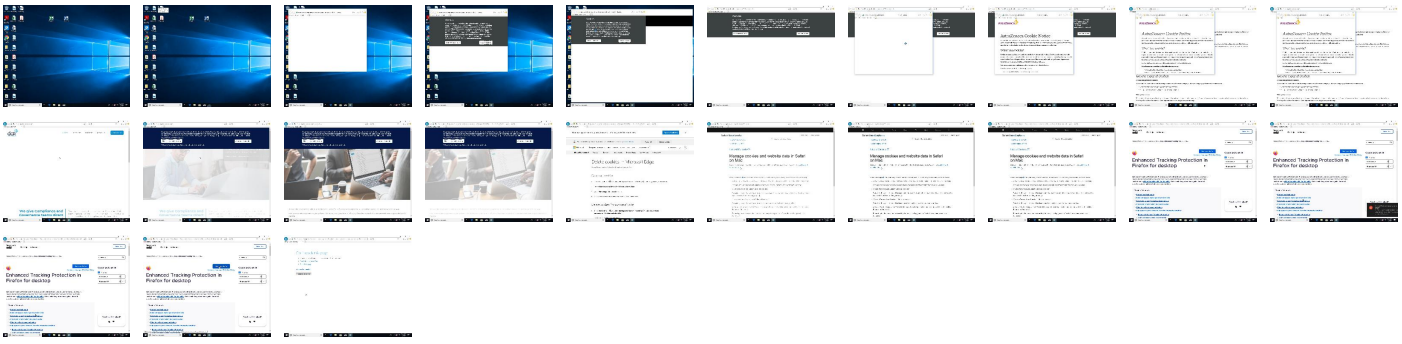
Copyright Joe Security LLC 2021

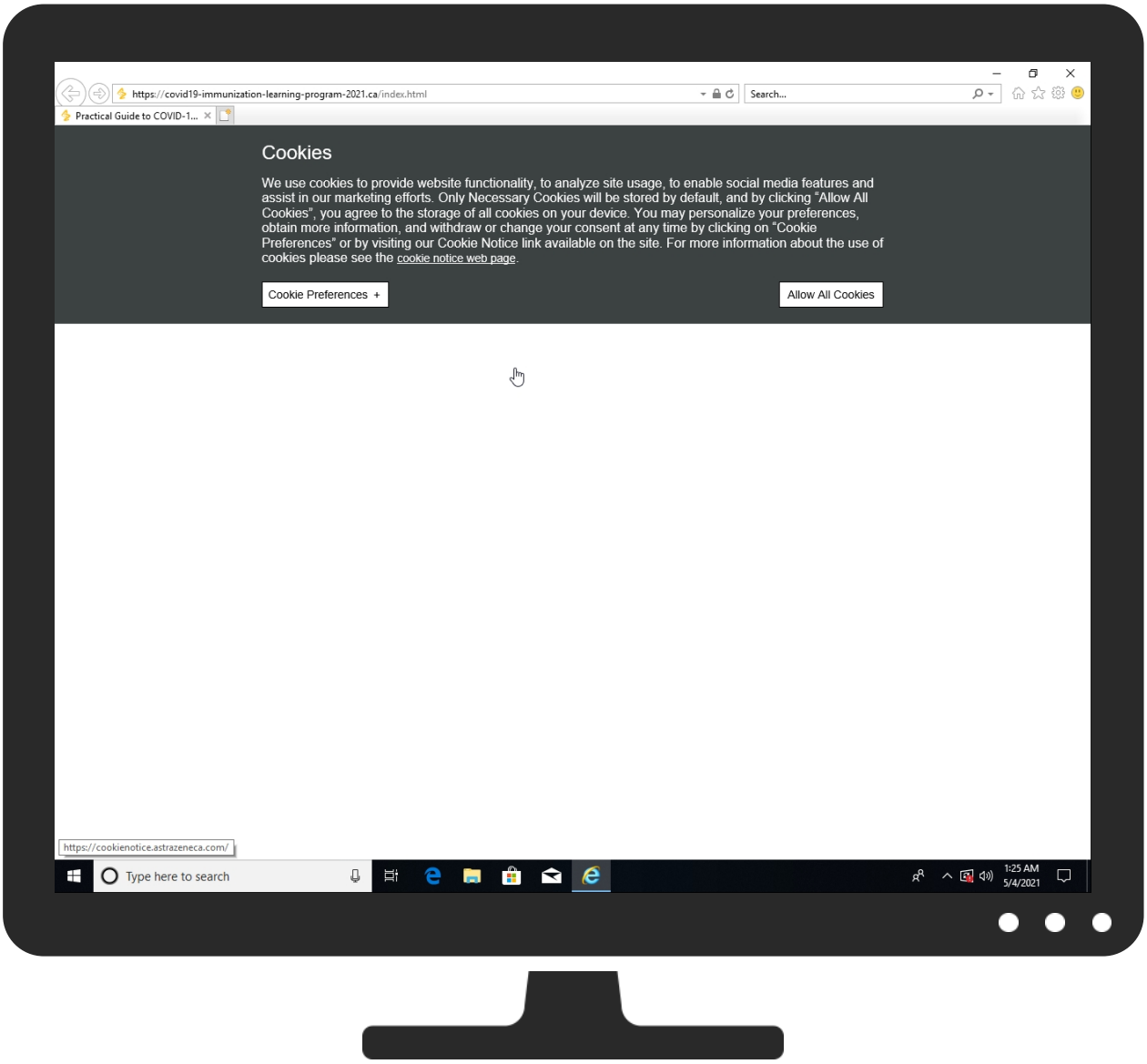


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://covid19-immunization-learning-program-2021.ca	0%	Virustotal		Browse
http://covid19-immunization-learning-program-2021.ca	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
covid19-immunization-learning-program-2021.ca	0%	Virustotal		Browse
www.digitalcontrolroom.com	0%	Virustotal		Browse
policy.cookiereports.com	0%	Virustotal		Browse
prod-tp.sumo.mozit.cloud	0%	Virustotal		Browse

URLs

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
http://https://www.digitalcontrolroom.com/wp-content/plugins/js_composer/assets/css/vc_lte_ie9.min.css	0%	Avira URL Cloud	safe	
http://https://www.digitalcontrolroom.com/wp-content/themes/cesis/includes/fonts/aileron/Aileron-BoldItalic	0%	Avira URL Cloud	safe	
http://https://www.digitalcontrolroom.com/wp-content/themes/cesis/js/lightgallery.js?ver=5.7.1	0%	Avira URL Cloud	safe	
http://https://www.digitalcontrolroom.com/terms-and-conditions/	0%	Avira URL Cloud	safe	
http://https://www.digitalcontrolroom.com/wp-content/plugins/revslider/public/assets/js/jquery.themepunch.r	0%	Avira URL Cloud	safe	
http://https://www.digitalcontrolroom.com/wp-content/uploads/2018/09/visa-logo.svg	0%	Avira URL Cloud	safe	
http://https://www.digitalcontrolroom.com/wp-content/plugins/revslider/public/assets/js/jquery.themepunch.t	0%	Avira URL Cloud	safe	
http://https://cookienotice.azation-learning-program-2021.ca/index.html	0%	Avira URL Cloud	safe	
http://https://www.digitalcontrolroom.com/wp-content/plugins/js_composer/assets/lib/bower/animate-css/anima	0%	Avira URL Cloud	safe	
http://https://www.digitalcontrolroom.com/wp-content/themes/cesis/js/cesis_easing.js?ver=5.7.1	0%	Avira URL Cloud	safe	
http://https://www.digitalcontrolroom.com/wp-content/plugins/js_composer/assets/css/js_composer.min.css?ver	0%	Avira URL Cloud	safe	
http://https://www.digitalcontrolroom.com/about-us/	0%	Avira URL Cloud	safe	
http://https://www.digitalcontrolroom.com/wp-content/themes/cesis/js/fitvids.js?ver=5.7.1	0%	Avira URL Cloud	safe	
http://https://www.digitalcontrolroom.com/wp-content/uploads/2018/09/astra-zeneca-logo.svg	0%	Avira URL Cloud	safe	
http://https://policy.cookiereports.com/consent/	0%	Avira URL Cloud	safe	
http://labs.skinkers.com/touchSwipe/	0%	URL Reputation	safe	
http://labs.skinkers.com/touchSwipe/	0%	URL Reputation	safe	
http://labs.skinkers.com/touchSwipe/	0%	URL Reputation	safe	
http://https://www.digitalcontrolroom.com/wp-content/plugins/contact-form-7/includes/js/scripts.js?ver=5.1.	0%	Avira URL Cloud	safe	
http://https://covid19-itrolroom.com/privacy-policy/Root	0%	Avira URL Cloud	safe	
http://https://www.digitalcontrolroom.com/wp-content/themes/cesis/js/owlcarousel.js?ver=5.7.1	0%	Avira URL Cloud	safe	
http://https://www.digitalcontrolroom.com/wp-content/uploads/2018/09/logo.svg	0%	Avira URL Cloud	safe	
http://https://www.digitalcontrolroom.com/wp-includes/wlwmanifest.xml	0%	Avira URL Cloud	safe	
http://https://www.digitalcontrolroom.com/wp-content/themes/cesis/includes/fonts/aileron/Aileron-Regular.ot	0%	Avira URL Cloud	safe	
http://https://www.digitalcontrolroom.com/wp-content/plugins/LayerSlider/static/layerslider/js/layerslider.	0%	Avira URL Cloud	safe	
http://https://www.digitalcontrolroom.com/cookie-policy/	0%	Avira URL Cloud	safe	
http://https://www.digitalcontrolroom.com/wp-content/themes/cesis/includes/fonts/aileron/Aileron-Italic.otf	0%	Avira URL Cloud	safe	
http://https://www.digitalcontrolroom.com/privacy-policy/JPrivacy	0%	Avira URL Cloud	safe	
http://fontello.comappleicons_textRegularappleicons_textappleicons_textVersion	0%	URL Reputation	safe	
http://fontello.comappleicons_textRegularappleicons_textappleicons_textVersion	0%	URL Reputation	safe	
http://fontello.comappleicons_textRegularappleicons_textappleicons_textVersion	0%	URL Reputation	safe	
http://https://www.digitalcontrolroom.com/wp-content/uploads/2018/09/nordea-logo.svg	0%	Avira URL Cloud	safe	
http://https://www.digitalcontrolroom.com/wp-admin/admin-ajax.php?action=dynamic_css&ver=5.7.1	0%	Avira URL Cloud	safe	
http://https://www.digitalcontrolroom.com/wp-content/themes/cesis/admin/redux-extensions/extensions/dev_ico	0%	Avira URL Cloud	safe	
http://https://www.digitalcontrolroom.com/wp-content/themes/cesis/js/cesis_fittext.js?ver=5.7.1	0%	Avira URL Cloud	safe	
http://https://www.digitalcontrolroom.com/wp-content/themes/cesis/js/scrollmagic.js?ver=5.7.1	0%	Avira URL Cloud	safe	
http://https://www.digitalcontrolroom.com/wp-content/uploads/2018/09/post-office-logo.svg	0%	Avira URL Cloud	safe	
http://https://www.digitalcontrolroom.com/wp-content/plugins/LayerSlider/static/layerslider/css/layerslider	0%	Avira URL Cloud	safe	
http://https://www.digitalcontrolroom.com/wp-content/themes/cesis/js/isotope.js?ver=5.7.1	0%	Avira URL Cloud	safe	
http://daneden.me/animate	0%	URL Reputation	safe	
http://daneden.me/animate	0%	URL Reputation	safe	
http://daneden.me/animate	0%	URL Reputation	safe	
http://https://covid19-is://www.digitalcontrolroom.com/	0%	Avira URL Cloud	safe	
http://https://www.digitalcontrolroom.com/wp-content/plugins/js_composer/assets/js/dist/js_composer_front.m	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
d388y12e46loke.cloudfront.net	13.32.21.43	true	false		high
covid19-immunization-learning-program-2021.ca	162.241.217.204	true	false	• 0%, Virustotal, Browse	unknown
dcr1.wpengine.com	35.197.225.6	true	false		high
www.digitalcontrolroom.com	35.197.225.6	true	false	• 0%, Virustotal, Browse	unknown
d1ygnxto00lnhl.cloudfront.net	13.32.21.74	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cdnjs.cloudflare.com	104.16.18.94	true	false		high
cookienotice.astrazeneca.com	13.32.21.91	true	false		high
policy.cookiereports.com	34.107.253.133	true	false	• 0%, Virustotal, Browse	unknown
prod-tp.sumo.mozit.cloud	34.210.184.158	true	false	• 0%, Virustotal, Browse	unknown
js.monitor.azure.com	unknown	unknown	false		high
support.mozilla.org	unknown	unknown	false		high
static-media-prod-cdn.itsre-sumo.mozilla.net	unknown	unknown	false		high
login.microsoftonline.com	unknown	unknown	false		high
user-media-prod-cdn.itsre-sumo.mozilla.net	unknown	unknown	false		high
mem.gfx.ms	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://cookienotice.astrazeneca.com/	false		high
http://https://www.digitalcontrolroom.com/privacy-policy/	false		unknown

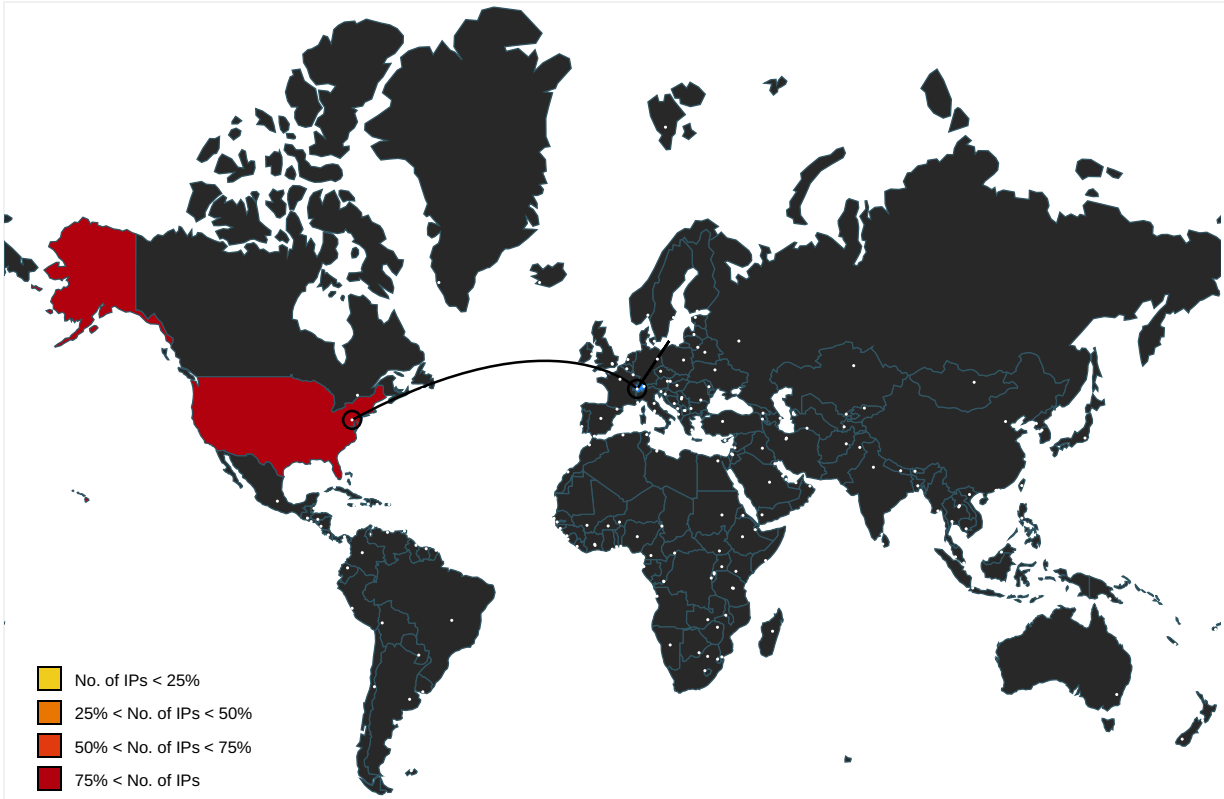
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://outlook.live.com/owa/	delete-cookies-in-microsoft-edge-63947406-40ac-c3b8-57b9-2a946a29ae09[1].htm.2.dr	false		high
http://https://www.digitalcontrolroom.com/wp-content/plugins/js_composer/assets/css/vc_lte_ie9.min.css	privacy-policy[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://greensock.com/club/	jquery.themepunch.tools.min[1].js.2.dr	false		high
http://https://www.digitalcontrolroom.com/wp-content/themes/cesis/includes/fonts/aileron/Aileron-BoldItalic	admin-ajax[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.digitalcontrolroom.com/wp-content/themes/cesis/js/lightgallery.js?ver=5.7.1	privacy-policy[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://twitter.com/tranmautritam	style[1].css.2.dr	false		high
http://daverupert.com	cesis_fittext[1].js.2.dr, fitvids[1].js.2.dr	false		high
http://www.smartmenus.org/	smartmenus[1].js.2.dr	false		high
http://https://static-media-prod-cdn.itsre-sumo.mozilla.net/static/sumo/img/favicon-32x32.png	imagestore.dat.2.dr, enhanced-tracking-protection-firefox-desktop[1].htm.2.dr	false		high
http://https://www.digitalcontrolroom.com/terms-and-conditions/	privacy-policy[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.digitalcontrolroom.com/wp-content/plugins/revslider/public/assets/js/jquery.themepunch.r	privacy-policy[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://static-media-prod-cdn.itsre-sumo.mozilla.net/static/img/pixel.gif	enhanced-tracking-protection-firefox-desktop[1].htm.2.dr	false		high
http://https://www.digitalcontrolroom.com/wp-content/uploads/2018/09/visa-logo.svg	1BTS334A.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/jquery/jquery-color	effect.min[1].js.2.dr	false		high
http://https://static-media-prod-cdn.itsre-sumo.mozilla.net/static/sumo/img/apple-touch-icon.png	enhanced-tracking-protection-firefox-desktop[1].htm.2.dr	false		high
http://https://www.digitalcontrolroom.com/wp-content/plugins/revslider/public/assets/js/jquery.themepunch.t	privacy-policy[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cookienotice.azation-learning-program-2021.ca/index.html	{2E0548C9-ACB2-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://user-media-prod-cdn.itsre-sumo.mozilla.net/uploads/gallery/images/2019-09-13-12-34-52-49baab	enhanced-tracking-protection-firefox-desktop[1].htm.2.dr	false		high
http://https://static-media-prod-cdn.itsre-sumo.mozilla.net/static/build/gtm-snippet-min.98ca663fd559.js	enhanced-tracking-protection-firefox-desktop[1].htm.2.dr	false		high
http://https://www.digitalcontrolroom.com/wp-content/plugins/js_composer/assets/lib/bower/animate-css/anima	1BTS334A.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.digitalcontrolroom.com/wp-content/themes/cesis/js/cesis_easing.js?ver=5.7.1	privacy-policy[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.digitalcontrolroom.com/wp-content/plugins/js_composer/assets/css/js_composer.min.css?ver	privacy-policy[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://scrollmagic.io	scrollmagic[1].js.2.dr	false		high
http://https://www.youtube.com/firefoxchannel	enhanced-tracking-protection-firefox-desktop[1].htm.2.dr	false		high
http://https://support.xbox.com/	delete-cookies-in-microsoft-edge-63947406-40ac-c3b8-57b9-2a946a29ae09[1].htm.2.dr	false		high
http://https://www.digitalcontrolroom.com/about-us/	privacy-policy[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.digitalcontrolroom.com/wp-content/themes/cesis/js/fitvids.js?ver=5.7.1	privacy-policy[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.digitalcontrolroom.com/wp-content/uploads/2018/09/astra-zeneca-logo.svg	1BTS334A.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cookienotice.astrazeneca.com/etc/designs/digital/assets/favicons/icon-favicon.ico~	imagestore.dat.7.dr	false		high
http://https://dcr1.wpengine.com/wp-content/uploads/2018/09/rawpixel-733989-unsplash.jpg?id=23)	privacy-policy[1].htm.2.dr	false		high
http://https://policy.cookiereports.com/consent/	7931d9d5_panel-en-gb[1].js.2.dr	false	• Avira URL Cloud: safe	unknown
http://theme-one.com/the-grid/	the-grid.min[1].js.2.dr	false		high
http://https://www.skype.com/en/	delete-cookies-in-microsoft-edge-63947406-40ac-c3b8-57b9-2a946a29ae09[1].htm.2.dr	false		high
http://labs.skinkers.com/touchSwipe/	jquery.themepunch.tools.min[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://bugzilla.mozilla.org/show_bug.cgi?id=1122305#c8	enhanced-tracking-protection-firefox-desktop[1].htm.2.dr	false		high
http://codeb.it/fontIconPicker	fonticonpicker[1].js.2.dr	false		high
http://www.modernizr.com/)	cesis_transition[1].js.2.dr	false		high
http://https://blog.mozilla.org/security/2021/02/23/total-cookie-protection/	enhanced-tracking-protection-firefox-desktop[1].htm.2.dr	false		high
http://https://user-media-prod-cdn.itsre-sumo.mozilla.net/uploads/gallery/images/2019-09-26-09-42-22-cb66b7	enhanced-tracking-protection-firefox-desktop[1].htm.2.dr	false		high
http://https://www.digitalcontrolroom.com/wp-content/plugins/contact-form-7/includes/js/scripts.js?ver=5.1.	privacy-policy[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://covid19-itrolroom.com/privacy-policy/Root	{2E0548C9-ACB2-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://user-media-prod-cdn.itsre-sumo.mozilla.net/uploads/gallery/images/2021-04-23-15-46-59-88478d	enhanced-tracking-protection-firefox-desktop[1].htm.2.dr	false		high
http://jqueryui.com/themeroller/?scope=&folderName=base&cornerRadiusShadow=8px&offsetLeftShadow=0px&	screen.845fb9a46a00[1].css.2.dr	false		high
http://https://github.com/douglascrockford/JSON-js	authorize[1].htm.2.dr	false		high
http://https://www.digitalcontrolroom.com/wp-content/themes/cesis/js/owlcarousel.js?ver=5.7.1	privacy-policy[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.digitalcontrolroom.com/wp-content/uploads/2018/09/logo.svg	privacy-policy[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.digitalcontrolroom.com/wp-includes/wlwmanifest.xml	privacy-policy[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://gmpg.org/xfn/11	privacy-policy[1].htm.2.dr	false		high
http://https://github.com/mozilla/kitsune/	enhanced-tracking-protection-firefox-desktop[1].htm.2.dr	false		high
http://https://mix.office.com/watch/	delete-cookies-in-microsoft-edge-63947406-40ac-c3b8-57b9-2a946a29ae09[1].htm.2.dr	false		high
http://https://www.digitalcontrolroom.com/wp-content/themes/cesis/includes/fonts/aileron/Aileron-Regular.ot	admin-ajax[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.onenote.com/	delete-cookies-in-microsoft-edge-63947406-40ac-c3b8-57b9-2a946a29ae09[1].htm.2.dr	false		high
http://https://user-media-prod-cdn.itsre-sumo.mozilla.net/uploads/gallery/images/2021-04-23-12-56-36-6bb740	enhanced-tracking-protection-firefox-desktop[1].htm.2.dr	false		high
http://https://www.digitalcontrolroom.com/wp-content/plugins/LayerSlider/static/layerslider/js/layerslider.	privacy-policy[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.opensource.org/licenses/mit-license.php)	authorize[1].htm.2.dr	false		high
http://https://jquery.com/	clientlib-site-min[1].js.7.dr	false		high
http://https://user-media-prod-cdn.itsre-sumo.mozilla.net/uploads/gallery/images/2019-10-16-09-26-24-6f7f2e	enhanced-tracking-protection-firefox-desktop[1].htm.2.dr	false		high
http://https://www.instagram.com/firefox	enhanced-tracking-protection-firefox-desktop[1].htm.2.dr	false		high
http://https://github.com/ded/bonzo	apd-sasskit.built[1].js.2.dr	false		high
http://https://static-media-prod-cdn.itsre-sumo.mozilla.net/static/sumo/img/spinner.gif	enhanced-tracking-protection-firefox-desktop[1].htm.2.dr	false		high
http://https://www.digitalcontrolroom.com/cookie-policy/	privacy-policy[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/twbs/bootstrap/blob/master/LICENSE)	cesis_transition[1].js.2.dr	false		high
http://https://www.digitalcontrolroom.com/wp-content/themes/cesis/includes/fonts/aileron/Aileron-Italic.otf	admin-ajax[1].css.2.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://sizzlejs.com/	clientlib-site-min[1].js.7.dr	false		high
http://https://www.digitalcontrolroom.com/privacy-policy/JPrivacy	~DF07B1C91B77A8F6EB.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://fontello.comappleicons_textRegularappleicons_textappleicons_textVersion	appleicons_text[1].ttf.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://js.monitor.azure.com/scripts/c/ms.analytics-web-3.0.2.min.js	delete-cookies-in-microsoft-edge-63947406-40ac-c3b8-57b9-2a946a29ae09[1].htm.2.dr	false		high
http://https://static-media-prod-cdn.itsre-sumo.mozilla.net/static/sumo/manifest.json	enhanced-tracking-protection-firefox-desktop[1].htm.2.dr	false		high
http://https://www.digitalcontrolroom.com/wp-content/uploads/2018/09/nordea-logo.svg	1BTS334A.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://sam.zoy.org/wtfpl/	cesis_fittext[1].js.2.dr, fitvids[1].js.2.dr	false		high
http://https://disconnect.me/trackerprotection	enhanced-tracking-protection-firefox-desktop[1].htm.2.dr	false		high
http://https://www.digitalcontrolroom.com/wp-admin/admin-ajax.php?action=dynamic_css&ver=5.7.1	privacy-policy[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.microsoftstore.com/store/msusa/en_US/DisplayFindYourOrderPage/nextAction.DisplayDownload	delete-cookies-in-microsoft-edge-63947406-40ac-c3b8-57b9-2a946a29ae09[1].htm.2.dr	false		high
http://getbootstrap.com/javascript/#collapse	cesis_collapse[1].js.2.dr	false		high
http://https://www.digitalcontrolroom.com/wp-content/themes/cesis/admin/redux-extensions/extensions/dev_ico	privacy-policy[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://products.office.com/en-us/academic/compare-office-365-education-plans	delete-cookies-in-microsoft-edge-63947406-40ac-c3b8-57b9-2a946a29ae09[1].htm.2.dr	false		high
http://https://www.digitalcontrolroom.com/wp-content/themes/cesis/js/cesis_fittext.js?ver=5.7.1	privacy-policy[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.digitalcontrolroom.com/wp-content/themes/cesis/js/scrollmagic.js?ver=5.7.1	privacy-policy[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://login.windows-ppe.net	Me[1].htm.2.dr	false		high
http://https://www.digitalcontrolroom.com/wp-content/uploads/2018/09/post-office-logo.svg	1BTS334A.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdnjs.cloudflare.com/ajax/libs/jquery/3.5.1/jquery.min.js	delete-cookies-in-microsoft-edge-63947406-40ac-c3b8-57b9-2a946a29ae09[1].htm.2.dr	false		high
http://https://foundation.mozilla.org	enhanced-tracking-protection-firefox-desktop[1].htm.2.dr	false		high
http://https://github.com/toddmotto/fluidvids/blob/master/dist/fluidvids.js	fitvids[1].js.2.dr	false		high
http://https://static-media-prod-cdn.itsre-sumo.mozilla.net/static/	enhanced-tracking-protection-firefox-desktop[1].htm.2.dr	false		high
http://https://www.digitalcontrolroom.com/wp-content/plugins/LayerSlider/static/layerslider/css/layerslider	privacy-policy[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.digitalcontrolroom.com/wp-content/themes/cesis/js/isotope.js?ver=5.7.1	privacy-policy[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.microsoftstore.com/store/msusa/en_US/DisplayEditProfilePage/tab.profile	delete-cookies-in-microsoft-edge-63947406-40ac-c3b8-57b9-2a946a29ae09[1].htm.2.dr	false		high
http://https://developer.mozilla.org/en-US/docs/Web/API/CustomEvent/CustomEvent	scripts[1].js.2.dr	false		high
http://https://static-media-prod-cdn.itsre-sumo.mozilla.net/static/sumo/css/screen.845fb9a46a00.css	enhanced-tracking-protection-firefox-desktop[1].htm.2.dr	false		high
http://schema.org	7TBY4BLD.htm.7.dr	false		high
http://https://login.microsoftonline.com	Me[1].htm.2.dr	false		high
http://https://user-media-prod-cdn.itsre-sumo.mozilla.net/uploads/gallery/images/2021-02-11-09-24-21-278ad4	enhanced-tracking-protection-firefox-desktop[1].htm.2.dr	false		high
http://daneden.me/animate	animate.min[1].css.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://codecanyon.net/licenses/	layerslider.transitions[1].js.2.dr	false		high
http://https://github.com/imakewebthings/jquery-waypoints/blob/master/licenses.txt	waypoints.min[1].js.2.dr	false		high
http://https://github.com/imakewebthings/cwaypoints/blob/master/licenses.txt	waypoints[1].js.2.dr	false		high
http://https://covid19-is://www.digitalcontrolroom.com/	{2E0548C9-ACB2-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	low
http://https://www.digitalcontrolroom.com/wp-content/plugins/js_composer/assets/js/dist/js_composer_front.m	privacy-policy[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.241.217.204	covid19-immunization-learning-program-2021.ca	United States		46606	UNIFIEDLAYER-AS-1US	false
34.107.253.133	policy.cookiereports.com	United States		15169	GOOGLEUS	false
13.32.21.89	unknown	United States		7018	ATT-INTERNET4US	false
13.32.21.43	d388y12e46loke.cloudfront.net	United States		7018	ATT-INTERNET4US	false
104.16.18.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
34.210.184.158	prod-tp.sumo.mozit.cloud	United States		16509	AMAZON-02US	false
35.197.225.6	dcr1.wpengine.com	United States		15169	GOOGLEUS	false
13.32.21.74	d1ygnxto00lnhl.cloudfront.net	United States		7018	ATT-INTERNET4US	false
13.32.21.91	cookienotice.astrazeneca.com	United States		7018	ATT-INTERNET4US	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	403292
Start date:	04.05.2021
Start time:	01:24:04
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs

Copyright Joe Security LLC 2021

Sample URL:	http://covid19-immunization-learning-program-2021.ca
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:	31
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.win@5/248@14/10
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://cookien otice.astrazeneca.com/ • Browsing link: https://www.digitalcontrolroom.com/ • Browsing link: https://www.dig italcontrolroom.com/privacy-policy/ • Browsing link: https://support.microsoft.com/en-us/microsoft-edge/delete-cookies-in-microsoft-edge-63947406-40ac-c3b8-57b9-2a946a29ae09 • Browsing link: https://support.apple.com/en-gb/guide/safari/sfri11471/mac • Browsing link: http://support.mozilla.org/en-US/kb/enable-and-disable-cookies-website-preferences
Warnings:	Show All • Excluded IPs from analysis (whitelisted): 168.61.161.212, 92.122.145.220, 104.43.193.48, 88.221.62.148, 52.147.198.201, 142.250.184.234, 142.250.185.227, 142.250.185.234, 142.250.185.200, 152.199.19.161, 23.218.208.112, 92.122.213.163, 92.122.213.160, 92.122.213.194, 92.122.213.247, 92.122.145.53, 152.199.19.160, 13.107.246.60, 13.107.213.60, 88.221.228.182, 23.37.44.90, 65.55.44.109, 20.190.160.134, 20.190.160.69, 20.190.160.136, 20.190.160.129, 20.190.160.75, 20.190.160.71, 20.190.160.67, 20.190.160.2, 40.126.31.143, 40.126.31.135, 20.190.159.132, 40.126.31.137, 20.190.159.134, 40.126.31.141, 40.126.31.139, 20.190.159.138, 52.114.128.43, 20.82.210.154, 2.17.181.200, 23.218.208.56, 92.122.247.86, 184.30.25.106, 205.185.216.42, 205.185.216.10, 8.252.5.126, 8.241.90.126, 67.26.83.254, 8.238.85.254, 8.238.30.126, 52.155.217.156, 20.54.26.129 • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, aijscdn2.afd.azureedge.net, arc.msn.com.nsatc.net, e13678.dscb.akamaiedge.net, browser.events.data.trafficmanager.net, support-china.apple-support.akadns.net, fs-wildcard.microsoft.com.edgekey.net, ev.support.microsoft.com.edgekey.net, e11290.dspg.akamaiedge.net, www.microsoft.com-c-3.edgekey.net, prod-support.apple-support.akadns.net, e3843.g.akamaiedge.net, login.live.com, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, videoplayercdn.osi.office.net, help.apple.com, watson.telemetry.microsoft.com, au-bg-shim.trafficmanager.net, fonts.googleapis.com, fs.microsoft.com, a1835.g2.akamai.net, ajax.googleapis.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, part-0032.t-0009.t-msedge.net, skypedataprdcolcus17.cloudapp.net, www.tm.a.prd.aadg.akadns.net, videoplayercdn.osi.office.net.edgekey.net, e6858.dscx.akamaiedge.net, web.vortex.data.trafficmanager.net, skypedataprdcolcus15.cloudapp.net, e2063.e9.akamaiedge.net, ris.api.iris.microsoft.com, e55.dspb.akamaiedge.net, store-images.s-microsoft.com,

	cdn.account.microsoft.com.akadns.net, blobcollector.events.data.trafficmanager.net, www.apple.com.edgekey.net, e9398.g.akamaiedge.net, cs9.wpc.v0cdn.net, dual.part-0032.t-0009.t-msedge.net, www.tm.lg.prod.aadmsa.trafficmanager.net, www.apple.com.edgekey.net.globalredir.akadns.net, km.support.apple.com, e11408.d.akamaiedge.net, support.microsoft.com, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, www.apple.com, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, go.microsoft.com, www.googletagmanager.com, support.apple.com, skypedataprdcolcus04.cloudapp.net, support.apple.com.edgekey.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, statics-marketingsites-neu-ms-com.akamaized.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fonts.gstatic.com, ie9comview.vo.msecnd.net, cs22.wpc.v0cdn.net, www-googletagmanager.l.google.com, mem.gfx.ms.edgekey.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, help-ar.apple.com.edgekey.net, firstparty-azurefd-prod.trafficmanager.net, login.msa.msidentity.com, web.vortex.data.microsoft.com, skypedataprdcoleus16.cloudapp.net, aijscdn2.azureedge.net, browser.events.data.microsoft.com, help.origin-apple.com.akadns.net, go.microsoft.com.edgekey.net, az725175.vo.msecnd.net, www.microsoft.com, displaycatalog-rp.md.mp.microsoft.com.akadns.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

