



ID: 425521
Cookbook: browseurl.jbs
Time: 12:17:59
Date: 27/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2

Analysis Report https://www.dickinsonsolicitors.co.uk/coronavirus-covid-19-notice-june-2020/ 4

- Overview 4
  - General Information 4
  - Detection 4
  - Signatures 4
  - Classification 4
- Process Tree 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 9
  - Contacted Domains 9
  - Contacted URLs 9
  - URLs from Memory and Binaries 9
  - Contacted IPs 12
  - Public 12
- General Information 13
- Simulations 14
  - Behavior and APIs 14
- Joe Sandbox View / Context 14
  - IPs 14
  - Domains 15
  - 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 52
  - HTTPS Packets 53
- Code Manipulations 57
- Statistics 57
  - Behavior 57
- System Behavior 57
  - Analysis Process: iexplore.exe PID: 4604 Parent PID: 792 57
    - General 57

Copyright Joe Security LLC 2021

File Activities 58
Registry Activities 58
Analysis Process: iexplore.exe PID: 4588 Parent PID: 4604 58
General 58
File Activities 58
Registry Activities 58
Disassembly 59

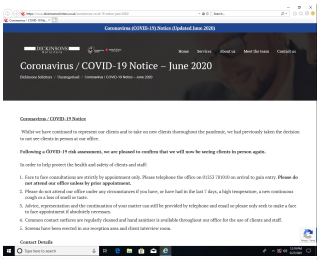
Analysis Report https://www.dickinsonsolicitors.co.uk/c…

Overview

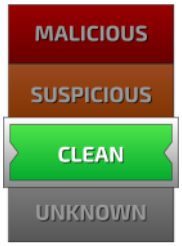
General Information

Sample URL:	http://https://www.dickinsonsolicitors.co.uk/coronavirus-covid-19-notice-june-2020/
Analysis ID:	425521
Infos:	

Most interesting Screenshot:



Detection

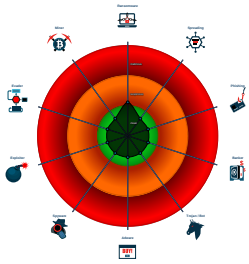


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- **System is w10x64**
- iexplore.exe (PID: 4604 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 4588 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4604 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

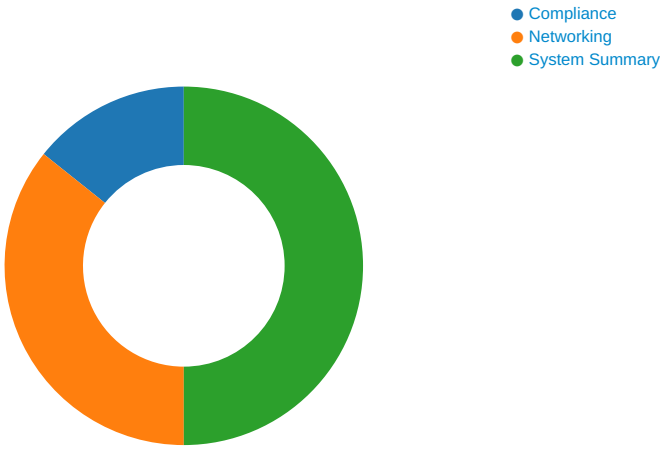
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

Copyright Joe Security LLC 2021



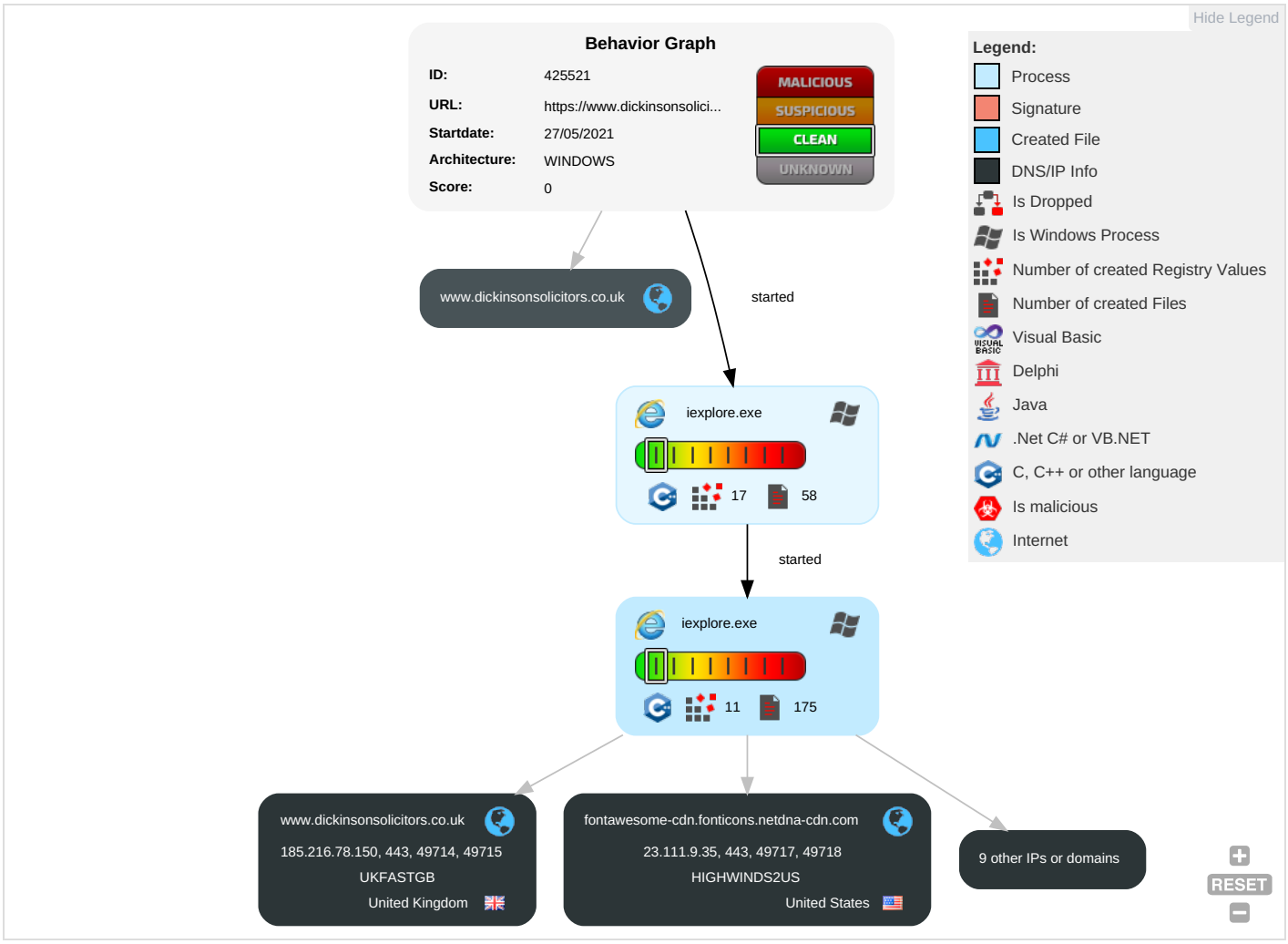
Click to jump to signature section

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

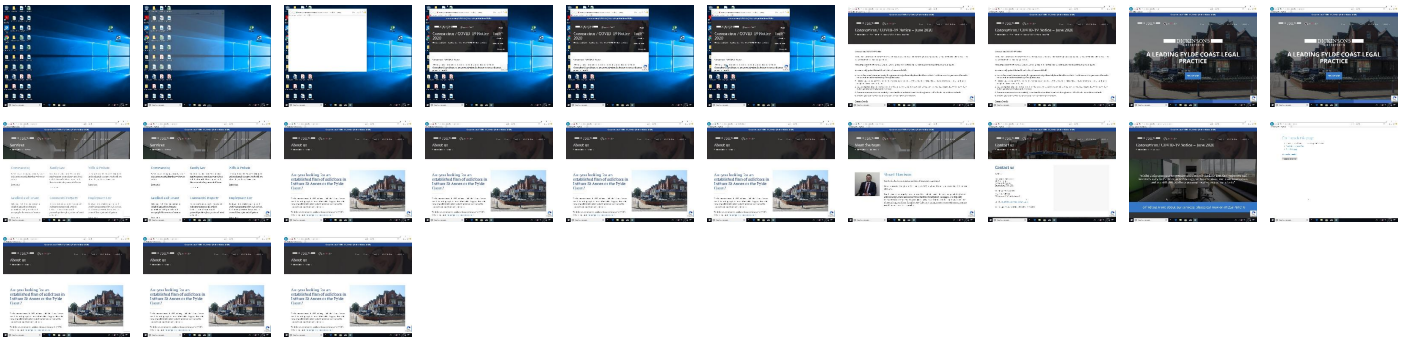
Behavior Graph

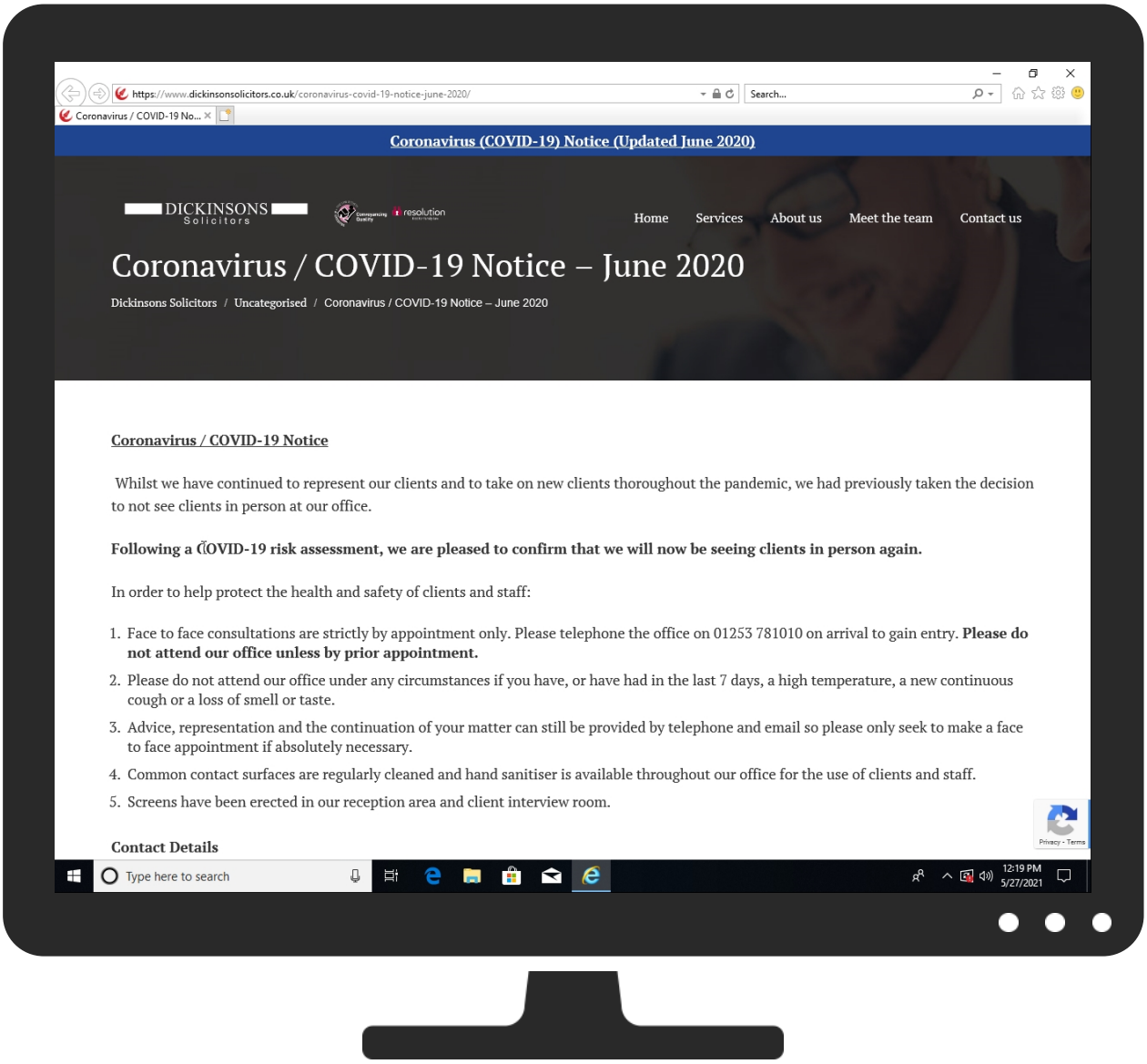


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://www.dickinsonsolicitors.co.uk/coronavirus-covid-19-notice-june-2020/	0%	Virustotal		Browse
http://https://www.dickinsonsolicitors.co.uk/coronavirus-covid-19-notice-june-2020/	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.dickinsonsolicitors.co.uk/wp-content/uploads/2018/07/dickinsons-logo-WHITE-600x70.png	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/services/landlord-and-tenant/	0%	Avira URL Cloud	safe	

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
http://https://www.dickinsonsolicitors.co.uk/wp-content/uploads/2018/07/cropped-favicon-180x180.png	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/wp-includes/js/dist/vendor/wp-polyfill-element-closest.min.js?	0%	Avira URL Cloud	safe	
http://https://cdn.yoshki.com/SRA/EnglishMono/275/0/Default.png	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/wp-content/plugins/contact-form-7/includes/js/index.js?ver=5.4	0%	Avira URL Cloud	safe	
http://https://www.gov.u	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/wp-content/plugins/js_composer/assets/js/dist/js_composer_fron	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/wp-json/wp/v2/pages/36	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/wp-includes/js/dist/vendor/wp-polyfill-fetch.min.js?ver=3.0.0	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/services/olicitors.co.uk/category/uncategorised/Root	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/category/uncategorised/feed/	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/services/Root	0%	Avira URL Cloud	safe	
http://www.quicklaunch.co/	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/coronavirus-covid-19-notice-june-2020/Root	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/coronavirus-covid-19-notice-june-2020/olicitors.co.uk/coronavi	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/wp-content/uploads/2018/07/cropped-favicon-192x192.png	0%	Avira URL Cloud	safe	
http://www.dickinsonsolicitors.co.uk/about-us/	0%	Avira URL Cloud	safe	
http://https://fontawesome.comhttps://fontawesome.comFont	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/?p=40	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/wp-includes/js/underscore.min.js?ver=1.8.3	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/wp-content/uploads/2018/07/dickinsons-logo-WHITE-768x90.png	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/wp-content/plugins/contact-form-7/includes/css/styles.css?ver=	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/ronavirus-covid-19-notice-june-2020/	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/wp-json/wp/v2/pages/40	0%	Avira URL Cloud	safe	
http://https://wpbakery.com)	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/about-us/ncategorised/-favicon-270x270.png	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/category/uncategorised/-favicon-270x270.png	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/wp-content/uploads/2018/06/slider-2.jpg	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/category/uncategorised/JUncategorised	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/wp-content/uploads/2018/07/dickinsons-logo-WHITE-300x35.png	0%	Avira URL Cloud	safe	
http://getbootstrap.com)	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/wp-includes/wlwmanifest.xml	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/wp-content/plugins/contact-form-7/modules/recaptcha/index.js?v	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/complaints/	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/wp-includes/js/dist/vendor/wp-polyfill-formdata.min.js?ver=3.0	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/contact-us/m/	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/services/employment-law/	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/services/powers-of-attorney/	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/wp-includes/js/jquery/jquery.min.js?ver=3.5.1	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/wp-content/plugins/js_composer/assets/lib/vc_waypoints/vc-wayp	0%	Avira URL Cloud	safe	
http://https://cdn.yoshki.com/responsive-ie.css	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fwww.dickinsonsolici	0%	Avira URL Cloud	safe	
http://https://www.dickiolicitors.co.uk/about-us/Root	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/wp-content/plugins/js_composer/assets/lib/bower/imagesloaded/i	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/wp-content/themes/quicklaunch-parent-theme/library/images/appl	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/wp-content/themes/quicklaunch-parent-theme/library/js/vendor/h	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/wp-json/wp/v2/posts/338	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/wp-content/uploads/2018/06/office-background.jpg	0%	Avira URL Cloud	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://www.google.co.uk/maps/dir/	0%	Avira URL Cloud	safe	
http://https://cdn.yoshki.com/yoshki-library.js	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/wp-content/uploads/2018/06/dickinsons-office-1024x768.jpg	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/wp-content/plugins/js_composer/assets/js/dist/vc_grid.min.js?v	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/about-us/://www.dickinsonsolicitors.co.uk/services/	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://cdn.yoshki.com/iframe/55849r.html	0%	Avira URL Cloud	safe	
http://https://www.google.%/ads/ga-audiences	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences	0%	URL Reputation	safe	
http://https://www.dickionavirusco.uk/category/uncategorised/Root	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/coronavirus-covid-19-notice-june-2020/olicitors.co.uk/ronaviru	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/about-us/07/cropped-favicon-270x270.png	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/contact-us/DContact	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/coronavirus-covid-19-notice-june-2020/feed/	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/wp-content/uploads/2018/07/IMG_3026-1-282x300.jpg	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/wp-includes/js/dist/vendor/wp-polyfill-node-contains.min.js?ve	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/wp-includes/js/wp-embed.min.js?ver=5.7.2	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/wp-content/plugins/google-analytics-for-wordpress/assets/js/fr	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/wp-content/plugins/js_composer/assets/lib/bower/animate-css/an	0%	Avira URL Cloud	safe	
http://https://www.gov.uk/cor	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/services/wills-probate/	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/wp-includes/js/dist/vendor/wp-polyfill-url.min.js?ver=3.6.4	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/?p=338	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/services/olicitors.co.uk/meet-the-team/Root	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/?p=218	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/wp-content/plugins/js_composer/assets/lib/owl-carousel2-dist/a	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/wp-content/uploads/2018/06/dickinsonsolicitors.seesites.biz_-_	0%	Avira URL Cloud	safe	
http://https://www.dickinsonsolicitors.co.uk/wp-json/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
googleads.g.doubleclick.net	216.58.207.130	true	false		high
i.ytimg.com	172.217.22.246	true	false		high
photos-ugc.l.googleusercontent.com	142.250.185.65	true	false		high
fontawesome-cdn.fonticons.netdna-cdn.com	23.111.9.35	true	false		high
maxcdn.bootstrapcdn.com	104.18.11.207	true	false		high
www.dickinsonsolicitors.co.uk	185.216.78.150	true	false		unknown
use.fontawesome.com	unknown	unknown	false		high
yt3.ggpht.com	unknown	unknown	false		high
cdn.yoshki.com	unknown	unknown	false		unknown
www.youtube.com	unknown	unknown	false		high
static.doubleclick.net	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.dickinsonsolicitors.co.uk/	false		unknown
http://https://www.dickinsonsolicitors.co.uk/services/	false		unknown
http://https://www.gov.uk/coronavirus	false		unknown
http://https://www.dickinsonsolicitors.co.uk/category/uncategorised/	false		unknown
http://https://www.dickinsonsolicitors.co.uk/meet-the-team/	false		unknown
http://https://www.dickinsonsolicitors.co.uk/about-us/	false		unknown