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\52DRT984\www.digitalcontrolroom[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	52
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aK1r0aK1r0aK1r0aKb:JFK1rFK1rFK1rFKb
MD5:	770DA68A4DE2539B5002B44767396AF9
SHA1:	E3A118B288CF426DE3027EFCE38AE7241560EC4C
SHA-256:	908FB85A6D01001B303E1030664D87BA5D193B56CA17FB2116D8696196D4DA4A
SHA-512:	B4AA2726B958DDA17F5D1E5A2EB109825D9CDBDBA1E1CFDDBE55BA94D5B6ED5EE7DBB0F15538099C44F0CC80DB2AF445EA4F60D11FE767943FFF99AA495D922
Malicious:	false
Reputation:	low
Preview:	<root></root><root></root><root></root><root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\HB8GKAHF\support.apple[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	954
Entropy (8bit):	5.217920418170421
Encrypted:	false
SSDEEP:	24:WUFhyvv00U1mKm6DYvU1mKm6DYvU1mKm6DY9VsWMH+cCKB4uTdCDcV:LgmsKYcsKYcsKYxMH+SHdCgV
MD5:	A1D95751CA5508E59D736806CDC92D7C
SHA1:	64C0025139CDB8BE49711E119C30BACC9DC9B03F
SHA-256:	1AED29CAC02894624DAE4CA6E492D46BAAD994F83CAA3A71976FD20F1A33AACB
SHA-512:	771BED2B278E846993646A514E92961DAABE6449A7ACC9C6C976E2246EA527C0C6CE73914607B4D9CF8F4F910E3AD6349DA1CE6BCA8C96B85086FB10ED36275
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="localStorage" value="1" ltime="108219824" htime="30884031" /></root><root></root><root></root><root><item name="com.adobe.reactor.dataElementCookiesMigrated" value="true" ltime="108689824" htime="30884031" /></root><root><item name="com.adobe.reactor.dataElementCookiesMigrated" value="true" ltime="108689824" htime="30884031" /></root><root><item name="com.adobe.reactor.dataElementCookiesMigrated" value="true" ltime="108689824" htime="30884031" /><item name="ac-storage-ac-store-cache" value="{"e":3806,"v":{"ttl":1620116902187,"items":0,"cn":null,"api":{"flyout":"//www.apple.com/%5Bstorefront%5D/shop/bag/flyout","addToBag":"//www.apple.com/%5Bstorefront%5D/shop/bag/add?product=%5Bpart%5D"},"key":"S2A49YFKJF2JAT22K","sfLoc":"uk"}}" ltime="114819824" htime="30884031" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\NPM76I19\support.microsoft[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	39
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aK1r0aK1r0aKb:JFK1rFK1rFKb
MD5:	B9C5EB570521110110BB7DFF12AF780D
SHA1:	27F5BEBC2200FD8D0B51A93D1357EA954BE44079

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\NPM76I19\support.microsoft[1].xml	
SHA-256:	90171F10A6467C9DC31143859BAB69D045B67B39E2E49D92BB7168B383C4D1AB
SHA-512:	BC81539E62D643808CBDA3D86050058F379B2F0347CE65CBBA9797D386401C886B22AC4C0B2BE68197AE10C83A1E22A14232CD531C8D139DD3C031DB423EA3
Malicious:	false
Reputation:	low
Preview:	<root></root><root></root><root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\OMJ28YSL\covid19-immunization-learning-program-2021[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aK1r0aKb:JFK1rFKb
MD5:	132294CA22370B52822C17DCB5BE3AF6
SHA1:	DD26B82638AD38AD471F7621A9EB79FED448A71C
SHA-256:	451ABBE0AEFC000F49967DABF8D42344D146429F03C8C8D4AE5E33FF9963CF77
SHA-512:	6D5808CAD199A785C82763C68F0AE1F4938C304B46B70529EA26B3D300EF9430AD496C688D95D01588576B3A577001D62245D98137FD5CD825AD62E17D36F15C
Malicious:	false
Reputation:	low
Preview:	<root></root><root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\OMJ28YSL\support.mozilla[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	117
Entropy (8bit):	4.44511143585926
Encrypted:	false
SSDEEP:	3:D90aK1ryRtFwsxAC5EJVqGCj5qBW2haIAqSf6UQK1r0aKb:JFK1rUFSC5EJVqGCj5q9ali61rFKb
MD5:	E3F05E3596613097454EBB257D078A66
SHA1:	1589E1632C12486CE34B0D393FE9656CD34A8552
SHA-256:	F0DD437D0DA44EBF901486BE881B99A21029F9C6A08BDDF5E8978307B9CAAA5D
SHA-512:	4400D3B8C875F2F101FFCA8B5E771B8E08B078CA77AE24FBDD7E0603280E510D9934E9773E3288FC561922250CED6213977DF5681EE759C02BE7435B5C1466FC
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="modernizr" value="modernizr" ltime="165139824" htime="30884031" /></root><root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{2E0548C7-ACB2-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	48360
Entropy (8bit):	2.042121212399369
Encrypted:	false
SSDEEP:	192:rVEZ7FZG42KLW7tCfoRM84ffpcr1NTWta6:rV07rGvKi5gx84Xk1Yta6
MD5:	5825DBEBD08BBCD5C6FCFA1E5CFD56D4
SHA1:	BD39C46810B17CFC3B4EA687BD48478BB9A39E7C
SHA-256:	DC4568A327E2C321B20A9791ED9E9981367E072EB935ADFEEB8572221A146ACE
SHA-512:	63692F886B538895A464A2EEC84634B91C61BB18F5C25DAAA44750502AD552B08834CBE3A2B819DBD177D434686D226B8BECB84AC2CCE3912854DE8BC891F07B
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\{2E0548C9-ACB2-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	157906

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{2E0548C9-ACB2-11EB-90E4-ECF4BB862DED}.dat	
Entropy (8bit):	2.909352800545921
Encrypted:	false
SSDEEP:	768:LoR5jrVs2m5jrVsX38tM8tCN060H0P0YUH0dw0VfTwm08/0LqbNu:Tkxwi+
MD5:	E28D6D47706CAE6241C1DC02EC506836
SHA1:	4337BF9C9D8D85DECB41068E2859085971F9E03E
SHA-256:	022EF376BB4337C58E30052F9F9D1BFBC895005644DB4E17312CEF44CBD6126A
SHA-512:	E4D93BD1E8E76195A4401F6790F7905B4AA8A9FE21B5F8491B2A8D90D1A4B4674ADA2AEF50067295D6BD71CE704C3F9D5096CCB255A68802DD0098D5B969189
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\{34120184-ACB2-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.56427990769012
Encrypted:	false
SSDEEP:	48:Iw+GcprbGwpaFG4pQtGrapbS6GQpKdG7HpRm7TGIpG:riZ1QX6NBSCA8TmA
MD5:	C4030789D402E5498EA4206E6A7D82DE
SHA1:	9527625B5C76D1B7DE76043D2CB9FFE7B90DE29F
SHA-256:	4C0255539F9198F678028DB404798E3814C3778C725BBC371074D39489E50056
SHA-512:	041F0E8C64C315458829E3F683E6FB1401F7270352B302F9B322E310BD1C9D7A4383EB961AA7180FEE9AD1D7FDED36B77972D4EDE5B2ECCA58BF1C951C84AB E
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\{34120186-ACB2-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27390
Entropy (8bit):	1.7676158343431265
Encrypted:	false
SSDEEP:	48:IwqGcprzGwpasG4pQsGrapbSUGQpBqGHHpcnVGTGUp8n+GzYpmnNwGopPmhNQuGT:rOZtQs6qBSMjx2VWWyMO0tHnGB9r
MD5:	1FC4246B1C852806040D6CECA3F46688
SHA1:	EF3CEBB19485CDDA85B8494AA0DCB097B920BE1A
SHA-256:	53D94C46410DA6B0A5419F9A901C6D67EC2B30C8A02DE5367E3086F238943258
SHA-512:	69E6F95E3232B29E9783B04F529E57B793FA19140D03D9D5F399108EE867ACF289E8928B552A2120BEDC1A361CA5EF023E6DD98F62E02CA90F35920A2A966410
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	modified
Size (bytes):	35598
Entropy (8bit):	3.083690423225009
Encrypted:	false
SSDEEP:	192:ToFBgxgBXJezAAeNuzdyrjcolz25CMXfYK8VSfwX/pWeZ2gtaINCN7jS5J:UFBJJXyZFl8Vf0wBN+7O7
MD5:	58B316661780597338O9AC17F7F53D75
SHA1:	6CEC7FF8CBD64332D6CD8316567DCA9B6CB4C9A7
SHA-256:	583AFA6B327962125F80AA8FF107136A2DFFFE90AE2E0E442D38B9A8D008F8E0

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
SHA-512:	84AD1602DA3C0BA8BC52F2EE2A6FEAE6A345309FA8C2E73D918540B0B32B315FA652C8DF78151CACC4BCCDC3289EC892ACC051FF247933718E9B170BE15422 92
Malicious:	false
Reputation:	low
Preview:	Y.h.t.t.p.s.:./.c.o.o.k.i.e.n.o.t.i.c.e...a.s.t.r.a.z.e.n.e.c.a...c.o.m./.e.t.c./.d.e.s.i.g.n.s./.d.i.g.i.t.a.l./.a.s.s.e.t.s./.f.a.v.i.c.o.n.s./.i.c.o.n.-.f.a.v.i.c.o.n...i.c.o.~..... .h.....(..... ....d.....l.....(.....@.....\.....).. .....l.....(.....d.....".....l.....Z.....$.....b.....,.....V.....<.....J.....(...H.... .....T..... .....t.....F...`.....F.....&..... ....."..... L2.....<.....4.....l.....8.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1Ptxg8zYS_SKggPN4iEgvnHyvveLxVs9pYCM[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 69524, version 1.1
Category:	downloaded
Size (bytes):	69524
Entropy (8bit):	**7.993040233849446**
Encrypted:	**true**
SSDEEP:	1536:vN5YFf7R7I4VrE1gQV9RsboIOQ6X2e8oV8aUe85EPzIo:vPofy/gQVbl7PXV8oV8eiu
MD5:	F11BE8ADC25D706E2CC93E8104A1E2CE
SHA1:	BD38B70C2817D79BD0F14F7CA04FBEA7BD1F70D4
SHA-256:	D7412B2EDF140EE1843A757814BE7CD2E945C52D4B103E7CA87B5B440514E040
SHA-512:	AE9A0578551A58EF852F98F8E9C9B44C4A28509BE04D6104BAB8A1D990E72E72D8DB13ACF6506CD125B9C41EDCBC91C1AF146F2856E58536402A7E887AEECF C6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/raleway/v19/1Ptxg8zYS_SKggPN4iEgvnHyvveLxVs9pYCM.woff
Preview:	wOFF.....GDEF.....F...(....GPOS.....M.....Y.6GSUB..P.....~TR(!OS/2..SP...P...`..g.STAT..S....9...D...&cmap..S.....V`.cvt ..[l...N.....fpgm..[..... .Zgasp..c.....glyf..c.....\..@head...8...6...6.b..hhea...p... ...$....hmtx.....a.....l..loca.....g..maxp..... ... .name.....-...B6.X.post.....f..!.#..prep...P...A....O(.. x....D.a.E.{.... E(... L$...$J.$.. .$$L*.TS....(!J.$.%.M.9..\Y..$I~S. ..HV3Y.d...'k..!.Jd..5N.4Y.d..F..Y;d..uN.5Y.dU..!.....wc.y.s.....G..".z....+^.u.c..<.1.../|.W.....*>._... ~.....XsM.,2..:.E....;..{...c..c.G...(.X..DL.dL.L..\..B,.R,.j.b9..[x.'x.gr*.M.....6=*.Lj`-.GV.v.^.O.t...J./....X...A..y...m[...x.t....l.....~...}X..^.vl.m..Al.....|..o5..f.....i.2-....K.T_[... .../a.P.9,J...2}u.....l..P.P&e.:+t.td.... .....x..,.....Nj.F&..-...yc..c-....,an.;t_."...'r...4..@q..).....z.....<..>Q}..\..Y...Q.7...=y.u.R...8..`....g..m..o.s.Tk=...J.f.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1Ptxg8zYS_SKggPN4iEgvnHyvveLxVuEooCM[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 67824, version 1.1
Category:	downloaded
Size (bytes):	67824
Entropy (8bit):	**7.991166938434615**
Encrypted:	**true**
SSDEEP:	1536:DJ1Zb4tA45yVaVSrAEn3bqGjH++YOSXvMp/4/lo:DxiA4eaeWGjHIOSXvMp/4S
MD5:	E9A17CDEE84C3FF6160653B5B12B5B42
SHA1:	0AA0ADD663440BF063127B5FFD240A864293B15D
SHA-256:	6DF60069066A417ED59CECC2EAEC229718666F6B9589E9B9AA90C2E638B724E2
SHA-512:	4318C25AA818A5A9567BAF464931DE3D86C93065D01AC20E62F7DEE1962A419EEFA244666C08E1FCF95A05406181BAC2B6F3B80525B6A9A878DA454E45E6CDF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/raleway/v19/1Ptxg8zYS_SKggPN4iEgvnHyvveLxVuEooCM.woff
Preview:	wOFF.....$.....GDEF.....F...(....GPOS.....J.....GSUB..L.....~TR(!OS/2..O....Q...`.ug8STAT..P....8...D.T."cmap..P@.....V`.cvt ..W....N.....fpgm..X .....Zgasp..._.....glyf..`.....PD.~.head.....6...6.a..hhea..... ...$....hmtx...,.....Q.sloca...L.....7...maxp..... ... .name.....2...p>.a.post...D...f..!.#..prep.....A....O(.. x....D.a.E.{.... E(... L$...$J.$.. .$$L*.TS....(!J.$.%.M.9..\Y..$I~S. ..HV3Y.d...'k..!.Jd..5N.4Y.d..F..Y;d..uN.5Y.dU..!.....wc.y.s.....G..".z....+^.u.c..<.1.../|.W.....*>._... ~.....XsM.,2..:.E....;..{...c..c.G...(.X..DL.dL.L..\..B,.R,.j.b9..[x.'x.gr*.M.....6=*.Lj`-.GV.v.^.O.t...J./....X...A..y...m[...x.t..t.\....Z.Fj..Of:.;uj.v..m.m.\~I.{.s.k.....epPix....;..Y7../8.... p.h.=.:.....;.:.:./.@..4.F..NX..7.{.....J.}f.v..R..0....+9.....Y..".o-.....\d.7.o.W.r.....x...-.)..#=}...ky.y.Q..s...m./.~%.v?..`.....X..W-..\$.V..]...O..DI.R..3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\2019-09-13-11-59-41-fc828d[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 80 x 80, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	2435
Entropy (8bit):	7.870023302741485
Encrypted:	false
SSDEEP:	48:V+pl6OjFrhsqBMNcXpRY4QSdfrT+H+BDzK1g7x27nqODXw3vSvnqEW0:V+f6OjTB0cXpG41m+BDO1g7xwnovS/qi
MD5:	24BB35C62953B5EDA6B22310731A25D4
SHA1:	8E880EECD1682297DB3F69A9A356FC91A0441124
SHA-256:	5A6989DE1C5EA19133000988A63F2D9AA479690F8080C5C1C3AAFEB75D9A0361
SHA-512:	22F2004689FE87663A32DE434A660DFE7958A6D039EA17EECB7B851395F9CCE309BF0D99773EA9EF00E81D49790834C88DD35FF931F45E1D2A9E5802400C33F4
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\2019-09-13-11-59-41-fc828d[1].png	
IE Cache URL:	http://https://user-media-prod-cdn.itsre-sumo.mozilla.net/uploads/gallery/images/2019-09-13-11-59-41-fc828d.png
Preview:	.PNG.....IHDR...P...P.....JIDATx..yl\W...}.y.x.$...];6Y....mJvP...F....A.JE*.Q*.*....".PTu.jK...".HT.0.$.I..8i..v.....-.x..{...u...<...z?i.E.>...9..s.....466.MMM.8.>"...b..(.....(.p...(..7...,..a.H$....KTU..z43Q.$%../.....o.y....s(..Cy.....P.@...:...<....t(..Cy.....P.@...:....\.`"U..._.:...._o.....r.....,).=.....R ../.X.....`.UR/..oM*.x..u`.....Gj..U.k..iE]..z.<'..BL.....G@....."..... i_.@Q0u.c.%....}-...8u..o..eSV.~u..E._.&..*...8..$.....q.kPQU...]...'Z..u..V...ye..$.B...:..... ..<.....=g.z...{...n...*<._)V.-.....6x...8..m.H....y....Z_.?X..07.RaqI.s~.....a.....f.....S.....S.....oV.D_.19..*.p._...`A\Tw..+.?..A.lt.`..2.....-).k...-...--.....s....Y].....(.../..&..X.'.. .`Y.....(..b.l...s.|.....yfg.....'.....5..]z{.....P.....e":.:.a..5x....7..F...Z.1@n...b.\.@...D.@b4Y.....,.|8?P.....="B. f.=.4..s"W."q4.%3.a8.).}...diN. .. ....;. s....D....N..@.h.'}.....j~@ ...H`j.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\6846073fc6f766d1ad3f66ae757c5e24[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 60 x 60, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	6885
Entropy (8bit):	7.963029007309932
Encrypted:	false
SSDEEP:	96:Aq5vShDlYxh/6oVgQkP09ID0OUzLj3APQGNrdITO6QlcTy8VQbWXR0mNuOCdF3q:U5KyoVgjWOUbM3IycTWWX6O66
MD5:	6846073FC6F766D1AD3F66AE757C5E24
SHA1:	8C671B71C623987D9F78C7D6C190D5B1C627AFCB
SHA-256:	0936874566D9A757F2D99FEBA7430E875387A37CAA1D9AC67D135B047ADAAFC3
SHA-512:	E6089FDF549406C643780CB586FB9698DA23E87C0D575877C4D4C14EEBB48AC32406881B9B5BE64E44D6A44C9F15CB57DDDDA7F3301426D761156DCBD21D56
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://help.apple.com/assets/5FC7BA6A0946225611C6FEFA/5FC7BA710946225611C6FF02/en_GB/6846073fc6f766d1ad3f66ae757c5e24.png
Preview:	.PNG.....IHDR...<...<.....:..r....gAMA.....a.....sRGB.7.MS....IDATh..yx.U..?....wv.C.SZ..t..R.L.T..Q.d8G.A..9.a.z..(r.q..=(....OA....4.m..I..;....]...w..6-...<.>w.Y....Y.....z.R.!...n.i.:.....MT...m.N*.JI)..Y).q6_....5k.\.j.....<...."///..z.n..PJ...bl.....d.J)5...B..i;.L&.....uuuu.m.e.-===.g..t.....z.....P.....}.{.)...<#.....Q.....O|..7....n..S...I%...0.....o ....RJ....W../O.X.....7n....I....>..a.#iN.%.6$..Qzt..0.1-.dQE.E..X5..a...).s.=w?..SO..pIIIYWW...&u..l.....a..Q`y /.n?y.^.f.35...$.r..O@:...Q.R.....h.KgV.]...W{...}..~..._..k..-..l>..[Z.eC..<((c.....<C..%...\`I.K...G)...B.h.k.iQ...H.$#\7...WWqa.....E.....jVkkk.....;C.+e.i....S..;.:......./..s..:..]...+..C:.Q..]..9MM...O(....M.0p.O/....j)....../+/.m..Rh#...;.u.?.....`...f...Y0..L...'x.h....p.....8h3%hP.g..C..1A.. aKvv..4..1&.q>7G.....n.._..K..>g.w.}.gF^..^.v..2.._.e..@.....0...96.[b,.WI.V..l..!.NI.aS.7.O...-b...)..>."........&

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\7931d9d5_panel-en-gb[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	89624
Entropy (8bit):	5.146800651886202
Encrypted:	false
SSDEEP:	1536:uG8F1NQiVG3BP2Yp+QGlc6GChJ4yQZhZVYZ3DZ3dZ6Pyks2:Cq+CV
MD5:	9FE3F340E33BCEF7F682440D77567FAF
SHA1:	82617CD99FFA22A6815E8C82A2AAFEF61B815F6C
SHA-256:	8884E614BDE9B7AD6300D16B7C20E686FFCF7D6F380BA2DF04EDA61D3637087F
SHA-512:	730C9E4BA9D5BCF96068C2FEE66EC5D77CBC773CCA71E924B0695869DB2B1B27B09F8183D38CFDBD86219C637C83663A5C3AA749D408FABB289539378E26C01
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://policy.cookiereports.com/7931d9d5_panel-en-gb.js
Preview:	(function(){var b={},d;b.load=function(){var c=document.createElement("div");c.innerHTML="\x3c!--[if lte IE 6]>a<![endif]--\x3e";if(!c.getElementsByTagName("i").length)if("undefined"!==typeof jQuery&&jQuery.fn&&/^(1\.([8-9]|[1-9][0-9]+)|(2|3)\.[0-9]+)|(2|3)\.[0-9]+)/.test(jQuery.fn.jquery)&&jQuery.ajax)d=jQuery,b.init();else{c=document.createElement("script");c.setAttribute("data-consent-checkpoint","ignore");c.src="https://ajax.googleapis.com/ajax/libs/jquery/3.5.1/jquery.min.js";c.type="text/javascript";.c.onload=c.onreadystatechange=function(){d||this.readyState&&"loaded"!=this.readyState&&"complete"!=this.readyState||(d=jQuery,jQuery.noConflict(!0),b.init())};var e=document.getElementsByTagName("body");(e.length?e:document.getElementsByTagName("head"))[0].appendChild(c)}};b.triggerEvent=function(c,e){e=e||{};e.consent=b.currentLevels;e.consent_string=b.serializeLevels(b.currentLevels);var f=document.createEvent("Event");f.initEvent("wscr."+c,!0,!0);f.detail=e;document.dispatchEvent(f);"con

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\7TBY4BLD.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	34295
Entropy (8bit):	4.914710807689846
Encrypted:	false
SSDEEP:	768:X7xAJOaejijsHIax7TxhkuIXCbuuv8l0THgshnB+W+f:iJZsHIo7Txhka1v8IELhB+W+f
MD5:	604A705C3DF947AA706001BFB7B81BD5
SHA1:	93324D45E02284B7AEA768CDB32F9D07667DEEB3
SHA-256:	5542F9DFCD9E4FF35F1B79CABF0DA6358E458C6AA5FFD396D3CB58B0433962D5
SHA-512:	1FACC9B2E2BD6248C0A7432B76450E27E324F9A100FAC39111892F9ECA13EBCACE443CE784F546A800F8201E1E8D12A7C6CF1D07C176BC1023B0FF37138541C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\7TBY4BLD.htm	
IE Cache URL:	http://https://cookienotice.astrazeneca.com/
Preview:	<!DOCTYPE HTML>..... ....<html lang="en">... cookienotice.astrazeneca.com--> . astrazeneca-digital-prod65-publish4useast1-->.. <head>. . <meta http-equiv="Content-Type" content="text/html; charset=UTF-8"/>. . .<title>Home</title>. . ... Add later -->. <meta name="viewport" content="width=device-width, user-scalable=no"/>. <meta name="HandheldFriendly" content="True"/>. <meta name="MobileOptimized" content="320"/>. <meta http-equiv="X-UA-Compatible" content="IE=Edge"/>. <meta http-equiv="cleartype" content="on"/>. <meta name="format-detection" content="telephone=no"/>. <meta template="homePage"/>. .... Add later -->..... favicon setup -->.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\JTURjIg1_i6t8kCHKm45_ZpC3gnD-A[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 23576, version 1.1
Category:	downloaded
Size (bytes):	23576
Entropy (8bit):	7.979995638545985
Encrypted:	false
SSDEEP:	384:evykH+9E9B49CndLoAUlGTJO8OzoRb1Jrb7ZlZ/EYh93e1rRykMKAZir2k4lyPmo:eqP9sC2dXUlF8Ozc5JrbNr/EM93eZRhl
MD5:	8B763220218FFC11C57C84DDB80E7B26
SHA1:	E85E6898C8FD8B095BD694B3F1350342C7BB3F35
SHA-256:	299E5F2B6E651BFD7B4C74AA12B06BB10A1200757CC4EBD1FC4C0D9D1AAFA00D
SHA-512:	4A93693CDE6B4BAEAD17A78C6B3FF7BD9F7489D20E5BE3815751B4A1E4E034E7BB54249DEF7F8E06B3ADE41E4333F45FDB232E67971C1817F66151F1440BDE32
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/montserrat/v15/JTURjIg1_i6t8kCHKm45_ZpC3gnD-A.woff
Preview:	wOFF.....\.....GDEF.....G...X.g.^GPOS.....2....GSUB.....,OS/2...I...O...`T..acmap.....h.cvt .....b....0...fpgm.....F...mM$.\|gasp...,..... ..glyf...4..3...\.)...head..R...6...6.P.xhhea..S.... ...$....hmtx..S,...'...>"...loca..UT.....(...maxp..Wt... ... .h.Wname..W.....*.Elpost..X.....D.z.prep..[\.....K..x.%....P.....@:D.. .$..]!....h.....2/.$.....D.^.F..ua.].N....%>./...x..ex#.....<..d.e.-.1..33333333..y...T.`.V^p.m._.{..9...z..z..5... .<....|...<.-.}9./..._....f.P.J?F.....d...b..DzFm.....&b...!...H..;a.XI.=6gEB..6 N.....]6.I...J..w.hU\6...I.u*ei..@..J.n. .2.D3.. .(ay.....<..j>....s@.n.....Z.U.H@.v..e.....!..s.`wW...u4.8P...x.r...z4...h.....H@.;.g.....,1..)..E.}".S.5..X.{E....._....."..D...=|D..Q... D7...q>.\ .\.E.s.Hp.Hr...r.....+..f..q...\+:.Q..,Bn...g#.l..l..l.i..&v.4;E..D=...I.....R.O.1-.fDDA.1+j8...A.D...?M..w.|.&F.f..1..z....j-o9.V.y.em...vRO.^..-.S..f.q.....j...c....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\JTURjIg1_i6t8kCHKm45_cJD3gnD-A[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 23256, version 1.1
Category:	downloaded
Size (bytes):	23256
Entropy (8bit):	7.977753236160612
Encrypted:	false
SSDEEP:	384:2gMWysI22L2wL/yhGTJO87uvLzyBFvQ3dol9ET1Em9FOgBhklkYaUpIJ8eQ0iUiJ:2gMWX12LvDyhF87GzUvSCjYD9FOgvsYl
MD5:	8DC95FAB9CF98D02CA8D76E97D3DFF60
SHA1:	FA51AFC9A31F67078FAA9124BEF881655DF4317B
SHA-256:	25F8F00A6FE95DED91A8E33E70154AEE1562760D0D969368D4BAD84BFE85F8D0
SHA-512:	992131CBE01D3DC13831557DD59368B6870BEE453D0C753A5814D001B11327DB60CDEB8D71E4B579E1A5C0238F08E07DF1267CB645738C96197C808E24443A4E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/montserrat/v15/JTURjIg1_i6t8kCHKm45_cJD3gnD-A.woff
Preview:	wOFF.....Z.....@.....GDEF.....G...X.g.^GPOS.....2....yGSUB.....,OS/2...L...O...`S6.Mcmap.....h.cvt ...`...b.....:.Gfpgm.....F...mM$.\|gasp..... ...glyf.....2...[H.xz.head..Q....6...6.<.ehhea..Q.... ...$....hmtx..R.....>....loca..T.....(.J.-maxp..V8... ... .h.Zname..VX.....)!Etpost..WD.....D.z.prep..Z.....K..x.%.... P.....@:D...$..]!....h.....2/.$.....D.^.F..ua.].N....%>./...x...p[I...'=..3[.G._.....WpL..... `.#o.)g9g.....2._=..==._.D@..x.....o....~.....{..)N$.0.Q...M...?..OQ.X..xo.i..Z...s...n".hI.K .%.a...m..U..l.....6...s...6..<...Z....@myrT...q.${....@.Sl1.@.....N/...k=`?...X..3G$.Z.@=^WK.....c..[a..@[hG.T.I...jF...NVqB..V..+....(...7h.^.i.rB.k.`'{.>.W....B..B.n!.W.h.F. '.=a...r.@.....?.j..0...3....."?..s.....d*W.1Ws..\+d.N.....n....[h.V!.6!.....+..._..".h.e.TV.....X%4.Zh.]hf.PO..g#.4~.0.2]*w.u..".....$.....-Q.%4...C....hf>.....6"..A.)S.....dK...N. ..._X.G....3.....*.uA

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\MemMDL2.3.61[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 138820, version 0.0
Category:	downloaded
Size (bytes):	138820
Entropy (8bit):	**7.997585394607156**
Encrypted:	**true**
SSDEEP:	3072:Rebzc+NJTfDpHweyl8w4/icyWp+wT2XwxDBXWB/lG:YzTjDmBdeB2gx4B9G
MD5:	E281F661640D81D30332EF75BEFC001C
SHA1:	369880CB2C0AFAD8B6D4D75CCFC1234C9628908A
SHA-256:	ED8637252D120D9B89BE660ADB8A70ACE29DDA03C0ABB3B351EE32B4F2AEA5DB
SHA-512:	FDC79264709114329F16F192BEB10D62752B18B58BE9EFAFE2452ED7146E4B4B27011F6935E1FD3A46D244C9C1B0B95CE47F563DBEEEF2F13267E41482FC4217
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\MemMDL2.3.61[1].woff	
IE Cache URL:	http://https://support.microsoft.com/socfonts/MemMDL2.3.61.woff
Preview:	wOFF.....D.....OS/2...X...G...`JM..VDMX.....^.qcmap.....v...<.#.Ucvt ... ... ...*....fpgm...@.....Y...gasp...0.....glyf...<.....head.....6...6.. .Jhhea...L.....$.y.khmtx...l...U.....loca.....<.W..maxp...D... ... ...Zname...d...@.....5q.post..... .Q.wprep.....x...x.c`..c.....:....Q.B3_dHc..`e.bdb... .`@..`.....`>.d. .c.....x...S....._..m.m.m.m.m;e..y.~.....<p..a.0t.&...a.pa.0B.1..F...Q.ha.0F.3....q.xa.0A.0L.&...l.da.0E.2L....i.ta.0C.1..f...Y.la.0G.3....y.\|a..@X0,.....E.ba.DX2,....e .ra..BX1..V...U.ja..FX3.....u.za..A.0l.6...M.fa.E.2l....m.va..C.1..v...].na..G.3.....}.~a.p@80.....C.a..pD82.....c.q..pB81..N...S.i..pF83.....s.y..pA.0\.....K.e..pE.2\....k.u..pC.1..n...[. m..pG.3.....{.}...@x0<.....G.c...Dx2<....g.s...Bx1..^...W.k...Fx3.....w.{...A.0\|.>...O.g...E.2\|....o.w...C.1..~...._.o..08.....?..0$.....x..w|....O..42..@B..."...A."..H/....#..[.A."..Dz.." .....cwv

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284F D
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/NewErrorPageTemplate.css
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #00 0000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt; ..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\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
Reputation:	low
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:xmpme ta 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...I.....wg.y.[k/

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\SOC-Linkedin[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 24 x 32, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	270
Entropy (8bit):	6.518823700284674
Encrypted:	false
SSDEEP:	6:6v/lhPktaIgpXpnZwaqY3Re8+Rvkc0wjm4ON0v20YnU//jp:6v/7Mta/pXpZwaj3IrXO0vTqUN
MD5:	A7BBC240D563DB6D4F2211B9BB6D0E47
SHA1:	3FBDF9C7B2378BC706013B52B355BF13346448A8
SHA-256:	292C4CABD66C25753CE8BBFA1E8A32B47703AB1F809670B056D5B59CFCAF5FB8
SHA-512:	693CBC364F42C1E1C75672FB84FE6A26B31A418F67ADDA732264550FB1B4E807DB8D6B33B6BB345A11B324CD253895653396324C29EE034CC8C78E77D3996B1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\SOC-Linkedin[1].png	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://support.microsoft.com/SocImages/SOC-Linkedin.png
Preview:	.PNG.....IHDR..... .....?.H....BPLTE...w..|||...y{{{||y|||||z}}www|}}.....PF.7....tRNS.@.0...p 6&.:...qIDAT(.....0.E.8.{.....ju!H..z.-.@..2UFMz.a5H....p.'.....XI...?g8...^.A...3X.h..P...GT..].s...:...j.@....n.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\ZillaSlab-Bold.be1d6507cb98[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 108128, version 1.1
Category:	downloaded
Size (bytes):	108128
Entropy (8bit):	**7.994466739430887**
Encrypted:	**true**
SSDEEP:	1536:jlGmG1DcfADiB43gui3M2YvPyek7Q/+zknjz+SUsLch8Nv4Mw3tOM57wQZwYbOYA:5xkAnBDu4pOeipjNhcCwdv7TKYb5A
MD5:	BE1D6507CB984AC565CBB9AD960EB579
SHA1:	DA6E88C0946C6CF93EBD8CFB7399006BB75919BE
SHA-256:	BB2EF9AE78E41A588A8AD808AF0ED209D3A1B521B33509F14A77CF95042AA690
SHA-512:	1878E20B8E09ADD659C28B721A14FC371F584332F6C1FC033FF8F6A8A68D99D28C626F4A11D34B879202EDD6798C719FB692EC42FCDB1A526330467C903B80E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static-media-prod-cdn.itsre-sumo.mozilla.net/static/protocol/fonts/ZillaSlab-Bold.be1d6507cb98.woff
Preview:	wOFF.....`.....8.....FFTM...D.....~@..GDEF..l....>...B...NGPOS.....%.....6E..GSUB..m0...O...,G;%.OS/2.....O...`MEk.cmap.....a.....@r.cvt .....{....0...fpgm..l...p...mM$.\|gasp..l.....glyf.....6W...iH.head.....6...6..9Vhhea.....!...$...Xhmtx...`.....n.loca.....0maxp..... ... ....name..V....?...S...[post..YT.....16.0 .prep..U.....B...]_.<.....U.....?eG.j.....x.c`d``.....Y<{..".E.....L.....#.@.*.....J.\.....`.U....x.c`a.c.....B3.e0b....00..`|R.....2(0(.fa....p.y.#..0.$.x.l.....1C...x..{pUW....I ...7..$.7.M...<"..`.@H.P.B.2.R.*....g.W.*..N....;.::.T.....u..>l..S..l.....o...&.22.....>g..^.[k.k..N.....2C.7;...T.9.F{R.....J.:.L].9.j.G.zY..P.^W...5KX.Ol[.....g.Uc.x...l..mL5...L.[.N.f..WU..*..r....?E.....}..2.!..P.....;..^...y..M.v.J..4..*.;!..(.~..R%&.e..!..s.f.....K.7.....*5.1w-:>."{..._i...l...*.x[.{.{NQ.].l.`..*3O..~..Q.6O..'.|[..sB.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\ZillaSlab-Regular.f7120c75de27[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 107784, version 1.1
Category:	downloaded
Size (bytes):	107784
Entropy (8bit):	**7.994285133692478**
Encrypted:	**true**
SSDEEP:	3072:SeU+kHNhQyI0O5l1qjTwErO5uBnA2Nx1wrdUoPJ:hU3thQdb5l1EbllINxyrxJ
MD5:	F7120C75DE27AFA908563DBF4B373105
SHA1:	FA2D9490230B4FEABE627BB0D09E90ABA465E8FF
SHA-256:	9F411B15BDB1D655112BF750C940A97BB478FAB857BE8506D7436A020ECA86D4
SHA-512:	3788C42DFA81A6574FBC2EFA8D4E2F7B2E99F112BAC44F4253D57812C5DEC45D51C63ED1671ACF78C1BEB0867A765954DE3A63225004688A0E8D255D90D05C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static-media-prod-cdn.itsre-sumo.mozilla.net/static/protocol/fonts/ZillaSlab-Regular.f7120c75de27.woff
Preview:	wOFF.....FFTM.....~@.OGDEF..nX...>...B...NGPOS.....#.....;.J.GSUB..n....O...,G;%.OS/2.....P...`L.l.cmap...(...a.....@r.cvt .....{.....X.Bfpgm..p...mM$.\|gasp..nP.....glyf.....7....\|X...head.....6...6..9.hhea.....!...$...]hmtx...`.....!..loca...4.....!.maxp..... ... .name..W....8...n.f.spost..Z.....16.5$.prep.....U.....B...._.<.....C.....?e..p.....s.....x.c`d``.....<{..".E.....W.....#.@.*.....J.\.....`.p....x.c`aRb.....B3.e0b....00..`\|R.....280(.fa....p.y.#....l...^.Y..<. ...x..)l...n..Z^.JK..[{.}....tv...k)cXE...P.M.{...ed.,...Y...a"..L..b\|..... .1t.a..3..>....Z&..e$_....9.9.y.....L.....W..T.]..9.&....)5...d.\.5..h.S.^V.....WQ{..7...j2..(.J.m....bMwc..|....2.v....m..n...G.?.\.....(n:.K.d.....g..I..y|;.....f.V..(....<...c.$....]...!.#.....y.{...9.....Q...I.L....x.....`.Jm..Z...S6vb..j~.:.8.6+.\.X{Y..*.$4..S5v...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\apd-sasskit.built[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	43882
Entropy (8bit):	5.16372272402054
Encrypted:	false
SSDEEP:	192:SLkSFanIWTRhvy5Ag2AvJUE6x7N1tArJhAcSsnI+0O4lJlMdCzDlMPzFlz3UzDz6:SBF1pmJ+HnmTdSnsLYd+EatYzB+C
MD5:	F8FE0687F70C4CB587A78B60873660DD
SHA1:	1C4D59365C8425ED964408EA435AC7F2256C817B
SHA-256:	F9CD784510AF9F7546E63D83DC764B011A845E126A08EC3CC5B654E709007106
SHA-512:	697310FAD074B22ABC4C39F38367D203A07D9F27844AEF9F85B24F6F438FD45CBEEC97A509638D6E922D446050FC7AA92857059C1F39F0F1EE49540DEAF41BD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://support.apple.com/clientside/build/apd-sasskit.built.css

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\apd-sasskit.built[1].css	
Preview:	/* version information. * ip_sasskit_version:1.2.25. * ip_sasskit_override_version:^1.0.37. */..Alert+.Alert,li p.Caution,li p.Important,li p.Note,li p.Notice,li p.Tip{margin-top:.75em}.TaskBody .Alert,div.note{margin-top:.75em;margin-bottom:.75em}p.Caution,p.Warning{margin-bottom:.75em}.yNote{font-style:italic;font-weight:700}ul+.Alert{margin-left:0}[dir=rtl] ul+.Alert{margin-left:0;margin-right:0}.Alert+p{margin-top:.8em}code{font-family:'SF Mono',monospace;overflow-wrap:break-word}td code,th code{padding-top:.05em}.CodeLine,.CodeLines{display:block;font-weight:400;white-space:pre-wrap;word-break:break-word;overflow:hidden;text-overflow:ellipsis}.CodeLines>.CodeLine{margin-top:.25em;margin-bottom:.25em}[dir=rtl] .CodeLines{text-align:left}.Copyright{padding-bottom:2em}.Copyright h1{display:none}.Copyright p:nth-of-type(1){margin-bottom:.1em}.Copyright p:nth-of-type(2){margin-top:.1em}.Copyright p{font-size:.823em;letter-spacing:-.016em}.HIStrings{margin-top:1.25em;margin-bottom:.25em

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\app-apd-route[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	117635
Entropy (8bit):	5.237686872406396
Encrypted:	false
SSDEEP:	1536:1NG/f8X2uVcgbl+o8qZTX8D3u0XLWrm7AtJtkJX9lvxH/TDcwr:1NG/fhuVhh8q0uHK7AtJtkhvxH/TDcwr
MD5:	AB328C457F9CE8CBF70D695539E41550
SHA1:	A108BB56B5947E66242899A24E6E23303A291959
SHA-256:	47D3A401060E91A6F3465777BE2F94F3FB24754893437145486D079FB51CD9F9
SHA-512:	C0B4B7BE13A2423B8A22F23CD974978B54F693C45414767F128ABACBFFA3F8918316986AABD4BE9C3782924084737B911ACC4430D239DE9E34CB567FBF1E13B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://support.apple.com/clientside/build/app-apd-route.js
Preview:	!function(e){var t={};function n(r){if(t[r])return t[r].exports;var o=t[r]={i:r,l:!1,exports:{}};return e[r].call(o.exports,o,o.exports,n),o.l=!0,o.exports}n.m=e,n.c=t,n.d=function(e,t,r){n.o(e,t)||Object.defineProperty(e,t,{configurable:!1,enumerable:!0,get:r})},n.r=function(e){Object.defineProperty(e,"__esModule",{value:!0})},n.n=function(e){var t=e&&e.__esModule?function(){return e.default}:function(){return e};return n.d(t,"a",t),t},n.o=function(e,t){return Object.prototype.hasOwnProperty.call(e,t)},n.p="",n(n.s=213)}([function(e,t){var n=e.exports="undefined"!=typeof window&&window.Math==Math?window:"undefined"!=typeof self&&self.Math==Math?self:Function("return this")();"number"==typeof __g&&(__g=n)},function(e,t,n){var r=n(38)("wks"),o=n(37),i=n(0).Symbol,s="function"==typeof i;(e.exports=function(e){return r[e]||(r[e]=s&&i[e]||(s?i:o)("Symbol."+e))}).store=r},function(e,t){var n=e.exports={version:"2.6.12"};"number"==typeof __e&&(__e=n)},function(e,t,n){var r=n(7);e.exports=fun

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\app-apd[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	388434
Entropy (8bit):	5.364204910111986
Encrypted:	false
SSDEEP:	6144:e4EO6ilBx/MPAzil9Bx/laF/ilBx/mg6E4kfv7RqTIuSkfv7Rv2Phkfv7RquYf8v:L
MD5:	23ADEDCB0B3C1A2DB8CB26ADB502F87B
SHA1:	71446BFDD7170F08D55E0AF9AC0403795269BC27
SHA-256:	301FE82BCAC63F4DFABE3090C4278A1854512D257CAA771305DE282358C508B2
SHA-512:	21FBCDE22BB9148BF7A0A9E01601B34AAFB9A70430D12203C6D5D5A6E1A2EC65126E879EA6AA34DEAB846BA86593B3BACD7CD0407F2BCA17E78391C1EFF9E0E0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://support.apple.com/clientside/build/app-apd.css
Preview:	html{-ms-text-size-adjust:100%;-webkit-text-size-adjust:100%}abbr,blockquote,body,button,dd,dl,dt,fieldset,figure,form,h1,h2,h3,h4,h5,h6,hgroup,input,legend,li,ol,p,pre,ul{margin:0;padding:0}address,caption,code,figcaption,pre,th{font-size:1em;font-weight:400;font-style:normal}fieldset,iframe,img{border:0}caption,th{text-align:left}table{border-collapse:collapse;border-spacing:0}article,aside,details,figcaption,figure,footer,header,hgroup,main,nav,section,summary{display:block}audio,canvas,progress,video{display:inline-block;vertical-align:baseline}button{background:none;border:0;box-sizing:content-box;color:inherit;cursor:pointer;font:inherit;line-height:inherit;overflow:visible;vertical-align:inherit}button:disabled{cursor:default}:focus{outline:3px solid #c1e0fe;outline:3px solid rgba(131,192,253,.5);outline-offset:1px}:focus[data-focus-method=mouse]:not(input):not(textarea):not(select),:focus[data-focus-method=touch]:not(input):not(textarea):not(select){outline:none}::-moz-focus-in

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\appleicons_thin[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 1040, version 1.0
Category:	downloaded
Size (bytes):	1040
Entropy (8bit):	6.981832609619338
Encrypted:	false
SSDEEP:	24:c2gNIj4AR4VlrSoCQSqHq47Q0N+NT+OOswJeY4J:cIUAR4hbpSqK47QHN9OLgY4J
MD5:	8A25E23850903182FB6FFED7F3E8995C
SHA1:	5F3431C0955717B0FDCCA1561B0BCCC27993FA31
SHA-256:	4E2F6F8E72625B9FD0527439AE9CBD4BA2A64ECC7C0E7788BD959BECC99BE7C2
SHA-512:	5775DCB9341124453E2E98C1CD050B06BC1DD7657FCEBF075067BD713EE6F077DA5C28409CF621699C1708E2F7943609ED58001B5EDF06D91020DE539A5E0A9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.apple.com/ac/globalfooter/3/en_GB/assets/ac-footer/legacy/appleicons_thin.woff

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\appleicons_thin[1].woff	
Preview:	wOFF.....p.....GSUB.....3...B....OS/2...<...C...VM.Nvcmap.....P...~.C..glyf.....I...XC.<head.....0...6....hhea...L.....$...Lhmtx...l.....loca...x..... ..,maxp..... ....name.....=...j....post.....D.k\|.x.c`d``.b.c.a`tq..a.``a....cNfz"P.....i. f.....#.O.x.c`d..8.....s7...V...`.....X.....4.....?.{.P...Q.(.....I....x....0....@.AA.0T...$o.1x.N.. +....%.....Z-...s.....2auO7i..>...OE}..M...x.c`d`...1.....mFU....Y...m..^.Q.Q...P..s2.s2.3.....7.Z..T.....x.c`d``.b.y.\..m.2p...E...$."....c..\..&.(.....x.c`d``....C.c...0.002..f.rU..... ..h...h.....,x.c`d```f`c....L@.....\|...H.!.x...MJ.@....OlA..e.."....q..\t.mI.I....i..O.I<.'.....&.*.;...{.....\|!@u.\...p...;.....x.....^=.p..7..K.!.=.p...m.O.....o....0.{.#..=.....2K.*Wn.....6l #..-3..$.7*.....I....T.V.b...y...z/...3..(.>Lt....C"C....+8.+,.8.....[....L.b|ffA..Nb.5..`...:..S.h..y.....=MB.rw5e0..6...../.kvX...x.c`b...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\appleicons_ultralight[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 1040, version 1.0
Category:	downloaded
Size (bytes):	1040
Entropy (8bit):	7.003951327615274
Encrypted:	false
SSDEEP:	24:c2EN9H0A4AR4VlrSoBbkgc/0BQJS1kUadAJ/Rwlk5ooqBl:sN9UhAR4hbVkdcBQs1UDI+6l
MD5:	3C9A9A14C68BB979669D2303FEC97AF9
SHA1:	6136F4FD4DC9263938E21439C095248F9E94949C
SHA-256:	17AE1B26C878CAB5A8F0C8FE383995624BDAE60C6DF54CCFD0A302DAA0449392
SHA-512:	1665AF0C43562DD390E271B65D71BF3ABD5DD9252790681DA27D58F6CB45460BB880FEB58D2547EA825063DC5C1C0EE2BF29376CBC64DAB55FE25F04447B994
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.apple.com/ac/globalfooter/3/en_GB/assets/ac-footer/legacy/appleicons_ultralight.woff
Preview:	wOFF.....GSUB.....3...B....OS/2...<...C...VM.Nvcmap.....P...~.C..glyf.....H...T.k..head.....0...6....hhea...H.....$...Lhmtx...h.....loca...t..... ...*maxp...\|..... ....name.....C.....2u.post.....D.k\|.x.c`d``.b.c.a`tq..a.``a....cNfz"P.....i. f.....#.O.x.c`d..8.....s7...V...`.....X.....4.....?.{.P...Q.(.....I....x....0....@.AA.0T. ..$o.1x.N..+....%.....Z-...s.....2auO7i..>...OE}..M...x.c`d`.....Q.....mFU....%%....x.....P....s2j2.....(..9B).X...x.c`d``..M*_....|e.f...0\.HvE...3.3u....L Q.7B..x.c`d``....C.c... 0.302..f.q^.....h...h.....*x.c`d```f`c....L@.....|...H.!.x...=n.0..._...RU.j...:P)|.. .e`E!8!.-. q..ga..z.>.....X?....)....".W.g..W.w<].Mz..!O.w1@..G.#p.....O6D.{*C|.n.....w0.z..x.. {..},#.x.....d..Y..*..[.b.R{.*..mJ].I<...e-m..F...9.S.r.[].D.N*...z'3.o.3..(.z...).GA.D....V.Sq.t...[.....I.s..Kf,....h..?...}G...k..7803.....>.M.)...h*.{;*...7;.3.8..|....N....x.c`b...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\cesis_icons[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	69369
Entropy (8bit):	4.718010151601473
Encrypted:	false
SSDEEP:	768:sHCKxeWS5KEvnwFYTsvCPvVnwtvuvAi3E5BAqwP+BiPrj74E8D:siKxebKGwFYYvCVwtvuvE5CqwPf74E8D
MD5:	F9D86A03FD6EE819B58962FA80B958F0
SHA1:	9BCD8F8D16A43C1986C8F7187AEF7B281D551855
SHA-256:	8FE444B84E3551DE4ADDD1260D27117A520B18E0F29B6B10A12CE9E6788E1192
SHA-512:	D3B0ECBC5C9F7B15D3A65AECF9D8E4B6F1A0F5AEDCCFE709275D67E7BEEB030D77D091668BBDB77F58E5AE55B1AF6A84EF83FA03CD1F3B7A088CB7213A73 12F2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.digitalcontrolroom.com/wp-content/themes/cesis/includes/fonts/cesis_icons/cesis_icons.css?ver=5.7.1
Preview:	@font-face {. font-family: 'tticons';. src: url('fonts/tticons.eot?7siik9');. src: url('fonts/tticons.eot?7siik9#iefix') format('embedded-opentype'),. url('fonts/tticons.ttf?7siik9') format('truetype'),. url('fonts/tticons.woff?7siik9') format('woff'),. url('fonts/tticons.svg?7siik9#tticons') format('svg');. font-weight: normal;. font-style: normal;.}...fa,[clas s*="fa-"] {. /* use !important to prevent issues with browser extensions that change fonts */. font-family: 'tticons' !important;. speak: none;. font-style: normal;. font-weig ht: normal;. font-variant: normal;. text-transform: none;. line-height: 1;.. /* Better Font Rendering ========== */. -webkit-font-smoothing: antialiased;. -moz-osx-font-smoothing: grayscale;.}...fa-bbpress:before {. content: "\eb54";.}..fa-buddies:before {. content: "\eb55";.}..fa-archive3:before {. content: "\eb56";.}..fa-footer:before {. content: "\eb57";.}..fa-general-setting:before {. content: "\eb58";.}..fa-header2:befo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\clientlib-site-min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	346938
Entropy (8bit):	5.290181993916704
Encrypted:	false
SSDEEP:	3072:a4NQOwPnbopJrqUFIg/0u7hQS2vMzgXZNHEb0I6ayyx5oHsfMKNkBda:PNQJMpJSgRn2LXTo6Xyx2HTB4
MD5:	7B3A0C428213B7337B45B058280C0384
SHA1:	57583F9C18A59EAF367E8D814C4E0BFA9F773EB4
SHA-256:	BC9C0165E4DD39F2D747B6F0083A35E321D51CF7366D004BC77B0985EF94FA65
SHA-512:	2EDCF6EDC8B06CC83A044FFC1AFA0F2D53D3A2395FA43A388F4795953463FBF6B6B04E6A428DBA1AD4BF0C151FDB3410A00EED9E1B1CBA9EA49E78E31B785 DB9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cookienotice.astrazeneca.com/etc.clientlibs/od-client/clientlibs/clientlib-site-min.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\clientlib-site-min[1].js	
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([[49],[function(t,e,n){var r;../*!. * jQuery JavaScript Library v3.5.1. * https://jquery.com/. *. * Includes Sizzle.js. * https://sizzlejs.com/. *. * Copyright JS Foundation and other contributors. * Released under the MIT license. * https://jquery.org/license. *. * Date: 2020-05-04T22:49Z. */!function(e,n){"use strict";"object"==typeof t.exports?t.exports=e.document?n(e,!0):function(t){if(!t.document)throw new Error("jQuery requires a window with a document");return n(t)}:n(e)}("undefined"!=typeof window?window:this,(function(n,i){"use strict";var o=[],a=Object.getPrototypeOf,u=o.slice,s=o.flat?function(t){return o.flat.call(t)}:function(t){return o.concat.apply([],t)},c=o.push,l=o.indexOf,f={},p=f.toString,h=f.hasOwnProperty,d=h.toString,v=d.call(Object),g={},y=function(t){return"function"==typeof t&&"number"!=typeof t.nodeType},m=function(t){return null!=t&&t===t.window},b=n.document,w={type:!0,src:!0,nonce:!0,noModule:!0};function x

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\close.73e5756fc7ce[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	194
Entropy (8bit):	4.966302415855526
Encrypted:	false
SSDEEP:	6:tnrwdhU3mc4slZs49/nZSKsKMwmqZUR4RR:trwdW3lNxxMwhUqRR
MD5:	086E3A7361E5798C9F26AF60A12A7A7C
SHA1:	32705456D348556666E22E083E1FE772C14743A2
SHA-256:	29C332F8A4A8FBBEAF0A4269789F870EA943E3CA0B5B53BCE39EEBB33E1A23D7
SHA-512:	FD5EE91C8263B3B53AFAAA9F9E1F6A901A48C1AE467B3177C841C728F12E1F0088E0EA7EC2D1FDDB1220D41D247C9018E4880ACCCCD26C41B8531A4544BCCBD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static-media-prod-cdn.itsre-sumo.mozilla.net/static/protocol/img/icons/close.73e5756fc7ce.svg
Preview:	<svg width="24" height="24" xmlns="http://www.w3.org/2000/svg"><g stroke="#000" stroke-width="2" fill="none" fill-rule="evenodd" stroke-linecap="round"><path d="M6 6l12 12M6 18L18 6"/></g></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\common-min.c217f307f53c[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	353739
Entropy (8bit):	5.36436302866219
Encrypted:	false
SSDEEP:	3072:iB0TCG4fcl5P/15jH418qLTW8xRrqSz8zGJ7pda98HrQv+sv+sv+8F7EmflirwcN:i3fcl5P/1lObW8xVdPda98Hr4Rfliko
MD5:	C217F307F53C335B42C033B57E45DDB1
SHA1:	92183E794C3900F530E685BEBF2F78C1C68AA56E
SHA-256:	5658294197C63EF3FD7C835B927C9D1653FFF729A4847FDD96219A42FA7E4252
SHA-512:	C944A0B2FB1354402A2768CB7B37111FA94FB1C6DDA0076177640DB2B89985E65272578D2ED9EB50B57EB6D9736C714C96939AA00B5A59F257B551FBF0C38662
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static-media-prod-cdn.itsre-sumo.mozilla.net/static/build/common-min.c217f307f53c.js
Preview:	if(typeof window.gettext==="undefined"){window.gettext=function(msgid){return msgid}}if(typeof window.ngettext==="undefined"){window.ngettext=function(singular,plural,count){return count===1?singular:plural}}if(typeof window.interpolate==="undefined"){window.interpolate=function(fmt,obj,named){if(named){return fmt.replace(/%\(\w+\)s/g,function(match){return String(obj[match.slice(2,-2)])})}else{return fmt.replace(/%s/g,function(match){return String(obj.shift())})}}}(function(){var root=this;var previousUnderscore=root._;var ArrayProto=Array.prototype,ObjProto=Object.prototype,FuncProto=Function.prototype;var push=ArrayProto.push,slice=ArrayProto.slice,toString=ObjProto.toString,hasOwnProperty=ObjProto.hasOwnProperty;var nativeIsArray=Array.isArray,nativeKeys=Object.keys,nativeBind=FuncProto.bind,nativeCreate=Object.create;var Ctor=function(){};var _=function(obj){if(obj instanceof _)return obj;if(!(this instanceof _))return new _(obj);this._wrapped=obj};if(typeof exports!=="undefined")

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\css2[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	1275
Entropy (8bit):	5.239601406927808
Encrypted:	false
SSDEEP:	24:5uOYGa9SuOY4a9HuOYN0a9htOYGaCObtOY4aCsZ9tOYN0aCO:oO1aJOXaYOpaNO1aCwOXaCsROpaCO
MD5:	CCB8579530AA196CC33A0A927C11818A
SHA1:	201BCC93C41E2563EE64635BA3AA9F3DFEBB40A4
SHA-256:	AD73FA7A50D7FC10AFF9B2EFE85D628C9049DDE81926857DAAEE3145A7D64CA0
SHA-512:	BEE40F8D88D8B71722339B39ACB2D0A68C12E40F05216B4E82A54771541A57A6C6BB426B069084706D12C4DAF876D3B6387BDB5BAE6F7D5D8F5D3BC8D6AD572
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.googleapis.com/css2?family=Raleway:wght@300;500;700&family=Zilla+Slab:wght@300;500;700&display=swap

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\css2[1].css	
Preview:	@font-face {. font-family: 'Raleway';. font-style: normal;. font-weight: 300;. font-display: swap;. src: url(https://fonts.gstatic.com/s/raleway/v19/1Ptxg8zYS_SKggPN4iEgvnHyvveLxVuEooCM.woff) format('woff');.}.@font-face {. font-family: 'Raleway';. font-style: normal;. font-weight: 500;. font-display: swap;. src: url(https://fonts.gstatic.com/s/raleway/v19/1Ptxg8zYS_SKggPN4iEgvnHyvveLxVvoooCM.woff) format('woff');.}.@font-face {. font-family: 'Raleway';. font-style: normal;. font-weight: 700;. font-display: swap;. src: url(https://fonts.gstatic.com/s/raleway/v19/1Ptxg8zYS_SKggPN4iEgvnHyvveLxVs9pYCM.woff) format('woff');.}.@font-face {. font-family: 'Zilla Slab';. font-style: normal;. font-weight: 300;. font-display: swap;. src: url(https://fonts.gstatic.com/s/zillaslab/v6/dFa5ZfeM_74wlPZtksIFYpEY2Hc.woff) format('woff');.}.@font-face {. font-family: 'Zilla Slab';. font-style: normal;. font-weight: 500;. font-display: swap;. src: url(https://fonts.gstatic.com/s/

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\djangojs-min.eba373c6bfad[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	downloaded
Size (bytes):	7202
Entropy (8bit):	5.23689235677338
Encrypted:	false
SSDEEP:	192:h7PGzfm3Bjq4VcGDPDIwOmWCjBUUkJQkS1:9PG63tqGICjGUkJQ1
MD5:	EBA373C6BFAD0962C350912320AB982F
SHA1:	F0B100A7F3DD68CAC9FD70CD16A29739172AEC61
SHA-256:	49B07FE239424CEC99131FF16F295DB8EA630C8D0EFD141553948FDD195C24F3
SHA-512:	90F5E0946FEAB05D15975E3184A7DA280BEE15218E06267C309EDFD130BEAE31F68B0B6A7E39FFEAC094F3F89B57CCC628E5D71F476DC8BFBC8A4F7682901F96
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static-media-prod-cdn.itsre-sumo.mozilla.net/static/jsi18n/en-us/djangojs-min.eba373c6bfad.js
Preview:	(function(globals){var django=globals.django||(globals.django={});django.pluralidx=function(n){var v=n!=1;if(typeof v=="boolean"){return v?1:0}else{return v}};django.catalog=django.catalog||{};var newcatalog={"%(num)s of %(total)s":"%(num)s of %(total)s","%s characters remaining":"%s characters remaining","1m":"1m","1y":"1y","3m":"3m","6m":"6m","Draft has been saved on: %s":"Draft has been saved on: %s","Draft is saving...":"Draft is saving...","Error saving draft":"Error saving draft","A document with this slug already exists in this locale.":"A document with this slug already exists in this locale.","A document with this title already exists in this locale.":"A document with this title already exists in this locale.","All:"All","All Articles: % Localized":"All Articles: % Localized","All Products":"All Products","An error occured.":"An error occured.","An

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/down.png
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~.....b.....$..s...7tRNS.a.o(,.s....e.....q*.....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\fontawesome-webfont[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), FontAwesome family
Category:	downloaded
Size (bytes):	70807
Entropy (8bit):	7.985254784033384
Encrypted:	false
SSDEEP:	1536:/PEOVdNaSNYXdU47Z67/Ry+YcWqlr7pq:UidIYYNUssAqlrg
MD5:	32400F4E08932A94D8BFD2422702C446
SHA1:	986EED8DCA049714E43EEEBCB3932741A4BEC76D
SHA-256:	E219ECE8F4D3E4AC455EF31CD3A7C7B5057EA68A109937FC26B03C6E99EE9322
SHA-512:	47F19282F19CFC7A40A31C6AF428F100C7011167858B46B415556FD9B65D48DA2783DC22B101A6A89D95B05CBCEE625652C87D421A83D40AC7482C2B0B3D86A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.digitalcontrolroom.com/wp-content/themes/cesis/admin/redux-extensions/extensions/dev_iconselect/dev_iconselect/include/fontawesome/fonts/fontawesome-webfont.eot?

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\fontawesome-webfont[1].eot	
Preview:	.....LP.....j..^.....F.o.n.t.A.w.e.s.o.m.e.....R.e.g.u.l.a.r...$.V.e.r.s.i.o.n. .4...4...1. .2.0.1.5...&.F.o.n.t.A.w.e.s.o.m.e. .R.e.g.u.l.a.r..... BSGP.....Y.D.M.F..x...>.....)[..1.H..-A)F...1.f.i..).U.'.&a.n;c)2nb$.'3..JV.@....y.|.....[....\A.X.FCp....-B.....V....U_^d.V/.....Hv..s.rx9..*c.N%]72F.b.-. $}3..*>q5N6.d.{*...q%}.B.H$.....Mx..{....2..}...d..!..... .C.._....u....g...K...~..E...y:.G*#.Ot..5ap.....O.....).....?HV.C..i...`.@'....@.....8..(..P..@..Ee.f.6..aG....u..?e$k.DYy..C..6 ...$FLf.....V.2v..Ukl..I...&..\..[/*.d.!.. .l 1..D. .X....CH?.d.....}....XB.s..H.'_.....5 .D....3....P.jmx.. ..@.....v..{.KI..J.V.4..p.%..Q..H,... .L..|.....9...@._.NS%...3h....G|E..H o.Fz.... .k._v.2&.....Z....I.\;.2H.!.#.nR5Q...>YT..!.~..J.Zf.<s.3K7...R//a@....s.#.2'19...y../+q.T.,f..O.._.....q.....h..BX.R)<....&m.....(...Nf.....B.[.x.3...x

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\icon_large[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1712
Entropy (8bit):	4.445883952550553
Encrypted:	false
SSDEEP:	24:tVLw95AFheDDKiEvdClGVox+heXiQ7X27LLEHy9bKa6/ccXDlD5kPrAQO1T7OlQ5:La5TDOdbVoiP6G6yBGhXHkDAQO1O+3
MD5:	FC0FE7DFE16BD2F9A53B1E4B99B76D05
SHA1:	42868DC2DBC849CFA1C289E398945FC0F5BCB0A3
SHA-256:	10CEBC15528E6215228F07B16CE3E388E6FF87A77028F4EB2178A5AA8E0AEE6D
SHA-512:	888D06FFA7393AB55268F07C1AFC2EF07A9049B350403915F05A45F9C4B22A527CAA9988E3B6B2E01161EF8157B8A1DCE271E095FB4BD4F97925DA2D9255632F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.apple.com/ac/globalfooter/3/en_GB/assets/ac-footer/breadcrumbs/apple/icon_large.svg
Preview:	<svg version="1.1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" width="14px" height="36px" viewBox="0 0 14 36" xml:space="preserve">..<defs>...<symbol id="apple">....<path d="M4.02,15.73c-0.25-0.16-0.51-0.39-0.77-0.71c-0.18-0.21-0.4-0.51-0.66-0.9c-0.45-0.65-0.82-1.4-1.1-2.25c-0.31-0.93-0.46-1.82-0.46-2.69c0-0.97,0.21-1.82,0.62-2.53C1.97,6.08,2.4,5.63,2.95,5.3C3.5,4.96,4.08,4.79,4.71,4.78c0.22,0,0.45,0.03,0.7,0.09C5.59,4.92,5.81,5,6.07,5.1c0.34,0.13,0.53,0.21,0.59,0.23c0.2,0.07,0.37,0.1,0.5,0.1c0.1,0,0.24-0.03,0.4-0.08c0.09-0.03,0.26-0.09,0.5-0.19C8.3,5.07,8.49,5,8.64,4.94c0.23-0.07,0.45-0.13,0.65-0.16C9.53,4.74,9.77,4.73,10,4.75c0.44,0.03,0.84,0.12,1.2,0.26c0.63,0.25,1.14,0.65,1.52,1.21c-0.16,0.1-0.31,0.21-0.45,0.34c-0.31,0.28-0.57,0.59-0.76,0.93c-0.27,0.48-0.4,1.01-0.4,1.56c0.01,0.67,0.18,1.26,0.52,1.77c0.24,0.37,0.56,0.69,0.95,0.95c0.19,0.13,0.36,0.22,0.52,0.28c-0.08,0.26-0.17,0.49-0.25,0.68c-0.22,0.52-0.48,0.99-0.77,1.43c-0.27,0.39-0.48,0.68-0.64,0.8