URLs from Memory and Binaries

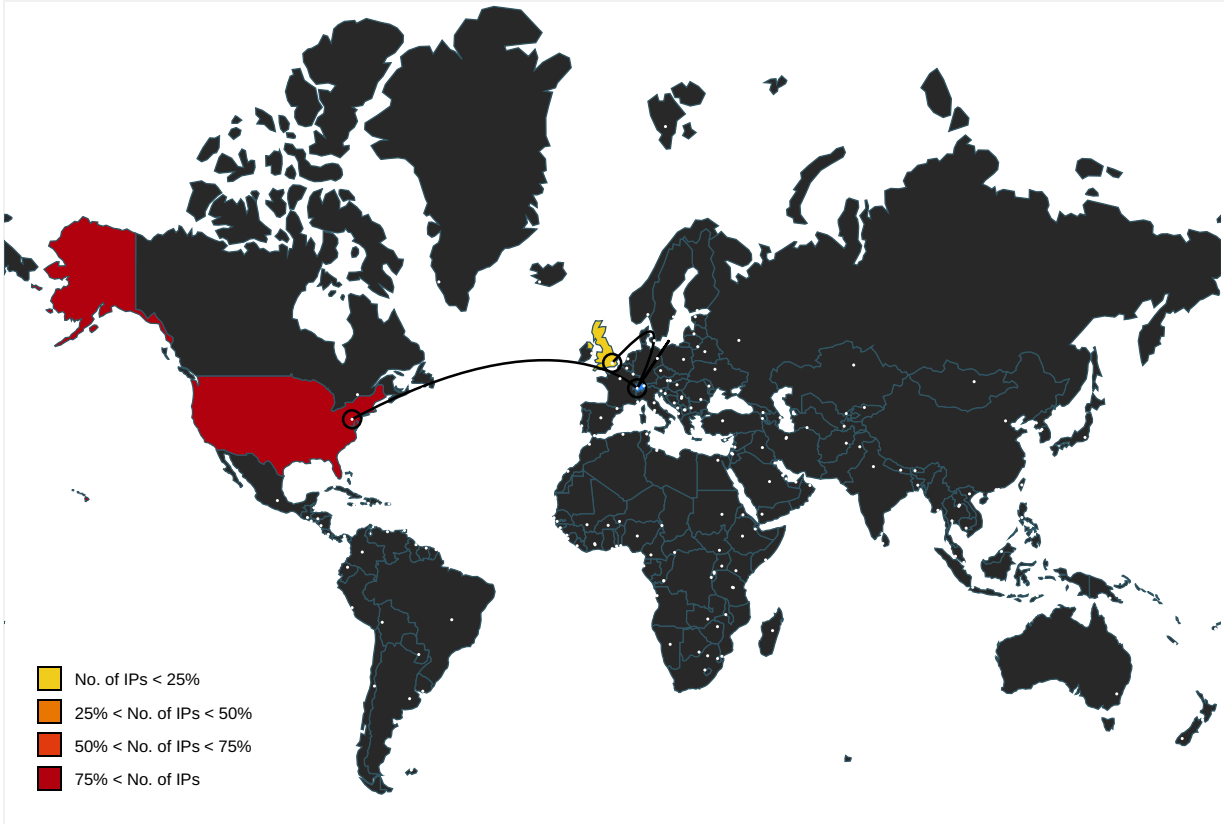
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.dickinsonsolicitors.co.uk/wp-content/uploads/2018/07/dickinsons-logo-WHITE-600x70.png	6QPJB2IQ.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://fontawesome.io	font-awesome.min[1].css.2.dr	false		high
http://https://ogp.me/ns#	coronavirus-covid-19-notice-june-2020[2].htm.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.dickinsonsolicitors.co.uk/services/landlord-and-tenant/	6QPJB2IQ.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.monsterinsights.com/	coronavirus-covid-19-notice-june-2020[2].htm.2.dr	false		high
http://https://www.dickinsonsolicitors.co.uk/wp-content/uploads/2018/07/cropped-favicon-180x180.png	coronavirus-covid-19-notice-june-2020[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.dickinsonsolicitors.co.uk/wp-includes/js/dist/vendor/wp-polyfill-element-closest.min.js?	coronavirus-covid-19-notice-june-2020[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn.yoshki.com/SRA/EnglishMono/275/0/Default.png	55849r[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.dickinsonsolicitors.co.uk/wp-content/plugins/contact-form-7/includes/js/index.js?ver=5.4	coronavirus-covid-19-notice-june-2020[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.gov.u	{5F0C331B-BF20-11EB-90E5-ECF4BB570DC9}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.dickinsonsolicitors.co.uk/wp-content/plugins/js_composer/assets/js/dist/js_composer_fron	coronavirus-covid-19-notice-june-2020[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.dickinsonsolicitors.co.uk/wp-json/wp/v2/pages/36	services[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.dickinsonsolicitors.co.uk/wp-includes/js/dist/vendor/wp-polyfill-fetch.min.js?ver=3.0.0	coronavirus-covid-19-notice-june-2020[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.dickinsonsolicitors.co.uk/services/olicitors.co.uk/category/uncategorised/Root	{5F0C331B-BF20-11EB-90E5-ECF4BB570DC9}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.dickinsonsolicitors.co.uk/category/uncategorised/feed/	uncategorised[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.dickinsonsolicitors.co.uk/services/Root	{5F0C331B-BF20-11EB-90E5-ECF4BB570DC9}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://youtube.com/streaming/otf/durations/112015	base[1].js.2.dr	false		high
http://www.quicklaunch.co/	style[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.dickinsonsolicitors.co.uk/coronavirus-covid-19-notice-june-2020/Root	{5F0C331B-BF20-11EB-90E5-ECF4BB570DC9}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.dickinsonsolicitors.co.uk/coronavirus-covid-19-notice-june-2020/olicitors.co.uk/coronavi	{5F0C331B-BF20-11EB-90E5-ECF4BB570DC9}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.dickinsonsolicitors.co.uk/wp-content/uploads/2018/07/cropped-favicon-192x192.png	coronavirus-covid-19-notice-june-2020[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.dickinsonsolicitors.co.uk/about-us/	coronavirus-covid-19-notice-june-2020[2].htm.2.dr, 6QPJB2IQ.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://fontawesome.comhttps://fontawesome.comFont	fa-regular-400[1].eot.2.dr, fa-solid-900[1].eot.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.dickinsonsolicitors.co.uk/?p=40	contact-us[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.dickinsonsolicitors.co.uk/wp-includes/js/underscore.min.js?ver=1.8.3	6QPJB2IQ.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.dickinsonsolicitors.co.uk/wp-content/uploads/2018/07/dickinsons-logo-WHITE-768x90.png	coronavirus-covid-19-notice-june-2020[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://fontawesome.com	fa-regular-400[1].eot.2.dr, all[1].js.2.dr, v4-shims.min[1].css.2.dr	false		high
http://https://www.dickinsonsolicitors.co.uk/wp-content/plugins/contact-form-7/includes/css/styles.css?ver=	coronavirus-covid-19-notice-june-2020[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://admin.youtube.com	base[1].js.2.dr	false		high
http://https://www.dickinsonsolicitors.co.uk/ronavirus-covid-19-notice-june-2020/	~DFBD2D6AD03682685D.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.dickinsonsolicitors.co.uk/wp-json/wp/v2/pages/40	contact-us[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://wpbakery.com)	vc_grid.min[1].js.2.dr	false	• Avira URL Cloud: safe	low
http://https://www.dickinsonsolicitors.co.uk/about-us/ncategorised/-favicon-270x270.png	~DFBD2D6AD03682685D.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.dickinsonsolicitors.co.uk/category/uncategorised/-favicon-270x270.png	~DFBD2D6AD03682685D.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.dickinsonsolicitors.co.uk/wp-content/uploads/2018/06/slider-2.jpg	coronavirus-covid-19-notice-june-2020[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.dickinsonsolicitors.co.uk/category/uncategorised/JUncategorised	{5F0C331B-BF20-11EB-90E5-ECF4BB570DC9}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.dickinsonsolicitors.co.uk/wp-content/uploads/2018/07/dickinsons-logo-WHITE-300x35.png	coronavirus-covid-19-notice-june-2020[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://getbootstrap.com)	bootstrap.min[1].js.2.dr, style[1].css.2.dr	false	• Avira URL Cloud: safe	low
http://https://www.dickinsonsolicitors.co.uk/wp-includes/wlwmanifest.xml	coronavirus-covid-19-notice-june-2020[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://stats.g.doubleclick.net/j/collect	analytics[1].js.2.dr	false		high
http://https://www.dickinsonsolicitors.co.uk/wp-content/plugins/contact-form-7/modules/recaptcha/index.js?v	coronavirus-covid-19-notice-june-2020[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.dickinsonsolicitors.co.uk/complaints/	coronavirus-covid-19-notice-june-2020[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.dickinsonsolicitors.co.uk/wp-includes/js/dist/vendor/wp-polyfill-formdata.min.js?ver=3.0	coronavirus-covid-19-notice-june-2020[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.dickinsonsolicitors.co.uk/contact-us/m/	~DFBD2D6AD03682685D.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.dickinsonsolicitors.co.uk/services/employment-law/	6QPJB2IQ.htm.2.dr, services[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://use.fontawesome.com/releases/v5.0.13/js/all.js	coronavirus-covid-19-notice-june-2020[2].htm.2.dr	false		high
http://https://www.dickinsonsolicitors.co.uk/services/powers-of-attorney/	services[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.dickinsonsolicitors.co.uk/wp-includes/js/jquery/jquery.min.js?ver=3.5.1	coronavirus-covid-19-notice-june-2020[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.dickinsonsolicitors.co.uk/	6QPJB2IQ.htm.2.dr, embed[1].htm.2.dr	false		unknown
http://https://www.dickinsonsolicitors.co.uk/wp-content/plugins/js_composer/assets/lib/vc_waypoints/vc-wayp	6QPJB2IQ.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn.yoshki.com/responsive-ie.css	55849r[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.youtube.com/generate_204?cpn=	base[1].js.2.dr	false		high
http://https://www.dickinsonsolicitors.co.uk/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fwww.dickinsonsolici	contact-us[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.dickiolicitors.co.uk/about-us/Root	{5F0C331B-BF20-11EB-90E5-ECF4BB570DC9}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.dickinsonsolicitors.co.uk/wp-content/plugins/js_composer/assets/lib/bower/imagesloaded/i	6QPJB2IQ.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.dickinsonsolicitors.co.uk/wp-content/themes/quicklaunch-parent-theme/library/images/appl	coronavirus-covid-19-notice-june-2020[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.dickinsonsolicitors.co.uk/wp-content/themes/quicklaunch-parent-theme/library/js/vendor/h	coronavirus-covid-19-notice-june-2020[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.dickinsonsolicitors.co.uk/wp-json/wp/v2/posts/338	coronavirus-covid-19-notice-june-2020[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.dickinsonsolicitors.co.uk/contact-us/	contact-us[1].htm.2.dr	false		unknown
http://https://www.dickinsonsolicitors.co.uk/wp-content/uploads/2018/06/office-background.jpg	services[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://youtube.com/yt/2012/10/10	base[1].js.2.dr	false		high
http://https://cct.google/taggy/agent.js	js[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.google.co.uk/maps/dir/	coronavirus-covid-19-notice-june-2020[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn.yoshki.com/yoshki-library.js	55849r[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.dickinsonsolicitors.co.uk/wp-content/uploads/2018/06/dickinsons-office-1024x768.jpg	about-us[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.dickinsonsolicitors.co.uk/wp-content/plugins/js_composer/assets/js/dist/vc_grid.min.js?v	6QPJB2IQ.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.dickinsonsolicitors.co.uk/about-us/://www.dickinsonsolicitors.co.uk/services/	~DFBD2D6AD03682685D.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn.yoshki.com/iframe/55849r.html	{5F0C331B-BF20-11EB-90E5-ECF4BB570DC9}.dat.1.dr, coronavirus-covid-19-notice-june-2020[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.google.%/ads/ga-audiences	analytics[1].js.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://maxcdn.bootstrapcdn.com/font-awesome/4.5.0/css/font-awesome.min.css?ver=5.7.2	coronavirus-covid-19-notice-june-2020[2].htm.2.dr	false		high
http://https://www.dickionavirusco.uk/category/uncategorised/Root	{5F0C331B-BF20-11EB-90E5-ECF4BB570DC9}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://www.youtube.com/videoplayback	base[1].js.2.dr	false		high
http://https://www.dickinsonsolicitors.co.uk/coronavirus-covid-19-notice-june-2020/olicitors.co.uk/ronaviru	{5F0C331B-BF20-11EB-90E5-ECF4BB570DC9}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/twbs/bootstrap/blob/master/LICENSE)	bootstrap.min[1].js.2.dr	false		high
http://https://www.dickinsonsolicitors.co.uk/about-us/07/cropped-favicon-270x270.png	~DFBD2D6AD03682685D.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.dickinsonsolicitors.co.uk/contact-us/DContact	{5F0C331B-BF20-11EB-90E5-ECF4BB570DC9}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.dickinsonsolicitors.co.uk/coronavirus-covid-19-notice-june-2020/feed/	coronavirus-covid-19-notice-june-2020[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.dickinsonsolicitors.co.uk/wp-content/uploads/2018/07/IMG_3026-1-282x300.jpg	meet-the-team[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.dickinsonsolicitors.co.uk/wp-includes/js/dist/vendor/wp-polyfill-node-contains.min.js?ve	coronavirus-covid-19-notice-june-2020[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.dickinsonsolicitors.co.uk/wp-includes/js/wp-embed.min.js?ver=5.7.2	coronavirus-covid-19-notice-june-2020[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.dickinsonsolicitors.co.uk/wp-content/plugins/google-analytics-for-wordpress/assets/js/fr	coronavirus-covid-19-notice-june-2020[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.youtube.com/embed/unXEs0crvtA?feature=oembed	{5F0C331B-BF20-11EB-90E5-ECF4BB570DC9}.dat.1.dr, about-us[1].htm.2.dr	false		high
http://https://www.dickinsonsolicitors.co.uk/wp-content/plugins/js_composer/assets/lib/bower/animate-css/an	6QPJB2IQ.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.gov.uk/cor	{5F0C331B-BF20-11EB-90E5-ECF4BB570DC9}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.dickinsonsolicitors.co.uk/services/wills-probate/	6QPJB2IQ.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://browsehappy.com/	coronavirus-covid-19-notice-june-2020[2].htm.2.dr	false		high
http://https://www.dickinsonsolicitors.co.uk/wp-includes/js/dist/vendor/wp-polyfill-url.min.js?ver=3.6.4	coronavirus-covid-19-notice-june-2020[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.dickinsonsolicitors.co.uk/?p=338	coronavirus-covid-19-notice-june-2020[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.dickinsonsolicitors.co.uk/services/olicitors.co.uk/meet-the-team/Root	{5F0C331B-BF20-11EB-90E5-ECF4BB570DC9}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.dickinsonsolicitors.co.uk/?p=218	meet-the-team[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.dickinsonsolicitors.co.uk/meet-the-team/	meet-the-team[1].htm.2.dr	false		unknown
http://https://www.dickinsonsolicitors.co.uk/wp-content/plugins/js_composer/assets/lib/owl-carousel2-dist/a	6QPJB2IQ.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.dickinsonsolicitors.co.uk/wp-content/uploads/2018/06/dickinsonsolicitors.seesites.biz_-_	6QPJB2IQ.htm.2.dr, meet-the-team[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.dickinsonsolicitors.co.uk/wp-json/	coronavirus-covid-19-notice-june-2020[2].htm.2.dr, about-us[1].htm.2.dr, 6QPJB2IQ.htm.2.dr, uncategorised[1].htm.2.dr, services[1].htm.2.dr, meet-the-team[1].htm.2.dr, contact-us[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
23.111.9.35	fontawesome-cdn.fonticons.netdna-cdn.com	United States		33438	HIGHWINDS2US	false
172.217.22.246	i.ytimg.com	United States		15169	GOOGLEUS	false
185.216.78.150	www.dickinsonsolicitors.co.uk	United Kingdom		61323	UKFASTGB	false
104.18.11.207	maxcdn.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false

Copyright Joe Security LLC 2021

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
216.58.207.130	googleads.g.doubleclick.net	United States		15169	GOOGLEUS	false
142.250.185.65	photos-ugc.l.googleusercontent.com	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	425521
Start date:	27.05.2021
Start time:	12:17:59
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 30s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://www.dickinsonsolicitors.co.uk/coronavirus-covid-19-notice-june-2020/
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:	13
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.win@3/139@10/6
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://www.dickinsonsolicitors.co.uk/coronavirus-covid-19-notice-june-2020/ • Browsing link: https://www.dickinsonsolicitors.co.uk/ • Browsing link: https://www.dickinsonsolicitors.co.uk/services/ • Browsing link: https://www.dickinsonsolicitors.co.uk/about-us/ • Browsing link: https://www.dickinsonsolicitors.co.uk/meet-the-team/ • Browsing link: https://www.dickinsonsolicitors.co.uk/contact-us/ • Browsing link: https://www.dickinsonsolicitors.co.uk/category/uncategorised/ • Browsing link: https://www.gov.uk/coronavirus • Browsing link: http://www.dickinsonsolicitors.co.uk/about-us/

Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 131.253.33.200, 13.107.22.200, 52.255.188.83, 52.147.198.201, 92.122.145.220, 88.221.62.148, 172.217.22.234, 172.217.23.8, 172.217.22.228, 142.250.185.238, 8.241.78.250, 8.238.30.250, 8.241.83.122, 142.250.186.99, 172.217.23.42, 216.58.207.163, 92.122.144.200, 152.199.19.161, 216.58.207.174, 172.217.20.238, 172.217.23.14, 172.217.23.46, 172.217.23.78, 172.217.22.206, 172.217.22.238, 216.58.207.142, 20.82.210.154, 172.217.22.198, 51.103.5.186, 92.122.213.194, 92.122.213.247 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, ssl.cdn.yoshki.com.c.footprint.net, store-images.s-microsoft.com-c.edgekey.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, go.microsoft.com, www.googletagmanager.com, www-bing-com.dual-a-0001.a-msedge.net, www.google.com, arc.trafficmanager.net, watson.telemetry.microsoft.com, www.gstatic.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, www.google-analytics.com, www.bing.com, fonts.googleapis.com, client.wns.windows.com, fs.microsoft.com, www-google-analytics.l.google.com, fonts.gstatic.com, ajax.googleapis.com, ie9comview.vo.msecnd.net, www-googletagmanager.l.google.com, e1723.g.akamaiedge.net, static-doubleclick-net.l.google.com, dual-a-0001.dc-msedge.net, skypedataprdcoleus16.cloudapp.net, skypedataprdcoleus17.cloudapp.net, youtube-ui.l.google.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, cs9.wpc.v0cdn.net • 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. • Report size getting too big, too many NtQueryAttributesFile 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\DSW732N5\www.google[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):	5255
Entropy (8bit):	5.659261132877846
Encrypted:	false
SSDEEP:	96:qiWii9hiB1FW3iB1FW3biB1FW3iB1FW3qiB1FW3iXiX/+iiAiAXpCRe3iixcii1g:9FnF5FnFQFiCcl4Q
MD5:	C41B99BF231ABD371F95AEEDE472237A
SHA1:	5ACB9B63D6F428691A3B255B614D73D39D3A9DCE
SHA-256:	F108DB74045E24CEEC49A59D15B91CF754ECB19F35F697C870194AF0847FF324
SHA-512:	13D8B9EA427A3173578CEA6C18320E581CF3869FAB26EA411FD0D5EB91DB1DDCFD4554EA72F23D0CB4A26BC6D5A98C5B7A000D20048298A1C282B8FEA1C256 87
Malicious:	false
Reputation:	low
Preview:	<root><item name="rc::a" value="MTU2bG91eDFnbnR2emU=" ltime="612997296" htime="30888749" /></root><root><item name="rc::a" value="MTU2bG91eD FnbnR2emU=" ltime="612997296" htime="30888749" /><item name="rc::d-1622143138354" value="MXU2MGV5OTF5b2JyajM=" ltime="614237296" htime="30888749" /></root><root><item name="rc::a" value="MTU2bG91eDFnbnR2emU=" ltime="612997296" htime="30888749" /></root><root><item name="rc::a" value="MTU2b G91eDFnbnR2emU=" ltime="612997296" htime="30888749" /><item name="rc::d-1622143158625" value="MW9zdHFraTE3MWRkaXk=" ltime="816887296" htime= "30888749" /></root><root><item name="rc::a" value="MTU2bG91eDFnbnR2emU=" ltime="612997296" htime="30888749" /><item name="rc::d-1622143158625-3f85708 c" value="ChNyYzo6ZC0xNjIyMTQzMTU4NjI1EAAaCDhjZDZmM2QxInEKaWltM050TjBSejhPRW05b2doOTF2YWE1OXpUUGhfYjJjdjlmUWdiWFpBYW1mUW JqenZiMm4zMmkzcy1DaHdRR1YyZEdTMTRHUzFNYmJxZDZfUWxYSE9pRl9UZzJaaTBRREhPYWNnWTlCaxCQ4f2KBioCMXI=" ltime="819217296" htime="30888749" /></root><root><item name="rc

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\DURNCK2N\www.dickinsonsolicitors.co[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):	1227
Entropy (8bit):	5.8361528226912744
Encrypted:	false
SSDEEP:	24:WUPGPzvklo0UPGNblo0UPGfpjh5wo0UPG2xe5FzXXo0UPGRK14o0UPGWStzo0UP3:LPGPsoVPGPoVPGrOoVPG6uToVPGRroVr
MD5:	ED3CBD425D034EFB358717DB62B2AF73
SHA1:	3AC74487310449C0689455A949571565E2221441
SHA-256:	0ADFE2D623C8C2076AF247B1510B0E5FF8A7E9052EEA8A8854F99C69CDF21B4F
SHA-512:	EF16E547D54B415B4725EDE71C71D0C2B7E05BC16FCAFB939BAAAC549B565B4F72E98D0258F94925B316DACB344D42D2D0E010B69D865E7F133FB3C9CFCFA5 69
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="_grecaptcha" value="09ANblmniGlghkrksCwgDYogCx_DV19165YdpPAiMHNXPvoIr2ev7YL3RK3JJqmqaPGqto_vs-YORF3 Bq9VXB08NQ" ltime="619657296" htime="30888749" /></root><root><item name="_grecaptcha" value="09ANblmniV9TYxvrsOSttCWMWCWOLzDHjuSx8dyZCiAb0i c81TT9REHKIpeCVpuUsq6KPJVJTRHiWQbCTEG2ev7GM" ltime="820857296" htime="30888749" /></root><root><item name="_grecaptcha" value="09ANblmniRfsn zPwaoscWXtQfdBlYl3wDKoPQn0Dd6xgjH0-uT5ticcYhwThfmSzVuMKS05zTPokzJkeK70peEFcs" ltime="855207296" htime="30888749" /></root><root><item name=" _grecaptcha" value="09ANblmnhMOQxWFoGktK6cjA-xf57aDUg3Q2umHKo4nyyxH1bkkr8R4xW-S0_ICyQY6sgUMxpPe9iLNQxC0ykeikA" ltime="906687296" h time="30888749" /></root><root><item name="_grecaptcha" value="09ANblmngbYPGr68Lejq5gWyFL55s0xpDerC4ed0t-2HCKRa-3d6KPVWqJr9M3FyUlv8IDb4rmRHl 8EEYYncb4E5I" ltime="1062587296" htime="30888749" /></root><root><item name="_grecaptcha" value="09ANblmnip4UOsfV1Jc4RfgfLS2b4eGmt4lWinB_wQ2BeLXjQ- BeGHjv5tx-m--Z3C0whWubK6CxCNwwa3B

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\QALADACS\www.youtube[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):	55391
Entropy (8bit):	4.943226150426723
Encrypted:	false
SSDEEP:	384:pVyu0Qr00tFmTXg6UOWEzVyu0Qr00tFmTXg6UOWErVyu0Qr00tFmTXg6UOWE3VyS:3EpERetEGEtEjaEjQEjQEjfEjW
MD5:	0C3175B44E8682032A2823F93123973E
SHA1:	DC6FFBAF32D5C35E48BA72F637523D6764A2DF3F
SHA-256:	B937377995FF846988C82D1A37C69FF46454549C1313A9EA41F2D86BDF307D15
SHA-512:	58AA32477D1A238CFACB66551EFF8476F325131449CFB957EE926C5E972857EB639EDC382409C9AF036712A5F2656CC2ABB6B13BD226676ED99B69C5AF676F9
Malicious:	false
Reputation:	low
Preview:	<root></root><root></root><root></root><root><item name="__sak" value="1" ltime="957867296" htime="30888749" /></root><root></root><root><item name="__sak" value="1" ltime="1035707296" htime="30888749" /></root><root></root><root><item name="yt.innertube::nextId" value="{"data":2,"expiration":1622229580556,"creation":1622143180561}" ltime="1036467296" htime="30888749" /></root><root><item name="yt.innertube::nextId" value="{"data":2,"expiration":1622229580556,"creation":1622143180561}" ltime="1036467296" htime="30888749" /><item name="yt.innertube::requests" value="{"data":{"1":{"method":"log_event","request":{"context":{"client":{"hl":"en","gl":"GB","clientName":56,"clientVersion":"1.20210524.1.1","configInfo":{"appInstallData":"CLLkvYUGEI6V/RIQ07itBQ=="}}},&

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{5F0C3319-BF20-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.855933555908248
Encrypted:	false
SSDEEP:	96:rIZvZxl2iWdtztd/bfdX6ZKMdJBqd37Qdq7xfdW6s6X:rIZvZv2iWTtFfNNMQ6ifsMX
MD5:	326E5C36A4292232B40109180E03735F
SHA1:	22DA85464637B0AF63FECDEF02BF42749632EA53
SHA-256:	F4442FB94DE75EB4FF62B2A22A3DB38372E79AA51C6234F6D523566B2C7446A2
SHA-512:	20E56546388325BF8BB11F99963C3E9B35BFABA465A005839F140707358C68274DAF08737B01B030ABEA1CAF5DBFCC01E18BCE99DE17E7FB72EA388E94D8566
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\{5F0C331B-BF20-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	225646
Entropy (8bit):	3.292884380542562
Encrypted:	false
SSDEEP:	768:lQqo+wKqo+4Te4r54pr/Tyo871WMGE6+HKngKj71WxGE6+HKngHCyVd54YCsk1ga:1GbU47b7ksk1gmMsk1gmB/zi29m
MD5:	62DD03EB22569988774C402D3CA9C943
SHA1:	4A47C434ECB38F2BEC8863D535F9AC1C1244249B
SHA-256:	979BAC7751BFDE826E00AB63D37CE680987B2DD810CF21248095E023104BF8D3
SHA-512:	DA31930A2D8F2CB95906A3F64D84C4E7C1B315240D01AF737F7F20C72C2ABEC98B602B586CEA08C09C3720CCE054464E629D143082E66D2BB41277DB7DBA434
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\{65D7FE5C-BF20-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5640729987330608