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\icon_large[2].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	267
Entropy (8bit):	5.214543468604978
Encrypted:	false
SSDEEP:	6:tIVYmc4slZKYnic4sG0nN0dlSTIccoLLyJVLc4KlBM:tV/KY7NklQl8LLyJVLzKTM
MD5:	42B9BA998E98814796D92163692CE747
SHA1:	316381460376ED45E7E8E5C159A9C6571E322258
SHA-256:	63BD44999BFEF2A50E8A7DE4BA86097AB78722AA8A6E4B1EC3E94E9CE69CD35B
SHA-512:	BCE933D885DE898F9487DEADF45A10F41BCB9F404D32F8F27652FA0FE2BE9EA908720DFB037313E25970AD1EE01E03922BD11E00431F8222F4CDBC1364E98F3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.apple.com/ac/globalfooter/3/en_GB/assets/ac-footer/breadcrumbs/separator/icon_large.svg
Preview:	<svg version="1.1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" width="8px" height="18px" viewBox="0 0 8 18" xml:space="preserve">..<path d="M1.29,0.98L7.5,9l-6.21,8.01l-0.68-0.54L6.42,9l-5.8-7.49L1.29,0.98z" fill="#d6d6d6" />.</svg>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\image_large[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	802
Entropy (8bit):	4.424093323511906
Encrypted:	false
SSDEEP:	24:t4hMViEmTYEo+y+csJtbCKZRXJE9bETa6uP+Koh:TITTyKJlUcuP+V
MD5:	A3434749345009DA205AC0E848654E85
SHA1:	615DEC701544BD85F757B20719B5AD881FBA64FC
SHA-256:	81849741DC42D40B8338A222866C5009893103EFB5BDC4101D0AE5CA4D6E1375
SHA-512:	8C517EED042331F74F55152164A348DEBE604790B8220393C501524E7EAF94245BD737C23B2B94C26D1B86B20D1621C22675DF6FD524608EF910C9026E85DD91
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.apple.com/ac/globalnav/5/en_GB/images/globalnav/links/mac/image_large.svg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\image_large[1].svg	
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="26" height="44" viewBox="0 0 26 44"><path d="M8.7 27v-7.53h-.08L5.5 26.93H4.47l-3.11-7.46h-.09V27H.12v-9.86h1.43l3.38 8.16h.11l3.38-8.16h1.43V27H8.7zm6.12-7.49c-1.57 0-2.73.78-2.89 1.96h1.19c.16-.58.78-.92 1.66-.92 1.1 0 1.67.5 1.67 1.41v.67l-2.13.13c-1.72.1-2.69.86-2.69 2.18 0 1.35 1.06 2.19 2.49 2.19.98 0 1.79-.43 2.27-1.22h.11V27h1.12v-5.04c0-1.53-1-2.45-2.8-2.45zm1.63 4.75c0 1.05-.9 1.85-2.11 1.85-.85 0-1.49-.44-1.49-1.19 0-.74.49-1.13 1.61-1.2l1.98-.13v.67zm8.11-2.37c-.19-.73-.84-1.33-1.9-1.33-1.33 0-2.16 1.06-2.16 2.73 0 1.7.85 2.78 2.16 2.78.99 0 1.68-.46 1.9-1.29h1.19c-.21 1.35-1.31 2.35-3.08 2.35-2.06 0-3.38-1.5-3.38-3.84 0-2.3 1.31-3.79 3.38-3.79 1.79 0 2.88 1.07 3.09 2.39h-1.2z" fill="#fff"/><path fill="none" d="M0 0h26v44H0z"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\image_large[2].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	264
Entropy (8bit):	5.058343997562709
Encrypted:	false
SSDEEP:	6:tI9mc4slzuX8UER4nhHURqadqWKHFpKmhOv6ASfmhN:t4IX8Rqn/vWMFp7hOvDow
MD5:	EE95A18FD56763A31ACA1D504802E089
SHA1:	ACA3406918FFE464B3ADC4F857B81FD66D40690D
SHA-256:	8B25224A4527ED4EFEE23B222227FE0F00F1EF2ECFC3A64D0D55F9BA8A77D06B
SHA-512:	C2404EFD5279333B478AAB3D4142A754DBB8FA5C0B40041411907749ACD9F95DA226ECA5B5AC6D2D0A6851AA93A331CF977FC2280FE18F560472E59D9F3C52AA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.apple.com/ac/globalnav/5/en_GB/images/globalnav/links/tv/image_large.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="18" height="44" viewBox="0 0 18 44"><path d="M3.65 27v-8.76H.47v-1.11h7.59v1.11H4.88V27H3.65zm9.02 0l-3.64-9.86h1.29l2.9 8.27h.11l2.9-8.27h1.29L13.89 27h-1.22z" fill="#fff"/><path fill="none" d="M0 0h18v44H0z"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\image_large[3].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1082
Entropy (8bit):	4.270480682935068
Encrypted:	false
SSDEEP:	24:t4PM/iEtPCL4iCtYd94vbvtH/SU2utETa6uP+KoFR:ZKxL4htUIbvtHuqcuP+D
MD5:	9C937381351FBDEF4480586B6AF7715E
SHA1:	444F95D791FA40BB4888663F3B2AA18089D53A97
SHA-256:	16E30F5480BC1DD538AD90AB859CDA8A78BADB4C3E9DDC3DFB5A5B6A358091E4
SHA-512:	5DF70F21A263CB809199575B1F0F461469DE81D8C7C37CB6733C295436B63A09AF16CABACB4564AFFB1571DEFE1883858193E9797E9252E0C646402A2E602142
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.apple.com/ac/globalnav/5/en_GB/images/globalnav/links/music/image_large.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="37" height="44" viewBox="0 0 37 44"><path d="M8.7 27v-7.53h-.08L5.5 26.93H4.47l-3.11-7.46h-.09V27H.12v-9.86h1.43l3.38 8.16h.11l3.38-8.16h1.43V27H8.7zm9.33.01h-1.12v-1.16h-.11c-.37.82-1.16 1.29-2.28 1.29-1.65 0-2.52-.98-2.52-2.73v-4.77h1.18v4.48c0 1.33.49 1.94 1.67 1.94 1.3 0 2.01-.77 2.01-2.06v-4.36h1.18v7.37zm4.65-7.5c1.54 0 2.62.77 2.78 1.98H24.3c-.16-.59-.73-.98-1.62-.98-.88 0-1.56.44-1.56 1.1 0 .51.41.82 1.28 1.03l1.13.27c1.39.33 2.06.94 2.06 2 0 1.32-1.28 2.23-2.95 2.23-1.64 0-2.77-.79-2.9-2.01h1.21c.2.62.79 1.02 1.73 1.02.99 0 1.7-.47 1.7-1.15 0-.51-.38-.85-1.17-1.04l-1.26-.31c-1.38-.33-2.01-.93-2.01-2 0-1.22 1.18-2.14 2.74-2.14zm4.41-2.2c0-.45.37-.82.82-.82s.82.37.82.82-.37.82-.82.82-.82-.37-.82-.82.37-.82.82-.82zm.23 2.32h1.18V27h-1.18v-7.37zm8.19 2.26c-.19-.73-.84-1.33-1.9-1.33-1.33 0-2.16 1.06-2.16 2.73 0 1.7.85 2.78 2.16 2.78.99 0 1.68-.46 1.9-1.29h1.19c-.21 1.35-1.31 2.35-3.08 2.35-2.06 0-3.38-1.5-3.38-3.84 0-2.3 1.31-3.79 3.38-3.79 1.79 0 2</svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\image_large[4].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1661
Entropy (8bit):	4.098060898847938
Encrypted:	false
SSDEEP:	48:0pUhvYFSFydL4hnjmbDdrjPmDdPNP3D3/VKPq4X:aUhvYEFl44OBxPWXX
MD5:	52A5A165C8306386B352AC17162DFA27
SHA1:	D6E74D86852625275E44FCD469626EEF00A5B847
SHA-256:	DB645E8610C56A69BE65CF9CF0CEEBBB20BC505F1B91661B1617F8F7F26DBFC9
SHA-512:	2115F83288C02EF55BC7CC32CC543009425B7A6A9D854D0276E3F23ACB40FAA511151AFDACFCA5E71BF2CEE5ED030411A2262FBA050F2C700BB54A0AA2E401ED
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.apple.com/ac/globalnav/5/en_GB/images/globalnav/links/support/image_large.svg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\image_large[4].svg	
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="52" height="44" viewBox="0 0 52 44"><path d="M1.76 24.42c.15 1.03 1.13 1.69 2.54 1.69 1.33 0 2.3-.72 2.3-1.7 0-.84-.62-1.37-1.98-1.72l-1.26-.33C1.58 21.91.8 21.1.8 19.7c0-1.67 1.4-2.81 3.49-2.81 1.91 0 3.33 1.13 3.43 2.73H6.49c-.17-1.01-1-1.61-2.24-1.61-1.31 0-2.18.66-2.18 1.65 0 .77.54 1.22 1.9 1.57l1.03.28c2.04.51 2.86 1.31 2.86 2.75 0 1.81-1.43 2.97-3.68 2.97-2.09 0-3.53-1.11-3.66-2.81h1.24zM15.58 27h-1.12v-1.16h-.11c-.37.82-1.16 1.29-2.28 1.29-1.65 0-2.52-.98-2.52-2.73v-4.77h1.18v4.48c0 1.33.49 1.94 1.67 1.94 1.3 0 2.01-.77 2.01-2.06v-4.36h1.18V27zm8.76-3.68c0 2.3-1.22 3.81-3.1 3.81-1.05 0-1.9-.46-2.3-1.24h-.11v3.57h-1.18v-9.83h1.12v1.23h.11c.47-.85 1.35-1.36 2.36-1.36 1.88 0 3.1 1.5 3.1 3.82zm-1.22 0c0-1.72-.81-2.75-2.15-2.75-1.33 0-2.17 1.06-2.17 2.75s.84 2.75 2.17 2.75c1.35 0 2.15-1.03 2.15-2.75zm9.61 0c0 2.3-1.22 3.81-3.1 3.81-1.05 0-1.9-.46-2.3-1.24h-.11v3.57h-1.18v-9.83h1.12v1.23h.11c.47-.85 1.35-1.36 2.36-1.36 1.89 0 3.1 1.5 3.1 3.1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\image_large[5].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1002
Entropy (8bit):	4.282770840470481
Encrypted:	false
SSDEEP:	24:t4stMgF3Hlpl+AtPEO2NUQv2U61yh19j53dzT5voq:pWA3lpQdO2GQe/1q19j5pJ
MD5:	F8E228778420068429AA8AF265C8D551
SHA1:	4A7A0A689857665F4A29FD31481F315FAB987842
SHA-256:	E3E8F864A3893B44258AEDEB6260D85723541A9CDB5DC4DAF141CCB769214648
SHA-512:	DC59CE5FC8AF30FAB2882DF68829CC337992A5DBA0980A6E42E6DE155C307CFB7A6F038970EBDCC42DCF64C419F7AC2242505F1E0778BE728B954BD3EF56AE2B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.apple.com/ac/globalnav/5/en_GB/images/globalnav/links/ipad/image_large.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="27" height="44" viewBox="0 0 27 44"><path d="M.5 17.31c0-.45.37-.82.82-.82s.82.37.82.82-.37.82-.82.82-.82-.37-.82-.82zm.23 2.32h1.18V27H.73v-7.37zm7.16-2.49c1.87 0 3.16 1.31 3.16 3.19 0 1.85-1.32 3.15-3.17 3.15H5.39V27H4.16v-9.86h3.73zm-2.5 5.25h2.17c1.4 0 2.21-.75 2.21-2.06 0-1.35-.79-2.1-2.21-2.1H5.39v4.16zm6.66 2.55c0-1.32.97-2.08 2.69-2.18l2.13-.13v-.67c0-.91-.57-1.41-1.67-1.41-.88 0-1.5.33-1.66.92h-1.19c.16-1.18 1.32-1.96 2.89-1.96 1.8 0 2.8.92 2.8 2.45V27h-1.12v-1.09h-.11c-.48.79-1.29 1.22-2.27 1.22-1.43 0-2.49-.85-2.49-2.19zm4.82-.69v-.68l-1.98.13c-1.12.08-1.61.46-1.61 1.2 0 .75.64 1.19 1.49 1.19 1.2.01 2.1-.79 2.1-1.84zm2.84-.93c0-2.31 1.22-3.81 3.1-3.81 1.03 0 1.89.49 2.31 1.29h.1v-4.09h1.18V27h-1.12v-1.18h-.11c-.46.82-1.34 1.31-2.36 1.31-1.89 0-3.1-1.5-3.1-3.81zm1.21 0c0 1.72.81 2.75 2.15 2.75 1.34 0 2.17-1.05 2.17-2.75 0-1.69-.83-2.75-2.17-2.75-1.33-.01-2.15 1.03-2.15 2.75z" fill="#fff"/><path fill="none" d="M0 0h27v44H0z"/></sv

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\image_large[6].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	554
Entropy (8bit):	4.287263920607484
Encrypted:	false
SSDEEP:	12:t4CX8fq0U3W7PlO0agSn//eEVh+RdLbSBMqLiCba6DRe:t4CM9UqOXWHrqL7ba6DRe
MD5:	5465CC591DA2AC562AE16BB33F3575B8
SHA1:	A4D805677D0CA6AA4041C0FA06AD2F9CB37551C7
SHA-256:	1E281E5D429981905E0C937ED7B9CA93559569504D49640C494AAE8DA7C58EF5
SHA-512:	5B57035C0236378C1C03198208EB24AF4CF6DCCB361317C799AFC55563521AFDC795592A52E46D7C7D6B5DE4E9CFBBEEBB33C249638E26B4AA6BECD53A8E72FF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.apple.com/ac/globalnav/5/en_GB/images/globalnav/apple/image_large.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="44" viewBox="0 0 16 44"><path d="M8.02 16.23c-.73 0-1.86-.83-3.05-.8-1.57.02-3.01.91-3.82 2.32-1.63 2.83-.42 7.01 1.17 9.31.78 1.12 1.7 2.38 2.92 2.34 1.17-.05 1.61-.76 3.03-.76 1.41 0 1.81.76 3.05.73 1.26-.02 2.06-1.14 2.83-2.27.89-1.3 1.26-2.56 1.28-2.63-.03-.01-2.45-.94-2.48-3.74-.02-2.34 1.91-3.46 2-3.51-1.1-1.61-2.79-1.79-3.38-1.83-1.54-.12-2.83.84-3.55.84zm2.6-2.36c.65-.78 1.08-1.87.96-2.95-.93.04-2.05.62-2.72 1.4-.6.69-1.12 1.8-.98 2.86 1.03.08 2.09-.53 2.74-1.31" fill="#fff"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\image_large[7].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1160
Entropy (8bit):	4.288697074014536
Encrypted:	false
SSDEEP:	24:t4goMvFZMHlplk8nrZSRPNGFaEF446hRuhdSQNRZY4qbg8tovN:L/dZulpNxP3jd7Ri9bg8u
MD5:	E0A682D11E5DA6756C00A9FB7F94CE93
SHA1:	47F240703CE0FCADA7A4FC00C6BA87371A395308
SHA-256:	A6184C9C55C75D613C2E81F5238D7E436714FAB15E116EB29059D22817A90EF2
SHA-512:	A0EE8BA1ADE6CB416B36823F9BB8FE57A4FF204F231E5E44026CC6FA223100669F89A64DEC70B013BF1F0204268E96304360ACD03DD91CBEA277E320E215A9DE
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\image_large[7].svg	
Reputation:	low
IE Cache URL:	http://https://www.apple.com/ac/globalnav/5/en_GB/images/globalnav/links/iphone/image_large.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="44" height="44" viewBox="0 0 44 44"><path d="M.5 17.31c0-.45.37-.82.82-.82s.82.37.82.82-.37.82-.82.82-.82-.36-.82-.82zm.23 2.32h1.18V27H.73v-7.37zm7.16-2.49c1.87 0 3.16 1.31 3.16 3.19 0 1.85-1.32 3.15-3.17 3.15H5.39V27H4.16v-9.86h3.73zm-2.5 5.25h2.17c1.4 0 2.21-.75 2.21-2.06 0-1.35-.79-2.1-2.21-2.1H5.39v4.16zm7.44-5.68h1.18v4.09h.11c.37-.81 1.14-1.29 2.27-1.29 1.56 0 2.54 1 2.54 2.73V27h-1.18v-4.48c0-1.31-.59-1.96-1.7-1.96-1.32 0-2.04.83-2.04 2.08V27h-1.18V16.71zm7.74 6.61c0-2.37 1.3-3.81 3.4-3.81s3.4 1.44 3.4 3.81-1.3 3.81-3.4 3.81-3.4-1.45-3.4-3.81zm5.58 0c0-1.75-.79-2.75-2.18-2.75s-2.18 1-2.18 2.75c0 1.74.79 2.75 2.18 2.75s2.18-1.01 2.18-2.75zm2.92-3.69h1.12v1.16h.11c.37-.81 1.09-1.29 2.21-1.29 1.65 0 2.58.98 2.58 2.73V27h-1.18v-4.48c0-1.33-.56-1.96-1.74-1.96s-1.93.79-1.93 2.08V27h-1.18v-7.37zm14.08 5.46c-.36 1.26-1.49 2.04-3.1 2.04-2.04 0-3.32-1.48-3.32-3.81 0-2.32 1.3-3.82 3.32-3.82 1.99 0 3.2 1.42 3.2 3.71v.45h-5.3v.05c.06 1.46.88 2.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\image_large[8].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1694
Entropy (8bit):	5.006804706577728
Encrypted:	false
SSDEEP:	48:cfkA8faChK22CfJfa4jT0fxlDLnPDFMOt7:u8fR2WJhHIxl/Lh9
MD5:	6BB5A35F8FF457E2F8B345BD6597E2E4
SHA1:	6F69F11B5C66326F2E4B63C8276195653C79A137
SHA-256:	D577C9D1BAD004BDABB9D0995CEC0714E98B76E6053F2765ED09C23DE6F328B0
SHA-512:	67FE0D03532384D53115259A9082D5C0AEE3BA28FF6111B01BB8C6E5CBC471C166CC7920AB4399633A16FE5C32D4477ECA05D4FDA126F11FB28B7DC341B6DF D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.apple.com/ac/globalnav/5/en_GB/images/globalnav/links/watch/image_large.svg
Preview:	<?xml version="1.0" encoding="utf-8"?>. Generator: Adobe Illustrator 21.1.0, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->.<svg version="1.1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px" width="40px".. height="44px" viewBox="0 0 40 44" style="enable-background:new 0 0 40 44;" xml:space="preserve">.<g id="Assets_Small">.</g>.<g id="Assets_Large">..<g id="Watch">...<path style="fill:#FFFFFF;" d="M4.1,27H2.93l-2.69-9.86h1.29l1.96,8.02h0.08l2.21-8.02h1.24l2.21,8.02h0.08l1.96-8.02h1.29....L9.88,27H8.72l-2.27-7.79H6.37L4.1,27z M13.03,24.94c0-1.32,0.97-2.08,2.69-2.18l2.13-0.13v-0.67c0-0.91-0.57-1.41-1.67-1.41....c-0.88,0-1.5,0.33-1.66,0.92h-1.19c0.16-1.18,1.32-1.96,2.89-1.96c1.8,0,2.8,0.92,2.8,2.45V27h-1.12v-1.09h-0.11....c-0.48,0.79-1.29,1.22-2.27,1.22C14.09,27.13,13.03,26.28,13.03,24.94z M17.84,24.25v-0.68l-1.98,0.13....c-1.12,0.08-1.61,0.46-1.61,1.2c0,0.75,0.64,1.19,1.49,1.19C16.94,26.1,17.84,25.31,17.84,24.25z M22.72,17.72v1.91h1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\image_large[9].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	718
Entropy (8bit):	4.975227697400887
Encrypted:	false
SSDEEP:	12:tvG1do1Nny+hoaFJKAvFE3Gb/NKXu6bZa+lBauBjtkGhBckmUcBTOcBLAct63cBr:tu1dENy+dJK+Fhb/NKbbZaKaurkCWN6S
MD5:	1B5D095BFE3AC689E90215A6DEB7302C
SHA1:	22D3E88D961BC2EB647B6007526938BAA5E69090
SHA-256:	F1CD98822BE46341B217B662DB5CF71AF58E176B471250D3099B1370DCCE57FA
SHA-512:	0200A3B8AC9FB40D7E7306F87A53EACDA2C1D83406B06FE94B845376BA9ADEAEA935ABDDFDA0082BBAC4915D289758C8BCC9727CFCFBA279903C73F83999C D7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.apple.com/ac/globalnav/5/en_GB/images/globalnav/bag/image_large.svg
Preview:	<svg id="Layer_1" data-name="Layer 1" xmlns="http://www.w3.org/2000/svg" viewBox="0 0 17 44">. <defs>. <style>. .cls-1 {. fill: none;. }.. .cls-2 {. fill: #fff;. }. </style>. </defs>. <title>image_large_1</title>. <g id="bag_large">. <rect id="boundingbox" class="cls-1" width="17" height="44"/>. <path id="bag" class="cls-2" d="M14.5,14H12.712a4.227,4.227,0,0,0-8.424,0H2.5A2.5,2.5,0,0,0,0,16.5v11A2.5,2.5,0,0,0,2.5,30h12A2.5,2.5,0,0,0,17,27.5v-11A2.5,2.5,0,0,0,14.5,14Zm-6-2.875A3.243,3.243,0,0,1,11.712,14H5.288A3.243,3.243,0,0,1,2.045,17.25v8.5a3.243,3.243,0,0,0,3.243,3.243h8.5a3.243,3.243,0,0,0,3.243-3.243v-8.5A3.243,3.243,0,0,0,14.5,14Z"/>. </g>.</svg>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\launch[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	247966
Entropy (8bit):	5.404959653715679
Encrypted:	false
SSDEEP:	6144:3/+AOVP2tuMIxHn7nWerPi9UgBkLDZrrLZC6AF+TmlzwTHq7EaMuKZ0YrTB7EbM1:3/+AOVm2BLDZDjAF+Koz
MD5:	8A79F1D9598877F7058F1680A7C2F731
SHA1:	B8D43C9C24BEA92C63A00B1B33F6F5ACFF2D9B43
SHA-256:	8CAE9440D5F8739FB7DD89FCD87F144D4750FF900B949E811E4F12753C4E1CE3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\launch[1].js	
SHA-512:	0F15401B363C1A4005417DC192ACDD5A3F8AB036DFD87929AFE534E1513E5F0D973E30A7AB68A3C48A3093F337EDC0180B8206874286CB2CEB332D3A3EB649AE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://km.support.apple.com/clientside/build/launch.js
Preview:	//LAUNCH-VERSION: packager-20200804AA.launch-20210113A-prod../**********. * Copyright 2019 Adobe. All rights reserved.. * This file is licensed to you under the Apache License, Version 2.0 (the "License");. * you may not use this file except in compliance with the License. You may obtain a copy. * of the License at http://www.apache.org/licenses/LICENSE-2.0. *. * Unless required by applicable law or agreed to in writing, software distributed under. * the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR REPRESENTATIONS. * OF ANY KIND, either express or implied. See the License for the specific language. * governing permissions and limitations under the License.. ********** ***********/.function AppMeasurement(e){var m=this;m.version="2.20.0";var u=window;u.s_c_in||(u.s_c_il=[],u.s_c_in=0),m._il=u.s_c_il,m._in=u.s_c_in,m._il[m._in

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\lexialight-webfont[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 28401, version 0.0
Category:	downloaded
Size (bytes):	28401
Entropy (8bit):	7.98121967089255
Encrypted:	false
SSDEEP:	768:Mckg5sHnKChEtsulxeiUq8vzXi2AT3upix:n4KCyz3v8LyVrupix
MD5:	0ADB91CB74176292A76F27633FF97DEE
SHA1:	8B1D2FC1EB21FAB2EEDD1BFBC0DDB19336BA82DE
SHA-256:	37B6BA9F1C7DF9E7656F7BCAE29CF2AF836FC1C9A54793707B9B8AF90E8E6D05
SHA-512:	BC1A9DE9AFB3E0EBDC9C6DCADAF0FF24EA387F4B1D12D54018935F3C8FB1367892E20F561CDC5AD85CBB6650BCA05D5B713482CDCF02D200C3709A545FFC724
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cookienotice.astrazeneca.com/etc.clientlibs/od-client/clientlibs/clientlib-assets/resources/fonts/lexiafont/lexialight-webfont.woff
Preview:	wOFF.....n.....h.....m,.....GPOS..W.... ..6n.U.hGSUB..d8.....2_..1LTSH..V.....24NOS/2.....[...`..c.VDMX..R....|.....p.cmap...H.....u.cvt ..U.....fpgm..U.....a.A..gasp..U.....glyf...|..>...x0....head.....6...6...Lhhea.....!...$...\hmtx.....Q...P..B5loca.....{.maxp..... ... ...ename...P.....s1m.Npost...h...../q.Hprep..V.....+.....~...r.....s.....B.._.<.....D5.....S..).*.....x.c`f.d.....B3.e0b.....0(D3@....#....o.f..N..2\R``...c..t.H)00.....*.x....+.Q....{.....=...`6.+.k...)+.....F...K..K..+..... .uus...).YsN.<.....!"AD>.r..s...'..J.rsJ.4*.~Z.5T ...0->..X..bO...}..u.\..K.s9Ws.....x....?.-R.$...d.,.,.,!.&;../D$3Z.K....dOd..UZ.gT..y..c.cO...9...#.'Vyb7.>....L#.?..FD$)J12"....s._o.^..zSo.%].3...o...../Dn..tk..7...~'.D.K...t..^..H.T3j..I.V#.O....;q.R.)..o....y.}.~..>.hB...1.0.1.I....1.Q....?X.o,./....m...|k...x.c`d``....p.E.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\main.1f02b685.chunk[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	3076
Entropy (8bit):	5.129069505283291
Encrypted:	false
SSDEEP:	48:NxvHFGDDbF5Af+InXXoEvl8gyodq6P9UYKZbYjV/QzNmZHzjV1sOfsEw9t:DYAn4ndZNpoO13et
MD5:	560921845F1672DB8600479066AE351E
SHA1:	03B72BA9AA804FF29F92246C5DEB6C692A6CBED7
SHA-256:	81D63BC418CBAC22062824A00AC09D1682CB3AEAC589353A2001568C20DF3390
SHA-512:	AF5A43C4A1A24B259D8593F3107E79918AD5287F0C9616F3139E831183764F5D97A41421C9EEE9B4FBD358B551B0CB2B5E3E1814A72F5848CB375B84463C4954
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://covid19-immunization-learning-program-2021.ca/static/css/main.1f02b685.chunk.css
Preview:	@import url(https://fonts.googleapis.com/css2?family=Raleway:wght@300;500;700&family=Zilla+Slab:wght@300;500;700&display=swap);body{margin:0;font-family:-apple-system,BlinkMacSystemFont,"Segoe UI","Roboto","Oxygen","Ubuntu","Cantarell","Fira Sans","Droid Sans","Helvetica Neue",sans-serif;-webkit-font-smoothing:antialiased;-moz-osx-font-smoothing:grayscale}code{font-family:source-code-pro,Menlo,Monaco,Consolas,"Courier New",monospace}.App{background-image:url(/static/media/background-covid.59dc326d.png);background-repeat:no-repeat}.consent{font-size:13px!important}.home-page-wrapper{max-width:900px;background:#fff;border-radius:10px;padding:3em;margin:-70px auto 0}*{font-family:"Raleway",sans-serif;color:#404040}li,p{font-size:16px!important}li{margin-bottom:1em!important}h3{font-family:"Zilla Slab",serif!important;color:#811c4b;font-size:20px!important}.date-bold{font-size:16px;text-transform:uppercase;color:#811c4b;font-weight:700}.keynote-title,.presented-by,.time-regular{font-weight

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\meCore.min[1].js	
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):	101866
Entropy (8bit):	5.2509724222666865
Encrypted:	false
SSDEEP:	3072:I7uoUCePnnlneqFpJrJjsV72lzTPH/cTOhz/Eo7oYnOG:2WleMXLz/Eo7oYnOG
MD5:	F3C5F58A5A3EE49C326755652A396448
SHA1:	63F37B3BD5C33C935C4E10FC3C00FF75175D6FC5

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\meCore.min[1].js	
SHA-256:	C965F854E2429F283AC9CA2F8F7641B10E6F43F7EF1F0AD6482F1F7B6B5A21F6
SHA-512:	5FA3F186DCF7838F54C46FE519298292170DC388325B1A972F5C24EE3FF94E5D6F10C7A883A743599043E01ED8E6F0F6D458384A5061554A25830FD5A2B0B7DC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://mem.gfx.ms/scripts/me/MeControl/10.21035.1/en-US/meCore.min.js
Preview:	MeControlDefine("meCore",["exports","@mecontrol/web-inline","@mecontrol/web-boot"],function(t,f,h){"use strict";var r=function(t,e){return(r=Object.setPrototypeOf||{__proto__:[]}instanceof Array&&function(t,e){t.__proto__=e}||function(t,e){for(var n in e)e.hasOwnProperty(n)&&(t[n]=e[n])})(t,e)};function e(t,e){function n(){this.constructo r=t}r(t,e),t.prototype=null===e?Object.create(e):(n.prototype=e.prototype,new n)}var d=function(){return(d=Object.assign||function(t){for(var e,n=1,r=arguments.length;n<r ;n++)for(var o in e=arguments[n])Object.prototype.hasOwnProperty.call(e,o)&&(t[o]=e[o]);return t}).apply(this,arguments)},s=function(){},i={},u=[],l=[];function v(t,e){var n,r,o,i,a=l;for(i=arguments.length;2<i--;)u.push(arguments[i]);for(e&&null!=e.children&&(u.length||u.push(e.children),delete e.children);u.length;)if((r=u.pop())&&void 0!==r.pop)for(i=r.length;i--;)u.push(r[i]);else"boolean"==typeof r&&(r=null),(o="function"!=typeof t)&&(null==r?r="":"number"==typeof r?r=String(r):"s

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\mem5YaGs126MiZpBA-UN_r8OXOhv[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 25004, version 1.1
Category:	downloaded
Size (bytes):	25004
Entropy (8bit):	7.978903570057148
Encrypted:	false
SSDEEP:	384:NQHZMrOEzGv0FkfCvQIW/HCt7oQy/u2NSXAF7Q57vRTVOq1SQgnYfScZfSmB7Mjr:lrzzGMFgCvLnt8Zuh2Q5VUCRZOr
MD5:	D2C6A4B3918B50C5F1854BB9C5D1DE0E
SHA1:	8DE0F3B153BE6114D55DAC6E69CE7AEF9CC98DB2
SHA-256:	6D764A8FFCF6DB322C1F2FB36473FBA60135B7AB93BE5969120152C0538C5EE4
SHA-512:	FC4E9632C1A6764A4C817DD0FEFF5E1FA70160FDCA8918ECA3B04BD351762E4BB93D4CC8CB2465BA0474766A48B23007432C985991047CC1B30E7605B536DD4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v18/mem5YaGs126MiZpBA-UN_r8OXOhv.woff
Preview:	wOFF.....a.....D.....GDEF.....6...:z..GPOS.....GSUB.....$5"OS/2...X...^...`}...cmap.....6.....cvt .....].....fpgm...P.....~a..gasp.....#glyf.. ....KK..}`.4.ahead..TH...6...6..F.hhea..T.... ...$....hmtx..T.....`....loca..W.....22..Kmaxp..Z.... ... .X..name..Z....."c?Jpost..[.....y. .prep..`.....:..]x.c`d``.a..&.v..F..FFWFW ....$=...d.c%..fl.....]r.2.....x.U....P.E.}.....5.\A.kX..k..\.....v.c.1.p...X8../....n.C...\.%...Z..u...\.p.}.1\....z.#.....)..KB8.~.9...]]...Rg.~.1xT.jH.....3.....x.c`fig.a`e``..j...(.../2.1..` b.ffcfeabbY.....@`...../..?....^..... 9.{.m@J....u.....x....]Q...o.....6..qm...~.....g..3..s. J..*.4o...>(.....|.76g;N.Ln....uFQM=..<6o.O.....m.M.#...T..bE..4...M..29-..r.j..5.....a ...3....s.ge..y-sH1.....&.c.r.jR[....k.p*s.Tx. .h@_.>...Z.==....n.^.....k.....`.....^...us\/..us]]...rM]}/.{.=.....R..Q.(.7.%.....Bx..<.0.F8. .G..Y.u...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\menu.79f1f0c795df[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	197
Entropy (8bit):	4.967383371279129
Encrypted:	false
SSDEEP:	6:tnrwdhU3mc4slZs49/nZSKsKMwmqZUR4nBXqusd/:trwdW3lNxxMwhUqxquW
MD5:	3C1A2E1B92E8C13E25DD96AA395A8521
SHA1:	146B6C583F4CBB7C874EB9BFB2BC8BC5BE60D96B
SHA-256:	608049FD531BB6F9C184D6F838BEEBCA785378CE3D0FBACBFB2F1300DA399EBC
SHA-512:	B3D86EBEAF9E5D266ABF3AB6C311EF9C328C1247565FF9E0F09AB48F5754A17E1CB19AB35C29375365E00146742357027492F614386A02D87D223470F2258326
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static-media-prod-cdn.itsre-sumo.mozilla.net/static/protocol/img/icons/menu.79f1f0c795df.svg
Preview:	<svg width="24" height="24" xmlns="http://www.w3.org/2000/svg"><g stroke="#000" stroke-width="2" fill="none" fill-rule="evenodd" stroke-linecap="round"><path d="M3 6h18M3 12h18M3 18h18"/></g></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\override[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	1531
Entropy (8bit):	4.797455242405607
Encrypted:	false
SSDEEP:	24:Udf0F+MOu2UOqD3426TKgR2Yyk9696TkMYqdfskeEkeGk/ksuF9qaSm9qags:Ud8FYqTj36TKgR2Yyk9696TkMYO0keEW
MD5:	A570448F8E33150F5737B9A57B6D889A
SHA1:	860949A95B7598B394AA255FE06F530C3DA24E4E
SHA-256:	0BD288D5397A69EAD391875B422BF2CBDCC4F795D64AA2F780AFF45768D78248
SHA-512:	217F971A8012DE8FE170B4A20821A52FA198447FA582B82CF221F4D73E902C7E3AA1022CB0B209B6679C2EAE0F10469A149F510A6C2132C987F46214B1E2BBBC
Malicious:	false
Reputation:	low

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\privacy-policy[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	34803
Entropy (8bit):	5.312120857156477
Encrypted:	false
SSDEEP:	768:/tRX+vm08RBd9TEg/JUsD3Qo9QMQlQOQIQDHQt3vqCfRqDqmuWKlrzLZ/ceB1hh0:/tRX+vm08RBd9TEg/JUsD3Qo9QMQlQO+
MD5:	CCAC451591E977C67B2890056F8EA8C6
SHA1:	CC2D4581E90B1112BABD7D9077E3E931B1D0CE16
SHA-256:	7C61E03A64E23BDF2CBD34624AAAB022CD79C5F519108959A2B1171A472ABEF5
SHA-512:	0833905BD606FCA396BD700B0B87EED9D12D090E2A14633712B91C83E72F5C9B8F2092B8173C088D856165E5C625244AD77A29C18C2BCEE8D8EFCE481814D42
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>..<html lang="en-GB">..<head>..<meta charset="UTF-8">..<meta name="viewport" content="width=device-width, initial-scale=1">....<link rel="shortcut icon" href="https://www.digitalcontrolroom.com/wp-content/uploads/2018/10/favicon.ico"/>..<link rel="profile" href="http://gmpg.org/xfn/11">..<link rel="pingback" href="https://www.digitalcontrolroom.com/xmlrpc.php">..<title>Privacy Policy – Digital Control Room</title>.<meta name='robots' content='max-image-preview:large' />.<link rel='dns-prefetch' href='//fonts.googleapis.com' />.<link rel='dns-prefetch' href='//s.w.org' />.<link rel="alternate" type="application/rss+xml" title="Digital Control Room » Feed" href="https://www.digitalcontrolroom.com/feed/" />...<script type="text/javascript">....window._wpemojiSettings = {"baseUrl":"https:\/\/s.w.org\/images\/core\/emoji\/13.0.1\/72x72\/","ext":".png","svgUrl":"https:\/\/s.w.org\/images\/core\/emoji\/13.0.1\/svg\/","svgExt":".svg","source":{"concatemoji":"https:\/

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\promotionBanner[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2332
Entropy (8bit):	5.275234008062234
Encrypted:	false
SSDEEP:	48:ymcachB3RchBtchB6GhBVnFoJhBynFoJhBvnJghJ3VzWz3nnkujQhglbfx3nnDu8:yH7hghch5hbchAchVChJ3V6LnkmDnDEm
MD5:	0071592C5C0964CD77E8D8AD2D1FBF3B
SHA1:	29DDF748437E9361FC4F263115F50ED6AC560BF1
SHA-256:	4BA819E20E5526FEF3F123FC4307D44F9C2367DDDAA3E1E40F149779383544E9
SHA-512:	B12E97405FE4C148D33598FCF4BDB76A964D8093575996885077B44CFB39BA505FFE36B159C452E4AD006433AA30F2913424D81A0BF1B8EE940992F1FB4FF250
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://support.microsoft.com/js/promotionBanner.js?v=S6gZ4g5VJv7z8SP8QwfUT5wjZ93ao-HkDxSXeTg1ROk
Preview:	/*! Copyright (C) Microsoft. All rights reserved. */....$(function ($) {.....var $uhfUpgradeBanner = $('#uhf-upgrade-banner');.....var dismissedBannerSet = {};.....var awaTags = {....content: {.....areaName: $uhfUpgradeBanner.data('bi-area'),.....contentId: $uhfUpgradeBanner.data('bi-id'),.....scn: $uhfUpgradeBanner.data('bi-scn'),.....containerName: 'growth_placement',.....contentName: [($uhfUpgradeBanner.data('bi-title') || "").replace("|", " "),..... ($uhfUpgradeBanner.data('bi-subtext') \|\| "").replace("\|", " "),..... ($uhfUpgradeBanner.data('bi-button') || "").replace("|", " ")].join('|')....},...};.....$('#uhf-banner-close').click(function () {....$uhfUpgradeBanner.hide();....document.cookie = "dismissedBanners=UHF; secure; path=/;";...../// Emit dismissed content update....emitDismissAction($(this));...});...../// Emit click update ...$('#upgradeUhfBannerButton').click(function () {....emitClickAction($(this));...});.....if (document.cookie.indexOf('dismissedBanners=') < 0)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\questions-min.4f2aea6368f6[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	66733
Entropy (8bit):	5.240742978907143
Encrypted:	false
SSDEEP:	768:jIn8hJyTrESRxDRMb7JkULyPBlUcu/A3i6l4WMEAnrYSti2cvO7YSvjfj37hRBid:O88PwJkUmPBlUvI3aXj37hRB0kMvKc
MD5:	4F2AEA6368F6F43E560F482DC4F95E71
SHA1:	878FA768C086BD3673198053268817449FCCB459
SHA-256:	3DC42EB60F7C2DF726BAADE89C341791E2929A29B6A580FC49FF8F5791228981
SHA-512:	DD431B0DDA297904993B74BA8AF44442B6DD8862D0BA9294EE1BECA2BCDED507133C0B2F094D3EA6BC427E82F2417336E49C5A2D8C0EA50570D2C84148DD46D
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\questions-min.4f2aea6368f6[1].js	
IE Cache URL:	http://https://static-media-prod-cdn.itsre-sumo.mozilla.net/static/build/questions-min.4f2aea6368f6.js
Preview:	(function($,gettext,document){var Marky={createSimpleToolbar:function(toolbarSel,textareaSel,options){var defaults={cannedResponses:false,privateMessaging:false};var settings=$.extend({},defaults,options);var SB=Marky.SimpleButton;var buttons=[new SB(gettext("Bold"),"","",gettext("bold text"),"btn-bold"),new SB(gettext("Italic"),"","","",gettext("italic text"),"btn-italic"),new Marky.Separator,new Marky.LinkButton,new Marky.Separator,new SB(gettext("Numbered List"),"# ","",gettext("Numbered list item"),"btn-ol",true),new SB(gettext("Bulleted List"),"* ","",gettext("Bulleted list item"),"btn-ul",true)];if(settings.mediaButton){buttons.splice(4,0,new Marky.MediaButton)}if(settings.cannedResponses){buttons.push(new Marky.Separator,new Marky.CannedResponsesButton)}if(settings.privateMessaging){buttons.push(new Marky.Separator,new Marky.QuoteButton)}Marky.createCustomToolbar(toolbarSel,textareaSel,buttons)},createFullToolbar:function(toolbarSel,textareaSel){var SB=Marky.SimpleButton,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\settings[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	39750
Entropy (8bit):	5.345791657554141
Encrypted:	false
SSDEEP:	768:jbdHZ2iJalSnGXtLgrhN7kpnxZHWonH8LWazBmU1h8D28P:ai5rcxBH8PlmUY3
MD5:	3562402588E3BD6410012CF058D1948C
SHA1:	16685FAF56B7AB684F50CD6876E4B2AC2C102545
SHA-256:	23A57AED407545BD964231BCB511674996BDD28A4F2A57CA66BCA72DE0BF3D2D
SHA-512:	2CF72E47309C32BF02AAF8118D69E5E1DC2E72618BBA1971C239990C3F0D171C71FF5CAE8D9ED78FD0EC44BF1709C58F1312E3E79290CC56E928E2DE167A28
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.digitalcontrolroom.com/wp-content/plugins/revslider/public/assets/css/settings.css?ver=5.4.8
Preview:	/*----------....-.Revolution Slider 5.0 Default Style Settings -....Screen Stylesheet....version: .5.4.5..date: .15/05/17..author:..themepunch..email: .info@themepunch.com..website: .http://www.themepunch.com..----------*/....#debungcontrolls {...z-index:100000;...position:fixed;...bottom:0px; width:100%;...height:auto;...background:rgba(0,0,0,0.6);...padding:10px;...box-sizing: border-box;..}.....debugtimeline {...width:100%;...height:10px;...position:relative;...display:block;...margin-bottom:3px;....display:none;...white-space: nowrap;....box-sizing: border-box;..}.....debugtimeline:hover {...height:15px;....}.....the_timeline_tester {...background:#e74c3c;...position:absolute;...top:0px;...left:0px;...height:100%;...width:0;...}.....rs-go-fullscreen {...position:fixed !important;...width:100% !important;...height:100% !important;...top:0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\show-fx-download.4fef4fded9ba[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	450
Entropy (8bit):	4.97623743672235
Encrypted:	false
SSDEEP:	12:2Qjvefw4NtRxTekq4S8461UcyySTzJaDRWvSfJ4JG:2Qjefw4NxTekht46CtzJyRWv8J4JG
MD5:	4FEF4FDED9BADD714BFDA7679C4FB6EE
SHA1:	723F8A8EBCD0CA8FFA7B46DC6D51C964287D8D69
SHA-256:	FB6FF687F16E7C8BC8B07B4729DBE663A60D97ABEDB616E61A4E88003C416BB5
SHA-512:	1EB11123DEB5FDFBFD9867928349C796A439365D0A34D5F0573FE3891871CF3CC903DA4415C953877EB6FC2F5C3B4D8A892AF761D1B6AAAEA13C50A02388C8AE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static-media-prod-cdn.itsre-sumo.mozilla.net/static/build/show-fx-download.4fef4fded9ba.js
Preview:	(function(){var isLikeFirefox=function(ua){return/iceweasel|icecat|seamonkey|camino|like\ firefox/i.test(ua)};var isFirefox=function(){var userAgent=navigator.userAgent.toLowerCase();return/\s(firefox|fxios)/.test(userAgent)&&!isLikeFirefox(userAgent)};if(!isFirefox()){var fxDownloadButtons=document.getElementsByClassName("firefox-download-button");for(var i=0;i<fxDownloadButtons.length;i++){fxDownloadButtons[i].classList.remove("hidden")}}})();.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\style[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	378684
Entropy (8bit):	5.1235118916915585
Encrypted:	false
SSDEEP:	1536:Mbvp7oP+QJeDsto3M5gLDP7msw+v629YUsbgDzbs2slgBPxagP5FQEBuQISIEATa:qpxDjbscnslgBPxPt387XM
MD5:	005AFE9153EB50957413DC4D56F6473B
SHA1:	3CB72654957856B02E2760B6D5145BC837F1EAD3
SHA-256:	ADED7BC649E9DA9F6BFFF0EF2583E5AEC9A8176CD1557F4D38AB75E17104EE54
SHA-512:	710A723F30BE86152907C0555461E139856B72E7B806CAB6D4E0BA174584F684B3493570A28B12C5E55AE06175716F83F22330BD15E4E058B6AEE8679B5EB304
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.digitalcontrolroom.com/wp-content/themes/cesis/style.css?ver=5.7.1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\style[1].css	
Preview:	/*..Theme Name: Cesis..Theme URI: http://cesis.co/..Description: A superflexible and responsive Business Theme by Tranmautritam team - Update notifications available on twitter and facebook: Follow me on twitter - Join the Facebook Group A theme by Tranmautritam Team...Version: 1.2.0.1..Author: Tranmautritam Team..Author URI: http://themeforest.net/user/tranmautritam?ref=tranmautritam..License: Themeforest Split Licence..License URI: -..Tags: buddypress, bbpress, woocommerce..Text Domain: cesis....*/..../*----------..>>> TABLE OF CONTENTS:..----------..# Normalize..# Typography..# Elements..# Forms..# Navigation...## Links...## Menus..# Accessibility..# Alignments..# Cl

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\style[2].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	1035
Entropy (8bit):	4.7464205221622455
Encrypted:	false
SSDEEP:	24:3y/WrMwEwaO1rF/8rK0ciorPrOrqJBcrqZrPr2tIKgRmD:JxEwtFGKLxzMWB+Ez6I3G
MD5:	C8C369CC11763ADA68E49366A04636FE
SHA1:	1EE6325D561ACAA9189AF1C0A2DB05357383396F
SHA-256:	3C3F39525EC9FDBC746202AD415807253841F9AD789579DCDE3C5A32B9EAD93C
SHA-512:	82C48F3B581EC224F92103BDFD7FF1751A473CC33F8BF20F593D2E7BB939A968778A40A9B409400F0296B4D63386819089A48E0AA13090506F74957D41702565
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.digitalcontrolroom.com/wp-content/themes/cesis_child_theme/style.css?ver=5.7.1
Preview:	/*.Template: cesis.Theme Name: cesis child theme.Theme URI: http://cesis.co.Description: A superflexible and responsive Business Theme by Tranmautritam team - Update notifications available on twitter and facebook: Follow me on twitter - Join the Facebook Group A theme by Tranmautritam Team..Version: 1.0.Author: Tranmautritam Team.Author URI: http://themeforest.net/user/tranmautritam?ref=tranmautritam.License: Themeforest Split Licence.License URI: -*/.../**********..Put your custom CSS below this block :)..**********/..#CookieReportsAccordion #CookieReportsConsentControls input {. -moz-appearance: checkbox;. -webkit-app

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\token[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:H:H
MD5:	99914B932BD37A50B983C5E7C90AE93B
SHA1:	BF21A9E8FBC5A3846FB05B4FA0859E0917B2202F
SHA-256:	44136FA355B3678A1146AD16F7E8649E94FB4FC21FE77E8310C060F61CAAFF8A
SHA-512:	27C74670ADB75075FAD058D5CEAF7B20C4E7786C83BAE8A32F626F9782AF34C9A33C2046EF60FD2A7878D378E29FEC851806BBD9A67878F3A9F1CDA4830763F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cookienotice.astrazeneca.com/libs/granite/csrf/token.json
Preview:	{}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\tticons[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), tticons family
Category:	downloaded
Size (bytes):	353640
Entropy (8bit):	6.4298773818238955
Encrypted:	false
SSDEEP:	6144:0eU6cYr83+mb07WttH/Zt+Pt5Y1eDhLkgBHjHlByGFJB4yIHgoR7CcNDdgVw5iap:LmZwfWgzVhVpfHy9cjbOOkrIh9cD29za
MD5:	CF5C5BAD370ED170A60839AC78FE4D4E
SHA1:	F113C70DCB7632DEBFCEEA3439B57DEFFA533C7C
SHA-256:	D2E2E614F08871E2CCE18EDE88A15839302B9A4EDE164BF0352A952E87C0FB86
SHA-512:	4F2056354C7413D3608C20753D8B8E551C94B924C7EF2D1039FB8BBBA78D64D056B3DD22386B9C2DCA503BFBF130CAB1BF7703B541EA76A9B0578B4D07B9006D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.digitalcontrolroom.com/wp-content/themes/cesis/includes/fonts/cesis_icons/fonts/tticons.eot?7siik9

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\tticons[1].eot	
Preview:	he...d.....LP.....O.....t.t.i.c.o.n.s.....R.e.g.u.l.a.r.....V.e.r.s.i.o.n. .1...4.....t.t.i.c.o.n.s.....0OS/2.....`cmapa.....4gasp.....P ....glyf.v....X..2.head.V....5....6hhea...0..6,...$hmtxj.....6P...Tloca..K...L....Xmaxp.....b.... name.n*...c.....post.....d.... .....3.....@.....@...@. ..... ..... ..... .....).9.I.Y.i.y.....).k.....>.N.^.n.~.....>.N.^.n.~.....-.>.N.^.n.~..... ..... .0.@.P.`.p..... .....!.@.P.`.p.... ..... .0.@.P.`.p.....!.0.@.P.`.p..... .....h.b.\..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\vendors~polyfills.chunk.bundle[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):	19725
Entropy (8bit):	5.22018267487359
Encrypted:	false
SSDEEP:	192:CModw4u6rnqjX9IMYREHgHbV4zgSQll799NGPyamt8olFoWhpgLuQcX72061qp6m:CXDnCi+HQSst3WXKRXY1qWlYEk
MD5:	F3FF583778D53E7BE7F6B5DD386679D4
SHA1:	3EA69BBFAC7E8C62E484B73C48FA50008A4B1A7D
SHA-256:	34EB720B629AB202AE2A6DC1D4E15E647FDDDAD75A710CF98CDA6016AFB599D6
SHA-512:	E82AE668C192D23A39132DE5739BC3053627D5B8DC83E95D6AFF79B76249840C80293E0060813A87A114D30FC7C0A0642735467F0A04189158254CA44EAB4565
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cookienotice.astrazeneca.com/etc.clientlibs/od-client/clientlibs/clientlib-site-min/resources/js/vendors~polyfills.chunk.bundle.js
Preview:	(window.webpackJsonp=window.webpackJsonp||[]).push([[48],Array(178).concat([function(t,r,e){var n=e(49),o=e(5),i=e(185),u=e(10).f;t.exports=function(t){var r=n.Symbol||(n.Symbol={});o(r,t)||u(r,t,{value:i.f(t)})}},function(t,r,e){var n=e(13),o=e(189);t.exports=n?o:function(t){return Set.prototype.values.call(t)}},,,,function(t,r,e){var n=e(15);t.exports=Array.isArray||function(t){return"Array"==n(t)}},,function(t,r,e){var n=e(3);r.f=n},function(t,r,e){var n=e(7),o=e(183),i=e(3)("species");t.exports=function(t,r){var e;return o(t)&&("function"!=typeof(e=t.constructor)||e!==Array&&!o(e.prototype)?n(e)&&null===(e=e[i])&&(e=void 0):e=void 0),new(void 0===e?Array:e)(0===r?0:r)}},function(t,r,e){"use strict";var n=e(42),o=e(10),i=e(23);t.exports=function(t,r,e){var u=n(r);u in t?o.f(t,u,i(0,e)):t[u]=e}},function(t,r,e){var n=e(24),o=e(7),i=e(5),u=e(10).f,a=e(40),f=e(225),c=a("meta"),s=0,l=Object.isExtensible||function(){return!0},p=function(t){u(t,c,{value:{objectID:"O"+ ++s,weakData:{}}})},

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\vxpiframe[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	18332
Entropy (8bit):	5.162171841483405
Encrypted:	false
SSDEEP:	384:LC/xEBsuUses94/ZxlOAblisn3C+qxvVqkllsYuYrSGKzVm50Z19jTYdGdEdydsw:+ruTG5b2lsHhGKzV519OE64sw
MD5:	7101B5156B2BDF4E5869078A6F15E606
SHA1:	75417AC2CB7F89E00047370D0ECA027CADA41040
SHA-256:	3A9548EB083D31A4DDACA69535CE9472C7D187ACF105C1ED773F04A2F7CD0636
SHA-512:	9B4D047F992D570478136CE533FD03E1333C369963B1B2B426FAB8745B3837ACC55AA84B1BB0BD38C36373BC469B18FA2137EF5F0C924BB358EA74CF8B20EE3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.microsoft.com/videoplayer/js/vxpiframe.js
Preview:	var MsOnePlayer;(function(n){function i(n,i,r){var u=new t(document.getElementById(n),i);u.onPlayerReady(r)}n.render=i;var t=function(){function n(t,i){var r=this,u;(this .playerDiv=t,this.playerData=i,this.playerReady=!1,this.onPlayerReadyCallbacks=[],this.playerEventListeners=[],this.onMessageReceived=function(t){if(t&&t.data&& t.origin===n.iframeOrigin)try{var i=JSON.parse(t.data);if(!i||i.playerId!==r.playerId)return;i.data&&(r.playPosition=i.data);switch(i.eventName.toLowerCase()){case"player ready":r.playerReady=!0;setTimeout(function(){var n=r.iframeElement.contentDocument.getElementById("primaryArea");n&&n.removeAttribute("role")},1e3);r.doCallbac k(r.onPlayerReadyCallbacks,r);break;case"postjsllmessage":r.sendTelemetyData(i.data)}r.doCallback(r.playerEventListeners,{name:i.eventName})}catch(u){}},t&&i&&i .metadata&&i.metadata.videoId)&&(n.iframeOrigin[0]==="%"&&(n.iframeOrigin=n.iframeOriginDefault),n.siteName[0]==="%"&&(n.siteName=n.defaultSiteName),this.player Ready=!1,n.playerCou

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\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:	F0A10A4C1CA4BAC8A2DBD41F80BBE1F83D767A4D289B149E1A7B6E7F4DBA41236C5FF244350B04E2EF485FDF6EB774B9565A858331389CA3CB474172465EB3E F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://wcpstatic.microsoft.com/mscc/lib/v2/wcp-consent.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\wcp-consent[1].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\0W10PBUV\wiki-min.2c7974ba20a5[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	138887
Entropy (8bit):	5.323031290066213
Encrypted:	false
SSDEEP:	1536:O88PwJkUmPBlUvI3ujJQYX2kUeoj37hRBm1oUFyUh9skHuI08xagv+sv+g:4QmfUsuvGjNVUh9skHuIrv+sv+g
MD5:	2C7974BA20A524FA3EDC1857E44A83EE
SHA1:	FCE21EEBB88BF7C263FC58D6F528C5AC236262B3
SHA-256:	E90757D0C01B14191A1FC9BB1AA72B537766F02D3964F7202DF0EE3180C283CD
SHA-512:	D597D514DFCA5F963A67E528AA7E386B0AC3C1AEBC0DCB93E56560F1339E50BB342F2D7DE794F50788A0A48DA64DEA32133FB6B0E8A6A57CC1AF30E3B715C4D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static-media-prod-cdn.itsre-sumo.mozilla.net/static/build/wiki-min.2c7974ba20a5.js
Preview:	(function($,gettext,document){var Marky={createSimpleToolbar:function(toolbarSel,textareaSel,options){var defaults={cannedResponses:false,privateMessaging:false};var settings=$.extend({},defaults,options);var SB=Marky.SimpleButton;var buttons=[new SB(gettext("Bold"),"","",gettext("bold text"),"btn-bold"),new SB(gettext("Italic"),"","","",gettext("italic text"),"btn-italic"),new Marky.Separator,new Marky.LinkButton,new Marky.Separator,new SB(gettext("Numbered List"),"# ","",gettext("Numbered list item"),"btn-ol",true),new SB(gettext("Bulleted List"),"* ","",gettext("Bulleted list item"),"btn-ul",true)];if(settings.mediaButton){buttons.splice(4,0,new Marky.MediaButton)}if(settings.cannedResponses){buttons.push(new Marky.Separator,new Marky.CannedResponsesButton)}if(settings.privateMessaging){buttons.push(new Marky.Separator,new Marky.QuoteButton)}Marky.createCustomToolbar(toolbarSel,textareaSel,buttons)},createFullToolbar:function(toolbarSel,textareaSel){var SB=Marky.SimpleButton,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\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):	135290
Entropy (8bit):	5.2254562447372
Encrypted:	false
SSDEEP:	3072:1f/HuFzpxJIS20i9d1EwgXA95KSqDCE4t:1f/HuXIZRjt
MD5:	07CB1B6723F61F949C862B399E06B3BF
SHA1:	83ABC38AB7E787F719E859E3EA97D4A634FE61FC
SHA-256:	82A7ACB7D942575069E4067375BEC0C33F1949EA2864BE8BD12E9D6DB74A345D
SHA-512:	D520D31E12A3D2D316347D96E4E3D20D7E5C988A4824228097D1DF0A5AB3F12334096C2ADD5D0A7345EF8A2E674712F84D9F8CFC2E973A2A4DEDA546337C940D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-neu-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-c07ea1/9d-b58f60/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/b7-0ad59f/e0-3c9860/91-97a04f/1f-100dea/33-abe4df/17-f90ef1?ver=2.0&_cf=20210415&iife=1
Preview:	(function(){/**. * @license almond 0.3.3 Copyright jQuery Foundation and other contributors.. * Released under MIT license, http://github.com/requirejs/almond/LICENSE. */.var requirejs,require,define,__extends;(function(n){function r(n,t){return w.call(n,t)}function s(n,t){var o,s,f,e,h,p,c,b,r,l,w,k,u=t&&t.split("/"),a=i.map,y=a&&a["*"]||{};if(n){for(n=n.split("/"),h=n.length-1,i.nodeIdCompat&&v.test(n[h])&&(n[h]=n[h].replace(v,"")),n[0].charAt(0)==="."&&u&&(k=u.slice(0,u.length-1),n=k.concat(n)),r=0;r<n.length;r++)if(w=n[r],w==="."")n.splice(r,1),r-=1;else if(w===".."){if(r===0||r===1&&n[2]===".."||n[r-1]==="..")continue;else r>0&&(n.splice(r-1,2),r-=2);n=n.join("/")}if((u||y)&&a){for(o=n.split("/"),r=o.length;r>0;r-=1){if(s=o.slice(0,r).join("/"),u)for(l=u.length;l>0;l-=1)if(f=a[u.slice(0,l).join("/")],f&&(f=f[s],f)){e=f;p=r;break}if(e)break;!c&&y&&y[s]&&(c=y[s],b=r)}!e&&c&&(e=c,p=b);e&&(o.splice(0,p,e),n=o.join("/"))}return n}function y(t,i){return function(){var r=b.call(arguments,0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\2019-09-13-12-33-58-e123dc[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 80 x 80, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	1038
Entropy (8bit):	7.816975469906525
Encrypted:	false
SSDEEP:	24:hDc2KSdQ8Ic44Yo4bo4Y4ofXQLo4LoXgMXI7gAgXILEDSwz4Ruz:hY2fXP3nfXfX/HXPX/HXhr4g
MD5:	5B7292CEB8EB2F56DFB5F7BAB56C2B6A
SHA1:	EDB3CC9438A13FB5FD70F6D2DEA9156ADE6D10F9
SHA-256:	9DEDB0DFCD0B9CFFE12209B2EC8D49D2CFFBE9758EF15B9BCC6443865CC0D8F1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\2019-09-13-12-33-58-e123dc[1].png	
SHA-512:	5FEE7416214DFCF5AF49A96B94EC3FFBC4A87DB34C762B6431561BB0DE178CF3DF01B0A691CD983763C13983D6E7AC43B95D3423319AE0C3D70618AA90D935 2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://user-media-prod-cdn.itsre-sumo.mozilla.net/uploads/gallery/images/2019-09-13-12-33-58-e123dc.png
Preview:	.PNG.....IHDR...P...P.....PLTE.....UUU..... !!!"""###$$$%%%&&&"'((()))***+++,,,---...///000111222333444 555666777888999:::;;;<<<===>>>???@@@AAABBBCCCDDDEEEFFFGGGHHHIIIJJJKKKLLLMMMNNNOOOPPPQQQRRRSSSTTTUUUVVVWWWXXXYYYZZZ[[[\\\ ]]]^^^___```aaabbbcccdddeeefffgggghhhiiijjjkkklllmmmnnnooopppqqqrrrssstttuuuvvvwwwxxxyyyzzz{{{|||}}}~~~.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\FujiStitchPath[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):	6321
Entropy (8bit):	5.3981279151775
Encrypted:	false
SSDEEP:	192:DtHUZjr4uwGkXgiU3JlwR2GWNPDqjoFwQfx:B0+uwGegiCKRYDLFw8
MD5:	C82C158AE3CE9FEF08DB76A234A99467
SHA1:	C9555D530E2B3C0CD7120463BFD40F944200A8A0
SHA-256:	00A4EC249DDC034C124FF7674D6F4730BA4C0F5CDA1140950490FD9AE9E398EF
SHA-512:	B874DAECB51C10322D9C206EAC868E3CD5A61BC30894077194F2247E02286F87883E21DA9D6D6340FA72D99A5879A6F8EC6621FFAE5E7F3BB9BF91E0034A632
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://support.apple.com/clientside/build/FujiStitchPath.js
Preview:	!function(e){var t={};function r(n){if(t[n])return t[n].exports;var i=t[n]={i:n,l:!1,exports:{}};return e[n].call(i.exports,i,i.exports,r),i.l=!0,i.exports}r.m=e,r.c=t,r.d=function(e,t,n){r. o(e,t)||Object.defineProperty(e,t,{configurable:!1,enumerable:!0,get:n})},r.r=function(e){Object.defineProperty(e,"__esModule",{value:!0})},r.n=function(e){var t=e&&e.__e sModule?function(){return e.default}:function(){return e};return r.d(t,"a",t),t},r.o=function(e,t){return Object.prototype.hasOwnProperty.call(e,t)},r.p="",r(r.s=5)}([function(e,t,r) {"use strict";var n=function(e){switch(typeof e){case"string":return e;case"boolean":return e?"true":"false";case"number":return isFinite(e)?e:"";default:return""}};e.e xports=function(e,t,r,c){return t=t||"&",r=r||"=",null===e&&(e=void 0),"object"==typeof e?o(a(e),function(a){var c=encodeURIComponent(n(a))+r;return i(e[a])?o(e[a],functi on(e){return c+encodeURIComponent(n(e))}).join(t):c+encodeURIComponent(n(e[a]))}).join(t):c?encodeURIComponent(n(c))+r+e

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\JTURjIg1_i6t8kCHKm45_bZF3gnD-A[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 23628, version 1.1
Category:	downloaded
Size (bytes):	23628
Entropy (8bit):	7.97652223541331
Encrypted:	false
SSDEEP:	384:aWXmwssTJH1/G6rbr24Jln5GTJO8XWSN2OyyW/nGGxnslEYe3cB68HOeHS9AVqmT:aW2wdx1/HPCQln5F8XL2frP5pMB68H/N
MD5:	7C839D15A6F54E7025BA8C0C4B333E8F
SHA1:	09FC9F1CA6B859952A3641EDBFB1424E1C873F5D
SHA-256:	46226ABFCDE5DB2598FED8FD0DE77AF9B96C8242DC0E72242971F0BBCF566A38
SHA-512:	239EDDCB1FE723077F1FDC76B265A3D5E6F946F5258C968B15AB99CDD817D0D67D85248DA13820D9EBF0EA256F1E29ADB975894707E1901BCBDB0C2908ABC8 C2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/montserrat/v15/JTURjIg1_i6t8kCHKm45_bZF3gnD-A.woff
Preview:	wOFF.....\L.....GDEF.....G...X.g.^GPOS.....2....!GSUB.....,.OS/2...|...M...`Ti.mcmap.....h.cvt .....d....2...fpgm.....F...mM$.|gasp...<..... ...glyf...D..4..._.F.1.head..S....6...6.Z..hhea..S@... ...$....hmtx..S`...$...>*...loca..U....!...(N.e.maxp..W.... ... .h.Wname..W.....+.FOpost..X.....D.z.prep..[.....K..x.%.... P.....@:D...$..]!....h.....2/.$.....D.^.F..ua.].N....%>./...x...p.I....RK..Z-...m.-.= .a.....1.0..n.....-h....C!.....Wm.F3....J~/..|.....*..._]F....Y.x.._.....s.w!.S...'..9d...(...5.).O. z.>...OQ..7J'....>...J.:..K$a6. .._P.IXP."....6....Ie.sY5.n.t'".C..-..5.2...4.}..H.P....w.....OX.....)8....7?..H..I.@|.....R.'..#R.:....{C}....V.%.i...v.L9K..C.....N".r.P.../..7.UN..'..0...- .Q..M..o.6.....-.&l..B.w..x.....e>....CB....&.....&..P.S....3..Y...Q>/..e...B.+..|.o0..I.#L.]a..../.....&..gLz....J...g!.,$..4#...2L..>.P...gF.67.@.}...IX.&....?Vi....ORR

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\OffSMDL2.4.00[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 28260, version 0.0
Category:	downloaded
Size (bytes):	28260
Entropy (8bit):	7.987056042735784
Encrypted:	false
SSDEEP:	768:8IjVhCYTl8JpAZvwxW/mZCE6Up2DGNnEM8bGOQ:9B8gZoxeO6R6D
MD5:	8D1B8A424DAD000770F3252B9014DDC3
SHA1:	ECC3C1B6A0209EE3F9D1DA9B9236E264D8C20757
SHA-256:	717D82DB7935874C7B7C1740B6710E9A9501595A4AA9F73754D95823058B547E

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\OffSMDL2.4.00[1].woff	
SHA-512:	3BB2623544A421A404E0578A31A2BE95E42F63A9331C411032DFA4F3A0861CB90E3FC684D6C0A965B45CAA4270A61A739AB6F277DFCB646DF86A6C3D5342E857
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://support.microsoft.com/socfonts/OffSMDL2.4.00.woff
Preview:	wOFF.....nd.....OS/2...X...H...`JM~.VDMX.....^.qcmap.....X.`..cvt ...X... ...*....fpgm...x.....Y...gasp...h.....glyf...t..]....d.hi{head..e....2...6.. Qzhhea..e.....$....hmtx..e.....;.&yloca..f.....$maxp..hX... ... .!.9name..hx...I....).A.post..m..... .Q.wprep..m.....x...x.c`f..8.....u..1...4.f...$.....@ .....q.....S``... ...x...S....._..m.m.m.m.m;e..y.~.....<p..a.0t.&...a.pa.0B.1..F...Q.ha.0F.3.....q.xa.0A.0L.&...I.da.0E.2L....i.ta.0C.1..f...Y.la.0G.3.....y.|a..@X0,.....E.ba.DX2,....e.ra..BX1.. V...U.ja..FX3.....u.za..A.0l.6...M.fa.E.2l....m.va..C.1..v...].na..G.3.....}.~a.p@80.....C.a..pD82.....c.q..pB81..N...S.i..pF83.....s.y..pA.0\.....K.e..pE.2\....k.u..pC.1..n...[.m..pG.3... ...{.}...@x0<.....G.c...Dx2<....g.s...Bx1..^...W.k...Fx3.....w.{...A.0|.>...O.g...E.2|....o.w...C.1..~..._.o..08.....?..0$.....x...kl.U...3}m....K).j.Y...%.BPIS.h.mC.....M.i.(..A1..h#JR