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{65D7FE5C-BF20-11EB-90E5-ECF4BB570DC9}.dat	
Encrypted:	false
SSDEEP:	48:IwvhGcprsGwpa7hG4pQxGrapbS1GQpKjG7HpRQTGIpG:rvXZEQ7z6BBS/AyTEA
MD5:	B7B1BBC41BAFB77E03548262D82B0B1E
SHA1:	1FD9837EBDB90C7C12DEE4052F49EF7A253A6246
SHA-256:	4D83EECEC9BCACFABEDA4FDB6C48381FF969C797899385C8A9E23D1E139AB77F
SHA-512:	D9C36AA17A287FF93FED9EEAA19234F6293951D42A20AA5B9C4CDACD51EAD7B29953D748E1841FF2BB9282B5AEB9EB2D03386353F5D6C4E24213C05FDE92B06E
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\dikxvqf\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	1402
Entropy (8bit):	4.168700262587641
Encrypted:	false
SSDEEP:	24:i7fft34wTwljtN4QOm6dbqUyjBVlgqX+sVe+W:i7nt31TcNXOmGbqUyjBVWqXvzW
MD5:	620A7CC8B0BD28B4B3E988366DB8583A
SHA1:	A73D88A2A34D418ADCC778EB25FBD2C305E3045C
SHA-256:	E8C93059854D3D7F7B6F4580C060D9E85796AD1F9BD0BEDB25C1960E66B5C4F8
SHA-512:	73EBE5251CD980139F570238DA5882DF4D2A1B81876A78EB9613C5F96312CACDBD7AEC5E20E8744D2DE16CFAB8733B5AFB1B85A17A402A62EFF13C27CF84A2B
Malicious:	false
Reputation:	low
Preview:	k.h.t.t.p.s.:././.w.w.w...d.i.c.k.i.n.s.o.n.s.o.l.i.c.i.t.o.r.s...c.o...u.k./.w.p.-.c.o.n.t.e.n.t./.t.h.e.m.e.s./.q.u.i.c.k.l.a.u.n.c.h.-.p.a.r.e.n.t.-.t.h.e.m.e./.l.i.b.r.a.r.y./.i.m.a.g.e.s./.f.a.v.i.c.o.n...i.c.o.~..... .h.....(..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\-Default[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 275 x 162, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	12252
Entropy (8bit):	7.947348323758577
Encrypted:	false
SSDEEP:	192:XlboKrXVTt07GK0BETY7GoZAkg3v8D3zoglxOlBVromLhqXYFk8hNCm1nECwa:XZ5rlTt0yKWETDo6iDtxOl/SYFZU6n3D
MD5:	6C4940B9945E18C533D26D648212EDF4
SHA1:	4EF6EC59A21303A241D51FBFFE0805FD8832B947
SHA-256:	2D99CB776E06C2FB595671122285A66C4DEBE4029EEE2813FA54E750723B30C3
SHA-512:	F915B9EDC1E6FAB50F4FAF6670EB913045CD8DF2DE31E6791FBD0E19B785E55B05A99CF3A21A9A2890CB5A67051FC66AB0275D1B352224E076CBCB05FFBEA141
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.yoshki.com/SRA/EnglishMono/275/0/-Default.png?a=121*012801280128@5501090=401$0=60=40=90124012@=90124012@=70=401$0=40125012@1230124@5501$012@05501260=6
Preview:	.PNG.....IHDR.....bH).....sRGB.....gAMA.....a.....pHYs.....o.d../qIDATx^...E..r...H.$....J.....T...IQ@@EA.Q..H.@.0...v.....>.{...3....o.....`0.....`0.....`0.....`0.....`0.....`0.....`0.....`0.....`0.....`0.....`0.....`0.....`0.....`0.....`0.....`0.....`0.....`0.....`0.....`0.....`0.....S...D.....].e.....?.I/L.....=.....-Y.Z.y..l.cC.>}.g....._...\|nY.....K.}q....e}.y4...[.>....M.~....._....d}....O.....G..t2@d.....f.|I.m.vHyp?z.w....H.....;.o...[.x...../.N...g...RV.?.w..+...{I9).~..?.=7v\|v..m.z..S?..q....}~.....ot.t...~u.kq.x.b..+;n..^.._.\.\|.4t.b...'.~....O...2 .P....n}.7p.l....;w$...![.v]6k....%..^.....Ei.....O...\.:[.pQ.y.....'..}o.(.....S..ym.v.|G..].f.^Y$.8= .....88.<u..Yq...W...-v.<t.S.e?..k6b.h.....U".ISrb...{.+.....<;\=.g+V..}..s..e.F.....K.'F..-{..q..i....8b.R...A.....z.5R.j+..}V....>.._..7...Z&..r.6..R....^.z.<.&Ou...O5....!.H .g.<.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\EJRVQgYoZZY2vCFuvAFWzrk[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 39452, version 1.1
Category:	downloaded
Size (bytes):	39452
Entropy (8bit):	7.987087512271223
Encrypted:	false
SSDEEP:	768:lykUM4jJfotbO2Oh3CfrR7AzhXQBrRgfbJ9vP8QcBPeISuo0lgpQixOd6a2:coYZ2Oi+zhXidAbJdZ8PeIvl7iKC

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\EJRVQgYoZZY2vCFuvAFWzrk[1].woff	
MD5:	F88B728C1448F05A4612C32BE163C55F
SHA1:	6AF02DE62CA7E4F5A89BE792A74F45C673BD3BD8
SHA-256:	C5DFD155D3BB4D5BE721DB7EEAFEE73464B65C5CBB6BB3AADC482625376B7FF9
SHA-512:	8C7117FDAB1F5F76C8CCD655C72DDB50E82F4F7076C831896813F651B503B1F2D4DD982612CEF57A7138FF832033AC00647980C386E19D29829535223BE4A390
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/ptserif/v12/EJRVQgYoZZY2vCFuvAFWzrk.woff
Preview:	wOFF.....GPOS.....0.I.MGSUB...x.....H{...OS/2...8...Z...`lm12cmap.....cvt ... ...>...>...Ifpgm...`.....H.ogasp...t.....glyf.....w....F. .LPhdmx.....&.].t.head...L...4...6....hhea.....$....hmtx.....m#0loca.....Fmaxp..... ... ...gname.....<Kpost.....prep...@.....d..x....$i....m.m..... m..Xt...0x.Lw/.V4gO..JU.u2....=..[..'E....q..w>..Cl...O=....H.C.l.}..'.a.....aF-P.FL....[9....A...{...xN.$.3.{.....3..|...e....u.?)O...lhE....V....f...i.....2;gv..9..eEG....F.[5)...q..1.....Y\. ..4..~.....`.4.....U3...M.....qs.gsn`Cn..f....c..S.fs..F=.s4'.'q0....+.....5.....*.]....'.k,P.....W.*.9..l(x...Ds..=...zW..G..Y%....nf..l..u.a.\q..S.n./-.y.+J.7:.RV.u..j.....,:;.4R.B{.cs.~.S!..X... a.;U..]3.....Nh.|.....zC9.....R.w..f...cV.U.....k....,..6.....#a.$a..y6..fj.'e.....Q....._...@.....m..T...Q..:..O+...A.B.3..9[....*.....D..~'Ro.'.k...Y..\..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\ad_status[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	29
Entropy (8bit):	4.142295219190901
Encrypted:	false
SSDEEP:	3:lZOwFQvn:lQw6n
MD5:	1FA71744DB23D0F8DF9CCE6719DEFCB7
SHA1:	E4BE9B7136697942A036F97CF26EBAF703AD2067
SHA-256:	EED0DC1FDB5D97ED188AE16FD5E1024A5BB744AF47340346BE2146300A6C54B9
SHA-512:	17FA262901B608368EB4B70910DA67E1F11B9CFB2C9DC81844F55BEE1DB3EC11F704D81AB20F2DDA973378F9C0DF56EAAD8111F34B92E4161A4D194BA902F82F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static.doubleclick.net/instream/ad_status.js
Preview:	window.google_ad_status = 1;.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\all[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	799550
Entropy (8bit):	4.273067152763634
Encrypted:	false
SSDEEP:	6144:R6omS6CxE5jUSDVXCsKBc/R5M/HVxQfJDsZR8wDK3I25VGEmRTwh/s7I+:z6CiB1/RKVxLu+
MD5:	C7015C8439E386A7507C597A5C4C6901
SHA1:	4DA7DC6BD5FC667B462724970F932D2D5749643D
SHA-256:	E629FD9F6785D9A4CB5F5CC1CD3D3A758F35AD8C4451DE510169E82A6DC4C78E
SHA-512:	2730EAE3328BBE0FD84798391BB04D743F9096B4CA608F4FFFC425A40B27AC347A078D432A6FE4CC15022589E0A26BA8F00BBBDD9A6BFEEFC4B461417A0C28B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://use.fontawesome.com/releases/v5.0.13/js/all.js
Preview:	/*!. * Font Awesome Free 5.0.13 by @fontawesome - https://fontawesome.com. * License - https://fontawesome.com/license (Icons: CC BY 4.0, Fonts: SIL OFL 1.1, Code: MIT License). */.!function(){"use strict";var c={};try{"undefined"!=typeof window&&(c=window)}catch(c){}var l=(c.navigator||{}).userAgent,h=void 0===l?"":l,v=c,z=(~h. indexOf("MSIE")||h.indexOf("Trident/"),"___FONT_AWESOME___"),e=function(){try{return!0}catch(c){return!1}}(),m=[1,2,3,4,5,6,7,8,9,10],a=m.concat([11,12,13,14,15 ,16,17,18,19,20]);["xs","sm","lg","fw","ul","li","border","pull-left","pull-right","spin","pulse","rotate-90","rotate-180","rotate-270","flip-horizontal","flip-vertical","stack","stack-1x","stack-2x","inverse","layers","layers-text","layers-counter"].concat(m.map(function(c){return c+"x"})).concat(a.map(function(c){return"w-"+c}));var s=v||{};s[z]||(s[z]={}),s[z].styles||(s[z].styles={}),s[z].hooks||(s[z].hooks={}),s[z].shims||(s[z].shims=[]);var t=s[z],f=Object.assign||function(c){for(var l=1;l<arguments

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\anchor[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	41735
Entropy (8bit):	5.894782484137692
Encrypted:	false
SSDEEP:	768:v/SGbK6r5mMzkoN1zBwwvB8FZYDhZUAd/7:xbK6MoN9vp8DYVZUAl
MD5:	EFA61D2C33BF06BBF9A5B42B75A76CCE
SHA1:	7ACD8A85B9CFEDF7B318D42A8FF01EEC4B8ECC1E
SHA-256:	3886DCD9AE6B7179FFF069D9361108D5A60A4056702A0B00BDC9DA0A5B4D7EF5

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\anchor[1].htm	
SHA-512:	2AA7B13CAF1DB98CF8416673F7043E5AFC3719A3E9257128E65107ACF5446C4303A5D1C3EC3ED30FE115A2741E6B9FBD653B520692AF6885EF0F1118EFA7EF4
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE HTML><html dir="ltr" lang="en"><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.<meta http-equiv="X-UA-Compatible" content="IE=edge">.<title>reCAPTCHA</title>.<style type="text/css">.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 400;. src: url(//fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4mxP.ttf) format('truetype');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 500;. src: url(//fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmEU9fBBc9.ttf) format('truetype');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 900;. src: url(//fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmYUtfBBc9.ttf) format('truetype');.}..</style>.<link rel="stylesheet" type="text/css" href="https://www.gstatic.com/recaptcha/releases/eWmgPeIYKJsH2R2FrgakEIkq/styles__ltr.css">.<script nonce="wa22l0ZEJNSi93q7qF4Qng" type="text/javascript">window['__recaptcha_api'] = 'https://www.google.com/rec

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\api[1].js	
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):	1768
Entropy (8bit):	5.612927321721572
Encrypted:	false
SSDEEP:	48:VKEcOKoeN1l2FLrwUngKEcOKoeN1l2FLrwUnG:f4Dl2tsuU4Dl2tsuG
MD5:	DB7E6557447F36E889AFD1F82FF750FE
SHA1:	3F8CA19EEF99A1858FD483FE37244A440DFB6D41
SHA-256:	6BFA8B05D0C8E17F9D065180456EE1B5CA79750A596CCFDF6DBA12D5AD889602
SHA-512:	7D1859337EFA95B938FF0A6A895E6EAFB0300E7EFDD019B0D4E23F30A12BC26886ACA8CDACCDFFA5D4C9EED8F08844C6D246BFD83553A536DD84FE9F53BA4EBD
Malicious:	false
Reputation:	low
Preview:	/* PLEASE DO NOT COPY AND PASTE THIS CODE. */(function(){var w=window,C='___grecaptcha_cfg',cfg=w[C]=w[C]||{},N='grecaptcha';var gr=w[N]=w[N]||{};gr.ready=gr.ready||function(f){(cfg['fns']=cfg['fns']||[]).push(f);};w['__recaptcha_api']='https://www.google.com/recaptcha/api2/';(cfg['render']=cfg['render']||[]).push('6LfmMJ0UAAAAADP280q3cebbJ7e0Xs9ffHLgUKeH');w['__google_recaptcha_client']=true;var d=document,po=d.createElement('script');po.type='text/javascript';po.async=true;po.src='https://www.gstatic.com/recaptcha/releases/eWmgPeIYKJsH2R2FrgakEIkq/recaptcha__en.js';po.crossOrigin='anonymous';po.integrity='sha384-3l+Dzjt73YLhXz+WejlQA/r4+koQU0wEJ+YZAtKZ8DTxOPwZ54aluvUaML5sjiPl';var e=d.querySelector('script[nonce]'),n=e&&(e['nonce']||e.getAttribute('nonce'));if(n){po.setAttribute('nonce',n);}var s=d.getElementsByTagName('script')[0];s.parentNode.insertBefore(po, s);})();/* PLEASE DO NOT COPY AND PASTE THIS CODE. */(function(){var w=window,C='___grecaptcha_cfg',cfg=w[C]=w[C]||{},N='gre

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	1887
Entropy (8bit):	5.180102741405681
Encrypted:	false
SSDEEP:	48:SY3QWeY3QLGY3QxTVY3QCMY3Qw6XOWjOLQOxTSOCMOw6u:SYgWeYgLGYgxTVYgCMYgw6XOWjOLQOx9
MD5:	F0DFBF035F5547DFF41229F461471228
SHA1:	BA54747E3E95B9D4957686D78DD266223AC7CAE5
SHA-256:	9DB4DCD3E0E45AD82801C1F61098610D7D6A1C56C6D8020F5C1CF62EDDDCB1A1
SHA-512:	AC3CBD20D428C1BA4DC0E2BB36E87E7EC73E6742D1B52D96010DF8A7EA86828F6E4FDED30FCCD433E8637078EBA48D015DA1DABCFA59637DFC399FECBF2EC6A6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.googleapis.com/css?family=Open+Sans%3A300%2C300italic%2Cregular%2Citalic%2C600%2C600italic%2C700%2C700italic%2C800%2C800italic&subset=latin&ver=6.6.0
Preview:	@font-face {. font-family: 'Open Sans';. font-style: italic;. font-weight: 300;. src: url(https://fonts.gstatic.com/s/opensans/v20/memnYaGs126MiZpBA-UFUKWyV9hrIqU.woff) format('woff');.}.@font-face {. font-family: 'Open Sans';. font-style: italic;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/opensans/v20/mem6YaGs126MiZpBA-UFUK0Zdcs.woff) format('woff');.}.@font-face {. font-family: 'Open Sans';. font-style: italic;. font-weight: 600;. src: url(https://fonts.gstatic.com/s/opensans/v20/memnYaGs126MiZpBA-UFUKXGUdhrIqU.woff) format('woff');.}.@font-face {. font-family: 'Open Sans';. font-style: italic;. font-weight: 700;. src: url(https://fonts.gstatic.com/s/opensans/v20/memnYaGs126MiZpBA-UFUKWiUNhrIqU.woff) format('woff');.}.@font-face {. font-family: 'Open Sans';. font-style: italic;. font-weight: 800;. src: url(https://fonts.gstatic.com/s/opensans/v20/memnYaGs126MiZpBA-UFUKW-U9hrIqU.woff) format('woff');.}.@font-face {. font-family: 'Open Sans';. font-s

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\css[2].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	738
Entropy (8bit):	5.217369785384063
Encrypted:	false
SSDEEP:	12:jFYjY3Q6ZRoT6pUeU0ZqFYjY3Q6ZN76pUJXU3HqFYjO6ZRoT6pU8UE+JqFYjO6ZO:5uY3QYsh90suY3QYN7heuuOYshTE+8u8
MD5:	10CB433A2EDD8E09740A3CF1A6ECC99E
SHA1:	D9101329FD0135F29132CEF265253D18470D2D4E

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\css[2].css	
SHA-256:	A7E7F4F3769FAAD26366D0CD637A4B88E1E07637240454D2AF21B8AB1F6FACAB
SHA-512:	7F9B9E17DA1E06D4F21E94A3EB2E5089514C132C62D4B7E169DAE319953F5C00FD69AFC174778E7FF031E95197081E47BFEB01CDF5402F763DE861E697D8AE0
Malicious:	false
Reputation:	low
Preview:	@font-face {. font-family: 'PT Serif';. font-style: italic;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/ptserif/v12/EJRTQgYoZZY2vCFuvAFT_r21dA.woff) form at('woff');.}.@font-face {. font-family: 'PT Serif';. font-style: italic;. font-weight: 700;. src: url(https://fonts.gstatic.com/s/ptserif/v12/EJRQQgYoZZY2vCFuvAFT9ga QZynfpg.woff) format('woff');.}.@font-face {. font-family: 'PT Serif';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/ptserif/v12/EJRVQ gYoZZY2vCFuvAFWzrk.woff) format('woff');.}.@font-face {. font-family: 'PT Serif';. font-style: normal;. font-weight: 700;. src: url(https://fonts.gstatic.com/s/ptseri f/v12/EJRSQgYoZZY2vCFuvAnt66qSVy0.woff) format('woff');.}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\dickinsons-office-shot[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 762x560, frames 3
Category:	downloaded
Size (bytes):	92327
Entropy (8bit):	7.9836137683458475
Encrypted:	false
SSDEEP:	1536:p2YHXBx7sD7mosBjzzATsvuRDRKqDstpLIliOwonSW9b9Uo3XnTpSiGeZU3r:B3Bx7k7mosNAgVhCiOVnSuUpiGEU3r
MD5:	98C33C4CE34E8A2086E9FEC019D3D227
SHA1:	7F786BA6BB2FD8C1713CEED7057FC98D3E1D160F
SHA-256:	D053CA2A2F884141FA56DDEA45BBC1B72017ECF6522C49FD941F2A554A009EC9
SHA-512:	C5CD53D6AE2481DF5A22E9D7458D300897CE896F7E90DCC23C81C05D6A461671056AB599955C5282902EB8DDFA7F03F374568C625FE79C44294D39B61C4910C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.dickinsonsolicitors.co.uk/wp-content/uploads/2018/06/dickinsons-office-shot.jpg
Preview:	.....Exif..II*.....Ducky.....<...../http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x: xmptk="Adobe XMP Core 5.6-c142 79.160924, 2017/07/13-01:06:39 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:a bout="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmp:CreatorTool="Adobe Photoshop CC 2018 (Windows)" xmpMM:InstanceID="xmp.iid:35EC86B972E711E8816098B8ADB8CC35" xmpMM:DocumentID="xmp. did:35EC86BA72E711E8816098B8ADB8CC35"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:35EC86B772E711E8816098B8ADB8CC35" stRef:documentID="xmp. did:35EC86B872E711E8816098B8ADB8CC35"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>....Adobe.d..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\dickinsons-office[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=15, height=3000, bps=194, PhotometricIntepretation=RGB, manufacturer=Canon, model=Canon IXUS 230 HS, orientation=upp er-left, width=4000], baseline, precision 8, 1600x1200, frames 3
Category:	downloaded
Size (bytes):	316433
Entropy (8bit):	7.940803898953299
Encrypted:	false
SSDEEP:	6144:buOw+sZ9bGnTy2QWwPgZm9lOtFDgtv+IKOBO6vX3fPZ2sE4RVZNNCa:buF+kUnTKWwPmdD+Ilg6v/PAM1N
MD5:	C530439A8D1E3E117DF70BD17D1882EF
SHA1:	5AFBE7221A6A370D56831C7127920EF3E1A7AC88
SHA-256:	42646006E0F3DB346D53B749A836CCD7757AB1B527910FF4E15C10CAA84406CF
SHA-512:	52878FE657F19BE0D6CEA43DF91572014EAAA0CB27B5A76484C2DE5148A64942B603C7125A8C730B31C191E4274C6319BDC2148DF5FC05AB2BF667D2542DE31
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.dickinsonsolicitors.co.uk/wp-content/uploads/2018/06/dickinsons-office.jpg
Preview:	.....Exif..II*.....(.....1..".....2.....i.....(...|.....Canon.Canon IXUS 230 HS..... .'.....'..Adobe Photoshop CC 2018 (Windows).2018:06:27 13:58:00...!.....'.....0.....0230..... .....".....0100.....@.....D.....*.....2.....:.....0..... . .....2018:06:27 11:06:14.2018:06:27 11:06:14.....I.. ...k... .....k... ...^..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\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:vlIJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\dnserror[1]	
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
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\4PB7FJMT\embed[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	3924
Entropy (8bit):	5.469914817305456
Encrypted:	false
SSDEEP:	48:yMjDJXlfQFaA8R3crd10zMl/7D7ySfzMojJGxQ1W/idSWSA4KwHhU64hqhJ5r+Y5:yMDJXdPB3SYyHy83w7/opwr/4hqhZ
MD5:	EBC844F8A9380CCA9C09450970E9B7AB
SHA1:	DEED3B7E0F470917630B14FA9C0D61B0554A62D4
SHA-256:	53CBC02400BD4C2C08E2E1B201AAC8D1D53C5D345B32AE9AE720C4B94EAD355E
SHA-512:	EFFAF17F749B4F042BC6D1FDD455A72E4631FFB1548A6D22012C3942BA58D5336CA0DECFC2AA7C505E25E6F583BC5BCED97F3D18028ED7D34F19AD6C30CB1B7
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>.<html>. <head>. <style type="text/css">. html, body, #mapDiv {. height: 100%;. margin: 0;. padding: 0;. }. </style>. </head>. <body>. . . <script nonce="04T3dz4gvdl8DyYbEZ5rbw==">. function onEmbedLoad() {. initEmbed([null,null,null,null,null,[[[2,"spotlight",null,null,null,null,null,[[null,null,null,null,null,null,null,null,null,null,[null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,1]],["0x0:0x48ce1abce44d1a7b","Dickinsons",null,[null,null,53.75082769999999,-3.0289884],0],null,null,null,null,null,null,null,null,11,null,[null,"a",null,null,null,null,null,null,null,null,null,null,null,null,1,null,null,null,[null,null,null,null,0,0,null,null,1,null,null,1,null,null,null,0,null,null,null,1,1],null,null,null,[null,null,null,null,null,null,2,3,2]],null,null,null,null,null,[12,14,29,37,30,61,70,1371340]]]],null,["en_US","uk"],[null,null,null,"/maps/

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\embed[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	25226
Entropy (8bit):	5.50544425253384
Encrypted:	false
SSDEEP:	384:2YRgyq+e8PXe8cyJ61OP4tWlQ54C90gABjUJm3ulet7VRrpjXKXleTe6CttBe:e+1feCQ1LAyaCzDmeqpC6P
MD5:	F52AA4B18BE3ABD7C51C57251CE073DC
SHA1:	7A5B8F915C776C07F597CF5E3FD41185D4F77D41
SHA-256:	32BCA00E47D0F75C52DA52741E92427FA59E4783B1190E52F959A29CF4A21719
SHA-512:	8DE5D74A4E68213AB1EFD2933A6B75CF9FA808F30E29F37BCE8B7B7E2F27D7C801430A81F6335115E3B5863DB29D92B4D21A61E8681D9B78A40D3D7645D60F0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.youtube.com/s/player/e467278e/player_ias.vflset/en_US/embed.js
Preview:	(function(g){var window=this;'use strict';var uJa=function(a,b){var c=(b-a.i)/(a.l-a.i);if(0>=c)return 0;if(1<=c)return 1;for(var d=0,e=1,f=0,h=0;8>h;h++){f=g.Jn(a,c);var l=(g.Jn(a,c+1E-6)-f)/1E-6;if(1E-6>Math.abs(f-b))return c;if(1E-6>Math.abs(l))break;else f<b?d=c:e=c,c-=(f-b)/l}for(h=0;1E-6<Math.abs(f-b)&&8>h;h++)f<b?(d=c,c=(c+e)/2):(e=c,c=(c+d)/2),f=g.Jn(a,c);return c},t3=function(){return{D:"svg",.U:{height:"100%",version:"1.1",viewBox:"0 0 110 26",width:"100%"},S:[{D:"path",Mb:!0,K:"ytp-svg-fill",U:{d:"M 16.68,.99 C 13.55,1.03 7.02,1.16 4.99,1.68 c -1.49,.4 -2.59,1.6 -2.99,3 -0.69,2.7 -0.68,8.31 -0.68,8.31 0,0 -0.01,5.61 .68,8.31 .39,1.5 1.59,2.6 2.99,3 2.69,.7 13.40,.68 13.40,.68 0,0 10.70,.01 13.40,-0.68 1.5,-0.4 2.59,-1.6 2.99,-3 .69,-2.7 .68,-8.31 .68,-8.31 0,0 .11,-5.61 -0.68,-8.31 -0.4,-1.5 -1.59,-2.6 -2.99,-3 C 29.11,.98 18.40,.99 18.40,.99 c 0,0 -0.67,-0.01 -1.71,0 z m 72.21,.90 0,21.28 2.78,0 .31,-1.37 .09,0 c .3,.5 .71,.88 1.21,1.18 .5,.3 1.08,.40 1.68,.40 1.1,0 1.99,-0

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\httpErrorPagesScripts[1]	
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\4PB7FJMT\js_composer.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	485416
Entropy (8bit):	4.947766377400057
Encrypted:	false
SSDEEP:	3072:vR/QvmKEBVJh/PJMcokaCeLYtz+RJwKZ1kkUSbxhJwdO8BEo2HwSMxnp5ANdl0gN:vR/3/+cQ
MD5:	E6049B1CA50005DCFBB1CDE5A4C57C7D
SHA1:	0356B14CBF3EAB635B2C59565F2DA80E3ACEAD55
SHA-256:	97B5B6BB0BFD4413504DA4A5B78546698C75A127FFF51B095080EE7FD3B8EC0C
SHA-512:	3DB95768859FD706DE6887F53CB03D546446CCB3AF67B9807B6230A26E510173D7947457964F1ACBDD816EEB302B94547055606810DFB8AD5E69F443E4D1826F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.dickinsonsolicitors.co.uk/wp-content/plugins/js_composer/assets/css/js_composer.min.css?ver=6.6.0
Preview:	/*!. * WPBakery Page Builder v6.0.0 (https://wpbakery.com). * Copyright 2011-2021 Michael M, WPBakery. * License: Commercial. More details: http://go.wpbakery.com/licensing. */...vc_row:after,.vc_row:before{content:" ";display:table}.vc_row:after{clear:both}@media (max-width:767px){.vc_hidden-xs{display:none!important}}@media (min-width:768px) and (max-width:991px){.vc_hidden-sm{display:none!important}}@media (min-width:992px) and (max-width:1199px){.vc_hidden-md{display:none!important}}@media (min-width:1200px){.vc_hidden-lg{display:none!important}}.vc_non_responsive .vc_row .vc_col-sm-1{position:relative;float:left;width:8.333333 3%;min-height:1px;padding-left:15px;padding-right:15px}.vc_non_responsive .vc_row .vc_col-sm-2{position:relative;float:left;width:16.66666667%;min-height:1px;padding-left:15px;padding-right:15px}.vc_non_responsive .vc_row .vc_col-sm-3{position:relative;float:left;width:25%;min-height:1px;padding-left:15px;padding-right:15px}.vc_non_responsive .vc_row .vc_col

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\lightbox.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	9702
Entropy (8bit):	5.259118425611288
Encrypted:	false
SSDEEP:	96:uui446kcz/2MYPtFdKZOevdieoTQTQR04FiAK0GhM5FLxER+65yCAmt0eYBJ/IwU:U6kcrr6dKIevdCTQkHCaFLxERMFZRbzk
MD5:	84B31717631A3AA90D9FFB13FA68674F
SHA1:	CA51A53908F8A2A8D9FE618F0E472B7BCF15478F
SHA-256:	E9E6D9973A70B579A231AFAF2861F48C1EB4ED7752FCF56D4AE4330285E60E54
SHA-512:	D63077B30837BBCA2BE39F517039CA9D2641444DB9943FA8079370CE5E0238B3DAE92E99B951F4237AAAB2B84D4AC1834B53BA41A56F9D9EBAC5D76F5C294AB 9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.dickinsonsolicitors.co.uk/wp-content/plugins/js_composer/assets/lib/bower/lightbox2/dist/js/lightbox.min.js?ver=6.6.0
Preview:	/*!. * WPBakery Page Builder v6.0.0 (https://wpbakery.com). * Copyright 2011-2021 Michael M, WPBakery. * License: Commercial. More details: http://go.wpbakery.com/licensing. */.// jscs:disable.// jshint ignore: start../*!. * Lightbox v2.11.3. * by Lokesh Dhakar. *. * More info:. * http://lokeshdhakar.com/projects/lightbox2/. *. * Copyright Lokesh Dhakar. * Released under the MIT license. * https://github.com/lokesh/lightbox2/blob/master/LICENSE. *. * @preserve. */.!function(a,b){"function"==typeof define &&define.amd?define(["jquery"],b):"object"==typeof exports?module.exports=b(require("jquery")):a.lightbox=b(a.jQuery)}(this,function(a){function b(b){this.album=[],this.currentImageIndex=void 0,this.init(),this.options=a.extend({},this.constructor.defaults),this.option(b)}return b.defaults={albumLabel:"Image %1 of %2",alwaysShowNavOnTouchDevices:!1,fadeDuration:600,fitImagesInViewport:!0,imageFadeDuration:600,positionFromTop:50,resizeDuration:700,showImageNumberLabel:!0,wrapAround:!1,d

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\loading[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 32 x 32
Category:	downloaded
Size (bytes):	8476
Entropy (8bit):	7.521581779536469
Encrypted:	false
SSDEEP:	192:e8mZU0o1P1rUssaXA6RJiqlrcDUpTQ+ZSIWl7QBhr5z:iZc1PvA6RJiqYUq/l7Md5z
MD5:	2299AD0B3F63413F026DFEC20C205B8F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\loading[1].gif	
SHA1:	CF720B50CF8DDE0E1A84CE1C6A77788BFC5882D5
SHA-256:	225AA88B6AB02C06222EC9468D62E15FA188E39CDB9431D1F55401AD380753ED
SHA-512:	DC299EE8DE6D5BB9D3A95A0FC200EA380C6DBAEB72FBFF74E1E8BB260EE3DEEC6C981D9CFC05BF2409B8760613EF1C02BD7396456BEC618F287CA56A7A939 57D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.dickinsonsolicitors.co.uk/wp-content/plugins/js_composer/assets/lib/bower/lightbox2/dist/images/loading.gif
Preview:	GIF89a . .....!..NETSCAPE2.0.....!.....,..... . .@..@.pH. ...PdCl:].d.....Xla[..@$.,..T..G!.c>..#..p..0.yzk.....#). .....k..rwv&... ./$/..._.B..}}..O\..(.O....'.O....e..N....'..0.,....n..` #.(.#.....&&.....tu..QH.P.....-R1..+..\,..."....@+".. 9 . 8.W..$...`L!I....H...f#S~h.Z"==.XP.....Z`.....*.@B7..K.4Y`.NCP'.&,. @..Y.yR%!..J.Q....!....3.,..... .....pH..D.M$.....Pqx=..I.....r-gc..P.y.He.R.Q.8/7i.....!!yn.....^ .....#j^.. ....^.....(.^*...P.Q.....R(....%.Q.....D.....C...i.B.....3.....3..."..#....."..'....,@...{.T .P'....=8.....=...@..5.4H.....#...0.....2....$..*%.tya.L2H(8&..Bg.1.Ji.b...-`.`....".HP...=3...Q.<. ...!.....,..... ....@.pH..D..... .T...H..c.....PmB..v..FL..Ta8.....6.RD%...!w$k.[]1.D....!.*.....!.E.I...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\logo_48[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 48 x 48, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	2228
Entropy (8bit):	7.82817506159911
Encrypted:	false
SSDEEP:	48:4/6MuQu6DYYEcBDlBVzqawiHI1Oupgl8m7NCnagQJFknwD:4SabhtXqMHyCl8m7N0ag6D
MD5:	EF9941290C50CD3866E2BA6B793F010D
SHA1:	4736508C795667DCEA21F8D864233031223B7832
SHA-256:	1B9EFB22C938500971AAC2B2130A475FA23684DD69E43103894968DF83145B8A
SHA-512:	A0C69C70117C5713CAF8B12F3B6E8BBB9CDAF72768E5DB9DB5831A3C37541B87613C6B020DD2F9B8760064A8C7337F175E7234BFE776EEE5E3588DC5662419D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/recaptcha/api2/logo_48.png
Preview:	.PNG.....IHDR...0...0.....W.....gAMA.....a.... cHRM..z&.....u0...`..:....p..Q<....bKGD.....C.....pHYs.....IDATh...P....=..8.....Nx. ..PlP8..;.C.1iL#6...*.Z..!.....3.po . o.L.i.I..1fl..4..ujL&6$.....w.....,Z..z. ~....\.._.C.eK...g..%..P..L7...96..q....L.....k6...*..,xz.._.....B."#...L(n..f..Yb...*.8.;....K)N...H).%.F"Ic.LB.....jG.uD..B....Tm....T. .).A.}D.f..3.V.....O.....t_..].x.{o.....*....x?!W...j..@..G=Ed.XF.....J..E?../]..?p..W..H..d5% WA+.....)2r..+..'qk8.../HS.[...u..z.P.*....-.A.}.....I .P.....S....|...)..KS4....I.....W...@....S. s..s..$`.X9.....E.x.=.u.*iJ.....k.....'...!.a....*+.....(...S..\h....@.....I.$..%.2....l.....a.|.....U....y.....t..8....TF.o.p.+.@<.g.....-.M.....:.@..(.....@.....>..=.ofm.WM{...e.,..D.r.. .....w....T.L.os..T@Rv..;.....9....56<.x.....2.k.1....dd.V.....m..y5../4|...G.p.V.....6...}.....B.....5...&..v..yTd.6...../m.K...(.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\mem5YaGs126MiZpBA-UN_r8OUuhv[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 18744, version 1.1
Category:	downloaded
Size (bytes):	18744
Entropy (8bit):	7.966883926264397
Encrypted:	false
SSDEEP:	384:zawWpQHZNpxHreHjc5bHhYc9ON58zWZnmiN4RHcSd2UrrMKCWX:zawPscLqqO/8zG/4RHvdh33X
MD5:	2A6051095E2330FB1A45B836E3BA038E
SHA1:	1DA733C279AA12C3D8857AED80CD910C2B209EAE
SHA-256:	C98B647124C63DEA93B52BCF6A97A76A6944B9894DC0377B70F8C3B47D91382A
SHA-512:	CB019D3D69A51FE9522AA22BF637886B9691270F0BA409167B5A1225CB50BCE494ADEAACC7C94D341A02B3AC751620E9E6A4B9AD9B3FF916C3FA12D710A3AC 6D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v20/mem5YaGs126MiZpBA-UN_r8OUuhv.woff
Preview:	wOFF.....I8.....n.....GDEF.....GPOS.....GSUB.....y.....;..OS/2...$...^...`}...cmap.....Y..cvt ...8...]....fpgm.....~a..gasp...4.....#glyf.. .D..8...W.._..head..A....6...6..F.hhea..AT.....$...dhmtx..At....._.loca..C.....K.`@maxp..EP... ... .name..Ep....."c?Jpost..F\.....5.".prep..H .....:..].... .....x.M...P.@..L..$$. .g..;..k.z...P.$K.....[.E..Z....B).a.:...i...!.....J ...U....l/..m.&*3.KO...#..-..%;7.V.....x.c`fig.a`e``..j...(.../2.1..`b.ffcfeabbi``Pg``..b.. 0t.vfp`P...M... C.G/S....|...=.6 .....m/....x.\.!..q.....#acf...#1Q@.'U..@..".llt.Aa#.f|c.W.....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN....:.....F....GG.g.s,x.>0....v..I;o..<.$G9.\f2...e{}.IS2..uc]p. .....M.x.c.a.g.c..$K..$..`.g.e..... .....R.g.....?.....x.)d.....$...."....0.#.A@X..0.....x.uTGw.F.....)..)7.W.$`*.....G.Kz.)e....t.|.1.7...s.g...3.7mgf..~{1...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\memnYaGs126MiZpBA-UFUKW-U9hrIqU[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 22088, version 1.1
Category:	downloaded
Size (bytes):	22088
Entropy (8bit):	7.976197045721412
Encrypted:	false
SSDEEP:	384:PnGPIpMdUGB5dC/q5f2Rh1T9+LraA27GnT4l5UcexDokQcH9slkDk1vRO2B:PnG5dzA/qN2RBIeA27GT4zAxDofcHeeY
MD5:	6B8620DD9B7F0DE6531FCC1D397B5361
SHA1:	15632276D3969AA6FCCC2231906FB44FA5479EB0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\memnYaGs126MiZpBA-UFUKW-U9hrIqU[1].woff	
SHA-256:	FC849DBB5A6BC86E49018BF353EAACA1DDA58427F5A0ED6E6B6CFBD6F90ADB77
SHA-512:	F4F6656EA257477CB1584D788BA8E0B79CD439DC41FADE2C3FD234E3FE8C927D7C802E9D49F0CFA7E9992A50F1F2887560C937B117E617770F840D369087A378
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v20/memnYaGs126MiZpBA-UFUKW-U9hrIqU.woff
Preview:	wOFF.....VH.....GDEF.....\.....GPOS.....R.c..GSUB...d...s.....,OS/2.....U...`t..%STAT...0...B...V^.B.cmap...t.....`cvt ...,.....8I.G.fpgm..... ..Zglyf.....;...Z....head..K....6...6...)hhea..KD...#...$....hmtx..Kh.....P..2,loca..N.....*!..Nmaxp..P$... ... .name..PD...$...`;.^.post..Qh.....y0>r.prep..T....B.....3)x.....@ ...}w.A...@.6.(t...A1T..i.. R@..Y...u.[1.ng/.%..J.]..M.=..K.K\|5....&:..1.f4..D..Mx.5...`...{zz.m.m.m.m.m...f.Nf....u!.B"+.._.h...G...c.V..I...A.....i....(.1...l.....(.EH$F...Q.1....LY0. ....0..1..P.;p..../.....]....]C.8.R.KT.-.%.^...Yrje.-.....R].Jci).e.t..[..{..ce.i.^...TV.^.m.(.m{XN.y.j....>.O...Z#R.5.&.Tz... U\...k.f.....Z;jw....F.x.....\.*...G..^..zW..K....+....X.IJF$]r)9..".0. ..)L..\L.g....I.....{&-...<.....$.....Ny/.)W...~...g.C.YL...D.!...../Y.\...R...7.9(.....@.....x...../w.zpu#..,72.L...z7.....=g....M.& .Y...F..n.cCN.`'.K..o.....}A>.{

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\next[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 50 x 45, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1350
Entropy (8bit):	7.795826172553452
Encrypted:	false
SSDEEP:	24:OgMSVQogiW6rN55Wfj2byDoY6nn1SoPthAOy79jQC7tVcaKE028k:ZBCiWYNvGjWyDop1SoPMr9ECxUk
MD5:	31F15875975AAB69085470AABBFEC802
SHA1:	777E92C050F600B4519299C3D786B8F2F459FEA4
SHA-256:	15B869B02C6FBAA8C6C26445A2DD2D9BAD80FD27B1409F8179E5DD89DC89D90A
SHA-512:	EDC920DCD2F5AC9A6E08098C6A59F888A9CB135FF4EF3DC2183931E065B6531E00E2C8ACD3C329A3D90EB939EA3DB318A9B677B5AA78A227815373D7008D40A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.dickinsonsolicitors.co.uk/wp-content/plugins/js_composer/assets/lib/bower/lightbox2/dist/images/next.png
Preview:	.PNG.....IHDR...2...-.....8.....IDATx..KL\U..3w.+0.b.gp.-a.Z.U.....Rjj.-.Z.va.i.....@.....HA...F.#a..C.M0. @x#e.O.|....9.'..2.Y..}..{y.4...@'..F<.....%..I?I....X.....#....=.".... .xA.8I..c ....r..J..D...u=j.....~.....T1],.N$.<.N.B...wvww.....7p...a.>.r.Ngdaaa6nZSSS..\|...S..e2N.Q...H..C+.....*.....eTWD.)..H....z.bMOO....>..R&..LS-..TWW..... Z.....z?..2&#..r....).-,,..2.....\|.*#....t../..h4....a%3666....e..p..h.DI .....d0.."3.....k.M2gAEiii.....F.].L.d..@..F2Nj3?.\(...X]]]....9...u....<.&.*..6.(((hA.....v...i.....3s.d..... .J..@..Ef.T..0..Q.M+....y.....,.Z6.....p.....Q..f... [...>.+ph.b...*.c. ..d.p..f.4....!..&...S ..}.@.-.e..x.\.D"_....2..2....ZLW%...A..y....4..:..Y.3333.#W.....7'.....}.\|600.W\....;..G...TD .:...tN.....~.....\|.....4."...!.c ...k...?.*...9.}...v...;U..A...rMM.."....Q.J.9 .$I.a....."....d.@"..O.W.9.$..D.T655....[[[o.l.J.-..q.M...Kd.L\nll..Ittt..}UL".$

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\office-background[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 1400x933, frames 3
Category:	downloaded
Size (bytes):	204176
Entropy (8bit):	7.9757798801235005
Encrypted:	false
SSDEEP:	3072:eaHaWurt5YRbRpBTWAyWp+sBXcG9Qz6JqespR1ACUzSBskC2y3+b0aYbqchbG3NQ:PH/jbnZd5cG9Qw81cSDRD0qPCJb
MD5:	EEDCE1AFF3F4B59A67222A804348E6EC
SHA1:	15486B32DB9D596F92342370F99C28D7B6607DC1
SHA-256:	E6B91D6B5F20425F0D257FA24B593B8DE2D1E4E0179AC6F304DF0E305F47D85A
SHA-512:	75182121BADAE03533D1A5344E59E3FB88161FCF77F5FB4259B9F317626FEF13C462E105DAC24601B4F376A54F300C8A21F1D6F726EA0A2AB4014F0597416F9A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.dickinsonsolicitors.co.uk/wp-content/uploads/2018/06/office-background.jpg
Preview:	.....Exif..II*.....Ducky.....<.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c140 79.160451, 2017/05/06-01:08:21 "> <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:6A766160634011E894F5A2F87AD01BE2" xmpMM:InstanceID="xmp.iid:6A76615F634011E894F5A2F87AD01BE2" xmp:CreatorTool="Adobe Photoshop CC 2018 Macintosh"> <xmpMM:DerivedFrom stRef:instanceID="1559E4F083B31F23837D87A02D82ABF7" stRef:documentID="1559E4F083B31F23837D87A02D82ABF7"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>....Adobe.d.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\prev[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 50 x 45, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1360
Entropy (8bit):	7.759688532707318
Encrypted:	false
SSDEEP:	24:GHSkQz3cCPNyzYiMy4T+awnPjXsjECJNuMCnyEiMn/k4GWkfAdU9:6SkO5YzfRCJ07Tn0W8
MD5:	84B76DEE6B27B795E89E3649078A11C2
SHA1:	6640A3432F7BA7AEA6129CDF7A5D3EABD47C295C

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\prev[1].png	
SHA-256:	7FD9273F20FDB1229C224341271A119020A5EEE74CCF6B4605730917C864CAF2
SHA-512:	F7128971CD4B6442EBAC344CAD93186E1FCC976470E2F5A4E758F3439C7B07421FB99A927450414B86B4BBFC0F2CC605B0E63C217057E094F9D866D9906960F5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.dickinsonsolicitors.co.uk/wp-content/plugins/js_composer/assets/lib/bower/lightbox2/dist/images/prev.png
Preview:	.PNG.....IHDR...2...-.....8.....IDATx..[L\U..=3g.S.p+...A.....30.Z...Z.Z..!.i..Gn..;1.`.#.bD.....F....:LM4.....).?...d....=..|..V.~...s..P$..O....0..0.5.xpN.....+}%../...h..R..".$..X...&..... ...<!..t.H.J.."......$P....].... .=.\$s...I.a...l..(...1333...........]..s.d.!i."..5F....._.".Y^^.Y...j...l...a.. .x@.....1gww..c....@:...D.n..D....paa.....H5e(...:...IT.....X__....@m...&Q. .6u"".P(.@b.....A!.....N.D!.@.....I...n.....^...;H.u.Q.q*....m..W=.....*&q.8h[%..."\|..D0...X].....^.V...g-A.I"++.6nvKz.....~.....H.I.d%..@...$.....`..JJJ:.....I. .....8...8..F...<I .q..1@D'.....{.N. .Q.....2a.....`G.IWbsss...uR'.).,.&.c...`..a.F'.`Gov.,.l;q.6LD.fp.d.....'...v.I... ...4R.P.L..N..'.....>C..p....0Z.=.....<.....?.I...Ml./P..T..p.h\....Z,....poDpFFF~G...]P.> (..m.hY@..(y...../..D.....~D.{."(.g)c*Pd..c.....c..466~.:... .d(#.D.@:.....M.d.....PJ2...3..G....{.....I.LKK..j..2.3$c.....%&.....s....ikk.Dm....$2.CE8.D..d....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\recaptcha__en[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	343376
Entropy (8bit):	5.708451910823472
Encrypted:	false
SSDEEP:	6144:DUIS85b0RNK4QFbDym2MXV817R9ryWv3hslGxl:bS85bIN6OuF817R9rvpvb
MD5:	4CB94B696DF4446AA6D4292BE0DFC2C0
SHA1:	626C41D96DC979EB9887EC603DB5A88E175B4E6D
SHA-256:	F8CB544F90B2C0399716BD41669BCEF24768DD8C509A7C7D1C26CA9FE4EFC0FB
SHA-512:	370E676EB3A4DB8265643C9EF89B578C708B8EC6F24D0AF70F3D249EEDC8EB0FEBFDC2441864DE74C7D69794803F14EB37A4855DBEB9E903D1506A43A5E21B B1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/recaptcha/releases/eWmgPeIYKJsH2R2FrgakEIkq/recaptcha__en.js
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var Q=function(){return[function(T,r,b,R,D,N,W,k,Y,X,E){if(1==((3==(((2==(T+7&(X=[66,15,"dg"],X[1]))&&n.setTimeout(function(){throw r;},0),T)^996)&X[1])&&(E=0<=rW(r,b)),(T^362)&13)||(Y=["bg","POST","ct"],DF.call(this,(new N6(u[7](3,"u serverify"))).K,u[32](X[1],"")]}'\n",Wd),Y[1]),f[41](X[0],this,"c",r),f[41](18,this,"response",b),null!=R&&f[41](18,this,"t",R),null!=D&&f[41](2,this,Y[2],D),null!=N&&f[41](2,this,Y [0],N),null!=W&&f[41](50,this,X[2],W),null!=k&&f[41](2,this,"mp",k)),T-3&X[1])&&(u[36](9,.function(t){P[23](14,b,r,R,t)},kx),O[18](20,!0,kx)||f[43](3)),!((T<<1)%19))){for(R in N=r,D=[],b)D[N++]=b[R];E=D}return E},function(T,r,b,R,D,N){return(T>>2)%((T+(N=[7,25,6],N[0]))%4||u[4](22,0,R,4,b)&&P[4](30,r,b,4,R),N)[2]||(b=["><div class="","">','"rc-doscaptcha-body-text"],r=' <div class="'+u[N[1]](N[0],"rc-doscaptcha-header")+b[0]+u[N[1]](N[0],"rc-doscaptcha-header-text")+b[1],r=r+'Try ag