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\S6u8w4BMUTPHjxsAXC-s[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 29836, version 1.1
Category:	downloaded
Size (bytes):	29836
Entropy (8bit):	7.982476349245973
Encrypted:	false
SSDEEP:	768:7MOwd36ZTRKgBw9se0XAJhOlj5AMQsMd3YVj3rensHMP:7MOz5KseUHQTqVj3GssP
MD5:	E652470B9572B86907B77A97F40DC915
SHA1:	517EA676C79F25EBE597F8C2BDDAC9BAA7DF7E5D
SHA-256:	D98792E1F2EAA92968F94C35F08DA7B23DB7333C79CDB657DCA3A819D8E6D0D9
SHA-512:	129510CE678CA0064ED600F3F70ADFCB68689B35C2E1FDF00E9F933A8DD1A9BCFFCC259374917B7446DA65D8CCCF90DCE90529836119BD2C3B84FE06BF0E58 2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/lato/v17/S6u8w4BMUTPHjxsAXC-s.woff
Preview:	wOFF.....t.....GPOS...l.....H,..GSUB...p...S...p.:.|OS/2.....Z...`y$`.cmap... .....cvt .....+.....fpgm.....rZr@gasp...X.....glyf...d..]....C.;shead..l. ...6...6...hhea..m0..."...$...&hmtx..mT...5...vI.F.loca..o.....Z.smaxp..qP... ... .name..qp...3....:.Rspost..r.....EW..tprep..t@...K...K....x.D..nd....Qq..m.m..`U;\..m.9...d..`... .....w.w.....`.b.On..S./....if.....Y...[..{.-...b.R.K...|.....U.Ge.i.2.y....._.....j..K%Nx..)q.Bi.6..V1T.....5.G..JK5.i..#=....#.{..)...\....]....v.vy.wW..g. "....3...f...d.0...d.s..<...b1KX. Z...le.....0...%.p.....x.C.....y.;>.O....L..D.I..|..?..ob.#...I".L..&.".)..2...*.....k}.b.f7....1.n...:q.....8.!.....dS.1.d{.....j.,..nv7.6.....E.i..GJK...CP.k.(..0.X...u.B..M.....%...]....~..{ o..)_....h=.QO..._.Q~Cl.o..y@.q...O...L.;.4)f.e.y.H.H.%.z..*kd.....y.....+.E.s>z=...B9.TREu...r.A....j.w..n.....4..b|+m.1.v};.T.%..u....1....1.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\S6uyw4BMUTPHjx4wWA[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 28660, version 1.1
Category:	downloaded
Size (bytes):	28660
Entropy (8bit):	7.986798426962959
Encrypted:	false
SSDEEP:	768:Rr8uuUMtVCqVsUnrZAT9vaxw9pi95vSVc+Dfpy:R9uZV9VnndAJvaCGPvwDhy
MD5:	B8EE546ACD6CC0C49F42AD3D48EF244F
SHA1:	7D8BFF4143A36AA9CC1C2801F60FA0E99969E3F6
SHA-256:	04050BAE4CC3B9CCD20D3C7F57F5B1BA249D4A54D6EFF75A1E4DF504362E8C00
SHA-512:	700D04F4CAF24A20919C2136DD3700BBE07F509F5BD0045084063B78EA8B6FD72BFEA6BBF2A94A5865A75CD6C7197DAB500B809122AA5A3910F46E1D9816D00
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/lato/v17/S6uyw4BMUTPHjx4wWA.woff
Preview:	wOFF.....o.....l.....GPOS...l.....z....GSUB...<...S...p.:.|OS/2.....Z...`y$aycmap.....cvt ...x...+.....fpgm.....rZr@gasp...$.....glyf...0..YY...H@ ...head..h....6...6...#hhea..h.....$...whmtx..h.....v}.O7loca..j.....9maxp..l.... ... ....name..l....8....:.TApost..n.....EW..xprep..o....K...K....x.T..l Q.EO....m.m.m;X...Fl..? us..p.$z3.....G.f.N...`Yv...p.a.N.*."b.3...]p..`...l,.5...]=.%U..D...]v?.xX.w...;.w>.....mt?....+.....]..G.>]:(.JO.+.J.R.=.k.....@9.+.....:(.UP.k.bZ...B..a....U....6\..Q.10....H'...../.....1. !.e....HF1..Lf...l.0.y,`.KY.rV....b7{....p...,.8...r.+..>.x.#....%.x.[...|.....7.._.....$.H..&.X.'.D.I!.^xX...=.....{XC.hySQy....p...n)..h..M.(..f)"..)..j...L.qw..R`).E..8..1*.X..7...\..9(q(. .32.PJ)K).....#)I(.X...{.....7.g..\s.:...7dL...K.>..0H.!.Y.v.U.Xg...m.-..a.=.:...<!..c.9~....?B...w...-..I(.>..TQM...X..5...G.J..P.\..=4.H31Z....q.j.6.....v.#..z.G..e.q

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\SFProIcons_light[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 10476, version 1.0
Category:	downloaded
Size (bytes):	10476
Entropy (8bit):	7.958728376519368
Encrypted:	false
SSDEEP:	192:nBTpuMN5zDRGlN1vo9QC2YVB/lSJwtLu1+5dmTIE+Y49xWsUg0Sq/:Bh5zl+kQCX//lSJwtLu1Fl1/WLg0d
MD5:	1252981C527C50FC1AC0E981FF12396B
SHA1:	DC498DE0B92622946920618 85ABB047CCBF41C39
SHA-256:	628A01BEBD49A4858DBE4B7E9224D754682A6A72102303C999122F9A265CB1F9
SHA-512:	E317B06900B64931EBA79EADCEE3D829AD655792F7F4B2C54176A54CEEFF1B631A009F38A42ED772D758503385C47B43360839CF904D5C502008443D898C0D5F
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\SFProIcons_light[1].woff	
Reputation:	low
IE Cache URL:	http://https://www.apple.com/wss/fonts/SF-Pro-Icons/v1/SFProIcons_light.woff
Preview:	wOFF.....(.....GSUB.....;...T .%zOS/2...D...D...V..pWcmap.....p..$.glyf...t.....head...0.../...6...Chhea...`.....$....hmtx...|...S....64..loca..... ....maxp..... ...:name.....{.4F.post..&....Q....Ajkx.c`d``.b0`.c`rq..a..l,.c.b`a...<2.1'3=.....i. f....&;.H.x.c`d?.8.....L..F9..|.!.I.....+.HsMapP...M.....y... 9.'..;x....R.W..... {.AH.&(.%&&&j..{A..QI.$.\..+.r5.....=]....Y..+..8.Pl...-..h.....i.;.....J..y.....sft.M..f..e.k[.....`.....mh'...G..~..5..'..7o.g...nr.....Xc..l..#..l..3vx..^..O../..+..M?];.t..g.>.....1....1.o....9.a. 9...|.|..G9..|.<.=.....%Nr.e..4_..g...8....9.s..Y."....r...`...?S..>z...^.....7..=..N..%..Jk8..f8#..pZ(...P:....t..D.....'.4Jo8s..p.(...R.....I....2..+e$.\.h8..p.)..\S&...L..N....r .....&P..w.r 8.....Q{@..].....>.fx.P[x.P{x.PG..Pgx.QW...;...'...7.../...?..h ..h0..h(..h8..h$..h4..h,..h<..h"..h2..h*..n.pk.#A=....lP..zv<.3.D.q.B.{.b...R....p3.S.B..B+A

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\SFProIcons_medium[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 10648, version 1.0
Category:	downloaded
Size (bytes):	10648
Entropy (8bit):	7.961953054480932
Encrypted:	false
SSDEEP:	192:lBTtSkC75Zs8f1C2UeGTzCJ5jFcWJC+ll5OITIepNmPy8BkXSq/:nhS5Zs8NhUeIA55flWITI4Negd
MD5:	CA928B2E864932590B44DD08AEF96383
SHA1:	AB1AE35755A5335398E82404FF8A110F9F3D7840
SHA-256:	6DE9B14E38B2B9BAFC567929424BCC27F9E2B8F1C60E8E6A6059C160D2461F08
SHA-512:	15675570492794908DFAD8A3F92A2C5571B8B56989EB443584D67E9883D9E1E561BE29FF652CC944F3760C0B6DF83BAA7D6ED181860EEB9D8DB9B3626988E7C1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.apple.com/wss/fonts/SF-Pro-Icons/v1/SFProIcons_medium.woff
Preview:	wOFF.....).....h.....GSUB.....;...T .%zOS/2...D...D...V..pWcmap.....p..$.glyf...t...]...$d].Lhead...../...6...Chhea.....$....hmtx... ...U....6?..loca...x..... ...maxp...P..... ...:name...p.....Q.post..'D...Q....Ajkx.c`d``.b0`.c`rq..a..l,.c.b`a...<2.1'3=.....i. f....&;.H.x.c`d?.8.....L..F9..|.!.I.....+.HsMapP...M.....y... 9.'..;x....R.W..... {.AH.&(.%&&&j..{A..QI.$.\..+.r5.....=]....Y..+..8.Pl...-..h.....i.;.....J..y.....sft.M..f..e.k[.....`.....mh'...G..~..5..'..7o.g...nr.....Xc..l..#..l..3vx..^..O../..+..M?];.t..g.>.....1....1.o....9.a.9 ...|.|..G9..|.<.=.....%Nr.e..4_..g...8....9.s..Y."....r...`...?S..>z...^.....7..=..N..%..Jk8..f8#..pZ(...P:....t..D.....'.4Jo8s..p.(...R.....I....2..+e$.\.h8..p.)..\S&...L..N....r .....&P..w.r8 .....Q{@..].....>.fx.P[x.P{x.PG..Pgx.QW...;...'...7.../...?..h ..h0..h(..h8..h$..h4..h,..h<..h"..h2..h*..n.pk.#A=....lP..zv<.3.D.q.B.{.b...R....p3.S.B..B+A

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\SFProIcons_regular[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 10380, version 1.0
Category:	downloaded
Size (bytes):	10380
Entropy (8bit):	7.960698675136466
Encrypted:	false
SSDEEP:	192:wTBTIh6auIWVQOv4Rh3hOpcN+Ho5E9Qdyi1vBH5eITpvRCobJNblSq/:wFW6aQwRFU4cwNdyifTH3Jd
MD5:	9CACA193FE7BFF016EF17E26937711D9
SHA1:	121E523FE8F27D18017C2F7A056F2F14BF43BFC9
SHA-256:	3B7D2B4C5417A697678081ED3B344955F0B25E694171178B0C01E029B4A18E8B
SHA-512:	280F17FBEFA9682CECCDAAEB9D4CB5B283F22F3B403FC03420FF3BB51084F8820AE726DD6D3F3308D0EB2939E1A067C28F6F466AD5E7C736A79FEC85AADD2E 31
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.apple.com/wss/fonts/SF-Pro-Icons/v1/SFProIcons_regular.woff
Preview:	wOFF.....(.....GSUB.....;...T .%zOS/2...D...D...V..pWcmap.....p..$.glyf...t...O...l...^head...../...6...Chhea.....$....hmtx.....S....64..loca...d..... .*.Xmaxp...<..... ...:name...\.....S\.post..&8...Q....Ajkx.c`d``.b0`.c`rq..a..l,.c.b`a...<2.1'3=.....i. f....&;.H.x.c`d?.8.....L..F9..|.!.I.....+.HsMapP...M.....y... 9.'..;x....R.W..... {.AH.&(.%&&&j..{A..QI.$.\..+.r5.....=]....Y..+..8.Pl...-..h.....i.;.....J..y.....sft.M..f..e.k[.....`.....mh'...G..~..5..'..7o.g...nr.....Xc..l..#..l..3vx..^..O../..+..M?];.t..g.>.....1....1.o....9.a. 9...|.|..G9..|.<.=.....%Nr.e..4_..g...8....9.s..Y."....r...`...?S..>z...^.....7..=..N..%..Jk8..f8#..pZ(...P:....t..D.....'.4Jo8s..p.(...R.....I....2..+e$.\.h8..p.)..\S&...L..N....r .....&P..w.r 8.....Q{@..].....>.fx.P[x.P{x.PG..Pgx.QW...;...'...7.../...?..h ..h0..h(..h8..h$..h4..h,..h<..h"..h2..h*..n.pk.#A=....lP..zv<.3.D.q.B.{.b...R....p3.S.B..B+A

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\SFProIcons_semibold[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 8868, version 1.0
Category:	downloaded
Size (bytes):	8868
Entropy (8bit):	7.953814906932304
Encrypted:	false
SSDEEP:	192:+/vakFl/W1gYNBlOjXC6LqycRFzxrH5LEZ8HMUdOgAHsQdrb3:+qkUzajxeRtaZTUdO/drb3
MD5:	55350BE83FE4B0CDEEC6E88AD7A66F03
SHA1:	A78FE67ACC4CFC8ADF1B5150683841015150C60B
SHA-256:	41DAAC81421329B7091D3EA33D91959EE08135224C28F3DCB523341FA2E90393
SHA-512:	FFFD17078729B685810896D3B81925EC770CAA160B3D37A3B5085196602011423OBE85DD462DA58240D49B9CD676EC9BC301D9B0CC874473FEBD190F4F8F5922
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.apple.com/wss/fonts/SF-Pro-Icons/v1/SFProIcons_semibold.woff

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\SFProIcons_semibold[1].woff	
Preview:	wOFF.....".....Z.....GSUB.....;...T .%zOS/2...D...D...V..o.cmap.....p.1!.glyf... ...i..80..B.head...../...6...Chhea.....$....hmtx.....Q...4!X..loca...,..... ...maxp..... .|.9name.....[..post.. .....y.x.c`d``.b0`.c`rq..a..I,.c.b`a...<2.1'3=.....i. f....&;.H.x.c`d.e.....u&.....f...$.....08(....&.O.a..<.w@aF.....x...rSA...,9g[...0...r F.d..1....G..PR.4<.%O..4..1....i~...3.....(..P...."Q.....^.!.....K[.....QMk^.....1.+..!.kF..h.W..*./.....W....w1..j..>.&.i.5..:).E7=.{...0....f.QNr..q....<.L.YL1..f.e.y.r..\.*...nr..... ..."K,..*k....T.S..^M.....X.....,K...,..\...-....r....-....rn...-....rn...-....r.[.].s...c9.Z.}.s..<`9.Z.',.!KYX...,u..,u....J....-f..XL.....@To.)P..T.F..DM....-f..XL/j..c.f1..b.Q...N.yGe..G]....-...X.. .h..g...p.....6b..Q#...im.g.E.)..A..-.f,...Z4....(4o.V.b.=.....\6.+.M.V....._7...F.....}..D.,..=.hN..C.c.6E[....X4,zj.h.u.E..g.M

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\SOC-Mail[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 32 x 32, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	284
Entropy (8bit):	6.545045554632694
Encrypted:	false
SSDEEP:	6:6v/lhPkdsEejylMSB8POk1SljdAOh06VJJtBafxJ0lX0hRCAp:6v/7sW3jk8POk6j9PJjt1A4K
MD5:	3C7700243B9493C12B1B682CAA47F5F2
SHA1:	D522ED9D356837FED083E4D69262C749F4807FC0
SHA-256:	8EF6E4F16AE501AD18088960B404AF57871BE54EA8A0C7088872B88EB5DC2B02
SHA-512:	F01BF3AB533D6CB7CCF5A26C2F23526BC107B79C9379ABC88922402DC044DFA852E3FF934415476960C8FFE756EE9988B758D602AB1FC6756ADEA50B603050F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://support.microsoft.com/SocImages/SOC-Mail.png
Preview:	.PNG.....IHDR... ... .D.....3PLTE...{{{|||y{{|||w..{||wwwy{{...y||||z}}z}}|||...|}}.....tRNS....`@. ....pP0.jdv....IDAT8..... .E..&.....V..&/'.$g...s..3.....tJ.8...Mh.k.\.o.c;D^.....n... fP.....T...p...1....vA....&n...f.]X.#/....A.....:.....s....d.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\TelemetryLogging[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	1352
Entropy (8bit):	4.872231653913572
Encrypted:	false
SSDEEP:	24:yKGUNphlp9hwCfldX5w2S5IkL60mwqpkL/prw/L/twBt852zp2TZ0TzY+Yzh0:yKGUjh79hw09wT5IC6XChUSt85292TZw
MD5:	094E9F6E4CA96BD9F40ED307707CFB97
SHA1:	9416F5CDB75486CC19D3438A81AB8549D01DF373
SHA-256:	7F8BC8B4E7D9E574828C4671D6D80468BCACAF587B966B0E19A05AA4F35D1D2A
SHA-512:	B97310A1F1BFE13A74853520E11545CB163763F6B4694E09898D29D2A32415DBD7EB4C32AA9F89C4C0475247B9993A945D4E7DB935E21AD9F3CAF03576AB84DF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://support.microsoft.com/js/TelemetryLogging.js?v=f4vItOfZ5XSCjEZx1tgEaLysr1h7lmsOGaBapPNdHSo
Preview:	/*! Copyright (C) Microsoft. All rights reserved. */....window.TelemetryLogging = (function () {...var events = {....'captureContentPageAction': 'captureContentPageAction ',....'capturePageAction': 'capturePageAction',....'captureContentUpdate': 'captureContentUpdate'...};.....function sendEvent(event, overrideTags, element, customProperti es) {....if (typeof window.awa === 'object') {.....if (typeof element === 'undefined') {......element = null;.....}.....if (event === events.capturePageAction) {......window.awa. ct.capturePageAction(element, overrideTags);.....}.....else if (event === events.captureContentPageAction) {......window.awa.ct.captureContentPageAction(overrideTags);... ..}.....else if (event) {......window.awa.ct.captureContentUpdate(overrideTags);.....}....}.....if (typeof window.analytics === 'object') {.....if (typeof element === 'undefined') {......element = null;.....}.....if (typeof customProperties === 'undefined') {......customProperties = null;.....}.....if (e

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\ac-globalfooter.built[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):	44748
Entropy (8bit):	4.986259710900239
Encrypted:	false
SSDEEP:	768:7S7p4S44vR3b8uuXTxXIXcDve1vee/LNVwA1NAGCR/65LblSuWhO7E9Z8ZyU3oE+:7S7p4S44vR3b8uuXTxXIXcDve1vee/L2
MD5:	9CF3D83970C7193B861764E87B26CC15
SHA1:	CE22750EB40A959C173C147207404894AFE16394
SHA-256:	13895610AC1508B0E69F7193000FC6ADFD246F65D778127F06F2CD97ACE0C236
SHA-512:	1D14A44FE5144C4DFBD7405B121FD76154CAB7DC62E8AD7CB1A78CF6CA72E236E8C419A7BECA582039D7286DF0D147977AE6A7E8E8C6D8905FC5CEFCA080C BEF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.apple.com/ac/globalfooter/3/en_GB/styles/ac-globalfooter.built.css

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\ac-globalfooter.built[1].css	
Preview:	@font-face{font-family:'Apple Legacy Chevron';font-style:normal;font-weight:100;src:local("."),url("../assets/ac-footer/legacy/appleicons_ultralight.woff") format("woff") ,url("../assets/ac-footer/legacy/appleicons_ultralight.ttf") format("truetype")}@font-face{font-family:"Apple Icons 100";src:url("../assets/ac-footer/legacy/appleicons_ul tralight.eot")}@font-face{font-family:'Apple Legacy Chevron';font-style:normal;font-weight:200;src:local("."),url("../assets/ac-footer/legacy/appleicons_thin.woff") forma t("woff"),url("../assets/ac-footer/legacy/appleicons_thin.ttf") format("truetype")}@font-face{font-family:"Apple Icons 200";src:url("../assets/ac-footer/legacy/appleicons _thin.eot")}@font-face{font-family:'Apple Legacy Chevron';font-style:normal;font-weight:300;src:local("."),url("../assets/ac-footer/legacy/appleicons_thin.woff") format(" woff"),url("../assets/ac-footer/legacy/appleicons_thin.ttf") format("truetype")}@font-face{font-family:"Apple Icons 300";src:url("../assets/ac-f

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\ac-globalnav.built[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	137312
Entropy (8bit):	5.3419858617971165
Encrypted:	false
SSDEEP:	1536:LqPVYhcRLDPmr1YnHR4JzsToYZXmq5ocTmlz2a7xgRItNJjluyw9zgBpl3:LqPj8qNY6CDjz/3
MD5:	95279645B87EBC9DA5321BED8F00771F
SHA1:	E8081FEFF8FF1DDBC92702487C763D248039EE27
SHA-256:	0722EEAA10A70434D2D68F09CCBEEED14E550A36357DEE0CCC13DE5E927E24DF
SHA-512:	E8C319E10D348CA7767112EB0C3E938A8059E44134D352B6DE41B6EBC740F0B3EEA9DC31B06DBBC8460F445CF221767B44A5032D8C5E9EB400A6C3330890C71 B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.apple.com/ac/globalnav/5/en_GB/scripts/ac-globalnav.built.js
Preview:	!function(){function t(e,n,i){function r(o,a){if(!n[o]){if(!e[o]){var c="function"==typeof require&&require;if(!a&&c)return c(o,!0);if(s)return s(o,!0);var l=new Error("Cannot find module '"+o+"'");throw l.code="MODULE_NOT_FOUND",l}var u=n[o]={exports:{}};e[o][0].call(u.exports,function(t){var n=e[o][1][t];return r(n?n:t)},u,u.exports,t,e,n,i)}return n[o].exports}for(var s="function"==typeof require&&require,o=0;o<i.length;o++)r(i[o]);return r}return t}()({1:[function(t,e,n){"use strict";t("@marcom/ac-polyfills/Promise"),t("@marcom/ac-polyfills/Object/create");var i=null;try{i=t("@marcom/ac-storage")}catch(r){}var s=t("@marcom/ac-event-emitter-micro").EventEmitterMicro,o=t("mustach e"),a=t("Base64"),c=t("./cookie.js"),l="ac-store-cache",u={items:t("../mustache/items.mustache")},h=function(t,e){this.message=t,this.type=e,this.name="AcStoreError",this .stack=(new Error).stack};h.prototype=new Error,h.Types={BAD_JSON_RESPONSE:0,MISSING_API_ADD_TO_BAG:1,MISSING_API_FLYOUT:2,ITEM_NOT_ADDED:3}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\accsoffer[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	31218
Entropy (8bit):	5.300950490475622
Encrypted:	false
SSDEEP:	768:5mB+TFlYgUCgWQg3U+8+7gHd+f+9avqDw1om:5mBMFUqmkWJi
MD5:	BE8AF9E5638FCE2A428BE5DFAB8223D0
SHA1:	F13116709C891F1487B89EC47243F0928A83FE3F
SHA-256:	279E188D579ED99D1F41A9B526ABBD8CDAE2E7B5CA888711B82662E00F6398E7
SHA-512:	05C9C2DECEF1A5EDA6E42F1E33BB3D61D6B654A6E4A1CBCCAF5D1FBB65640D6EE352DDEEAEDC29B817EAC76C9B384A700830BFF5D44CE0CD8F8648E91A5 9174
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://support.apple.com/etc/designs/support/publish/JS/pattern/accsoffer.js
Preview:	var ACCSOffer = {. domain: "https://support.apple.com/",. acceptSurvey: function() {. var e = document.getElementById("accs_survey_offer");. null != e && (this.showThankYou(), this.launchSurvey(), this.setCookie("accs", "a", 90, "/", ".apple.com", !1)). },. check: function() {. this.isAppleCom() && this.hasCookiesEn abled() && this.hasValidPOD() && this.hasGlobalHeader() && this.isSelectBrowser() && this.isSelectedSample()&&!this.isSnkp()&&!this.hasACCS() && (this.showOffer(), this.setCookie("accs", "o", 90, "/", ".apple.com", !1)). },. closeOffer: function() {. var e = document.getElementsByClassName("accsoffer-wrapper");. null != e[0] && (!e[0].classList.contains("hide")) && (e[0].classList.add("hide")). },. declineSurvey: function() {. var e = document.getElementById("accs_survey_offer");. null != e && (this.closeOffer(), this.setCookie("accs", "d", 90, "/", ".apple.com", !1)). },. getAgent: function() {.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\admin-ajax[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):	80215
Entropy (8bit):	4.981882259312356
Encrypted:	false
SSDEEP:	768:TRDTwThTvTeTYiL4/fd5ne8tb1bR564SzhFtucXUh4cvoQwvVtQ9Md94Yk/RdJat:TRDTwThTvTeTY//F5nptDcfd4h9dJrg
MD5:	EE96154C37A8CAFF926558F434456188
SHA1:	5C174E278F858D9D08CC10E4E100034D124E6E0C
SHA-256:	6A90C54035905C9DD2657A066B546F6C5D9E6DEAF305CD6797B1CE96AE8B4FCF
SHA-512:	FB65783B0C5AB5EBB532E6F66040F20A0F601CB2FD1FA3B50134DA11AEAD03E68DFD8BB68EF1DF0A863C273D395F988E0610E2471A4F692456994D9A44FEE06 5
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\admin-ajax[1].css	
Reputation:	low
IE Cache URL:	http://https://www.digitalcontrolroom.com/wp-admin/admin-ajax.php?action=dynamic_css&ver=5.7.1
Preview:	...../*----------..#0 Body settings..----------*/.... body{.. background-color:#191a1b;.. }...../*----------..#1 Fonts / Typography..----------*/.....@font-face {.. font-family: "Aileron";.. src: url("https://www.digitalcontrolroom.com/wp-content/themes/cesis/includes/fonts/aileron/Aileron-Italic.otf");.. }..@font-face {.. font-family: "Aileron";.. src: url("https://www.digitalcontrolroom.com/wp-content/themes/cesis/includes/fonts/aileron/Aileron-BoldItalic.otf");.. font-weight: bold;..}..@font-face {.. font-family: "Aileron";.. src: url("https://www.digitalcontrolroom.com/wp-content/themes/cesis/includes/fonts/aileron/Aileron-LightItalic.otf");.. font-weight: 300;..}..@font-face {.. font-family: "Aileron";.. src: url("https://www.digitalco

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\appleicons_text[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 1032, version 1.0
Category:	downloaded
Size (bytes):	1032
Entropy (8bit):	6.965472723181528
Encrypted:	false
SSDEEP:	24:cq+HUax4AR4VlrSojyS0bFRQkw2F5oQDV45q9huw:s4AR4hbxuFRQIkq
MD5:	DBFB39700C2AE4BE64E11F56F67B8800
SHA1:	594A44BAFBE3C796DCD000C8A8A6EBBDEA553F6B
SHA-256:	B36E10199AE62E788FAB5E154B2694409745E146F026219436B71D5BCA185C69
SHA-512:	B22AE2A3127C972CD9249AF89759C14B8D36E76A41B1D556BE896E51F8C16DEB22CC612AB02F92C200842269CBB2EE90F78EBDFE683A67ADCF793C5BD7CA4A74
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.apple.com/ac/globalfooter/3/en_GB/assets/ac-footer/legacy/appleicons_text.woff
Preview:	wOFF.....h.....GSUB.....3...B....OS/2...<...C...VM.Nvcmap.....P...~.C..glyf.....C...Pm.9.head.....0...6.&..hhea…D.....$...Lhmtx...d.....loca...p.....(maxp...x..... ....name.....>...j...:post.....D.k\|.x.c`d``.b.c.a`tq..a.``a....cNfz"P.....i. f.....#.O.x.c`d..8.....s7...V...`.....X.....4.....?.{.P...Q.(.....I....x....0....@.AA.0T...$o.1x.N..+....%.....Z-...s.....2auO7i..>...OE}..M...x.c`d`...1.....A.YX...1..w....Ue....M.m.....E..0.9'#3P.....c..<.x.c`d``.....Y..m.2p...E...$."....:.\..&.(..U..x.c`d``....C.c...0.102..f.s.....h...h.....(x.c`d```f`c....L@.....\|...H.!.x...=N.0.....BBJ?.....:t...iS%..U.p.N..8.G.$.....~...s,.....Z...Y.....q.t.E...F..;./..x...nq..A..w..\..s...s.....x..t=w...=....EZg2.UQ..<.....l-]HS....pX..d!Md.Z.N.<l..&"1*.SUX.eJh.v2...Z=.....X..3H...P.....q.=.....FC.....!.gff.....[sn..#.u.....=.9i.n..3nE.]mG...)....I.?t....<.v...x.c`b.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\authorize[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	159505
Entropy (8bit):	5.495257419585801
Encrypted:	false
SSDEEP:	3072:B4HVHiQ+Btzhg/wZwouiqnnYJBa0ebb9ngYwniQYGf:BG+j3Zwo+YZelngJYM
MD5:	778373BB245C1F41FE7A0EB0B605BDDE
SHA1:	A5A1190AE5F288D69BC9FB38FA032B966A2241C0
SHA-256:	8498ED32B75DBDE58D1924A6E99B8B5528375FA41390E73AB355BDC262052DC2
SHA-512:	DE2F372B5728E6B191131D9B2A1F93915CE36757E1D08302B4F6B486E10093946E349F32683880F466B8B513DBE91DAD57AF925AA3E1AF9B2590F513FD8A42D5
Malicious:	false
Reputation:	low
Preview:	.... Copyright (C) Microsoft Corporation. All rights reserved. -->..<!DOCTYPE html>..<html>..<head>.. <title>Redirecting</title>.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <meta http-equiv="X-UA-Compatible" content="IE=edge">.. <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=2.0, user-scalable=yes">.. <meta http-equiv="Pragma" content="no-cache">.. <meta http-equiv="Expires" content="-1">.. <meta name="PageID" content="FetchSessions" />.. <meta name="SiteID" content="" />.. <meta name="ReqLC" content="1033" />.. <meta name="LocLC" content="en-US" />.... ..<meta name="robots" content="none" />....<script type="text/javascript">//<![CDATA[.$Config={"urlGetCredentialType":"https://login.microsoftonline.com/common/GetCredentialType?mkt=en-US","urlGoToAADError":"https://login.live.com/oauth20_authorize.srf?client_id=ee272b19-4411-433f-8f28-5c13cb6fd407\u0026scope=openid+profile+offline_acce

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\cesis_media_queries[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	9282
Entropy (8bit):	5.030730291225078
Encrypted:	false
SSDEEP:	192:dK/A7/sxcMEtxfPxeYservR+kw+MQTw+8QLDolwHCIguS:dK/O/sxcMEtxfPxe1ervR+kw+MQTw+8R
MD5:	EB99BD67EA8F79DE91A005862E7BC2F8
SHA1:	93E94316D8F7DAAA93BF8FA9EC992BE8F4E48665
SHA-256:	4CEFE7CD32CACA89D5F349C326C940AC5682A2ABA401C6D1827DC7B99CC1E0DC
SHA-512:	AFAA9D82C299FFCAC9820EEFEF19D94BF7EA006BB5502735CC68DCEE1D3AFE071824D100891951C7B7F553AD293DD71FAC5F841728D5140050CFC81CF58D9FD
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\cesis_media_queries[1].css	
Reputation:	low
IE Cache URL:	http://https://www.digitalcontrolroom.com/wp-content/themes/cesis/css/cesis_media_queries.css?ver=5.7.1
Preview:	/* WP ADMIN TOP BAR ADJUST */.....@media screen and (max-width: 782px){....cesis_nav_numbers { display: none;}...body.admin-bar .cesis_stuck {....top:46px;...} ....comments-layout-eight .depth-2, .comments-layout-eight .depth-3 {.. margin: 0 0 0 12px;...}..}..@media screen and (max-width: 600px){...body.admin-bar .cesis_stuck {....top:0px;...}..}.....}...../* MAX WIDTH ADJUST */.....@media only screen and (max-width: 1200px) {...desktop_full_width,...vc_column_container.desktop_full_width{..width: 100%;..}....}....@media only screen and (max-width: 1024px) {.....cesis_isotope.col_6 .cesis_iso_item,.cesis_isotope.col_5 .cesis_iso_item,.cesis_isotope.col_4 .cesis_iso_item{ width:calc(100% / 3); }...article_ctn.has_sidebar .cesis_isotope.col_6 .cesis_iso_item,.article_ctn.has_sidebar .cesis_isotope.col_5 .cesis_iso_item,...article_ctn.has_sidebar .cesis_isotope.col_4 .cesis_iso_item,.article_ctn.has_sidebar .cesis_isotope.col_3 .cesis_iso_item{ width:50%; }..}....@media only screen and (m

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\clientlib-site-min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	292913
Entropy (8bit):	4.985197955606192
Encrypted:	false
SSDEEP:	1536:hw/f1kv68/9kK2sOEsqbfR476HLSfRLNuu5+NPh1GQcQGQKQAFfH4m0TP1fMmMc8:SSPR47/9HP9FfHpyfhk84
MD5:	62F2C0B3B0591110D23F202A1092EF90
SHA1:	C11B9D62C38671E7D8E4C6DB65FB1307E74FE3DC
SHA-256:	BED0A97428BB147C0B759A4FFDFB03D1AEB406FC4B5471DB38B67F89AA3DBB0E
SHA-512:	F4DEF81303C5F191C3E7566055C2238C2CFD936AD8BFFEA37C0937F8BD56EEF9BF2E3A81BEFBDDDA0832F93073FAD6998EF85421773DBEB1BBFE08AF3B8476 2F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cookienotice.astrazeneca.com/etc.clientlibs/od-client/clientlibs/clientlib-site-min.css
Preview:	/*! normalize.css v3.0.3 | MIT License | github.com/necolas/normalize.css */html{font-family:sans-serif;-ms-text-size-adjust:100%;-webkit-text-size-adjust:100%}body{margin:0}article,aside,details,figcaption,figure,footer,header,hgroup,main,menu,nav,section,summary{display:block}audio,canvas,progress,video{display:inline-block;vertical-align:baseline}audio:not([controls]){display:none;height:0}[hidden],template{display:none}a{background-color:transparent}a:active,a:hover{outline:0}abbr[title]{border-bottom:none;text-decoration:underline;-webkit-text-decoration:underline dotted;text-decoration:underline dotted}b,strong{font-weight:bold}dfn{font-style:italic}h1{font-size:2em;margin:0.67em 0}mark{background:#ff0;color:#000}small{font-size:80%}sub,sup{font-size:75%;line-height:0;position:relative;vertical-align:baseline}sup{top:-0.5em}sub{bottom:-0.25em}img{border:0}svg:not(:root){overflow:hidden}figure{margin:1em 40px}hr{box-sizing:content-box;height:0}pre{overflow:auto}code,kbd,pre,samp{f

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	688
Entropy (8bit):	5.146868689676918
Encrypted:	false
SSDEEP:	12:jF3Y3Q6ZRoT6pa7aqF3Y3Q6ZN76pagBDNhqF3O6ZRoT6pamDaqF3O6ZN76paK2Y:53Y3QYslt3Y3QYN7l+503OYslG3OYN76
MD5:	73DB1B48682B0811B6D487E17AE38241
SHA1:	EF7688F4CEC8AA60FCC7D56BA0E3835FAD2E957D
SHA-256:	A47CFA3A7DF287053FB5084968E30A3563CE8235D08AA227008213CD33CF9DA9
SHA-512:	C7451D75E9EB8CFD8BC6D906913DFED94F9C516E3FB6BDD8393D70207E3150EABFE713F19FDEBE8C65EE043D72463550EEAD20D914976F16D73CFD0D785066 7
Malicious:	false
Reputation:	low
Preview:	@font-face {. font-family: 'Lato';. font-style: italic;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/lato/v17/S6u8w4BMUTPHjxsAXC-s.woff) format('woff');.}.@font-face {. font-family: 'Lato';. font-style: italic;. font-weight: 700;. src: url(https://fonts.gstatic.com/s/lato/v17/S6u_w4BMUTPHjxsI5wq_Gwfr.woff) format('woff');.}.@font-face {. font-family: 'Lato';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/lato/v17/S6uyw4BMUTPHjx4wWA.woff) format('woff');.}.@font-face {. font-family: 'Lato';. font-style: normal;. font-weight: 700;. src: url(https://fonts.gstatic.com/s/lato/v17/S6u9w4BMUTPHh6UVSwiPHw.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\css[2].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):	143792
Entropy (8bit):	5.380440401000318
Encrypted:	false
SSDEEP:	768:jbQbQbpPBUtdVoW4j7mb8Kjg0Opwv62zj9NGZdje3mdz5Amwih6u3LjWG58OOg/v:jcc5pp2zjnv3mN5VFh6u3LjR5v
MD5:	210D976F6F8131C3E335E330A53F4E01
SHA1:	BBF60A5AF4F20312CE65CE79490BC06160CDE04F
SHA-256:	D5B65695391D9739165E331D56512DA07D4DE09AC29AB908D3FEC8437FDAF015
SHA-512:	6145FBD5E2B6BF8D6B7536DBD4FA8C97CA7FA2AD3AE29DEC87633BDD66B31616608955CBA48C47A84208498612F69AE4A7FEA11ECDD89F360FA918C0913A3D D0
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\css[2].css	
IE Cache URL:	http://https://support.microsoft.com/SocContent/css
Preview:	@font-face{font-family:'OffSMDL2';src:url('/socfonts/OffSMDL2.4.00.woff') format('woff')}.HeaderUIFont{font-size:10pt;font-family:'Segoe UI Light','Segoe WP Light','wf_segoe-ui_light','wf_segoe-ui_normal','Segoe UI','Segoe WP',Helvetica,Tahoma,Arial,sans-serif;font-weight:300}.HeaderUIFont.macexcel,.HeaderUIFont.maconenote,.HeaderUIFont.macoutlook,.HeaderUIFont.macpowerpoint,.HeaderUIFont.macword{font-family:-apple-system,'Segoe UI Light','Segoe WP Light','wf_segoe-ui_light','wf_segoe-ui_normal','Segoe UI','Segoe WP',Helvetica,Tahoma,Arial,sans-serif}.HeaderUIFont.macexcel,.HeaderUIFont.maconenote,.HeaderUIFont.macoutlook,.HeaderUIFont.macpowerpoint,.HeaderUIFont.macword{font-family:-apple-system,'Segoe UI Light','Segoe WP Light','wf_segoe-ui_light','wf_segoe-ui_normal','Segoe UI','Segoe WP',Helvetica,Tahoma,Arial,sans-serif}.FooterUIFont{font-size:9pt;font-family:'wf_segoe-ui_semilight','wf_segoe-ui_light','Segoe UI Light','Segoe WP Light','wf_segoe-ui_normal','Segoe UI','Segoe WP',Ta

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\defaultlinks[1].json	
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):	637
Entropy (8bit):	5.0790684922947085
Encrypted:	false
SSDEEP:	12:Y9W/1Gg2rqZ9o8xJ/GMZwXhZ9o8yvo49rhZ9o8LGyhZ9o8CxqMN1hZ9o86KlviL+:Y0l2ua8xua8yg45a8Pa8CxqW9a8hlKL+
MD5:	2AD6CA866922DB633AB6A22719A297C8
SHA1:	5A3A964BE2E0334B852E46CFDD099FD4E0D747CF
SHA-256:	110D94EFA07E4AFDA7C2C14F49B8112E69C8EC031BE420DC7E19A01021D42994
SHA-512:	6004C5DD90D1C04FB289A4AE3037066B3501A9FCE8970FAC71FE6463CA2A604799C91B6B01C473F8B851E225A2D44F67B05BBDC914B4E5F6CDBDBCC564FCD31
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.apple.com/search-services/suggestions/defaultlinks/?src=globalnav_support&locale=en_GB
Preview:	{"id":"leo_pPheTbO3LgtHQl1KOw","results":[{"sectionName":"quickLinks","sectionResults":[{"url":"https://support.apple.com/en-gb/HT201487","label":"If you forgot your Apple ID password"},{"url":"https://support.apple.com/en-gb/HT204306","label":"If you forgot the passcode for your iPhone, iPad, or iPod touch"},{"url":"https://support.apple.com/en-gb/HT202039","label":"View, change, or cancel your subscriptions"},{"url":"https://support.apple.com/en-gb/HT204204","label":"Update iOS on your device"},{"url":"https://support.apple.com/en-gb/contact","label":"Contact Apple Support"}]},{"sectionName":"suggestions","sectionResults":[]}]}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\delete-cookies-in-microsoft-edge-63947406-40ac-c3b8-57b9-2a946a29ae09[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	94911
Entropy (8bit):	5.24486741990694
Encrypted:	false
SSDEEP:	768:QUaf0M9gPt90tA7rBBP1BM6UKjYcWgeAvvBAWCiT7dnPj1q2:vt6G7rBBRUGeAvvnCi1l
MD5:	1C2D11AAEBFCEC2B20228845A088C7E5
SHA1:	13C8FD39395047D33CFAA1F2A1648F5569A15AB4
SHA-256:	0DB0F190AD76CD1B7AD8687513E1DAAB2E5CAAA80F18E0156D9000B0438C8081
SHA-512:	53EC1444386CF3FB329C1C12AEB088BB401F410E7D8B882262644B854991F391BEE6C2131D56D433ED3EA6ED7EF2C95F4BE48AF5E9EC45B57EE755ECC306926A
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>..<html lang="en-US" dir="ltr">..<head>...<meta charset="utf-8" />...<meta name="viewport" content="width=device-width, initial-scale=1.0" />...<title>Delete cookies in Microsoft Edge</title>.....<link rel="canonical" href="https://support.microsoft.com/en-us/microsoft-edge/delete-cookies-in-microsoft-edge-63947406-40ac-c3b8-57b9-2a946a29ae09" />.....<meta name="description" content="Get the steps for how to delete cookies in Microsoft Edge." />...<meta name="firstPublishedDate" content="2020-09-13" />...<meta name="awa-kb_id" content="4027947" />...<meta name="lastPublishedDate" content="2020-10-28" />...<meta name="ms.lang" content="en" />...<meta name="ms.loc" content="US" />...<meta name="ms.product" content="a77ee9b7-b6b6-aa08-d7b9-887ebe228207,c6cab6e3-6598-6a1f-fbb2-f66d3740139d,31feb23d-f680-e1e0-1f97-ef7b00c80cdf,f825ca23-c7d1-aab8-4513-64980e1c3007,eb817b49-3474-1d34-f85a-76e229214fe7" />...<meta name="ms.productName" content="Microsoft Edge,Windows 10,Window

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vIlJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\dnserror[1]	
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/dnserror.htm?ErrorStatus=0x800C0005&DNSError=1460
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMoreInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\favicon-32x32[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 32 x 32, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	631
Entropy (8bit):	6.391875872958697
Encrypted:	false
SSDEEP:	12:6v/7s6UVprYe6IZeuLgou+/CAztgbbvCR00aJzS4VQIjXuYEMwoQIjXuHBOLPMdo:hX7rRkf+/rMcCJzAIjNEMwNIj8Efl9
MD5:	FB2ED9313C602F40B7A2762ACC15FF89
SHA1:	8A390D07A8401D40CBC1A16D873911FA4CB463F5
SHA-256:	B241D02FAB4B17291AF37993EB249F9303EB5897610ABAFAC4C9F6AA6A878369
SHA-512:	9CBCF5C7B8409494F6D543434ECAFF42DE8A2D0632A17931062D7D1CC130D43E61162EEDB0965B545E65E0687DED4D4B51E29631568AF34B157A7D02A385250
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://support.microsoft.com/favicon-32x32.png
Preview:	.PNG.....IHDR... ... .D.....gAMA.....a.... cHRM..z&.....u0...`.:....p..Q<...{PLTE.P".J$x.....P".P".J$x.....K..K..K..D.o..w..w..w.....P"...$tRNS.DD...CC..DEC..CEDDEC..CED...CC...DD.c,8....bKGD(.....pHYs.....~.....tIME.....'4...4...QIDAT8...G.. ...Q..s....?.....s.f..a`.A... .bA!.../dYQ.....a.((j^.m?4..Q.?.....2>.....%tEXtdate:create.2020-05-28T22:34:52+02:00.t.....%tEXtdate:modify.2020-05-28T22:34:52+02:00.)<'...WzTXtRaw profile type iptc..x.....qV((.O..I.R..#..c..#.K.... D.4.d.#.T .....H.J.....t.B5.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\favicon-32x32[2].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 32 x 32, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	1679
Entropy (8bit):	7.677946558535747
Encrypted:	false
SSDEEP:	48:hUloqMLT76V+BmqCtRRd1X9E4AzHOZXvYUykbX:+lg76V+cqCtTd1XAOZwULX
MD5:	6D2D6DC045E34A84AE2AED7ACD8BA786
SHA1:	DE31FBC3296B7075C6FC211223FDB305D7CEE310
SHA-256:	AEBBB1FA2B1BD20020B7E1B6BFE391EF607998E1A7AAB8C0E8D76853A8DE10F5
SHA-512:	F9E3AC368E4AC037805C09D049D03EAFBB15FE7A663E67666429C0766598FF6F5304F1ED4445B408722D27DED0507603AD1CC33D1AAB250ACC6697891AC438E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static-media-prod-cdn.itsre-sumo.mozilla.net/static/sumo/img/favicon-32x32.png
Preview:	.PNG.....IHDR... ... .D.....PLTE....'j..a.,e..W.Cg.&c.-l./..-j.4..&h..^.:...a.R..)h.4...K.D...d..Z.5..9k.B...U.7...aeW.B...k.l[Y]...\.qYy_...._.F...U..R..Y.<..&i..J..Z.&j.m\.&jb]..bl..O..a.9.5...R.*k..h.-g.6...[.Gg.3f..c..WmZ.;.R..'k.gd..|..^.b]l].9..'m..h.u....5^.Ph.=h..e..\..I.y...c..IPU..Pm.W..&c..h.)k.Bj..d..J.....y..:`.r.xa..UpXY...].Z\..M.>.7..Hl..h..R.L...Y....bq`...W.N].v[MU...Y.Z...dYd..~..^..K..YES...Z..o..h..i..]._..X.bo.Zo.9.U...e.J...c..\.....[?W..'i.CT..T.JT.SS..W..V..V.fS.]S..M..X.,X.vV.*V.[T.?T..T.nS.OS.AS.cR..G..b.._..^.&\..Z..X.pU.<U.HT.9T.XS.iO..I..H..G.R..K...}..e..d.)b.(`..\..\..\..[..Z..Y.&Y.UX.1X.cU..T.zS.iS.tR..P.pK.yF..E.[..[.g\.WV.sh..5d..a.O`..\.)\..Z.BY.zV.fU.@U..Q..P..H.jH.nG..F..F{^.}m.y.kh.x.....z..u..g.0]..[..Z.aZ..U..R..Q..P..O.}M-.pK....tRNS.o.....).QH.....~X'$.....|||oonlli@7410.'$.....{yvtnif\ZXWONEB><3$".^.i....IDAT8.b .p.qY..Zu9zb...2.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 1 icon, 256x256 withPNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced, 32 bits/pixel
Category:	downloaded
Size (bytes):	10715
Entropy (8bit):	7.9157754405002585
Encrypted:	false
SSDEEP:	192:cWwTt0ExGIIgwKrwQIW7ArhVCRG5aDiCQ1SqmyMVh0tBqS9Kx7:cWwTtf7K0XTHai71S5yyOqScV
MD5:	B20BEA7517931EBD5256F9717ECF171A
SHA1:	9EE48FD6E60E202A440E521A5DB9180409FCB921
SHA-256:	0D481AB07F79C252F66873FC9D89DE495B22EFC0E58E014E53A493E93CC9790A
SHA-512:	7753849D85D085CBC3A58E74CF6EA290067996A9288FA5C9EFD866733EA57C985FB73E0DFA85C37B2756399E1B814FE9EF8C108DE1C991767BFD6348C12C156
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\favicon[1].ico	
IE Cache URL:	http://https://covid19-immunization-learning-program-2021.ca/favicon.ico
Preview:	....).....PNG.....IHDR.....\r.f..).IDATx..g...._.4..... 0.+.....l.....^c.L2.&G.6i..X...`..a.....I(..H..j..SuU...>O?#.LW.....a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a..a.F...` ...G.....f=L#AL...J...&.....0...(`.`4....~..X.L.^....._IB._L...._....:.#0..W...Y...}...../M...@..a.....C./.}.<d...p1....&.y.....A.q..@....9p.p...L...@..2.^.....;~).....{.6...&..H....'..... r.p&p.....&..D.Z.'d..S.t..3....'L..'...!.....|.k.?A.F#'..4.!._...M...Pv@K....2... .l+.f.d`@FC...(2r..@.....m.>d..Y..@...`T..@N.../...M.....?.ih.....z.Fu....8.8.....(`?..b..f.9"d....[..Z..v.l..0& .9!dDCQ.....W./..e=..4&.9 "...4.O2.7i..{`.fNc..8!.....8.|x.w.[..nb..0!...\..L~....G....&...2.....Y..J..B#....8H._...yd{..`8...c.1.}..W.l.....!B.>.7~..&..g8...#Dx./'....b...1.p...Ry'd=.....;w..... ..Z....0... .1L.2$d.....}.J..9.....g.G..I...0G.c4.....O.4.:...B.0V.. .....8.8...{j.'...p...:...s,.c.#RnT..g.0..#...a..4.w\....hZL..D.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\hero-header-home[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=2, orientation=upper-left], progressive, precision 8, 1920x1256, frames 3
Category:	downloaded
Size (bytes):	177220
Entropy (8bit):	7.8377151982992155
Encrypted:	false
SSDEEP:	3072:Craqs9PTdhRHDaphrE6Cy4r/sgQ1hzF2BTMmVbz8fSbnLERlAC0q:CraqsBXaph1W/s3LzF2BT1AmnLo5
MD5:	EB7CB7D03AB514F9DA9EBD58ED2F9202
SHA1:	778AC27D49414EE074D9E6385F841BDEE93DCB62
SHA-256:	26ED9AA25711EBE90A644794D6E1E28BE98276A15350F710480EFE797DBC3D05
SHA-512:	911BEE67E1B711E6386A7ADEC51B174CA5FBD5445EBD373E9B82853153A6796A878591F1F07440396F5812CD1EACA0BC493834D26BE22DCC042A1216558805D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://dcr1.wpengine.com/wp-content/uploads/2018/09/hero-header-home.jpg?id=77
Preview:	......JFIF.....H.H.....XExif..MM.*.....i.....&.....8Photoshop 3.0.8BIM.....8BIM.%.....B~....."..... .....s.....!.1."..AQ2.aq#.. .B..R3.$b0..r.C.4...S@%c.5.s.PD...&T6d.t.`...p.'E7e.Uu.....Fv..GVf.....()*89:HIJWXYZghijwxyz..... .....!. 1A..0"2Q.@.3#aB.qR4.P$..C...b5S..%`.D.r...c6p&ET.'.....()*789:FGHIJUVWXYZdefghijstuvwxyz..... .....C.....&""&0-0>>T...C.....&""&0-0>>T.....r.-+B:..#)Y ..2.'..'D.N.5..2.x...OB.6....(-..Q`t.}p..... {..W...IY.6....I'H...G9F..2U..l)J..*.I.DS..4.m.&'Cm1.j.....b.....&&*!i.aQI.G%Q.J.ZaJb...TR...i"b$. ...U..I.Q...E%$.).S,.3&.X.FCT....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/httpErrorPagesScripts.js
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\icon-favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 5 icons, 16x16, 32 bits/pixel, 24x24, 32 bits/pixel
Category:	downloaded
Size (bytes):	34494
Entropy (8bit):	3.006582696711426
Encrypted:	false
SSDEEP:	192:LoFBgtgBXJezAAeduzdyrncolz25CMXfYK8pSfwX/pWeZ2gtaINCN7jS5O:MFB1J3ydFl8pf0wBN+7OA
MD5:	9E144A0398F4DC5CD6965650287D8200
SHA1:	DA4ECF3420FF2EEAFE36CB9C4CE46059DA839B5E
SHA-256:	DDFC903C81595BBA6B8A124DEAA4C7A32D5CA175829050247A54B2864C585418
SHA-512:	52969637EE99659F7A65A659B9C293EF9AC23A3EB7295DF4F424CC5A2E47AEEDA4E01F79ABF4134AA4B74F30B0AE37C7F02E35ABF7EC6A530ADD8EF9341E52F8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cookienotice.astrazeneca.com/etc/designs/digital/assets/favicons/icon-favicon.ico

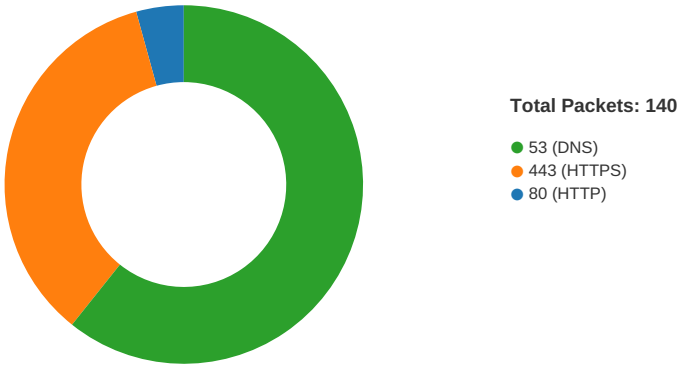
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\icon-favicon[1].ico	
Preview:	..... .h...V..... ....F...00.... ..%.....@@.... .(B...D..(..... ....d..... .....I.....(.....@.....\.....).....I.....(.....d.....".."..I.....Z..... .$.....b.....,,.....V.....<.....J.....(...H.... .....T.....t.....F..`.....F.....&..... ....."..... L2..... <.....4.....I.....8.....*.....2.....*.

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 01:24:47.247925997 CEST	49711	80	192.168.2.3	162.241.217.204
May 4, 2021 01:24:47.248343945 CEST	49712	80	192.168.2.3	162.241.217.204
May 4, 2021 01:24:47.408269882 CEST	80	49712	162.241.217.204	192.168.2.3
May 4, 2021 01:24:47.408390045 CEST	49712	80	192.168.2.3	162.241.217.204
May 4, 2021 01:24:47.409138918 CEST	49712	80	192.168.2.3	162.241.217.204
May 4, 2021 01:24:47.412139893 CEST	80	49711	162.241.217.204	192.168.2.3
May 4, 2021 01:24:47.412291050 CEST	49711	80	192.168.2.3	162.241.217.204
May 4, 2021 01:24:47.568977118 CEST	80	49712	162.241.217.204	192.168.2.3
May 4, 2021 01:24:47.580990076 CEST	80	49712	162.241.217.204	192.168.2.3
May 4, 2021 01:24:47.581170082 CEST	49712	80	192.168.2.3	162.241.217.204
May 4, 2021 01:24:47.605207920 CEST	49714	443	192.168.2.3	162.241.217.204
May 4, 2021 01:24:47.770730972 CEST	443	49714	162.241.217.204	192.168.2.3
May 4, 2021 01:24:47.770984888 CEST	49714	443	192.168.2.3	162.241.217.204
May 4, 2021 01:24:47.777338028 CEST	49714	443	192.168.2.3	162.241.217.204
May 4, 2021 01:24:47.941281080 CEST	443	49714	162.241.217.204	192.168.2.3
May 4, 2021 01:24:47.945332050 CEST	443	49714	162.241.217.204	192.168.2.3
May 4, 2021 01:24:47.945364952 CEST	443	49714	162.241.217.204	192.168.2.3
May 4, 2021 01:24:47.945408106 CEST	443	49714	162.241.217.204	192.168.2.3
May 4, 2021 01:24:47.945477009 CEST	49714	443	192.168.2.3	162.241.217.204
May 4, 2021 01:24:47.945547104 CEST	49714	443	192.168.2.3	162.241.217.204
May 4, 2021 01:24:47.976507902 CEST	49714	443	192.168.2.3	162.241.217.204
May 4, 2021 01:24:47.983603001 CEST	49714	443	192.168.2.3	162.241.217.204
May 4, 2021 01:24:47.984473944 CEST	49714	443	192.168.2.3	162.241.217.204
May 4, 2021 01:24:48.140089035 CEST	443	49714	162.241.217.204	192.168.2.3
May 4, 2021 01:24:48.140142918 CEST	443	49714	162.241.217.204	192.168.2.3

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 01:24:48.140209913 CEST	49714	443	192.168.2.3	162.241.217.204
May 4, 2021 01:24:48.140258074 CEST	49714	443	192.168.2.3	162.241.217.204
May 4, 2021 01:24:48.149275064 CEST	443	49714	162.241.217.204	192.168.2.3
May 4, 2021 01:24:48.149307013 CEST	443	49714	162.241.217.204	192.168.2.3
May 4, 2021 01:24:48.149408102 CEST	49714	443	192.168.2.3	162.241.217.204
May 4, 2021 01:24:48.157895088 CEST	443	49714	162.241.217.204	192.168.2.3
May 4, 2021 01:24:48.157954931 CEST	443	49714	162.241.217.204	192.168.2.3
May 4, 2021 01:24:48.158010960 CEST	49714	443	192.168.2.3	162.241.217.204
May 4, 2021 01:24:48.161552906 CEST	49714	443	192.168.2.3	162.241.217.204
May 4, 2021 01:24:48.171736002 CEST	49714	443	192.168.2.3	162.241.217.204
May 4, 2021 01:24:48.223685026 CEST	49714	443	192.168.2.3	162.241.217.204
May 4, 2021 01:24:48.224108934 CEST	49714	443	192.168.2.3	162.241.217.204
May 4, 2021 01:24:48.242922068 CEST	49714	443	192.168.2.3	162.241.217.204
May 4, 2021 01:24:48.243339062 CEST	49714	443	192.168.2.3	162.241.217.204
May 4, 2021 01:24:48.320313931 CEST	49715	443	192.168.2.3	34.107.253.133
May 4, 2021 01:24:48.321082115 CEST	49716	443	192.168.2.3	34.107.253.133
May 4, 2021 01:24:48.361437082 CEST	443	49715	34.107.253.133	192.168.2.3
May 4, 2021 01:24:48.361665010 CEST	49715	443	192.168.2.3	34.107.253.133
May 4, 2021 01:24:48.361990929 CEST	443	49716	34.107.253.133	192.168.2.3
May 4, 2021 01:24:48.362102032 CEST	49716	443	192.168.2.3	34.107.253.133
May 4, 2021 01:24:48.376386881 CEST	443	49714	162.241.217.204	192.168.2.3
May 4, 2021 01:24:48.386512041 CEST	443	49714	162.241.217.204	192.168.2.3
May 4, 2021 01:24:48.386569977 CEST	443	49714	162.241.217.204	192.168.2.3
May 4, 2021 01:24:48.392992020 CEST	443	49714	162.241.217.204	192.168.2.3
May 4, 2021 01:24:48.393148899 CEST	49714	443	192.168.2.3	162.241.217.204
May 4, 2021 01:24:48.414959908 CEST	443	49714	162.241.217.204	192.168.2.3
May 4, 2021 01:24:48.417172909 CEST	443	49714	162.241.217.204	192.168.2.3
May 4, 2021 01:24:48.417310953 CEST	49714	443	192.168.2.3	162.241.217.204
May 4, 2021 01:24:48.417439938 CEST	443	49714	162.241.217.204	192.168.2.3
May 4, 2021 01:24:48.417500019 CEST	443	49714	162.241.217.204	192.168.2.3
May 4, 2021 01:24:48.417517900 CEST	49714	443	192.168.2.3	162.241.217.204
May 4, 2021 01:24:48.417551994 CEST	443	49714	162.241.217.204	192.168.2.3
May 4, 2021 01:24:48.417557955 CEST	49714	443	192.168.2.3	162.241.217.204
May 4, 2021 01:24:48.417604923 CEST	443	49714	162.241.217.204	192.168.2.3
May 4, 2021 01:24:48.417607069 CEST	49714	443	192.168.2.3	162.241.217.204
May 4, 2021 01:24:48.417655945 CEST	443	49714	162.241.217.204	192.168.2.3
May 4, 2021 01:24:48.417659044 CEST	49714	443	192.168.2.3	162.241.217.204
May 4, 2021 01:24:48.417706966 CEST	443	49714	162.241.217.204	192.168.2.3
May 4, 2021 01:24:48.417711973 CEST	49714	443	192.168.2.3	162.241.217.204
May 4, 2021 01:24:48.417757988 CEST	443	49714	162.241.217.204	192.168.2.3
May 4, 2021 01:24:48.417762995 CEST	49714	443	192.168.2.3	162.241.217.204
May 4, 2021 01:24:48.417814970 CEST	49714	443	192.168.2.3	162.241.217.204
May 4, 2021 01:24:48.417821884 CEST	443	49714	162.241.217.204	192.168.2.3
May 4, 2021 01:24:48.417881012 CEST	49714	443	192.168.2.3	162.241.217.204
May 4, 2021 01:24:48.485899925 CEST	49715	443	192.168.2.3	34.107.253.133
May 4, 2021 01:24:48.486553907 CEST	49716	443	192.168.2.3	34.107.253.133
May 4, 2021 01:24:48.527062893 CEST	443	49715	34.107.253.133	192.168.2.3
May 4, 2021 01:24:48.527523994 CEST	443	49716	34.107.253.133	192.168.2.3
May 4, 2021 01:24:48.527837038 CEST	443	49715	34.107.253.133	192.168.2.3
May 4, 2021 01:24:48.527889967 CEST	443	49715	34.107.253.133	192.168.2.3
May 4, 2021 01:24:48.527932882 CEST	443	49715	34.107.253.133	192.168.2.3
May 4, 2021 01:24:48.527955055 CEST	49715	443	192.168.2.3	34.107.253.133
May 4, 2021 01:24:48.527967930 CEST	443	49715	34.107.253.133	192.168.2.3
May 4, 2021 01:24:48.527991056 CEST	49715	443	192.168.2.3	34.107.253.133
May 4, 2021 01:24:48.527997971 CEST	49715	443	192.168.2.3	34.107.253.133
May 4, 2021 01:24:48.528012037 CEST	49715	443	192.168.2.3	34.107.253.133
May 4, 2021 01:24:48.529001951 CEST	443	49716	34.107.253.133	192.168.2.3
May 4, 2021 01:24:48.529048920 CEST	443	49716	34.107.253.133	192.168.2.3
May 4, 2021 01:24:48.529076099 CEST	49716	443	192.168.2.3	34.107.253.133
May 4, 2021 01:24:48.529087067 CEST	443	49716	34.107.253.133	192.168.2.3
May 4, 2021 01:24:48.529104948 CEST	49716	443	192.168.2.3	34.107.253.133
May 4, 2021 01:24:48.529133081 CEST	49716	443	192.168.2.3	34.107.253.133
May 4, 2021 01:24:48.529133081 CEST	443	49716	34.107.253.133	192.168.2.3
May 4, 2021 01:24:48.529181957 CEST	49716	443	192.168.2.3	34.107.253.133

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 01:24:48.538295031 CEST	49715	443	192.168.2.3	34.107.253.133
May 4, 2021 01:24:48.538754940 CEST	49715	443	192.168.2.3	34.107.253.133
May 4, 2021 01:24:48.538980961 CEST	49715	443	192.168.2.3	34.107.253.133
May 4, 2021 01:24:48.545327902 CEST	49716	443	192.168.2.3	34.107.253.133
May 4, 2021 01:24:48.545766115 CEST	49716	443	192.168.2.3	34.107.253.133
May 4, 2021 01:24:48.555763960 CEST	443	49714	162.241.217.204	192.168.2.3
May 4, 2021 01:24:48.555814028 CEST	443	49714	162.241.217.204	192.168.2.3
May 4, 2021 01:24:48.555890083 CEST	49714	443	192.168.2.3	162.241.217.204
May 4, 2021 01:24:48.555922031 CEST	49714	443	192.168.2.3	162.241.217.204
May 4, 2021 01:24:48.579632998 CEST	443	49715	34.107.253.133	192.168.2.3
May 4, 2021 01:24:48.579674959 CEST	443	49715	34.107.253.133	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 01:24:39.772430897 CEST	64938	53	192.168.2.3	8.8.8.8
May 4, 2021 01:24:39.834428072 CEST	53	64938	8.8.8.8	192.168.2.3
May 4, 2021 01:24:40.796560049 CEST	60152	53	192.168.2.3	8.8.8.8
May 4, 2021 01:24:40.845299959 CEST	53	60152	8.8.8.8	192.168.2.3
May 4, 2021 01:24:41.267678022 CEST	57544	53	192.168.2.3	8.8.8.8
May 4, 2021 01:24:41.327374935 CEST	53	57544	8.8.8.8	192.168.2.3
May 4, 2021 01:24:41.697935104 CEST	55984	53	192.168.2.3	8.8.8.8
May 4, 2021 01:24:41.746921062 CEST	53	55984	8.8.8.8	192.168.2.3
May 4, 2021 01:24:42.588962078 CEST	64185	53	192.168.2.3	8.8.8.8
May 4, 2021 01:24:42.643205881 CEST	53	64185	8.8.8.8	192.168.2.3
May 4, 2021 01:24:43.553642988 CEST	65110	53	192.168.2.3	8.8.8.8
May 4, 2021 01:24:43.605556965 CEST	53	65110	8.8.8.8	192.168.2.3
May 4, 2021 01:24:44.690043926 CEST	58361	53	192.168.2.3	8.8.8.8
May 4, 2021 01:24:44.742558956 CEST	53	58361	8.8.8.8	192.168.2.3
May 4, 2021 01:24:45.993046999 CEST	63492	53	192.168.2.3	8.8.8.8
May 4, 2021 01:24:46.062752962 CEST	53	63492	8.8.8.8	192.168.2.3
May 4, 2021 01:24:46.229286909 CEST	60831	53	192.168.2.3	8.8.8.8
May 4, 2021 01:24:46.287730932 CEST	53	60831	8.8.8.8	192.168.2.3
May 4, 2021 01:24:47.177257061 CEST	60100	53	192.168.2.3	8.8.8.8
May 4, 2021 01:24:47.239017963 CEST	53	60100	8.8.8.8	192.168.2.3
May 4, 2021 01:24:47.283437014 CEST	53195	53	192.168.2.3	8.8.8.8
May 4, 2021 01:24:47.333779097 CEST	53	53195	8.8.8.8	192.168.2.3
May 4, 2021 01:24:48.253345013 CEST	50141	53	192.168.2.3	8.8.8.8
May 4, 2021 01:24:48.315568924 CEST	53	50141	8.8.8.8	192.168.2.3
May 4, 2021 01:24:48.647979021 CEST	53023	53	192.168.2.3	8.8.8.8
May 4, 2021 01:24:48.696866035 CEST	53	53023	8.8.8.8	192.168.2.3
May 4, 2021 01:24:49.095041037 CEST	49563	53	192.168.2.3	8.8.8.8
May 4, 2021 01:24:49.156732082 CEST	53	49563	8.8.8.8	192.168.2.3
May 4, 2021 01:24:49.536240101 CEST	51352	53	192.168.2.3	8.8.8.8
May 4, 2021 01:24:49.596420050 CEST	53	51352	8.8.8.8	192.168.2.3
May 4, 2021 01:24:49.828206062 CEST	59349	53	192.168.2.3	8.8.8.8
May 4, 2021 01:24:49.885930061 CEST	53	59349	8.8.8.8	192.168.2.3
May 4, 2021 01:24:50.483705997 CEST	57084	53	192.168.2.3	8.8.8.8
May 4, 2021 01:24:50.532836914 CEST	53	57084	8.8.8.8	192.168.2.3
May 4, 2021 01:24:51.295516014 CEST	58823	53	192.168.2.3	8.8.8.8
May 4, 2021 01:24:51.346648932 CEST	53	58823	8.8.8.8	192.168.2.3
May 4, 2021 01:24:52.089411974 CEST	57568	53	192.168.2.3	8.8.8.8
May 4, 2021 01:24:52.140088081 CEST	53	57568	8.8.8.8	192.168.2.3
May 4, 2021 01:24:52.904548883 CEST	50540	53	192.168.2.3	8.8.8.8
May 4, 2021 01:24:52.955344915 CEST	53	50540	8.8.8.8	192.168.2.3
May 4, 2021 01:24:53.742089033 CEST	54366	53	192.168.2.3	8.8.8.8
May 4, 2021 01:24:53.793060064 CEST	53	54366	8.8.8.8	192.168.2.3
May 4, 2021 01:24:55.039926052 CEST	53034	53	192.168.2.3	8.8.8.8
May 4, 2021 01:24:55.099745989 CEST	53	53034	8.8.8.8	192.168.2.3
May 4, 2021 01:24:56.443106890 CEST	57762	53	192.168.2.3	8.8.8.8
May 4, 2021 01:24:56.497252941 CEST	53	57762	8.8.8.8	192.168.2.3
May 4, 2021 01:24:57.215476036 CEST	55435	53	192.168.2.3	8.8.8.8
May 4, 2021 01:24:57.272572994 CEST	53	55435	8.8.8.8	192.168.2.3
May 4, 2021 01:25:03.523101091 CEST	50713	53	192.168.2.3	8.8.8.8