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\slider-2[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 1920x851, frames 3
Category:	downloaded
Size (bytes):	72717
Entropy (8bit):	7.614519881929936
Encrypted:	false
SSDEEP:	1536:dx3wnx81KxxVvsmd9HRNrz1iMw7uv+GNgeTjhVo/:UxB2mfr3w7/6TjhU
MD5:	63F439E8160FA215FF8211A89806B0B4
SHA1:	1559B20D022BA7365E0E7A8173FB89C67F67C68A
SHA-256:	D547FBEB195EC3AD96E3F7831311252A36F60DE11BCF27F84948F6782A74BE51
SHA-512:	6ED417770FE55041677B81588B0A9AE8491440D29DE565947B46F2EEF9788B7A4D030CBBBF19E0E8C2B2432F3CAA8FE6A322DA82C4084C8875187BF045DED31
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.dickinsonsolicitors.co.uk/wp-content/uploads/2018/06/slider-2.jpg
Preview:	.....Exif..II*.....Ducky.....<.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x: xmptk="Adobe XMP Core 5.3-c011 66.145661, 2012/02/06-14:56:27 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:a bout="" 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:OriginalDocumentID="xmp.did:c9a2b572-e9aa-2a4e-834e-3cd99fe23045" xmpMM:DocumentID="xmp.did:AF07702BDB7011E7B0748FA1D5727E37" xm pMM:InstanceID="xmp.iid:AF07702ADB7011E7B0748FA1D5727E37" xmp:CreatorTool="Adobe Photoshop CC 2015.5 (Windows)"> <xmpMM:DerivedFrom stRef:in stanceID="xmp.iid:1bba93e6-7f2e-0847-9c44-39124ccad7f7" stRef:documentID="xmp.did:c9a2b572-e9aa-2a4e-834e-3cd99fe23045"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>....Adobe.d.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\style[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):	146943
Entropy (8bit):	5.0668924765480865
Encrypted:	false
SSDEEP:	1536:VOJX77J2PqBhAFliWj+gYNG1Z2sRoxhq+xovTxWXaKKiEzDw8GFb/Wvtf5bgO1AC:1u5Fb/WvtB
MD5:	6A742E22F73ED1091251FD192BAC9EE8
SHA1:	7CD989A77EA00F5A9CA1CE4694996AF174551312

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\style[1].css	
SHA-256:	14D38F9C161BCDAC5A6C165B0F3A8CDDD77512046AD8658E81411F42F98551DA
SHA-512:	D1194008664785572CFD828A4D3470E7C064405AD665508109FBBD9A35CA112014932254DDC6A10C8DA3F2D9BBCEDDA2D43D6E02F0685B676585ACBF6FACC0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.dickinsonsolicitors.co.uk/wp-content/themes/quicklaunch-parent-theme/style.css?ver=5.7.2
Preview:	@charset "UTF-8";./*.Theme Name: QuickLaunch.Theme URI:.Author: Quicklaunch.Author URI: http://www.quicklaunch.co/.Description: Parent theme..Version: 1.0.*/./*!. * Bootstrap v3.3.7 (http://getbootstrap.com). * Copyright 2011-2016 Twitter, Inc.. * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */./*! 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 { di splay: 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: 1px dotted; }..b, strong { font-weight: bold; }..dfn { font-style: italic; }

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\underscore.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	16045
Entropy (8bit):	5.126324377314635
Encrypted:	false
SSDEEP:	384:R2rjVXPfHMYfSCSy5ZMdn01dcs/qQavic0cz68Be:RyVX3C8rEi+za
MD5:	203EEB8DD53E84FB53B7AEFFB562D825
SHA1:	B4B4361A61EE78717BDCFFE5C46EA79CDC3E04AE
SHA-256:	6CD0D6897B3D4779F7D88CE72531F22FBF75851B195FB14E6F3F23D051B3D1E9
SHA-512:	4CCB1643EE93B0245002FD7EBD31D515D9E67F00DB3ED1EA506E09CE30E725DD1C49860F90B8036FB8A3F0554CFDCB89D7198A46267EF9DB456D23F1168968
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.dickinsonsolicitors.co.uk/wp-includes/js/underscore.min.js?ver=1.8.3
Preview:	/*! This file is auto-generated */.!function(){function t(){}var n=this,r=n._,e=Array.prototype,o=Object.prototype,u=Function.prototype,i=e.push,c=e.slice,l=o.toString,a= o.hasOwnProperty,f=Array.isArray,s=Object.keys,p=u.bind,h=Object.create,v=function(n){return n instanceof v?n:this instanceof v?void(this._wrapped=n):new v(n)}; "undefined"!=typeof exports?(exports="undefined"!=typeof module&&module.exports?module.exports=v:exports)._=v:n._=v,v.VERSION="1.8.3";var y=function(u,i,n){if(void 0===i)return u;switch(null==n?3:n){case 1:return function(n){return u.call(i,n)};case 2:return function(n,t){return u.call(i,n,t)};case 3:return function(n,t,r){return u.call(i ,n,t,r)};case 4:return function(n,t,r,e){return u.call(i,n,t,r,e)}}return function(){return u.apply(i,arguments)}},d=function(n,t,r){return null==n?v.identity:v.isFunction(n)?y(n,t ,r):v.isObject(n)?v.matcher(n):v.property(n)};v.iteratee=function(n,t){return d(n,t,1/0)};function g(n){return v.isObject(n)?h?h(n):(t.prototype=n,n=n

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\vc_grid.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	26345
Entropy (8bit):	5.067814330753913
Encrypted:	false
SSDEEP:	384:SezbnrNyKX9Qr7vDTNxmJOJ1MAkZL6Qv5gZ:0r7bJxmo0L6KgZ
MD5:	BF35404EC410297F390AAC8056DCA830
SHA1:	A250A1588B2FB2B71EE8A2D11A00E576D037BFB2
SHA-256:	3EDE42F7B6632487687A839DEF8F082B7564D792A7093F5FB8B20547F5891CB8
SHA-512:	8D63C4796C103B166D2042FF2ED07ABFF9DF877F0ED8F29083E685A10055D282958E7E88E07AE91AC473144748FBC797760730F3525C3BB7F96E83C1C321C5FC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.dickinsonsolicitors.co.uk/wp-content/plugins/js_composer/assets/js/dist/vc_grid.min.js?ver=6.6.0
Preview:	/*!. * WPBakery Page Builder v6.0.0 (https://wpbakery.com). * Copyright 2011-2021 Michael M, WPBakery. * License: Commercial. More details: http://go.wpbakery.c om/licensing. */.// jscs:disable.// jshint ignore: start..!function($){"use strict";var vcGridStyleAll=function(grid){this.grid=grid,this.settings=grid.settings,this.filterValue=n ull,this.$el=!1,this.$content=!1,this.isLoading=!1,this.$loader=$(' '),this.init()};vcGridStyleAll.prototype.init=function(){_.bindAll(this,"addIt ems","showItems","setIsLoading")},vcGridStyleAll.prototype.render=function(){this.$el=this.grid.$el,this.$content=this.$el,this.$content.find(".vc_grid-item").length?(thi s.grid.initFilter(),this.filter(),this.showItems(),this.filterValue=-1,window.vc_prettyPhoto()):(_.defer(this.setIsLoading),this.grid.ajax({},this.addItems))},vcGridStyleAll.protot ype.setIsLoading=function(){this.$content.append(this.$loader),this.isLoading=!0},vcGridStyleAll.prototype.unsetIsLoading=function

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\webworker[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	102
Entropy (8bit):	4.808572706096191
Encrypted:	false
SSDEEP:	3:JSbMqSL1cdXWKQKeAsCGEOgvUMXWaee:PLKdXNQKeAzGgjXL
MD5:	2FE5BB59FB909B8AE80DDDEFCF36E870
SHA1:	224FAE6E9EFACEBEAF23F5CA02DB137F872561C0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\webworker[1].js	
SHA-256:	ECD9CC5899B95B6F83EA990FA831EF25BB33C11A5FC22C7C5DACDA7E1239783A
SHA-512:	35D4B5BB705592F07F2D2857536FB60B4CB595BCF3488D2E7389B04ADB6ABF3B1D5FC7A9B561F75273C3C67E82B378A2E98C9442772F0195C0B20295D12386D1
Malicious:	false
Reputation:	low
Preview:	importScripts('https://www.gstatic.com/recaptcha/releases/eWmgPeIYKJsH2R2FrgakElkq/recaptcha__en.js');

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\wp-emoji-release.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	14229
Entropy (8bit):	4.959165424851354
Encrypted:	false
SSDEEP:	384:inJ5kNuPTbUUh31//bEP+XgA3FqC2effJmp3:iJ5aUUUh31//YWXgA7ffC3
MD5:	EAA8641BCDA2371F4024A71FBB67DE3B
SHA1:	0E46C39D3821683C856605A82254115F9A6A7792
SHA-256:	0C5F584D1EA2C3313DC8C55824C2A572D3CF2EAE87C5CA62A58E598AEC9DDB5C
SHA-512:	82B6B84D0A7A28D6A8B013EE41EEF27E1DF8C1FCA396DFB4ED6D01249E12479230CB2D3683A56EB80651D22046C74506D194FA34B05E2A8AD8A08AE297F79AB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.dickinsonsolicitors.co.uk/wp-includes/js/wp-emoji-release.min.js?ver=5.7.2
Preview:	/*! This file is auto-generated */.// Source: wp-includes/js/twemoji.min.js.var twemoji=function(){"use strict";var f={base:"https://twemoji.maxcdn.com/v/13.0.1/",ext:".png",size:"72x72",className:"emoji",convert:{fromCodePoint:function(d){d="string"==typeof d?parseInt(d,16):d;if(d<65536)return a(d);return a(55296+((d-=65536)>>10),56320+(1023&d))},toCodePoint:i},onerror:function(){this.parentNode&&this.parentNode.replaceChild(g(this.alt,!1),this)},parse:function(d,u){u&&"function"!=typeof u||(u={callback:u});return("string"==typeof d?function(d,b){return o(d,function(d){var u,f,c=d,e=x(d),a=b.callback(e,b);if(e&&a){for(f in c="")}return c})}:function(d,u){var f,c,e,a,b,t,n,r,o,i,s,l=function d(u,f){var c,e,a=u.childNodes,b=a.length;for(;b--;)c=a[b]

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\wp-polyfill-element-closest.min[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):	417
Entropy (8bit):	4.878288491780445
Encrypted:	false
SSDEEP:	6:qQ2noFarYvLN+XKxNk6GRciALMEnwu0sbYXpX9Y4qoCJgcnll6VAzPPqXXA8hSqf:66aIkaxNkNvQN0s659Vq/3lPmQ8hP
MD5:	89A4E64830CE633B60F1E4060FAA5726
SHA1:	DC8A0693095BBC56E745DE78C8D1D2333169D575
SHA-256:	1D1CC2B1811B4EBEDA7BE9B00999AA3330C7D16D1EA4DEBD33D3DEDF3A956AE0
SHA-512:	ACB81858E24A58253B556FB4B83161756CF8E5C52A929597B56987A6F5E57C22F41F958FE49E78E885EA52CC809AD4DE95FFE98AD1F9289B380F45233F82E6C2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.dickinsonsolicitors.co.uk/wp-includes/js/dist/vendor/wp-polyfill-element-closest.min.js?ver=2.0.2
Preview:	!function(e){"function"!=typeof e.matches&&(e.matches=e.msMatchesSelector||e.mozMatchesSelector||e.webkitMatchesSelector||function(e){for(var t=this,o=(t.document||t.ownerDocument).querySelectorAll(e),n=0;o[n]&&o[n]!==t;)++n;return Boolean(o[n])}),"function"!=typeof e.closest&&(e.closest=function(e){for(var t=this;t&&1===t.nodeType;){if(t.matches(e))return t;t=t.parentNode}return null})}(window.Element.prototype);

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\wp-polyfill-node-contains.min[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):	353
Entropy (8bit):	4.82144644832395
Encrypted:	false
SSDEEP:	6:qQQTMhM8Frv1nX/JR/X0QXQeLZ+AWGeNuhLeSqGvSqLifqWpqLlldALnRtgAlSqY:cdUrBPXpAe9+/NEi2v7/BlldoRtgAl7s
MD5:	B32D5CEA64B4FD156F47C0EC0A9D8532
SHA1:	2479F764DE67D2CD836CCB27F97DD4A42232AC0C
SHA-256:	24A4D8749750DA00649D2A24744F109D7E0B2C96755282A65E4BC13B62ED18CE
SHA-512:	DEED55D5DC985E1B7A09A839FD753D634C1BDE9646CD4B709950FCE3A99158FB8494103A1C78C23CBE35A1FD2716F44CD4D28B0E94980125FE50CD92D70D09
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.dickinsonsolicitors.co.uk/wp-includes/js/dist/vendor/wp-polyfill-node-contains.min.js?ver=3.42.0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\wp-polyfill-node-contains.min[1].js	
Preview:	!function(){function t(t){if(!(0 in arguments))throw new TypeError("1 argument is required");do{if(this===t)return!0}while(t=t&&t.parentNode);return!1}if("HTMLElement"in this&&"contains"in HTMLElement.prototype)try{delete HTMLElement.prototype.contains}catch(t){}"Node"in this?Node.prototype.contains=t:document.contains=Element.prototype.contains=t}();

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\=Default[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 275 x 162, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	28050
Entropy (8bit):	7.972475683392406
Encrypted:	false
SSDEEP:	768:mMpzMlezVmerh2o2Lif9aoPNTAK7/NtBXoDxw5+kUA:9yLQZ9LNtBXoDxw5+kUA
MD5:	AC130C64CF413D496E4CC09AD408FBEF
SHA1:	C06570BF5888421F9D3C93D6E13D152199E71E24
SHA-256:	E1943B6A5FAD0AFA1E4CA2EC418C4DAF49853E8FAE760129A5F6F61391C48199
SHA-512:	CF7BFF164114F298F0701C2906003BB2D3A77D66B4BD35622896BBCBE140E4356678D56CDBFEA497E963721AE031C160CC822E5803698F4DABA219023DD7433(
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.yoshki.com/SRA/EnglishMono/275/0/=Default.png?a=121*012801280128@5501090=401$0=60=40=90124012@=90124012@=70=401$0=40125012@1230124@5501$012@05501260=6
Preview:	.PNG........IHDR.....bH).....sRGB.....gAMA.....a.....pHYs.....o.d..m'IDATx^...'.q..0...8..Pq%...l'.$....X..,>..bf:.N|....N..KwbfFK2..w>.....=..;S.....n.....b....k..[l%..o.....m.'t.s.....t....:..\....kMW....._.U...7|.#.:.x.....9.>.....z?....z2./\.}{...C~.....]xz....,i..%m....^zj..M.Gi-.<.G4...9....k..^.L:Z4.....~.W.O.Fn.w.uB#~.t.^].....z..W.g.9[^..n{V.n.C..'....}.9`....o.....[.9F...:X..yNx..... .....N.t.{p.[}MX..t.j.l...<.i3....i...O.....$...eErc....<..3.,,+.Ob..r.2...{T.....[v0g...z..O..d.q.....#.G.6./.e....r2.;.>.....na..+...,.*.k6^G.G?./...o..S..)%P1.>5.L.$q8.p6.Tv..vhf..]5.QF. ..$N.....0.....V.....$Nhf.[.J...p.06}..s..."..1R\....yc"...t"..w....4|.....LK.....~<.i.t9.d..{ ?b.d.....{~...k.k.~....L.8 c(.N...:~.:..)@._Jg..[h8.m..l..Ih..1..Mp..?..X.fH.....mxx..').)..w....r.....)Jh.D..F..<,..n...6.?.."....1]..i.NZ.....FfK.9)....w.;aQB.....ly.J...b3fD&..x

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\Default[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 275 x 162, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	26171
Entropy (8bit):	7.9568467029709
Encrypted:	false
SSDEEP:	768:CFlk9ApSaWy2Jvb3giHSjn8yEyamTxCAzHDXub40wYkL1LAk:CFl6FatIvb3THSj5amTHPWsbLAk
MD5:	479A4AE60F32707C50F4F598E51096D6
SHA1:	42AAA85DC4C05CFEDF87DCB1295BD71CB99E2C2B
SHA-256:	841D8BCF4774A44E7EAA3ACBCB6422282A16B7E876A628D0CFE1EBABBD84DAAC
SHA-512:	17AE35958DC3A7365E06B759F8248C7D6196DA4A2D2F2D34EACFF9067DC15B368420DD2700F1C0478656004E384074709654A8ED5CD5BE5FA5AB5FDAD7C4EC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.yoshki.com/SRA/EnglishMono/275/0/Default.png
Preview:	.PNG........IHDR.....bH).....sRGB.....gAMA.....a.....pHYs.....o.d..e.IDATx^...?E..;/.5w..y...Wp.8.9...D2H..D@rF. H..AA..P$.H..(.*9....S...w.....<03.....jWu.....'......_..#>.s./.....P.O.....\wG.7....<_Mn]...'.K|kz%.....t.x=/..{...5.W.;.h.+.|99./.[{..c.|.o.O.?.....=..k..n{.v.mO9Na.8.k{n1..tz.(..s=..)...."..i...w.q.-..s.#..-.q.k.g.yG..kn...8*"z...x....$.iy..l#.1..5.c...bZ....x...Q{..N....a..>..>.??....a.....>..0`....#.Z...5t...5..G-.....(3.....5.C.j:3.!..x...+..F..::..46.G.i..1.o/..oR.-z:.....l.....r...>....i`....f....".."..F_.{9.{uGM..%.....<y.V]%.umZG&....=...x.X7?K.....1..Ji..e@....<d..>j...3&Q..h.....YGNP)....O5/..,^.....d.4kw.<<r:k.Gt.||...''...C...R.m.....4'..^M..m....o_.f...-.....v.Db..)O.....=]W..2....l.X....WK..j.....Y.W.)Zx...&.#.C.6.....e{ .m.(.@...|..Ai....g.U.3..L..I.9#..)}Bs...N.}.^....8....B.t...r....(...N...2..+.k..U]..{)....My.....dJ.V....u'.....{&z>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\EJRQQgYoZZY2vCFuvAFT9gaQZynfpg[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 34100, version 1.1
Category:	downloaded
Size (bytes):	34100
Entropy (8bit):	7.986853384950331
Encrypted:	false
SSDEEP:	768:BySzGhgrBBXE/X69x3uy4zFoUn0VDYWmcGSn:QS4EBu/X69x3uycFJyn
MD5:	ABCD0499DDF538CFAB2DA3036DACE8B6
SHA1:	1260A46C69670620D521E380F8483DCF8453C991
SHA-256:	805044805F50602191A9CE6F555AED9041DF6823A8848B1FB5FE1895432CC5D1
SHA-512:	8A00FDA76715FB0257A3E6C41179AC891417BD20E9426B9E7135ACE0D84FE064749D0A68EFD2B6A07F7A7E1EEC4AF3D2242973905A9EF8D12CFD5243E785DF05
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/ptserif/v12/EJRQQgYoZZY2vCFuvAFT9gaQZynfpg.woff

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\EJRQQgYoZZY2vCFuvAFT9gaQZynfpg[1].woff	
Preview:	wOFF.....4.....l.....GPOS.....e...T.H*FGSUB.....H{..OS/2.....\...`m.2vcmap.....cvt .....4...4....fpgm.....H.ogasp.....glyf.....a.....hdmx..k. ...#..&.~...head..}$...6...6.;..hhea..}\...!...$....hmtx..}....B.....B Rloca.....%.P.maxp..... ... .name.....&-D.post.....yY.f.prep...P.....x.....I...$.....m.....m..{zl .....=os2....?.....V@.(.P.$.....=x7.....x.....<.....1...J.....y...Q.....^!.jFH..;...s8Gp$Gq.....y...\|.G\|.'\|..\..).R.$....o....*..!.h#.E.....Z.....SC..m.f~..-.....]....Z..6.vzv.....'US.Z. ..r..-..-e....ll{k'.P...'1.o.....|v'..}U.....'.7V.....l...T.}..z+U..O.6E....c9Y...q&.Q.=U.y...../)_V...q....3.h'. vk.~.D..:.c...P...wl..j+-kSl..Z....v.....@...y...d.@..-.o.Y.....T..Zs.I..F`C]3..^. ...*..&..5..E.....6W.T.....J...k.`.....T.....j..)..e.O.....n~..e}.Y.X.R.....$u/.9/j..|...I...u..6W.\M....Yc... .P..&..k.st.n..RN...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\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\B87Z87FM_Default[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 275 x 162, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	303
Entropy (8bit):	2.6808781527959216
Encrypted:	false
SSDEEP:	3:yionv//thPkUjllvolp3MLts7CX9/gm6KppsyxWkPFQAa///+/5up:6v/lhPkU0ZMR/C+MygkPFQAquhup
MD5:	5C0F57365CD4F64E9DFC056B5B6B00D2
SHA1:	159A395B182D8EB5EADF5BF49F0E43028F6BE92C
SHA-256:	F33A29217ED3D9B61368E4A69FA485109CC6324BCBDF9C64B533072ACC79DD35
SHA-512:	BEADBF631EB0816042DB07FFEA6B71C57787793BF270952AFAEBB09852D8E614D7AAD0B410F30212298BAFC61DFD3DB7D5567A3AE10D8038312622B4D27D2B 3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.yoshki.com/SRA/EnglishMono/275/0/_Default.png
Preview:	.PNG.....IHDR.....bH).....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..1.....Om.O ....NN.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\all.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	56425
Entropy (8bit):	4.710699752289595
Encrypted:	false
SSDEEP:	768:V6C31sPizPq4/vBUAUHJUkQdR/WMQyYJrX75CsmZQzF:V6TPUC4/pMHGBdcfd7ssjR
MD5:	F7409F91A34EA35236D98702F4E69F4C
SHA1:	3A3C16CBB1114F8E210B87CF3102A99968BF6A26
SHA-256:	04950E48CD4097FB4A540C3ABCF445CD92D59BDF9BA40F49CFB180CC94387A2F
SHA-512:	66A8F8FB2DE3E2116D2EF1895570A65300239E8B8F8BC9DDD50BB86874821741E9CB6EADB28A1441F91496CC394FFDF08117275C7F6713981B030F1B216C3DE2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.dickinsonsolicitors.co.uk/wp-content/plugins/js_composer/assets/lib/bower/font-awesome/css/all.min.css?ver=6.6.0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\all.min[1].css	
Preview:	/*!. * Font Awesome Free 5.11.2 by @fontawesome - https://fontawesome.com. * License - https://fontawesome.com/license/free (Icons: CC BY 4.0, Fonts: SIL OFL 1.1, Code: MIT License). */.fa,.fab,.fad,.fal,.far,.fas{-moz-osx-font-smoothing:grayscale;-webkit-font-smoothing:antialiased;display:inline-block;font-style:normal;font-variant:normal;text-rendering:auto;line-height:1}.fa-lg{font-size:1.33333em;line-height:.75em;vertical-align:-.0667em}.fa-xs{font-size:.75em}.fa-sm{font-size:.875em}.fa-1x{font-size:1em}.fa-2x{font-size:2em}.fa-3x{font-size:3em}.fa-4x{font-size:4em}.fa-5x{font-size:5em}.fa-6x{font-size:6em}.fa-7x{font-size:7em}.fa-8x{font-size:8em}.fa-9x{font-size:9em}.fa-10x{font-size:10em}.fa-fw{text-align:center;width:1.25em}.fa-ul{list-style-type:none;margin-left:2.5em;padding-left:0}.fa-ul>li{position:relative}.fa-li{left:-2em;position:absolute;text-align:center;width:2em;line-height:inherit}.fa-border{border:solid .08em #eee;border-radius:.1em;padding:.2em .25em .15em}.fa-pul

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\anchor[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	125901
Entropy (8bit):	5.895222642245439
Encrypted:	false
SSDEEP:	1536:J3892MoN9vEvpz1Z9BaMoN9vejNBVYUtMLMoN9vdYbo1VhP:J3Tv4znmvC5BZt+vhYb6P
MD5:	F55CFE78CF5DF8DBCF826A214486E54B
SHA1:	CB0AB58254E71DD7F25922861589F1AB6D0A7F30
SHA-256:	7FFAE55C29AE0D9C27472B868C1CA1F6555DF1A90568531453F59454435812CE
SHA-512:	724C850ABCDFF1F730DD65D67E0ED39EEEEEDAEAAD2F11FF59E85739274828C72D56F91C395EA3C205626E66354AE11ADB0292DAEAE66EDE6A2279CC4E541FC
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE HTML><html dir="ltr" lang="en"><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.<meta http-equiv="X-UA-Compatible" content="IE=edge">.<title>reCAPTCHA</title>.<style type="text/css">.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 400;. src: url(//fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4mxP.ttf) format('truetype');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 500;. src: url(//fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmEU9fBBc9.ttf) format('truetype');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 900;. src: url(//fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmYUtfBBc9.ttf) format('truetype');.}..</style>.<link rel="stylesheet" type="text/css" href="https://www.gstatic.com/recaptcha/releases/eWmgPeIYKJsH2R2FrgakElkq/styles__ltr.css">.<script nonce="3nXaMvsr3WHgRzqKcFq8hw" type="text/javascript">window['__recaptcha_api'] = 'https://www.google.com/rec

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\api[1].js	
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):	1768
Entropy (8bit):	5.612927321721572
Encrypted:	false
SSDEEP:	48:VKEcOKoeN1l2FLrwUngKEcOKoeN1l2FLrwUnG:f4Dl2tsuU4Dl2tsuG
MD5:	DB7E6557447F36E889AFD1F82FF750FE
SHA1:	3F8CA19EEF99A1858FD483FE37244A440DFB6D41
SHA-256:	6BFA8B05D0C8E17F9D065180456EE1B5CA79750A596CCFDF6DBA12D5AD889602
SHA-512:	7D1859337EFA95B938FF0A6A895E6EAFB0300E7EFDD019B0D4E23F30A12BC26886ACA8CDACCDFFA5D4C9EED8F08844C6D246BFD83553A536DD84FE9F53BA4EBD
Malicious:	false
Reputation:	low
Preview:	/* PLEASE DO NOT COPY AND PASTE THIS CODE. */(function(){var w=window,C='___grecaptcha_cfg',cfg=w[C]=w[C]||{},N='grecaptcha';var gr=w[N]=w[N]||{};gr.ready=gr.ready||function(f){(cfg['fns']=cfg['fns']||[]).push(f);};w['__recaptcha_api']='https://www.google.com/recaptcha/api2/';(cfg['render']=cfg['render']||[]).push('6LfmMJ0UAAAAADP280q3cebbJ7e0Xs9ffHLgUKeH');w['__google_recaptcha_client']=true;var d=document,po=d.createElement('script');po.type='text/javascript';po.async=true;po.src='https://www.gstatic.com/recaptcha/releases/eWmgPeIYKJsH2R2FrgakElkq/recaptcha__en.js';po.crossOrigin='anonymous';po.integrity='sha384-3l+Dzjt73YLhXz+WejlQA/r4+koQU0wEJ+YZAtKZ8DTxOPwZ54aluvUaML5sjiPl';var e=d.querySelector('script[nonce]'),n=e&&(e['nonce']||e.getAttribute('nonce'));if(n){po.setAttribute('nonce',n);}var s=d.getElementsByTagName('script')[0];s.parentNode.insertBefore(po, s);})();/* PLEASE DO NOT COPY AND PASTE THIS CODE. */(function(){var w=window,C='___grecaptcha_cfg',cfg=w[C]=w[C]||{},N='gre

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\base[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	1668746
Entropy (8bit):	5.580908133830736
Encrypted:	false
SSDEEP:	12288:MB4ljd5/9rlJjCpVoOVwKoHpkUl7WAkRUROCgvu4xDKxwd3Z:g4/x9RJGpHwKoHOUlCAkRUPg/Uxwd3Z
MD5:	3E96605E6B0B91730FC7EF848C22CD26
SHA1:	63D9518C9C11C4EF12AFE4472D4C36BA996F4783
SHA-256:	6B072B4759B5545EDE303930F6C13F22A76D726FC862FB2AC39896B4E61C108B
SHA-512:	5FB93AC0B610C518D9C1CDFDF174A44FED4D162792971322DE4513CE388B8EAD1C1EC6F3AD26CFA4FBA7AB45B55FCEF09718C2E3A6E117239344243AA0766D64
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\base[1].js	
IE Cache URL:	http://https://www.youtube.com/s/player/e467278e/player_ias.vflset/en_US/base.js
Preview:	var _yt_player={};(function(g){var window=this;/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.'use strict';var ba,da,xaa,ia,ka,la,pa,qa,ra,ta,ua,va,wa,xa,yaa,zaa,za,Aa,Faa,Ba,Ca,Da,Ea,Fa,Ja,Ka,Haa,Iaa,Ta,Ua,Va,Jaa,Kaa,Xa,Laa,Ya,$a,Maa,Naa,bb,ib,Oaa,pb,qb,Paa,vb,sb,Qaa,tb,Raa,Saa,Taa,Db,Fb,Gb,Hb,Kb,Mb,Nb,Qb,Wb,Yb,ac,bc,ec,gc,hc,Waa,ic,jc,mc,uc,vc,xc,Cc,Kc,Lc,Rc,Nc,$aa,cba,dba,eba,Vc,Wc,Yc,Xc,$c,cd,fba,gba,bd,hba,hd,id,jd,kd,ld,od,pd,qd,rd,kba,sd,td,xd,yd,zd,Ad,Bd,Cd,Dd,Ed,Gd,Id,Jd,Nd,Od,Pd,mba,Qd,Sd,nba,Ud,Vd,Wd,Xd,Yd,Zd,fe,he,ke,oe,pe,ue,ve,ye,we,Ae,De,Ce,Be,sba,me,Te,Re,Se,Ve,Ue,Ie,We,uba,.$e,bf,Ze,df,ef,ff,gf,hf,jf,kf,lf,mf,nf,vba,wf,of,yf,Bf,Cf,wba,Ef,If,Hf,Jf,Kf,Lf,Mf,Nf,Of,Pf,Qf,Rf,Tf,Sf,Uf,Vf,zba,Bba,Cba,Eba,Yf,Zf,$f,bg,cg,dg,fg,hg,ng,og,rg,Fba,ug,tg,vg,Gba,Dg,Gg,Hg,Hba,Ig,Jg,Kg,Lg,Mg,Ng,Og,Iba,Pg,Qg,Rg,Jba,Kba,Sg,Ug,Tg,Wg,Xg,$g,Yg,Mba,Zg,ah,bh,dh,ch,Oba,Nba,eh,Qba,Pba,Rba,hh,Sba,jh,kh,lh,ih,mh,Tba,nh,Uba,Vba,ph,Zba,qh,rh,sh,$ba,uh,wh,Bh,Eh,Gh

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\contact-us[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines
Category:	downloaded
Size (bytes):	34867
Entropy (8bit):	5.401450195563468
Encrypted:	false
SSDEEP:	768:P++k60wKYNr5n4VRbbowbERZV+T2MvZDcfnztKI:P+96UYNr2XHdiZ7MvZDcfnztKI
MD5:	3F9B4455A6DA8A542A34FF3237D37B2C
SHA1:	6146DB9117018F5C596973B03B0EFD7CB86F0F28
SHA-256:	37159873E36E27A63618185268A1CF199D18F633BF2884CECA149DD149978A39
SHA-512:	0AC31581BD7F598069B1B0121BF909B5A9A816529DBB28CC96113B9B377AA30B64D57E8CD448054B68E4F04646DF879BB0A1C11E26B480325CFCCAB61EA1D73
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.dickinsonsolicitors.co.uk/contact-us/
Preview:	.<!DOCTYPE html>. [if lt IE 7]> <html class="no-js lt-ie9 lt-ie8 lt-ie7"> <![endif]-->. [if IE 7]> <html class="no-js lt-ie9 lt-ie8"> <![endif]-->. [if IE 8]> <html class="no-js lt-ie9"> <![endif]-->. [if gt IE 8]> >.<html lang="en-GB"..prefix="og: https://ogp.me/ns#" class="no-js"> <![endif]-->.<head >. <meta charset="UTF-8">. <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">. <meta name="viewport" content="width=device-width, initial-scale=1">. <meta name="format-detection" content="telephone=no">. <link rel="apple-touch-icon" href="https://www.dickinsonsolicitors.co.uk/wp-content/themes/quicklaunch-parent-theme/library/images/apple-touch-icon.png">. <link rel="icon" href="https://www.dickinsonsolicitors.co.uk/wp-content/themes/quicklaunch-parent-theme/library/images/favicon.ico" type="image/x-icon" />..<script defer src="https://use.fontawesome.com/releases/v5.0.13/js/all.js" integrity="sha384-xymdQtn1n3lH2wcu

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\convayancing-quality[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 175 x 85, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	10524
Entropy (8bit):	7.955455688158903
Encrypted:	false
SSDEEP:	192:N7Fcp9czVYUoObynnzsE6l6pCSaaNGj1gFVLE2EpUsbO:N6puzV/HynnzsELm8bLEpha
MD5:	BA1AD126AC6CF03825E05B8A96E95CA3
SHA1:	3CE30141BB61A23D2C0504C44867922E6B3CCBCB
SHA-256:	766B53FC5BD5A68175398D7854876B44937ED7A7FC5C43CE18FF910235D5CAED
SHA-512:	AD93F816F5D87E37B542C4A6517CA49235F8AABE8F08F0846FF937DACE00ACC7DE94E50E07448A2E6DB82E12C89F03603FBAF82F1AE088DF234926C19079A4C3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.dickinsonsolicitors.co.uk/wp-content/uploads/2017/10/convayancing-quality.png
Preview:	.PNG.....IHDR.....U.....?.....tEXtSoftware.Adobe ImageReadyq.e<...&iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c142 79.160924, 2017/07/13-01:06:39 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmp:CreatorTool="Adobe Photoshop CC 2018 (Windows)" xmpMM:InstanceID="xmp.iid:682E203872EA11E8838AE5B7F114207B" xmpMM:DocumentID="xmp.did:682E203972EA11E8838AE5B7F114207B"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:682E203672EA11E8838AE5B7F114207B" stRef:documentID="xmp.did:682E203772EA11E8838AE5B7F114207B"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>B.#...%.IDATx..].xT..-.A..H...{..RBS,.Q.E.D.?....HIB.).....(..D.&.4.4..zI()@..R.....|.|..s.=...3gf...2

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\coronavirus-covid-19-notice-june-2020[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines
Category:	dropped
Size (bytes):	38987
Entropy (8bit):	5.385057127892103
Encrypted:	false
SSDEEP:	768:9atuUk60wKYNrW1LnrlyfbbowbuRZV+T2MvZDcfnztKI:9atu/6UYNrqnrlyfHdgZ7MvZDcfnztKI
MD5:	346FF7DE8EFA72A8722B1C14E6EEAF4D
SHA1:	076971E52409EA4A50E2B2FAF8296DE55EDACFEF
SHA-256:	E48EF8161E04969A71362DD21031AD362911C0BE1C4321D41881C6C6A33FD2C9
SHA-512:	783B2DE123F35BEA307450A1A132D0D9C2B6E590C5B8A4E4CD759EF051FE2AEA1D38E64B9FB32DF24687D00228D0019949088BEAA54F23272743DDF40B0696C

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\coronavirus-covid-19-notice-june-2020[1].htm	
Malicious:	false
Reputation:	low
Preview:	.<!DOCTYPE html>. [if lt IE 7]> <html class="no-js lt-ie8 lt-ie7"> <![endif]-->. [if IE 7]> <html class="no-js lt-ie9 lt-ie8"> <![endif]-->. [if IE 8]> <html class="no-js lt-ie9"> <![endif]-->. [if gt IE 8]> >.<html lang="en-GB"..prefix="og: https://ogp.me/ns#" class="no-js"> <![endif]-->.<head >. <meta charset="UTF-8">. <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">. <meta name="viewport" content="width=device-width, initial-scale=1">. <meta name="format-detection" content="telephone=no">. <link rel="apple-touch-icon" href="https://www.dickinsonsolicitors.co.uk/wp-content/themes/quicklaunch-parent-theme/library/images/apple-touch-icon.png">. <link rel="icon" href="https://www.dickinsonsolicitors.co.uk/wp-content/themes/quicklaunch-parent-theme/library/images/favicon.ico" type="image/x-icon" />..<script defer src="https://use.fontawesome.com/releases/v5.0.13/js/all.js" integrity="sha384-xymdQtn1n3lH2wcu

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\coronavirus-covid-19-notice-june-2020[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines
Category:	downloaded
Size (bytes):	38987
Entropy (8bit):	5.385057127892103
Encrypted:	false
SSDEEP:	768:9atuUk60wKYNrW1LnrlyfbbowbuRZV+T2MvZDcfnztKI:9atu/6UYNrqnrlyfHdgZ7MvZDcfnztKI
MD5:	346FF7DE8EFA72A8722B1C14E6EEAF4D
SHA1:	076971E52409EA4A50E2B2FAF8296DE55EDACFEF
SHA-256:	E48EF8161E04969A71362DD21031AD362911C0BE1C4321D41881C6C6A33FD2C9
SHA-512:	783B2DE123F35BEA307450A1A132D0D9C2B6E590C5B8A4E4CD759EF051FE2AEA1D38E64B9FB32DF24687D00228D0019949088BEAA54F23272743DDF40B0696C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.dickinsonsolicitors.co.uk/coronavirus-covid-19-notice-june-2020/
Preview:	.<!DOCTYPE html>. [if lt IE 7]> <html class="no-js lt-ie8 lt-ie7"> <![endif]-->. [if IE 7]> <html class="no-js lt-ie9 lt-ie8"> <![endif]-->. [if IE 8]> <html class="no-js lt-ie9"> <![endif]-->. [if gt IE 8]> >.<html lang="en-GB"..prefix="og: https://ogp.me/ns#" class="no-js"> <![endif]-->.<head >. <meta charset="UTF-8">. <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">. <meta name="viewport" content="width=device-width, initial-scale=1">. <meta name="format-detection" content="telephone=no">. <link rel="apple-touch-icon" href="https://www.dickinsonsolicitors.co.uk/wp-content/themes/quicklaunch-parent-theme/library/images/apple-touch-icon.png">. <link rel="icon" href="https://www.dickinsonsolicitors.co.uk/wp-content/themes/quicklaunch-parent-theme/library/images/favicon.ico" type="image/x-icon" />..<script defer src="https://use.fontawesome.com/releases/v5.0.13/js/all.js" integrity="sha384-xymdQtn1n3lH2wcu

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	198
Entropy (8bit):	5.153548140325187
Encrypted:	false
SSDEEP:	6:0IFFii+56ZRWHTizlpdvW8XEq3iKcz14WNin:jFhO6ZRoT6ppvEofY14WY
MD5:	057478F16847AB850D12B85AF5A27C4A
SHA1:	159BB9DE1356C699DC07C2CC175F7BD5916A2167
SHA-256:	E3C0DF8842E1CAE3E3ECD92373C966B334F701E7A9014C40FF89F1F729E950AC
SHA-512:	18749A2F00FAFB24F819DB8F194BCAEE42D240855C4E7BF8A0F84C6FC13119AB06C25DFF739C86BF51A3430EDEDBE6A1EDAE8F22AA4A6A19CE7586602FABAF22
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.googleapis.com/css?family=Abril+Fatface%3Aregular&subset=latin&ver=6.6.0
Preview:	@font-face {. font-family: 'Abril Fatface';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/abrilfatface/v12/zOL64pLDlL1D99S8g8PtiKchq-dmiw.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\dickinson-logo-white-1[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 900 x 96, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	27383
Entropy (8bit):	7.964305012412191
Encrypted:	false
SSDEEP:	768:rDhLHSunLJJ5C2UbhPxJu9govpKTBQffPRvN:3h1n1bUhPxA9ouRV
MD5:	DF2EAC595039FCF2D8C1D1595168131F
SHA1:	0EE1778677D57D0858EA0ED8AA5FCCE5093BD014
SHA-256:	0D6BA15A25187BAB8AEEB50F176DBFEA82CEB9B65D8406DB96D23653DEF5DCE7
SHA-512:	4B285B66CCBA51146B06A4CEF4336B352A7B8DC2F10DDB37152168B20C096FF38A3F6B89466775FE6FD85987B16094A70D4D81074A98B1CE69CBD10A1B0AC88
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.dickinsonsolicitors.co.uk/wp-content/uploads/2018/07/dickinson-logo-white-1.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\dickinson-logo-white-1[1].png	
Preview:	.PNG.....IHDR.....`.....Es.2....pHYs.....iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c142 79.160924, 2017/07/13-01:06:39 "> <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:stEvt="http://ns.adobe.com/xap/1.0/sType/ResourceEvent#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/" xmpMM:DocumentID="xmp.did:22366F727A1A11E8A2E5809E4DEE262F" xmpMM:InstanceID="xmp.iid:0d165277-2433-4d44-8d48-5472892539d4" xmpMM:OriginalDocumentID="xmp.did:22366F727A1A11E8A2E5809E4DEE262F" xmp:CreatorTool="Adobe Photoshop CC 2018 (Macintosh)" xmp:CreateDate="2018-07-26T13:43:50+01:00" xmp:ModifyDate="2018-07-26T13:45:22+01:00" xmp:MetadataDate

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\dickinsons-logo-WHITE-300x35[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 300 x 35, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	4962
Entropy (8bit):	7.9038407324027915
Encrypted:	false
SSDEEP:	96:Zqn6CH9OCNS3GDglsN5hkjreZUJLneZE3XY9zeLbxh:ZUOKSWECnGjNcf6
MD5:	1CA31EB13132DAEC2A0EDE10AA60FFBB
SHA1:	A8D3A10A3CF10CAC46197B0336DFBDD9F6A01FE1
SHA-256:	4B58E5ABEABD8546DF16F68C4210C9D3DF79FA490C67AB30BA47537C4B290719
SHA-512:	7A11C8C660E94E8BC9CA3FB856945F2A9F114A7E9B85496FB6C4CC5FE60B6859193964BD8BBA0D27C2D16A0EA7F081CB8F6DC18A388CF75448B7DC80CE7CD98
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.dickinsonsolicitors.co.uk/wp-content/uploads/2018/07/dickinsons-logo-WHITE-300x35.png
Preview:	.PNG.....IHDR....,...#.....\7.....gAMA.....a.....sRGB..... cHRM..z&.....u0...`..:....p..Q<....bKGD.....pHYs...H...H.F.k>...2IDATx..yxU..?/!....VDQ..GA.Z.....q\k..8n..;.V.u..j.eZu.j..v.:##nu.V..,.(V.Bd.%,..;....p<.s.&....'O.{.....7.H.....!....$5...[....3k...{...;._.9!....$.....B.S2.....6r.m...0.x.8..(..*is`.`.?. .s&0).0_...A..&.[.....Bx....>...$..W.....kb.V.7.SB.d..'.e?..P.,.....^M.....1n...+.'...z.[....[d.7.8.....]...BG....-.....B..ioW`'`{.o..".....'.C<.5....J.sy._.....*..BKi.u.....I.$MS...~/.{.N.4N.M.fJZ$.5I.J.$.C.....ks].H...C..c$.$i.....g[....W%=a`DR.....*..$5..K..K..x]..6..'U.~..t}.%.$.....%-s.....u"...E..I..d..$]+.]I.$...../..w%./.2`.(.;.fKzP.^.....3$..\.D?.K.....ym.y....\....d...3s%]/i.IC$.....ei.r..,i.zpV.K....Z...2..F.m.....Z$..!..!=...+idN.....P..Ic.6....v.4.m....$.....Q..~.>I.W8.}<>. .f.i..#.i.t....^...0.I.1_'Ij58...-i.....K.. .+.I..e..P..D..e.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\fetch-polyfill[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Pascal source, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	8543
Entropy (8bit):	5.238064281324506
Encrypted:	false
SSDEEP:	192:oQHdiEslZc0rsNYNU5mSJHqI03aej6tZoaMLQO/x5/P80+HcW:ocHslLsP5muHqI0Jj6tZcUO/x5+V
MD5:	04E3CC8A9641B3F9F9C9370F4E9B5BDD
SHA1:	9602A891F583094BB04FD407B253ABCAFFB8C8D0
SHA-256:	DE6C4FFA2BD9FD283610E28D0DB2EC48607AAB39D213A51AEF248673A0A7E980
SHA-512:	58942BCC0F39D620A475B65C1AEB4F18872F68F22C89DEC076906A0DB8BC2B7CCA9357710A7824A0FA7404FF73F41013AECA34609CAACD2187414F7BD0D490D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.youtube.com/s/player/e467278e/fetch-polyfill.vflset/fetch-polyfill.js
Preview:	/*.. Copyright (c) 2014-2016 GitHub, Inc... Permission is hereby granted, free of charge, to any person obtaining. a copy of this software and associated documentation files (the. "Software"), to deal in the Software without restriction, including. without limitation the rights to use, copy, modify, merge, publish,. distribute, sublicense, and/or sell copies of the Software, and to. permit persons to whom the Software is furnished to do so, subject to. the following conditions:.. The above copyright notice and this permission notice shall be. included in all copies or substantial portions of the Software... THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,. EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF. MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND. NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE. LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION. OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\fontawesome-webfont[1].eot	
IE Cache URL:	http://https://maxcdn.bootstrapcdn.com/font-awesome/4.5.0/fonts/fontawesome-webfont.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.l;.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\B87Z87FM\imagesloaded.pkgd.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	7168
Entropy (8bit):	5.039172189542361
Encrypted:	false
SSDEEP:	192:5wlC7Gd4QY6Pm+OrOJ42uVOpDsu1mx3AJzE8f:5eC7Gd4QPm+Or0WOpou1mxQlEy
MD5:	0AF4891DB7B7FA46FBFCD40FFF9764EE
SHA1:	6E7F052ABFB3B19DB01917FFDFABFD48DC8A2A51
SHA-256:	D925A27DC99BBD3BC04AE6B5587E224A096E87DBD432DF552DEBE2A62971E5AA
SHA-512:	AE4138D2BCCB052212E25F24BC69DEA94C6CF2DDDFA25C2730B84EE497DA533A5C3BEA5119371FC5D2111BE4B4263C98B4534EE72C07772E790418745F127A 8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.dickinsonsolicitors.co.uk/wp-content/plugins/js_composer/assets/lib/bower/imagesloaded/imagesloaded.pkgd.min.js?ver=6.6.0
Preview:	/*!. * WPBakery Page Builder v6.0.0 (https://wpbakery.com). * Copyright 2011-2021 Michael M, WPBakery. * License: Commercial. More details: http://go.wpbakery.c om/licensing. */.// jscs:disable.// jshint ignore: start../*!. * imagesLoaded PACKAGED v3.1.8. * JavaScript is all like "You images are done yet or what?". * MIT License. */..(function(){function e(){}function t(e,t){for(var n=e.length;n--;)if(e[n].listener===t)return n;return-1}function n(e){return function(){return this[e].apply(this,arguments)}}var i=e.prototype,r=this,o=r.EventEmitter;i.getListeners=function(e){var t,n,i=this._getEvents();if("object"==typeof e){t={};for(n in i)i.hasOwnProperty(n)&&e.test(n)&&(t[n]=i[n]) }else t=i[e]||(i[e]=[]);return t},i.flattenListeners=function(e){var t,n=[];for(t=0;e.length>t;t+=1)n.push(e[t].listener);return n},i.getListenersAsObject=function(e){var t,n=this.getListeners(e);return n instanceof Array&&(t={},t[e]=n),t||n},i.addListener=function(e,n){var i,r=this.getListenersAsObject(e),o=

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\jquery.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	89496
Entropy (8bit):	5.289738088208255
Encrypted:	false
SSDEEP:	1536:AjExXUqrnxDjoXEZxkMV4SYSt0zvDD6ip3h8cApwEjOPrBeU6QLiTFbc0QlQvakU:AYh8eip3huuf6lidlrvakdtQ47GKE
MD5:	B6F7093369A0E8B83703914CE731B13C
SHA1:	D1889F5C173C2A4B20288F1F84758599AFD346EF
SHA-256:	60240D5A27EDE94FD35FEA44BD110B88C7D8CFC08127F032D13B0C622B8BE827
SHA-512:	D6AA7835D7B256B94DDD2F9D8DB84484F0413EBC502762C1BA21CBA7A392C6F550DB2418CDC8BD6D1DA6ED2CEA55BF22473C778493D416B1A1C38E6FFDB8(79D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.dickinsonsolicitors.co.uk/wp-includes/js/jquery/jquery.min.js?ver=3.5.1
Preview:	/*! jQuery v3.5.1	(c) JS Foundation and other contributors	jquery.org/license */.!function(e,t){"use strict";"object"==typeof module&&"object"==typeof module.exports?module.exports=e.document?t(e,!0):function(e){if(!e.document)throw new Error("jQuery requires a window with a document");return t(e)}:t(e)}("undefined"!=typeof window?window:this,function(C,e){"use strict";var t=[],r=Object.getPrototypeOf,s=t.slice,g=t.flat?function(e){return t.flat.call(e)}:function(e){return t.concat.apply([],e)},u=t.push,i=t.indexOf,n={},o=n.toString,v=n.hasOwnProperty,a=v.toString,l=a.call(Object),y={},m=function(e){return"function"==typeof e&&"number"!=typeof e.nodeType},x=function(e){return null!=e&&e===e.window},E=C.document,c={type:!0,src:!0,nonce:!0,noModule:!0};function b(e,t,n){var r,i,o=(n=n||E).createElement("script");if(o.text=e,t)for(r in c)(i=t[r]||t.getAttribute&&t.getAttribute(r))&&o.setAttribute(r,i);n.head.appendChild(o).parentNode.removeChild(o)}function w(e){return null==e?e+"":"o

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\js_composer_front.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	20637
Entropy (8bit):	5.264554129614354
Encrypted:	false
SSDEEP:	384:sekk5QRKhEJhCoJptuxOqU5SE3RG0F+D/W5OhS4uLSav4Rd57q:sekk5xhEJhCoJptuQSEhG0F+DO514uuA
MD5:	B00A0FD5E283160549DE2C7B36243B7B
SHA1:	F2401243950CD9624002921265E46A518851F12B
SHA-256:	314CE6BAAA3218EB171FA2C278D7FDF1B9872305DFA667E9CBF2DF77C83A9A88
SHA-512:	E5E5A424AE0B221F578433025184DEAB93115575391A7FEB1528F45E621976B3049F6BC5E1FD484B469A60C2D4706F7156B61C614C28DA5BD41E110F1E49D2A6
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\js_composer_front.min[1].js	
IE Cache URL:	http://https://www.dickinsonsolicitors.co.uk/wp-content/plugins/js_composer/assets/js/dist/js_composer_front.min.js?ver=6.6.0
Preview:	/*!. * WPBakery Page Builder v6.0.0 (https://wpbakery.com). * Copyright 2011-2021 Michael M, WPBakery. * License: Commercial. More details: http://go.wpbakery.com/licensing. */.// jscs:disable.// jshint ignore: start..document.documentElement.className+=" js_active ",document.documentElement.className+="ontouchstart"in document.documentElement?" vc_mobile ":" vc_desktop ",function(){for(var prefix=["-webkit-","-moz-","-ms-","-o-",""],i=0;i<prefix.length;i++)prefix[i]+"transform"in document.documentElement.style&&(document.documentElement.className+=" vc_transform ")}(),function($){"function"!=typeof window.vc_js&&(window.vc_js=function(){"use strict";vc_toggleBehaviour(),vc_tabsBehaviour(),vc_accordionBehaviour(),vc_teaserGrid(),vc_carouselBehaviour(),vc_slidersBehaviour(),vc_prettyPhoto(),vc_pinterest(),vc_progress_bar(),vc_plugin_flexslider(),vc_gridBehaviour(),vc_rowBehaviour(),vc_prepareHoverBox(),vc_googleMapsPointer(),vc_ttaActivation(),jQuery(document).trigger("vc_js"),window.s

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\main[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	42
Entropy (8bit):	4.350068910616443
Encrypted:	false
SSDEEP:	3:RAM7SpRoc2LGRFEaSn:z+iLzn
MD5:	BB41ABF56C7CAD709F1A391A65578F8C
SHA1:	55AE96391DB5F6C45A50F4D25CC84DEB63AF028E
SHA-256:	60BFA43AF3E6A61AC546EEB920EAA8C10570473F4096AFB15671815B1C394946
SHA-512:	57CF1EDC15877353B48ADE757E7B3656A6D1136CA937BAF4FC5E720FF339BA55D7483DC06C3C6113FF9C3F1D53F34BDB1D2546DA2069B7DC40577F92AEBE19F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.dickinsonsolicitors.co.uk/wp-content/themes/quicklaunch-parent-theme/library/js/main.js?ver=5.7.2
Preview:	jQuery(document).ready(function() { });.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\mem5YaGs126MiZpBA-UNirkOUuhv[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 18784, version 1.1
Category:	downloaded
Size (bytes):	18784
Entropy (8bit):	7.964699694030365
Encrypted:	false
SSDEEP:	384:4YQHZJ+ZXshfYjP0lJ9WnX/zJuKvvaIYjSS4yKrtVIGPvRGq6:BchgjGJ9WnX/zJ1JcG3gf
MD5:	CA0CC58FE4C481D2486F836E8B7ACD98
SHA1:	B9988071248F824BA2D5FA88CB16DA1971AA0945
SHA-256:	B332B402229655660F0DDC7D916618F44ACA71D0ECAA68A1DF7B5AD5A5F1D6F9
SHA-512:	95E3C7674FFF4E934F252605CD3DCDF169986EE754964C703F1BFEAD52AB33F8DFE3764A8FD507E39E4C058985CCC90F6B0F69A766AAA1C8508DB806095904A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v20/mem5YaGs126MiZpBA-UNirkOUuhv.woff
Preview:	wOFF.....l`.....nl.....GDEF.....GPOS.....GSUB.....y....;..OS/2...$...^...`.-..cmap.....Y..cvt ...8...[.....4fpgm.....~a..gasp...0.....glyf...<..9...WXZ..uhead..AL...6...6...Mhhea..A.....$...$hmtx..A....#.....T.loca..C.....6.Kkmaxp..E.... ... .u..name..E.....#.@Ppost..F.....5.".prep..H`.....x..n.....x.M...P.@..L..$$. .g..;..k.z...P.$K.....[.E..Z....B )..a.:...i...!.....J ...U....l/..m.&*3.KO...#..-..%;7.V.....x.c`fy.....:....Q.B3_dHc.....@`...../..?....^..... 9..m@J.....x.\.!..q.....#acf...#1Q@.'U..@..".llt.Aa#.f|c.W....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN....:....F....GG.g.s,x.>0....v..l;o..<.$G9.\f2...e{}.IS2..uc]p.....M.x.c.a.g.c..$KY...e@.,A.".m....x.....3.....?.[.o...2...:...a..b.)@.Y.....v1.b4d...36 ..x.uTGw.F.....)..)7.W.$`*.....G.Kz.)e....t.|.1.7...s.g...3.7mgf..~{1...s.3.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\mem8YaGs126MiZpBA-UFVZ0d[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 18160, version 1.1
Category:	downloaded
Size (bytes):	18160
Entropy (8bit):	7.961831708897042
Encrypted:	false
SSDEEP:	384:K9BQHZEFEbXlSNPoWvbYZbX9rnztP94u6pZ4nmrOmbSi+x:KLSb1GIbN76j4oO8j+x
MD5:	20890DE1FB4E49EA0B36F058BCA1B7E7
SHA1:	023D6720D92A54A3BB0AB219818D2E6E6AAD24A7
SHA-256:	C71180612EA84F5F9882D35DF024707E5B5E1BB18EFB2C8123FA5BDD30D3E079
SHA-512:	E6B921D20C0B7BFEA5A79D18D1C23DA7C79BB4E4D76A29AF48D7705C9C1F43E9E6578F1F36E00624DACD97411B68A214E750D0EDEB7BF12E889F16B6C522E1B0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v20/mem8YaGs126MiZpBA-UFVZ0d.woff

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\mem8YaGs126MiZpBA-UFVZ0d[1].woff	
Preview:	wOFF.....F.....j8.....GDEF.....GPOS.....GSUB.....y.....;..OS/2...$...^...`~]..cmap.....Y..cvt ...8...Y.....M..fpgm.....~a..gasp...0.....#glyf.. .@..6...S.Ug:}head..>....6...6..cphhea..?$.....$....hmtx..?D.....[Xloca..Ad.....I.maxp..C,... ... .name..CL.....&:A.post..D<.....5.".prep..F.....C..... .....x.M...P.@..L..$$. .g..;..k.z...P.$K.....[.E..Z....B)..a.:..i...l.....J ...U....l/..m.&*3.KO...#..-..%;7.V.....x.c`f..8.....u..1...<.f.....A.....5....1...A.._6..".-..L.....Ar ,.....3..(....x.\.!..q.....#acf...#1Q@.'U..@..".llt.Aa#.f|c.W.....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN....:.....F....GG.g.s,x.>0....v..l;o..<.$G9.\f2...e{}.IS2..uc]p.....M.x.c .a.g.c..$KY...e@.,.."".....?....%.g....Z.....("o..Y..Bu342.e.....0.....M=.....x.uTGw.F.....)..)7.W.$`*.....G.Kz.)e....t.|.1.7...s.g...3.7mgf..~{1...s.3.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\owl.carousel.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	41985
Entropy (8bit):	5.032833619909774
Encrypted:	false
SSDEEP:	768:AyWO0MF5ToHpuNCzHRbPZYLDOSlkIIe5EVEEJiZIH:ArO0MFGJyUW6Jt
MD5:	FC20CCAAD0CF5CE51D7B7A1B66589CD3
SHA1:	9E398996CFF9A8FA2877766B3D11734CD774A68D
SHA-256:	689C9AC02B0A03FD9A206833DF33EC989DD5ED79EAB24A1802FB281BB9ACCC26
SHA-512:	EBB77A321AF31F55CDE6AC5672ACFA45C4CB7A95D3093B0A73535ABFCDB16D2F2E0C0EFF32A1D6492DBE023A607E0ACE763E06E271541B0CA60E1D3C25D53 4FD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.dickinsonsolicitors.co.uk/wp-content/plugins/js_composer/assets/lib/owl-carousel2-dist/owl.carousel.min.js?ver=6.6.0
Preview:	/*!. * WPBakery Page Builder v6.0.0 (https://wpbakery.com). * Copyright 2011-2019 Michael M, WPBakery. * License: Commercial. More details: http://go.wpbakery.c om/licensing. */.// jscs:disable.// jshint ignore: start../*!. * WPBakery Page Builder v6.0.0 (https://wpbakery.com). * Copyright 2011-2019 Michael M, WPBakery. * License: Commercial. More details: http://go.wpbakery.com/licensing. */.// jscs:disable.// jshint ignore: start../*!. * WPBakery Page Builder v6.0.0 (https://wpbakery.com). * Copyright 2011-2019 Michael M, WPBakery. * License: Commercial. More details: http://go.wpbakery.com/licensing. */.// jscs:disable.// jshint ignore: start..!function(t,e,i,s) {function n(e,i){this.settings=null,this.options=t.extend({},n.Defaults,i),this.$element=t(e),this._handlers={},this._plugins={},this._supress={},this._current=null,this._spee d=null,this._coordinates=[],this._breakpoint=null,this._width=null,this._items=[],this._clones=[],this._mergers=[],this._widths=[],this._invalidated={

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\styles__ltr[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):	52732
Entropy (8bit):	5.959269303940443
Encrypted:	false
SSDEEP:	768:+LUmmAWTe2uXYp8Mi+yKSrKebyBwd/Dl+x2dtYyPoiDH1fkQJVEwY:4UcW6v+2rKwFDlXP7dnY
MD5:	182B64B9E3032D6BA48A0A6C854032B0
SHA1:	879537EC1D2CE611AE82B784A25A3E2CDC1EC6FC
SHA-256:	94B328F86382CDA7D83CEBB40EE8DD8F567582A60BA91A90A37F490B0F0EDEFA
SHA-512:	2CEDB007DB16B0F25287F85D8E945172CE01C26E514FB6A2F8F2278A716B89ED327EDA9897A704E08F1715B94177B69178BC499DF56683C9CE2BFB8DE364A53
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/recaptcha/releases/eWmgPeIYKJsH2R2FrgakEIkq/styles__ltr.css
Preview:	.goog-inline-block{position:relative;display:-moz-inline-box;display:inline-block}* html .goog-inline-block{display:inline}*:first-child+html .goog-inline-block{display:inline}.rec aptcha-checkbox{border:none;font-size:1px;height:28px;margin:4px;width:28px;overflow:visible;outline:0;vertical-align:text-bottom}.recaptcha-checkbox-border{-webkit- border-radius:2px;-moz-border-radius:2px;border-radius:2px;background-color:#fff;border:2px solid #c1c1c1;font-size:1px;height:24px;position:absolute;width:24px;z-in dex:1}.recaptcha-checkbox-borderAnimation{background-image:url(A/wD/AP+gvaeTAAAACXBIWXMAAABIAAAASABGyWs+AAAACXZwQWcAAABUAAADSAC4K4y8AAA4oElEQVR42u2dCZRV1ZX3qQ/dQIBt0JLEIAIQKCCRU 7pBNFiRMajZrIl9aOLZ8sY4CWdkDbT2McooaAEmNixFhpaYE2dCiLScWiQHCgoGGQoGQuhGArKKl7+V+n3fO7JWuVhEWvXv9vV4w733nJ+VhEXUv9V/rrnvP2XuEIlEXCZ3X1ZX3q5iE4IQIKtEWCK 7vP+c5/n33fO/V4w733nVuheXuv9V/rrnvP2Xud3zvTPee+ewsKxMTEx MTExMTExMTExM

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\unXEs0crvtA[1].htm	
Preview:	<!DOCTYPE html><html lang="en" dir="ltr" data-cast-api-enabled="true"><head><meta name="viewport" content="width=device-width, initial-scale=1"><style name="www-roboto" nonce="m6SkTxf0/7qTdoCcPuG5JQ">@font-face{font-family:'Roboto';font-style:normal;font-weight:400;src:url(//fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4mxM.woff)format('woff');}</style><script name="www-roboto" nonce="yJ9pE1WPY3KOHIIQEvJ7Hg">if (document.fonts && document.fonts.load) {document.fonts.load("400 10pt Roboto", "E"); document.fonts.load("500 10pt Roboto", "E");}</script><link rel="stylesheet" href="/s/player/e467278e/www-player.css" name="www-player" nonce="m6SkTxf0/7qTdoCcPuG5JQ"><style nonce="m6SkTxf0/7qTdoCcPuG5JQ">html {overflow: hidden;}body {font: 12px Roboto, Arial, sans-serif; background-color: #000; color: #fff; height: 100%; width: 100%; overflow: hidden; position: absolute; margin: 0; padding: 0;}#player {width: 100%; height: 100%;}h1 {text-align: center; color: #fff;}h3 {margin-top: 6px; margi

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\wp-embed.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	1426
Entropy (8bit):	5.158381671009404
Encrypted:	false
SSDEEP:	24:Q77OUdqIoZ2zsben5WlLysyIOKI1mQqRhoj3v2rFEgRuLUMB9/RUCXXmC3+:Q7SUyEsyKystOKumTsOrFEmu7Bl6CX2P
MD5:	905225D5711B559D3092387D5FFBEDBD
SHA1:	6F6C39075263BAFB9E8C10F1B34A1A0F7EE03C9D
SHA-256:	5BE614BCE53F767993A5F5F14A6BADD6AAE6BF3AF7CBDBF4D31520DE49E27991
SHA-512:	5AD34CF11ACF45AE256B2641496BE13939CD5E0212810C43AB20CADBB313A1D99CB3A451148E160D80F1F952A8514480C2953BC6CA0C4697A466A01E1C3D5F8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.dickinsonsolicitors.co.uk/wp-includes/js/wp-embed.min.js?ver=5.7.2
Preview:	/*! This file is auto-generated */.!function(c,d){"use strict";var e=!1,n=!1;if(d.querySelector)if(c.addEventListener)e=!0;if(c.wp=c.wp||{},!c.wp.receiveEmbedMessage)if(c.wp.receiveEmbedMessage=function(e){var t=e.data;if(t)if(t.secret||t.message||t.value)if(!/[^a-zA-Z0-9]/.test(t.secret)){for(var r,a,i,s=d.querySelectorAll('iframe[data-secret="'+t.secret+'"]'),n=d.querySelectorAll('blockquote[data-secret="'+t.secret+'"]'),o=0;o<n.length;o++)n[o].style.display="none";for(o=0;o<s.length;o++)if(r=s[o],e.source===r.contentWindow){if(r.removeAttribute("style"),"height"===t.message){if(1e3<(i=parseInt(t.value,10)))i=1e3;else if(~~i<200)i=200;r.height=i}if("link"===t.message)if(a=d.createElement("a"),i=d.createElement("a"),a.href=r.getAttribute("src"),i.href=t.value,i.host===a.host)if(d.activeElement===r)c.top.location.href=t.value}},e)c.addEventListener("message",c.wp.receiveEmbedMessage,!1),d.addEventListener("DOMContentLoaded",t,!1),c.addEventListener("load",t,!1);function t(){if(!n){n=!

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\www-embed-player[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	196313
Entropy (8bit):	5.596469760701508
Encrypted:	false
SSDEEP:	3072:+aLk3ytPTfr6xngfEHjpQ6MQNo0ru7E5WdyDNlCHmshH:P6xngfEH+Ko0ruoDDNlG
MD5:	0C36B8352D23B2EDDD7EC0F0A717EB4E
SHA1:	E7CEB0F79E9C21C08A0E02F4EEFDAEBB044BF270
SHA-256:	7AF5B0F3908EF5196C81BDBA087950891681F2158CEAD3F3DE9F072F580E7556
SHA-512:	E603BDBB3B4B8E5E7D9CC47A614F563D6A55299EFBA0501511BD90773A86F93C494AE6A1F55464AAA02349032D9574C3090EC96BD44428D6B94D4AC6F47A1B4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.youtube.com/s/player/e467278e/www-embed-player.vflset/www-embed-player.js
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.'use strict';var m;function aa(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}}.var ba="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a;a[b]=c.value;return a};.function ca(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("Cannot find global object");}.var da=ca(this);function r(a,b){if(b)a:{var c=da;a=a.split(".");for(var d=0;d<a.length-1;d++){var e=a[d];if(!(e in c))break a;c=c[e]}a=a[a.length-1];d=c[a];b=b(d);b!=d&&null!=b&&ba(c,a,{configurable:!0,writable:!0,value:b})}}.r("Symbol",function(a){function b(f){if(this instanceof b)throw new TypeError("Symbol is not a constructor");return new c(d+(f||"")+"_"+e+

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\www-player[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):	365036
Entropy (8bit):	5.24370695052713
Encrypted:	false
SSDEEP:	1536:BDQI0irpHrpj/fn8Mq5S0jDrzltP3Su3EMFfy9OP5FRrDJciM/ByDE4r6D6S7eTd:F4Drzz1xgAyxjFLk
MD5:	42AB47C4FFEA885004B805A6B6C9AABD
SHA1:	55A151606648A1A6080671EAE2432B50EAAB7EA0
SHA-256:	3CB6ABDABFB34937B1B320E5EEBFD33CA837CC0A8B83AAD9F0782158486C950B
SHA-512:	94E5C7E8B807C440B1D151EA0346A55DBD5F02227FE6346FEBC122D6189B7299EC339B898884DCDE6BF2712FB0352A4DE11DE80AD2FBABE542ADF4026F09246 3
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\www-player[1].css	
IE Cache URL:	http://https://www.youtube.com/s/player/e467278e/www-player.css
Preview:	.html5-video-player{position:relative;width:100%;height:100%;overflow:hidden;z-index:0;outline:0;font-family:"YouTube Noto",Roboto,Arial,Helvetica,sans-serif;color:#eee;text-align:left;direction:ltr;font-size:11px;line-height:1.3;-webkit-font-smoothing:antialiased;-webkit-tap-highlight-color:rgba(0,0,0,0);touch-action:manipulation;-ms-high-contrast-adjust:none}.html5-video-player:not(.ytp-transparent),.html5-video-player.unstarted-mode,.html5-video-player.ad-showing,.html5-video-player.ended-mode,.html5-video-player.ytp-fullscreen{background-color:#000}.ytp-big-mode{font-size:17px}.ytp-autohide{cursor:none}.html5-video-player a{color:inherit;text-decoration:none;-moz-transition:color .1s cubic-bezier(0.0,0.0,0.2,1);-webkit-transition:color .1s cubic-bezier(0.0,0.0,0.2,1);transition:color .1s cubic-bezier(0.0,0.0,0.2,1);outline:0}.html5-video-player a:hover{color:#fff;-moz-transition:color .1s cubic-bezier(0.4,0.0,1,1);-webkit-transition:color .1s cubic-bezier(0.4,0.0,1,1);transition:co

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\yoshki-library[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	43842
Entropy (8bit):	5.324037024651209
Encrypted:	false
SSDEEP:	384:zIw/x6Fp0AZqUdl750Y5RyoylyWpy/yQyLyn0pVsQOSJxctd0EVSl9TzHLo8WSH/:Ecx6TzqvXEnKf3Kt1sLvWSHlh9aAl
MD5:	8F36FFD477D7466707F08E43FD6442EE
SHA1:	3349B3D8EE57AF80226B1B883316D39432C029A4
SHA-256:	17DD40E3DFEBCA4CC55DA1407621EA12260DE36EE89FB38D59DFF99D87DBEE24
SHA-512:	BD34DA09DF14FFB8B54E8B36871F42F534F54056B27970DEA94522764468844A845D9B4E005A32EED9BB23AF8B31865A052AE1B723A90E9E219B6AFDC7C7844E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.yoshki.com/yoshki-library.js
Preview:	/***** COPYRIGHT YOSHKI LTD 2019 v4.07 *****/..function getBrandingCode(e){var t=getBrand(e),o=getProject(e),r=getImageFileName(e),n="";for(i=0;i<t.length;i++){var a,s=t.charCodeAt(i);a=10>s?"00"+s:100>s?"0"+s:s,n+=a}for(n+="+",i=0;i<o.length;i++){var a,s=o.charCodeAt(i);a=10>s?"00"+s:100>s?"0"+s:s,n+=a}for(n+="+",i=0;i<r.length;i++){var a,s=r.charCodeAt(i);a=10>s?"00"+s:100>s?"0"+s:s,n+=a}if(1==iframe){var g=window.location!=window.parent.location?document.referrer:document.location;try{console.log("window.location: "+window.location)}catch(u){console.log("no window.location")}try{console.log("window.parent.location: "+window.parent.location)}catch(u){console.log("no window.parent.location")}try{console.log("document.referrer: "+document.referrer)}catch(u){console.log("no document.referrer")}try{console.log("document.location: "+document.location)}catch(u){console.log("no document.location")}for(null!=g&&0!=g.length||(g=""),console.log("burl: "+g),n+="+",i=0;i<g.length;i++){var a,s=g.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\zOL64pLDlL1D99S8g8PtiKchq-dmiw[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 16896, version 1.1
Category:	downloaded
Size (bytes):	16896
Entropy (8bit):	7.972167444840726
Encrypted:	false
SSDEEP:	384:rfQPKX/yW8wPdhphjk3p4QOqeK1CeI/+Csg2yRUKFFI6siz:2KXigdrhQb1zC9/7sg2vKvIa
MD5:	9D61EE7EB9108E20D74775FA6A75554B
SHA1:	526CFF8E5E1706E24C43C6D1B51C4504D3E6F5A9
SHA-256:	95CFE9730055566FA1D27D04004D8148CB088222AC4F5969AA2251995166B072
SHA-512:	549DF880F30DA3468102CCEA32BEA94058F1E38110840473CF8DFC6C3913A75AA4AF9E2AF7ADA3F856B3C154F547F7F87CC92C7509BE43074BC7471F113D0EA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/abrilfatface/v12/zOL64pLDlL1D99S8g8PtiKchq-dmiw.woff
Preview:	wOFF.....B.....~.....GDEF...X...-...4.@..GPOS.....R...(...GSUB.....&...b..z9OS/2.....Q...`5t(.cmap...X.....gasp.....glyf.....,...P~e90dhead..:....2...6..U.hhea..;(.....$....hmtx..;H.....o..loca..=h.....maxp..?0... ... .5..name..?P.....Z4.L.post..@P.....U.9..prep..A.....h...x...E..@.....I.k.n....*..c.M....]^.....A.R...x.L....@.....m.m..qm....j.v.g.j..o.....4E*[...)..R.....z...X...Km....~x..8W.....5F.4&.&..'.'..bsn.r...?.-..s..RZ.J}-.5.....".e.v..<.h..on.5.X..)_...[....w.C.....czV.._c}..A..Dd..5c..D.s...&.8b....M.RY.T.1..Kw..;.z~.v..7..1)....{W..wE(O.....Q....EI.....KA...v..2t..5.NOj..v>.av6...`...''...3..I..q.....9.e.s..,.)oX.;>.. ..J..N.....4.5....8.0.b33333.....03....6J%fVrb....g.7`Z...f..WS..p'.._.uOOO..V.....P.I....].7RK...{7..q.....+..:8....oO./)...=bKVv.w0.j}7../.Tk.1...y$X..=.{Y..f|C.2..b...deK6S.....s.Yx.F...QE.O#.i..WtWg..c../i..Z.U+.g...J.v.9.=C.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\1px[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	3.0314906788435274
Encrypted:	false
SSDEEP:	3:CUkwltxlHh/:P/
MD5:	325472601571F31E1BF00674C368D335
SHA1:	2DAEAA8B5F19F0BC209D976C02BD6ACB51B00B0A
SHA-256:	B1442E85B03BDCAF66DC58C7ABB98745DD2687D86350BE9A298A1D9382AC849B
SHA-512:	717EA0FF7F3F624C268ECCB244E24EC1305AB21557ABB3D6F1A7E183FF68A2D28F13D1D2AF926C9EF6D1FB16DD8CBE34CD98CACF79091DDDC7874DCEE21E FDC
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\1px[1].gif	
IE Cache URL:	http://https://cdn.yoshki.com/images/1px.gif
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\55849r[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	501
Entropy (8bit):	5.16330325873308
Encrypted:	false
SSDEEP:	12:FgNXVNXWuEJPEWt9z8NWQhRNVMcqJmW7XolVMZXFk+Vg2qO:FY7FcNj8dLNVMDHyVMZ3Vgq
MD5:	2DE4B26FE1D1A20FE39C957B1AC68343
SHA1:	E234661F6C49CC7FBEA764AC906A6977CA7D20E0
SHA-256:	1A2FA2B37B9B349EE331BB55577AA4B48C4B5DB69C5BA2917764B769C9328D11
SHA-512:	1293F010E404A0D0974EBFA2BC43CB883B4F1C743F44AEF9FE651BDB376581AE41078F8BFBE6F0C0009FDC75E82EDEB69019F67FA5E8FF9C588FEA2330EC0E7 6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.yoshki.com/iframe/55849r.html
Preview:	<link rel='stylesheet' href='https://cdn.yoshki.com/responsive.css' />.. [if lt IE 9]>..<link rel='stylesheet' href='https://cdn.yoshki.com/responsive-ie.css' />..<![endif]-->.... <body style="margin:0px;padding:0px;">..<script src="https://ajax.googleapis.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>..<script type="text/javascript" src="http s://cdn.yoshki.com/yoshki-library.js"></script>....</body>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\EJRTQgYoZZY2vCFuvAFT_r21dA[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 41388, version 1.1
Category:	downloaded
Size (bytes):	41388
Entropy (8bit):	7.987665790343517
Encrypted:	false
SSDEEP:	768:YLq7B+3O7otNbigIOpcsTuktd0nCONwhSYpCiM8kgdVRnH5j3khz68GKGcauW0ln:YW7BHojWHcTu60nI0SCHgdbHV3kDGVFc
MD5:	E080E39A107716904EAA71669F6894D9
SHA1:	CB5DCE015E746C7032EEB3FAE002D07B83A5316F
SHA-256:	3D443A293450708EE465E62DA32B3B19618D55EF4A551C8C1C1C9D88E8CB57C0
SHA-512:	F7DEFEDEA019DFEA85978CCD60B04777E219529B77BCDCD8264C22AE89AC4AF7DD3DA83DCBBDCCC750D16EDBD043475D68F0FBE597735D2A404C07FB958E 62C5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/ptserif/v12/EJRTQgYoZZY2vCFuvAFT_r21dA.woff
Preview:	wOFF.....GPOS.....I...X....GSUB.....H{..OS/2.....]...`ln1/cmap.....cvt ...x...J...J...vfpgm.....H.ogasp.....glyf.....~o.../1c.hdmx...X. ..)..%..YGhead.....5...6...hhea.....!...$.).ehmtx.....>.....[%)loca... .....S.maxp..... ... .name.....#.?.post.....yY.f.prep.....6.r~.x....dW....zz.o..m.m{..m;=. X.h mo.2vR.Oe.....I}..S.u.....Kt.MW_J.g]{9..... w..K..r..^..Y@.$H...$.;....6..6U.Sn..."]....;.N... M.l..l.6l.v..N...r..s..q?.. ...O...C..2VcU..`..!D._...s6.....{..g.....N.M....<c-.|U.i^.VU.y.Z ..@...H.5K.&m.R~O.}M..S.LK.....K...S.n..7..K=U...@.i...H.....L..WQ.....s...9.s.:I]..5.S.;.....u.P..... A-;.;Ag../G.u...).+.(.*.).+.;.(__'J~.z.8..W..l.5k.`#.M{...{..r[h...f...RXFu.1.2.. ..x.\.....uO.....l..$.....J....6SL..?."..^p.....j.-$.....].`..6.l....M.#X...;. ....Y.|...L....F .....E.F..I@ x.5.X[*...}.I...6.@..{^.9E.f.dM..4w...Z....!E..0S.`

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\IMG_3026-1[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=25, height=4000, bps=0, PhotometricIntepretation=RGB, description=, manufacturer=Canon, model=Canon IXUS 230 HS, orient ation=upper-left, width=3000], baseline, precision 8, 500x531, frames 3
Category:	downloaded
Size (bytes):	59207
Entropy (8bit):	7.443214195693966
Encrypted:	false
SSDEEP:	1536:9yP4/yP4mYPmmsePwmooA1IZmyT8tNwfJ4bK3:s424PPAePqIMm8fwfJ4s
MD5:	56A8688BB540DC64F370A5C7A589FB14
SHA1:	C4037C8AB0FC89D1DFB255E007124EBFD63F6F8D
SHA-256:	97156E148D5AE815B3B28DF4734AA534E36419AD4A6E68F77F619484403372B8
SHA-512:	E77242A52AC5444E1BFC5F3E67C0173CDCEAF513463DAD58D1E3AE9D3B7C4D819D2C88E81870CC989DF259F239161B22C14E867A6C06496D4C596A0589F139
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.dickinsonsolicitors.co.uk/wp-content/uploads/2018/07/IMG_3026-1.jpg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\IMG_3026-1[1].jpg	
Preview:	....'.Exif..MM.*.....:.....@.....G.....M....._.....g.(.....1....."...o.2.....GF.....GI .....0.....@.....@....0.....%.i.....4.....Canon.Canon IXUS 230 HS.....'.....'.Adobe Photoshop CC 2018 (Windows).2018:07:06 15:44:01. . . . .

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\KFOlCnqEu92Fr1MmEU9fBBc9[1].ttf	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	TrueType Font data, 18 tables, 1st "GDEF", 8 names, Microsoft, language 0x409, Copyright 2011 Google Inc. All Rights Reserved.Roboto MediumRegularVersion 2.137; 2017Roboto-Me
Category:	downloaded
Size (bytes):	35588
Entropy (8bit):	6.410135551455154
Encrypted:	false
SSDEEP:	768:6yVJgIpAqZsXgDNHOBBPXNOKdhT1N+06XAxGrzmoqpxk0SnuUR:enq805OBBdhT1NP6XAxGryoqp2
MD5:	4D88404F733741EAACFDA2E318840A98
SHA1:	49E0F3D32666AC36205F84AC7457030CA0A9D95F
SHA-256:	B464107219AF95400AF44C949574D9617DE760E100712D4DEC8F51A76C50DDA1
SHA-512:	2E5D3280D5F7E70CA3EA29E7C01F47FEB57FE93FC55FD0EA63641E99E5D699BB4B1F1F686DA25C91BA4F64833F9946070F7546558CBD68249B0D853949FF85C5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmEU9fBBc9.ttf
Preview:	..... GDEF.....{....dGPOS.....|<....GSUB7b.....8....OS/2t.#...r....`cmap.....st...Lcvt 1..K..y....\fpgm..$...v.....gasp.....{.....glyf.'.....,..j.hdmx.....r\|....head...r..n....6hhea.....q. ...$hmtx..MO..n@....loca\v@z..l(....maxp.....l.... name..:...z,....post.m.d..{.... prep...)..x|...S...d...(.....o.....9.....EX../... >Y..EX../....>Y.....9.....9.....9.....9.....9.....9.....01!!.!.....!.5.!.(.<..6.....}.w...x.^.^..^.....<.....9.....EX../... >Y..EX../....>Y.....+X!...Y..../01.#.!.462...."&.~.....J.JH.H.....9KK97JJ....e...@..... %...EX../..."...>Y..../..../...../01..#.3..#.3..#...-#...w.}....}.....`.....EX../... >Y..EX../... >Y..EX../....>Y..EX../....>Y.....9../.....+X!...Y...../.....+X!...Y.....01.#. #.#5!.#5!.3.3.3.3.#.3.#.#.3.#...L.L...:...N.N.N.N..:..L.v.:....f....9....`...`....f.8.9...d.-.&...,...*-...9...EX../... >Y..EX../... >Y..EX.#/.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\KFOlCnqEu92Fr1MmYUtfBBc9[1].ttf	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	TrueType Font data, 18 tables, 1st "GDEF", 8 names, Microsoft, language 0x409, Copyright 2011 Google Inc. All Rights Reserved.Roboto BlackRegularVersion 2.137; 2017Roboto-Bla
Category:	downloaded
Size (bytes):	35208
Entropy (8bit):	6.392518822467014
Encrypted:	false
SSDEEP:	768:53Dmu13ucOmpIN22bN8o6Ze0XlGV+uM49pSeCu7XniviDffw6mo/quUR:lD13DjSNz0XlG0uL9YeCu7Xn4iTo9o/4
MD5:	4D99B85FA964307056C1410F78F51439
SHA1:	F8E30A1A61011F1EE42435D7E18BA7E21D4EE894
SHA-256:	01027695832F4A3850663C9E798EB03EADFD1462D0B76E7C5AC6465D2D77DBD0
SHA-512:	13D93544B16453FE9AC9FC025C3D4320C1C83A2ECA4CD01132CE5C68B12E150BC7D96341F10CBAA2777526CF72B2CA0CD64458B3DF1875A184BBB907C5E3D71
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmYUtfBBc9.ttf
Preview:	..... GDEF.....z\...dGPOS.....z.....GSUB7b.....OS/2ve#...p....`cmap.....r....Lcvt ...=..xX...Zfpgm..#...ud....gasp.....zP....glyf.....,..i~hdmx.....q ....head...R..l....6hh ea.]....p....$hmtx..<...l.....locaK./...j.....maxp.....j.... name..9...x....|post.m.d..z0... prep...C..w ...8...d...(.....P...EX../....>Y..EX../....>Y.....9.....9.....9.....9.....9.....9.....0 1!!.!.....!.5.!.(.<..6.....}.w...x.^.^..^....g.....<.....9.....EX../....>Y..EX../....>Y.....+X!...Y..../01.!.!.462..."&....+.g..k.kk.k.....J__.__.....^.....&.....9...../.....9../. .....01..#.3..#.3.+..._+...v.S.8..S.8.....z..... !..9.....EX../....>Y..EX../....>Y..EX../....>Y..EX../....>Y.....9../.....+X!...Y...../.....+X!...Y.....01.#.#.#5 3.#53.3.3.3.3.!.3.!.#.3.#.d.C.C..,..E.D.E.E...,...C.@.,....f....`...`.....f.Q.....S.&.Q...-.r.+./..9...EX../....>Y..EX.!/..!.>Y..!...9.....!..9.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\KFOmCnqEu92Fr1Mu4mxP[1].ttf	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	TrueType Font data, 18 tables, 1st "GDEF", 8 names, Microsoft, language 0x409, Copyright 2011 Google Inc. All Rights Reserved.RobotoRegularVersion 2.137; 2017Roboto-Regularht
Category:	downloaded
Size (bytes):	35408
Entropy (8bit):	6.412277939913633
Encrypted:	false
SSDEEP:	768:PX4i+tezjtQYgu30G0xL9nQbuEL7LQo9SBxQbptqKmomjJlvh:PJ2z3G0xpUusLEBKptqNomjV
MD5:	372D0CC3288FE8E97DF49742BAEFCE90
SHA1:	754D9EAA4A009C42E8D6D40C632A1DAD6D44EC21
SHA-256:	466989FD178CA6ED13641893B7003E5D6EC36E42C2A816DEE71F87B775EA097F
SHA-512:	8447BC59795B16877974CD77C52729F6FF08A1E741F68FF445C087ECC09C8C4822B83E8907D156A00BE81CB2C0259081926E758C12B3AEA023AC574E4A6C9885
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4mxP.ttf

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\KFOmCnqEu92Fr1Mu4mxP[1].ttf	
Preview:	..... GDEF.....{`...dGPOS...h..{.....GSUB7b.....OS/2tq#...q....`cmap.....s....Lcvt +.....yl...Tfpgmw.`...vd....gasp.....{T....glyf.....,..j.hdmx.....r ....head.j.z..m....6hh ea.....q....$hmtx..Vl..m.....loca?.#...k.....maxp.....k.... name.U9..y....tpost.m.d..{4... prep.f....x ...l...d...(.....q.....9.....EX../....>Y..EX../....>Y.....9.....9.....9.. ....9.....9.....9.....01!!.!.....!.5.!.(.<..6.....}.w...x.^.^..^.....{.....0...EX../....>Y..EX../....>Y.....+X!...Y.....901.#.3.462..."&.[....7l88l7.....-==Z;;.....#...../.....9 ../.....01..#.3..#.3...o.....o...x.....w.....EX../....>Y..EX../....>Y..EX../....>Y..EX../....>Y.....9|../.....+X!...Y...../.....+X!...Y.....01.!.#.#5!.!5!.3.!.3.3.# .3.#.#.!.!....P.P...E....R.R..R.R..E..P....E.....f....b....`...`.....f.#.b....n.0.....+.i...EX../....>Y..EX."/..">Y.."...9.....+X!.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\about-us[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines
Category:	dropped
Size (bytes):	37866
Entropy (8bit):	5.387618114345256
Encrypted:	false
SSDEEP:	768:PG/k60wKYNrSYdxD9qrP9EzxbbowbQRZV+T2MvZDcfnztKI:PGs6UYNrSYdHqrP9EzxHdeZ7MvZDcfn1
MD5:	E5BC6A8C00492DCC9C36E370841E998B
SHA1:	C2BF0BB7080EBFA92D1767A8BB49BE697953AC05
SHA-256:	379531308480769BF4649B550F7ECC922285613B8FA0376870D8521FAB81CD0D
SHA-512:	693EE186B54988EDEE2C0F5B8781843F440622A965247CE4A2CE58C9AC42BDF443E5BF4BE612E2E7F74FD3DF7C141A8AB352DFE0A3928D8E641106E901905DD 4
Malicious:	false
Reputation:	low
Preview:	.<!DOCTYPE html>. [if lt IE 7]> <html class="no-js lt-ie9 lt-ie8 lt-ie7"> <![endif]-->. [if IE 7]> <html class="no-js lt-ie9 lt-ie8"> <![endif]-->. [if IE 8]> <html c lass="no-js lt-ie9"> <![endif]-->. [if gt IE 8]> >.<html lang="en-GB"..prefix="og: https://ogp.me/ns#" class="no-js"> <![endif]-->.<head >. <meta charset="UTF-8">. <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">. <meta name="viewport" content="width=device-width, initial-scale=1">. <meta name="format-detection" content="telephone=no">. <link rel="apple-touch-icon" href="https://www.dickinsonsolicitors.co.uk/wp-content/themes/quicklaunch-parent-theme/library/ima ges/apple-touch-icon.png">. <link rel="icon" href="https://www.dickinsonsolicitors.co.uk/wp-content/themes/quicklaunch-parent-theme/library/images/favicon.ico" type="i mage/x-icon" />..<script defer src="https://use.fontawesome.com/releases/v5.0.13/js/all.js" integrity="sha384-xymdQtn1n3lH2wcu

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\analytics[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	49153
Entropy (8bit):	5.520906949461031
Encrypted:	false
SSDEEP:	768:/yR3fYFBLbfs5sP5XqY3TyPnHpl1WY3SoavFVv6PU+CgYUD0lgEw0stZM:/y9gZfl5h3UHpaY3SoRCw0sk
MD5:	6DF1787C4BE82D1BB24F8BFFA10C7738
SHA1:	3634E839429E462E49C5F42B75FBFB4BA318AF6D
SHA-256:	2CB09C7B3E19BFC41743CA3624EF81C3258D56525647FEAC76AA757E0292627A
SHA-512:	CB3CE2BCEB61F390298C21E470423CCEB6DD93E648A7DD0467195B11FEF30BF7A086DFF47C4494E2533498D1448C1A22AAB1414C14FD73278F1C92E0F7BC3F 4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google-analytics.com/analytics.js
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var n=this||self,p=function(a,b){a=a.split(".");var c=n;a[0]in c||"undefin ed"==typeof c.execScript||c.execScript("var "+a[0]);for(var d;a.length&&(d=a.shift());)a.length||void 0===b?c=c[d]&&c[d]!==Object.prototype[d]?c[d]:c[d]={}:c[d]=b};var q= {},r=function(){q.TAGGING=q.TAGGING||[];q.TAGGING[1]=!0};var t=function(a,b){for(var c in b)b.hasOwnProperty(c)&&(a[c]=b[c])},v=function(a){for(var b in a)if(a. hasOwnProperty(b))return!0;return!1};var x=/^(?:(?:https?|mailto|ftp):|[^:/?#]*(?:[/?#]|$))/i;var y=window,z=document,A=function(a,b){z.addEventListener?z.addEventListene r(a,b,!1):z.attachEvent&&z.attachEvent("on"+a,b)};var B=/:[0-9]+$/,C=function(a,b,c){a=a.split("&");for(var d=0;d<a.length;d++){var e=a[d].split("=");if(decodeURIComponen t(e[0]).replace(/\+/g," ")===b)return b=e.slice(1).join("="),c?b:decodeURIComponent(b).replace(/\+/g," ")}},F=function(a,b){b&&(b=String(b).toLowerCase());if("p

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\anchor[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	83970
Entropy (8bit):	5.8961912896711155
Encrypted:	false
SSDEEP:	768:v/Sx24neDZXr5mMzkoN1zBwwraL48WGZS/SJd0Lvr5mMzkoN1zBww4tkx4Yars5E:S2ieVXMoN9vmL4nIReLvMoN9v4sUmhy
MD5:	B5787DA3E7447C779F17A9B5FDA0F76F
SHA1:	8AF2E4A59358BD7AA5331C1D80CB180C828EC819
SHA-256:	6FC6939B1526B581D9FADF552B28C766F0D737BAC06F4CCAABA0A8C2E53A07B6
SHA-512:	A17263FF3AB3F0BEA6AAA788A11D99AA5FD9957D5F4ACFDAC8DBE4CEC509BEA6979827363A179C4DBD3495E646C16EDDBC932DB70B602FF5A005ECCCDCF8 D783
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\anchor[1].htm	
Preview:	<!DOCTYPE HTML><html dir="ltr" lang="en"><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.<meta http-equiv="X-UA-Compatible" content="IE=edge">.<title>reCAPTCHA</title>.<style type="text/css">.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 400;. src: url(//fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4mxP.ttf) format('truetype');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 500;. src: url(//fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmEU9fBBc9.ttf) format('truetype');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 900;. src: url(//fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmYUtfBBc9.ttf) format('truetype');.}..</style>.<link rel="stylesheet" type="text/css" href="https://www.gstatic.com/recaptcha/releases/eWmgPeIYKJsH2R2FrgakEIkq/styles__ltr.css">.<script nonce="vuK04+fO3TPBq8VNczbMDA" type="text/javascript">window['__recaptcha_api'] = 'https://www.google.com/rec

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\api[1].js	
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):	1768
Entropy (8bit):	5.612927321721572
Encrypted:	false
SSDEEP:	48:VKEcOKoeN1l2FLrwUngKEcOKoeN1l2FLrwUnG:f4Dl2tsuU4Dl2tsuG
MD5:	DB7E6557447F36E889AFD1F82FF750FE
SHA1:	3F8CA19EEF99A1858FD483FE37244A440DFB6D41
SHA-256:	6BFA8B05D0C8E17F9D065180456EE1B5CA79750A596CCFDF6DBA12D5AD889602
SHA-512:	7D1859337EFA95B938FF0A6A895E6EAFB0300E7EFDD019B0D4E23F30A12BC26886ACA8CDACCDFFA5D4C9EED8F08844C6D246BFD83553A536DD84FE9F53BA4EBD
Malicious:	false
Reputation:	low
Preview:	/* PLEASE DO NOT COPY AND PASTE THIS CODE. */(function(){var w=window,C='___grecaptcha_cfg',cfg=w[C]=w[C]||{},N='grecaptcha';var gr=w[N]=w[N]||{};gr.ready=gr.ready||function(f){(cfg['fns']=cfg['fns']||[]).push(f);};w['__recaptcha_api']='https://www.google.com/recaptcha/api2/';(cfg['render']=cfg['render']||[]).push('6LfmMJ0UAAAAADP280q3cebbJ7e0Xs9ffHLgUKeH');w['__google_recaptcha_client']=true;var d=document,po=d.createElement('script');po.type='text/javascript';po.async=true;po.src='https://www.gstatic.com/recaptcha/releases/eWmgPeIYKJsH2R2FrgakEIkq/recaptcha__en.js';po.crossOrigin='anonymous';po.integrity='sha384-3l+Dzjt73YLhXz+WejlQA/r4+koQU0wEJ+YZAtKZ