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 01:25:03.582927942 CEST	53	50713	8.8.8.8	192.168.2.3
May 4, 2021 01:25:03.850909948 CEST	56132	53	192.168.2.3	8.8.8.8
May 4, 2021 01:25:03.913827896 CEST	53	56132	8.8.8.8	192.168.2.3
May 4, 2021 01:25:05.770162106 CEST	58987	53	192.168.2.3	8.8.8.8
May 4, 2021 01:25:05.838104010 CEST	53	58987	8.8.8.8	192.168.2.3
May 4, 2021 01:25:08.063203096 CEST	56579	53	192.168.2.3	8.8.8.8
May 4, 2021 01:25:08.137366056 CEST	53	56579	8.8.8.8	192.168.2.3
May 4, 2021 01:25:08.507436991 CEST	60633	53	192.168.2.3	8.8.8.8
May 4, 2021 01:25:08.551635027 CEST	61292	53	192.168.2.3	8.8.8.8
May 4, 2021 01:25:08.572285891 CEST	53	60633	8.8.8.8	192.168.2.3
May 4, 2021 01:25:08.615670919 CEST	53	61292	8.8.8.8	192.168.2.3
May 4, 2021 01:25:16.009303093 CEST	63619	53	192.168.2.3	8.8.8.8
May 4, 2021 01:25:16.069305897 CEST	53	63619	8.8.8.8	192.168.2.3
May 4, 2021 01:25:16.647789001 CEST	64938	53	192.168.2.3	8.8.8.8
May 4, 2021 01:25:16.711483955 CEST	53	64938	8.8.8.8	192.168.2.3
May 4, 2021 01:25:17.020159006 CEST	63619	53	192.168.2.3	8.8.8.8
May 4, 2021 01:25:17.070732117 CEST	53	63619	8.8.8.8	192.168.2.3
May 4, 2021 01:25:17.348227978 CEST	61946	53	192.168.2.3	8.8.8.8
May 4, 2021 01:25:17.410413980 CEST	53	61946	8.8.8.8	192.168.2.3
May 4, 2021 01:25:17.658730030 CEST	64938	53	192.168.2.3	8.8.8.8
May 4, 2021 01:25:17.720824003 CEST	53	64938	8.8.8.8	192.168.2.3
May 4, 2021 01:25:18.090729952 CEST	52123	53	192.168.2.3	8.8.8.8
May 4, 2021 01:25:18.091070890 CEST	64910	53	192.168.2.3	8.8.8.8
May 4, 2021 01:25:18.094573975 CEST	56130	53	192.168.2.3	8.8.8.8
May 4, 2021 01:25:18.097388983 CEST	63619	53	192.168.2.3	8.8.8.8
May 4, 2021 01:25:18.148113966 CEST	53	63619	8.8.8.8	192.168.2.3
May 4, 2021 01:25:18.151289940 CEST	53	52123	8.8.8.8	192.168.2.3
May 4, 2021 01:25:18.154629946 CEST	53	56130	8.8.8.8	192.168.2.3
May 4, 2021 01:25:18.164729118 CEST	53	64910	8.8.8.8	192.168.2.3
May 4, 2021 01:25:18.175074100 CEST	56338	53	192.168.2.3	8.8.8.8
May 4, 2021 01:25:18.238605976 CEST	53	56338	8.8.8.8	192.168.2.3
May 4, 2021 01:25:18.413026094 CEST	59420	53	192.168.2.3	8.8.8.8
May 4, 2021 01:25:18.473867893 CEST	53	59420	8.8.8.8	192.168.2.3
May 4, 2021 01:25:18.646018982 CEST	58784	53	192.168.2.3	8.8.8.8
May 4, 2021 01:25:18.674361944 CEST	64938	53	192.168.2.3	8.8.8.8
May 4, 2021 01:25:18.717649937 CEST	63978	53	192.168.2.3	8.8.8.8
May 4, 2021 01:25:18.719945908 CEST	53	58784	8.8.8.8	192.168.2.3
May 4, 2021 01:25:18.736723900 CEST	53	64938	8.8.8.8	192.168.2.3
May 4, 2021 01:25:18.758080006 CEST	62938	53	192.168.2.3	8.8.8.8
May 4, 2021 01:25:18.785808086 CEST	53	63978	8.8.8.8	192.168.2.3
May 4, 2021 01:25:18.837960958 CEST	53	62938	8.8.8.8	192.168.2.3
May 4, 2021 01:25:19.064469099 CEST	55708	53	192.168.2.3	8.8.8.8
May 4, 2021 01:25:19.125322104 CEST	53	55708	8.8.8.8	192.168.2.3
May 4, 2021 01:25:19.540093899 CEST	56803	53	192.168.2.3	8.8.8.8
May 4, 2021 01:25:19.613876104 CEST	53	56803	8.8.8.8	192.168.2.3
May 4, 2021 01:25:19.675334930 CEST	57145	53	192.168.2.3	8.8.8.8
May 4, 2021 01:25:19.755296946 CEST	53	57145	8.8.8.8	192.168.2.3
May 4, 2021 01:25:20.102020025 CEST	63619	53	192.168.2.3	8.8.8.8
May 4, 2021 01:25:20.161333084 CEST	53	63619	8.8.8.8	192.168.2.3
May 4, 2021 01:25:20.262464046 CEST	55359	53	192.168.2.3	8.8.8.8
May 4, 2021 01:25:20.321536064 CEST	53	55359	8.8.8.8	192.168.2.3
May 4, 2021 01:25:20.602355003 CEST	58306	53	192.168.2.3	8.8.8.8
May 4, 2021 01:25:20.662208080 CEST	53	58306	8.8.8.8	192.168.2.3
May 4, 2021 01:25:20.684313059 CEST	64938	53	192.168.2.3	8.8.8.8
May 4, 2021 01:25:20.746216059 CEST	53	64938	8.8.8.8	192.168.2.3
May 4, 2021 01:25:21.235915899 CEST	64124	53	192.168.2.3	8.8.8.8
May 4, 2021 01:25:21.286818981 CEST	53	64124	8.8.8.8	192.168.2.3
May 4, 2021 01:25:22.002759933 CEST	49361	53	192.168.2.3	8.8.8.8
May 4, 2021 01:25:22.067234039 CEST	53	49361	8.8.8.8	192.168.2.3
May 4, 2021 01:25:22.420224905 CEST	63150	53	192.168.2.3	8.8.8.8
May 4, 2021 01:25:22.475182056 CEST	53279	53	192.168.2.3	8.8.8.8
May 4, 2021 01:25:22.477579117 CEST	56881	53	192.168.2.3	8.8.8.8
May 4, 2021 01:25:22.490744114 CEST	53642	53	192.168.2.3	8.8.8.8
May 4, 2021 01:25:22.494678974 CEST	55667	53	192.168.2.3	8.8.8.8

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 01:25:22.496942043 CEST	53	63150	8.8.8.8	192.168.2.3
May 4, 2021 01:25:22.538800955 CEST	53	53279	8.8.8.8	192.168.2.3
May 4, 2021 01:25:22.538834095 CEST	53	56881	8.8.8.8	192.168.2.3
May 4, 2021 01:25:22.557235003 CEST	53	55667	8.8.8.8	192.168.2.3
May 4, 2021 01:25:22.579062939 CEST	53	53642	8.8.8.8	192.168.2.3
May 4, 2021 01:25:24.106790066 CEST	63619	53	192.168.2.3	8.8.8.8
May 4, 2021 01:25:24.163892984 CEST	53	63619	8.8.8.8	192.168.2.3
May 4, 2021 01:25:24.353290081 CEST	54833	53	192.168.2.3	8.8.8.8
May 4, 2021 01:25:24.412828922 CEST	53	54833	8.8.8.8	192.168.2.3
May 4, 2021 01:25:24.685015917 CEST	64938	53	192.168.2.3	8.8.8.8
May 4, 2021 01:25:24.747102976 CEST	53	64938	8.8.8.8	192.168.2.3
May 4, 2021 01:25:26.751672029 CEST	62476	53	192.168.2.3	8.8.8.8
May 4, 2021 01:25:26.778603077 CEST	49705	53	192.168.2.3	8.8.8.8
May 4, 2021 01:25:26.815376043 CEST	53	62476	8.8.8.8	192.168.2.3
May 4, 2021 01:25:26.841543913 CEST	53	49705	8.8.8.8	192.168.2.3
May 4, 2021 01:25:33.197815895 CEST	61477	53	192.168.2.3	8.8.8.8
May 4, 2021 01:25:33.255875111 CEST	53	61477	8.8.8.8	192.168.2.3
May 4, 2021 01:25:34.197284937 CEST	61477	53	192.168.2.3	8.8.8.8
May 4, 2021 01:25:34.254617929 CEST	53	61477	8.8.8.8	192.168.2.3
May 4, 2021 01:25:34.899647951 CEST	61633	53	192.168.2.3	8.8.8.8
May 4, 2021 01:25:34.960094929 CEST	53	61633	8.8.8.8	192.168.2.3
May 4, 2021 01:25:35.213160038 CEST	61477	53	192.168.2.3	8.8.8.8
May 4, 2021 01:25:35.274631023 CEST	53	61477	8.8.8.8	192.168.2.3
May 4, 2021 01:25:37.302902937 CEST	61477	53	192.168.2.3	8.8.8.8
May 4, 2021 01:25:37.314934015 CEST	55949	53	192.168.2.3	8.8.8.8
May 4, 2021 01:25:37.353507996 CEST	53	61477	8.8.8.8	192.168.2.3
May 4, 2021 01:25:37.373075962 CEST	53	55949	8.8.8.8	192.168.2.3
May 4, 2021 01:25:37.881292105 CEST	57601	53	192.168.2.3	8.8.8.8
May 4, 2021 01:25:37.938509941 CEST	53	57601	8.8.8.8	192.168.2.3
May 4, 2021 01:25:41.313769102 CEST	61477	53	192.168.2.3	8.8.8.8
May 4, 2021 01:25:41.364413023 CEST	53	61477	8.8.8.8	192.168.2.3
May 4, 2021 01:25:48.943474054 CEST	49342	53	192.168.2.3	8.8.8.8
May 4, 2021 01:25:49.008601904 CEST	53	49342	8.8.8.8	192.168.2.3
May 4, 2021 01:26:11.890301943 CEST	56253	53	192.168.2.3	8.8.8.8
May 4, 2021 01:26:11.949265003 CEST	53	56253	8.8.8.8	192.168.2.3
May 4, 2021 01:26:18.956798077 CEST	49667	53	192.168.2.3	8.8.8.8
May 4, 2021 01:26:19.070085049 CEST	53	49667	8.8.8.8	192.168.2.3
May 4, 2021 01:26:20.036361933 CEST	55439	53	192.168.2.3	8.8.8.8
May 4, 2021 01:26:20.096797943 CEST	53	55439	8.8.8.8	192.168.2.3
May 4, 2021 01:26:20.667891979 CEST	57069	53	192.168.2.3	8.8.8.8
May 4, 2021 01:26:20.728195906 CEST	53	57069	8.8.8.8	192.168.2.3
May 4, 2021 01:26:20.881407976 CEST	57659	53	192.168.2.3	8.8.8.8
May 4, 2021 01:26:20.954644918 CEST	53	57659	8.8.8.8	192.168.2.3
May 4, 2021 01:26:21.145883083 CEST	54717	53	192.168.2.3	8.8.8.8
May 4, 2021 01:26:21.203392029 CEST	53	54717	8.8.8.8	192.168.2.3
May 4, 2021 01:26:21.743024111 CEST	63975	53	192.168.2.3	8.8.8.8
May 4, 2021 01:26:21.851202011 CEST	53	63975	8.8.8.8	192.168.2.3
May 4, 2021 01:26:22.765949965 CEST	56639	53	192.168.2.3	8.8.8.8
May 4, 2021 01:26:22.828380108 CEST	53	56639	8.8.8.8	192.168.2.3
May 4, 2021 01:26:23.708231926 CEST	51856	53	192.168.2.3	8.8.8.8
May 4, 2021 01:26:23.765518904 CEST	53	51856	8.8.8.8	192.168.2.3
May 4, 2021 01:26:25.156766891 CEST	56546	53	192.168.2.3	8.8.8.8
May 4, 2021 01:26:25.217286110 CEST	53	56546	8.8.8.8	192.168.2.3
May 4, 2021 01:26:26.037811041 CEST	62152	53	192.168.2.3	8.8.8.8
May 4, 2021 01:26:26.089303017 CEST	53	62152	8.8.8.8	192.168.2.3
May 4, 2021 01:26:26.547549009 CEST	53470	53	192.168.2.3	8.8.8.8
May 4, 2021 01:26:26.605398893 CEST	53	53470	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 01:24:47.177257061 CEST	192.168.2.3	8.8.8.8	0x531c	Standard query (0)	covid19-immunization-learning-program-2021.ca	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 01:24:48.253345013 CEST	192.168.2.3	8.8.8.8	0x12a3	Standard query (0)	policy.cookiereports.com	A (IP address)	IN (0x0001)
May 4, 2021 01:25:03.523101091 CEST	192.168.2.3	8.8.8.8	0x6721	Standard query (0)	covid19-immunization-learning-program-2021.ca	A (IP address)	IN (0x0001)
May 4, 2021 01:25:03.850909948 CEST	192.168.2.3	8.8.8.8	0xe9dd	Standard query (0)	cookienotice.astrazeneca.com	A (IP address)	IN (0x0001)
May 4, 2021 01:25:05.770162106 CEST	192.168.2.3	8.8.8.8	0xbb73	Standard query (0)	cookienotice.astrazeneca.com	A (IP address)	IN (0x0001)
May 4, 2021 01:25:08.063203096 CEST	192.168.2.3	8.8.8.8	0x3501	Standard query (0)	www.digitalcontrolroom.com	A (IP address)	IN (0x0001)
May 4, 2021 01:25:08.551635027 CEST	192.168.2.3	8.8.8.8	0x3e6a	Standard query (0)	dcr1.wpengine.com	A (IP address)	IN (0x0001)
May 4, 2021 01:25:18.175074100 CEST	192.168.2.3	8.8.8.8	0x71cf	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
May 4, 2021 01:25:18.646018982 CEST	192.168.2.3	8.8.8.8	0xe13d	Standard query (0)	js.monitor.azure.com	A (IP address)	IN (0x0001)
May 4, 2021 01:25:18.758080006 CEST	192.168.2.3	8.8.8.8	0x90f	Standard query (0)	mem.gfx.ms	A (IP address)	IN (0x0001)
May 4, 2021 01:25:19.675334930 CEST	192.168.2.3	8.8.8.8	0x9b01	Standard query (0)	login.microsoftonline.com	A (IP address)	IN (0x0001)
May 4, 2021 01:25:24.353290081 CEST	192.168.2.3	8.8.8.8	0xd83f	Standard query (0)	support.mozilla.org	A (IP address)	IN (0x0001)
May 4, 2021 01:25:26.751672029 CEST	192.168.2.3	8.8.8.8	0x59b0	Standard query (0)	static-media-prod-cdn.itsre-sumo.mozilla.net	A (IP address)	IN (0x0001)
May 4, 2021 01:25:26.778603077 CEST	192.168.2.3	8.8.8.8	0xe6c7	Standard query (0)	user-media-prod-cdn.itsre-sumo.mozilla.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 01:24:47.239017963 CEST	8.8.8.8	192.168.2.3	0x531c	No error (0)	covid19-immunization-learning-program-2021.ca		162.241.217.204	A (IP address)	IN (0x0001)
May 4, 2021 01:24:48.315568924 CEST	8.8.8.8	192.168.2.3	0x12a3	No error (0)	policy.cookiereports.com		34.107.253.133	A (IP address)	IN (0x0001)
May 4, 2021 01:25:03.582927942 CEST	8.8.8.8	192.168.2.3	0x6721	No error (0)	covid19-immunization-learning-program-2021.ca		162.241.217.204	A (IP address)	IN (0x0001)
May 4, 2021 01:25:03.913827896 CEST	8.8.8.8	192.168.2.3	0xe9dd	No error (0)	cookienotice.astrazeneca.com		13.32.21.91	A (IP address)	IN (0x0001)
May 4, 2021 01:25:03.913827896 CEST	8.8.8.8	192.168.2.3	0xe9dd	No error (0)	cookienotice.astrazeneca.com		13.32.21.89	A (IP address)	IN (0x0001)
May 4, 2021 01:25:03.913827896 CEST	8.8.8.8	192.168.2.3	0xe9dd	No error (0)	cookienotice.astrazeneca.com		13.32.21.47	A (IP address)	IN (0x0001)
May 4, 2021 01:25:03.913827896 CEST	8.8.8.8	192.168.2.3	0xe9dd	No error (0)	cookienotice.astrazeneca.com		13.32.21.54	A (IP address)	IN (0x0001)
May 4, 2021 01:25:05.838104010 CEST	8.8.8.8	192.168.2.3	0xbb73	No error (0)	cookienotice.astrazeneca.com		13.32.21.89	A (IP address)	IN (0x0001)
May 4, 2021 01:25:05.838104010 CEST	8.8.8.8	192.168.2.3	0xbb73	No error (0)	cookienotice.astrazeneca.com		13.32.21.91	A (IP address)	IN (0x0001)
May 4, 2021 01:25:05.838104010 CEST	8.8.8.8	192.168.2.3	0xbb73	No error (0)	cookienotice.astrazeneca.com		13.32.21.54	A (IP address)	IN (0x0001)
May 4, 2021 01:25:05.838104010 CEST	8.8.8.8	192.168.2.3	0xbb73	No error (0)	cookienotice.astrazeneca.com		13.32.21.47	A (IP address)	IN (0x0001)
May 4, 2021 01:25:08.137366056 CEST	8.8.8.8	192.168.2.3	0x3501	No error (0)	www.digitalcontrolroom.com		35.197.225.6	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 01:25:08.615670919 CEST	8.8.8.8	192.168.2.3	0x3e6a	No error (0)	dcr1.wpengine.com		35.197.225.6	A (IP address)	IN (0x0001)
May 4, 2021 01:25:18.238605976 CEST	8.8.8.8	192.168.2.3	0x71cf	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
May 4, 2021 01:25:18.238605976 CEST	8.8.8.8	192.168.2.3	0x71cf	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
May 4, 2021 01:25:18.719945908 CEST	8.8.8.8	192.168.2.3	0xe13d	No error (0)	js.monitor.azure.com	aijscdn2.azureedge.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 01:25:18.785808086 CEST	8.8.8.8	192.168.2.3	0x6bb8	No error (0)	consentdeliveryfd.azurefd.net	firstparty-azurefd-prod.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 01:25:18.837960958 CEST	8.8.8.8	192.168.2.3	0x90f	No error (0)	mem.gfx.ms	cdn.account.microsoft.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 01:25:19.755296946 CEST	8.8.8.8	192.168.2.3	0x9b01	No error (0)	login.microsoftonline.com	a.privatelink.msidentity.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 01:25:19.755296946 CEST	8.8.8.8	192.168.2.3	0x9b01	No error (0)	a.privatelink.msidentity.com	prda.aadg.msidentity.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 01:25:19.755296946 CEST	8.8.8.8	192.168.2.3	0x9b01	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 01:25:20.321536064 CEST	8.8.8.8	192.168.2.3	0xd3f5	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 01:25:24.412828922 CEST	8.8.8.8	192.168.2.3	0xd83f	No error (0)	support.mozilla.org	prod-tp.sumo.mozit.cloud		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 01:25:24.412828922 CEST	8.8.8.8	192.168.2.3	0xd83f	No error (0)	prod-tp.sumo.mozit.cloud		34.210.184.158	A (IP address)	IN (0x0001)
May 4, 2021 01:25:24.412828922 CEST	8.8.8.8	192.168.2.3	0xd83f	No error (0)	prod-tp.sumo.mozit.cloud		35.165.126.227	A (IP address)	IN (0x0001)
May 4, 2021 01:25:26.815376043 CEST	8.8.8.8	192.168.2.3	0x59b0	No error (0)	static-media-prod-cdn.itsre-sumo.mozilla.net	d1ygnxto00lnhl.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 01:25:26.815376043 CEST	8.8.8.8	192.168.2.3	0x59b0	No error (0)	d1ygnxto00lnhl.cloudfront.net		13.32.21.74	A (IP address)	IN (0x0001)
May 4, 2021 01:25:26.815376043 CEST	8.8.8.8	192.168.2.3	0x59b0	No error (0)	d1ygnxto00lnhl.cloudfront.net		13.32.21.64	A (IP address)	IN (0x0001)
May 4, 2021 01:25:26.815376043 CEST	8.8.8.8	192.168.2.3	0x59b0	No error (0)	d1ygnxto00lnhl.cloudfront.net		13.32.21.104	A (IP address)	IN (0x0001)
May 4, 2021 01:25:26.815376043 CEST	8.8.8.8	192.168.2.3	0x59b0	No error (0)	d1ygnxto00lnhl.cloudfront.net		13.32.21.94	A (IP address)	IN (0x0001)
May 4, 2021 01:25:26.841543913 CEST	8.8.8.8	192.168.2.3	0xe6c7	No error (0)	user-media-prod-cdn.itsre-sumo.mozilla.net	d388y12e46loke.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 01:25:26.841543913 CEST	8.8.8.8	192.168.2.3	0xe6c7	No error (0)	d388y12e46loke.cloudfront.net		13.32.21.43	A (IP address)	IN (0x0001)
May 4, 2021 01:25:26.841543913 CEST	8.8.8.8	192.168.2.3	0xe6c7	No error (0)	d388y12e46loke.cloudfront.net		13.32.21.114	A (IP address)	IN (0x0001)
May 4, 2021 01:25:26.841543913 CEST	8.8.8.8	192.168.2.3	0xe6c7	No error (0)	d388y12e46loke.cloudfront.net		13.32.21.118	A (IP address)	IN (0x0001)
May 4, 2021 01:25:26.841543913 CEST	8.8.8.8	192.168.2.3	0xe6c7	No error (0)	d388y12e46loke.cloudfront.net		13.32.21.32	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

Copyright Joe Security LLC 2021

- covid19-immunization-learning-program-2021.ca
- support.mozilla.org

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49712	162.241.217.204	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 01:24:47.409138918 CEST	1190	OUT	GET / HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: covid19-immunization-learning-program-2021.ca Connection: Keep-Alive
May 4, 2021 01:24:47.580990076 CEST	1191	IN	HTTP/1.1 301 Moved Permanently Date: Mon, 03 May 2021 23:24:47 GMT Server: Apache Content-Security-Policy: upgrade-insecure-requests; Location: https://covid19-immunization-learning-program-2021.ca/index.html Content-Length: 272 Keep-Alive: timeout=5, max=75 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 63 6f 76 69 64 31 39 2d 69 6d 6d 75 6e 69 7a 61 74 69 6f 6e 2d 6c 65 61 72 6e 69 6e 67 2d 70 72 6f 67 72 61 6d 2d 32 30 32 31 2e 63 61 2f 69 6e 64 65 78 2e 68 74 6d 6c 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49803	34.210.184.158	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 01:25:24.619030952 CEST	10336	OUT	GET /en-US/kb/enable-and-disable-cookies-website-preferences HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: support.mozilla.org Connection: Keep-Alive
May 4, 2021 01:25:24.827683926 CEST	10337	IN	HTTP/1.1 301 Moved Permanently Content-Type: text/html; charset=utf-8 Date: Mon, 03 May 2021 23:25:24 GMT Location: https://support.mozilla.org/en-US/kb/enable-and-disable-cookies-website-preferences Server: meinheld/1.0.2 X-Backend-Server: sumo-prod-web-66d59b69dd-l9wzb.oregon-b.mozit.cloud X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block Content-Length: 0 Connection: keep-alive

HTTPS Packets

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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 01:24:47.945408106 CEST	162.241.217.204	443	192.168.2.3	49714	CN=cpcalendars.covid19-immunization-learning-program-2021.ca CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Mar 24 15:21:44 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Tue Jun 22 16:21:44 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
May 4, 2021 01:24:48.527967930 CEST	34.107.253.133	443	192.168.2.3	49715	CN=policy.cookiereports.com, OU=Gandi Standard SSL, OU=Domain Control Validated CN=Gandi Standard SSL CA 2, O=Gandi, L=Paris, ST=Paris, C=FR CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Gandi Standard SSL CA 2, O=Gandi, L=Paris, ST=Paris, C=FR CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AddTrust External CA Root, OU=AddTrust External TTP Network, O=AddTrust AB, C=SE	Tue May 14 02:00:00 CEST 2019 Fri Sep 12 02:00:00 CEST 2014 Tue May 30 12:48:38 CEST 2000	Tue May 25 01:59:59 CEST 2021 Thu Sep 12 01:59:59 CEST 2024 Sat May 30 12:48:38 CEST 2020	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=Gandi Standard SSL CA 2, O=Gandi, L=Paris, ST=Paris, C=FR	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Sep 12 02:00:00 CEST 2014	Thu Sep 12 01:59:59 CEST 2024		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AddTrust External CA Root, OU=AddTrust External TTP Network, O=AddTrust AB, C=SE	Tue May 30 12:48:38 CEST 2000	Sat May 30 12:48:38 CEST 2020		
May 4, 2021 01:24:48.529133081 CEST	34.107.253.133	443	192.168.2.3	49716	CN=policy.cookiereports.com, OU=Gandi Standard SSL, OU=Domain Control Validated CN=Gandi Standard SSL CA 2, O=Gandi, L=Paris, ST=Paris, C=FR CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Gandi Standard SSL CA 2, O=Gandi, L=Paris, ST=Paris, C=FR CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AddTrust External CA Root, OU=AddTrust External TTP Network, O=AddTrust AB, C=SE	Tue May 14 02:00:00 CEST 2019 Fri Sep 12 02:00:00 CEST 2014 Tue May 30 12:48:38 CEST 2000	Tue May 25 01:59:59 CEST 2021 Thu Sep 12 01:59:59 CEST 2024 Sat May 30 12:48:38 CEST 2020	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=Gandi Standard SSL CA 2, O=Gandi, L=Paris, ST=Paris, C=FR	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Sep 12 02:00:00 CEST 2014	Thu Sep 12 01:59:59 CEST 2024		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AddTrust External CA Root, OU=AddTrust External TTP Network, O=AddTrust AB, C=SE	Tue May 30 12:48:38 CEST 2000	Sat May 30 12:48:38 CEST 2020		
May 4, 2021 01:25:03.911166906 CEST	162.241.217.204	443	192.168.2.3	49736	CN=cpcalendars.covid19-immunization-learning-program-2021.ca CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Mar 24 15:21:44 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Tue Jun 22 16:21:44 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 01:25:04.018722057 CEST	13.32.21.91	443	192.168.2.3	49737	CN=www.cookienotice.astrazeneca.com, OU=IT Security, O=AstraZeneca Pharmaceuticals LP, STREET=1800 Concord Pike, L=Wilmington, ST=Delaware, OID.2.5.4.17=19850, C=US CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Fri May 22 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Mon May 23 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
May 4, 2021 01:25:04.019361973 CEST	13.32.21.91	443	192.168.2.3	49738	CN=www.cookienotice.astrazeneca.com, OU=IT Security, O=AstraZeneca Pharmaceuticals LP, STREET=1800 Concord Pike, L=Wilmington, ST=Delaware, OID.2.5.4.17=19850, C=US CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Fri May 22 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Mon May 23 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 01:25:05.928510904 CEST	13.32.21.89	443	192.168.2.3	49739	CN=www.cookienotice.astrazeneca.com, OU=IT Security, O=AstraZeneca Pharmaceuticals LP, STREET=1800 Concord Pike, L=Wilmington, ST=Delaware, OID.2.5.4.17=19850, C=US CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Fri May 22 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Mon May 23 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
May 4, 2021 01:25:05.930614948 CEST	13.32.21.89	443	192.168.2.3	49740	CN=www.cookienotice.astrazeneca.com, OU=IT Security, O=AstraZeneca Pharmaceuticals LP, STREET=1800 Concord Pike, L=Wilmington, ST=Delaware, OID.2.5.4.17=19850, C=US CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Fri May 22 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Mon May 23 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 01:25:08.265456915 CEST	35.197.225.6	443	192.168.2.3	49741	CN=www.digitalcontrolroom.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sun Apr 25 00:38:22 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Sat Jul 24 00:38:22 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
May 4, 2021 01:25:08.267318010 CEST	35.197.225.6	443	192.168.2.3	49742	CN=www.digitalcontrolroom.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sun Apr 25 00:38:22 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Sat Jul 24 00:38:22 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
May 4, 2021 01:25:08.758420944 CEST	35.197.225.6	443	192.168.2.3	49745	CN=*.wpengine.com CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Jul 01 02:00:00 CEST 2019 Mon Nov 06 13:23:33 CET 2017 Fri Nov 10 01:00:00 CET 2006	Sun Aug 29 14:00:00 CEST 2021 Sat Nov 06 13:23:33 CET 2027 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=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:33 CET 2017	Sat Nov 06 13:23:33 CET 2027		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
May 4, 2021 01:25:08.763842106 CEST	35.197.225.6	443	192.168.2.3	49746	CN=*.wpengine.com CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Jul 01 02:00:00 CEST 2019 Mon Nov 06 13:23:33 CET 2017 Fri Nov 10 01:00:00 CET 2006	Sun Aug 29 14:00:00 CEST 2021 Sat Nov 06 13:23:33 CET 2027 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=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:33 CET 2017	Sat Nov 06 13:23:33 CET 2027		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 01:25:18.354413986 CEST	104.16.18.94	443	192.168.2.3	49759	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Oct 21 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
May 4, 2021 01:25:18.404577017 CEST	104.16.18.94	443	192.168.2.3	49760	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Oct 21 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Thu Oct 21 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
May 4, 2021 01:25:25.331906080 CEST	34.210.184.158	443	192.168.2.3	49804	CN=support.mozilla.org CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Sat Apr 17 02:00:00 CEST 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Tue May 17 01:59:59 CEST 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 01:25:26.954447031 CEST	13.32.21.74	443	192.168.2.3	49810	CN=*.itsre-sumo.mozilla.net CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Apr 19 02:00:00 CEST 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu May 19 01:59:59 CEST 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 4, 2021 01:25:26.954570055 CEST	13.32.21.74	443	192.168.2.3	49805	CN=*.itsre-sumo.mozilla.net CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Apr 19 02:00:00 CEST 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu May 19 01:59:59 CEST 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 01:25:26.955080986 CEST	13.32.21.43	443	192.168.2.3	49808	CN=*.itsre-sumo.mozilla.net CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Apr 19 02:00:00 CEST 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu May 19 01:59:59 CEST 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 4, 2021 01:25:26.955518961 CEST	13.32.21.74	443	192.168.2.3	49811	CN=*.itsre-sumo.mozilla.net CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Apr 19 02:00:00 CEST 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu May 19 01:59:59 CEST 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 01:25:26.956201077 CEST	13.32.21.43	443	192.168.2.3	49806	CN=*.itsre-sumo.mozilla.net CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Apr 19 02:00:00 CEST 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu May 19 01:59:59 CEST 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 4, 2021 01:25:26.956379890 CEST	13.32.21.74	443	192.168.2.3	49807	CN=*.itsre-sumo.mozilla.net CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Apr 19 02:00:00 CEST 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu May 19 01:59:59 CEST 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 01:25:26.956471920 CEST	13.32.21.74	443	192.168.2.3	49809	CN=*.itsre-sumo.mozilla.net CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Apr 19 02:00:00 CEST 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu May 19 01:59:59 CEST 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 4, 2021 01:25:26.993940115 CEST	13.32.21.74	443	192.168.2.3	49812	CN=*.itsre-sumo.mozilla.net CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Apr 19 02:00:00 CEST 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu May 19 01:59:59 CEST 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 3008 Parent PID: 792

General

Start time:	01:24:44
Start date:	04/05/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff73b9c0000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Copyright Joe Security LLC 2021

Analysis Process: iexplore.exe PID: 4800 Parent PID: 3008

General

Start time:	01:24:45
Start date:	04/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3008 CREDAT:17410 /prefetch:2
Imagebase:	0xcd0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 4744 Parent PID: 3008

General

Start time:	01:25:02
Start date:	04/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3008 CREDAT:17418 /prefetch:2
Imagebase:	0xcd0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly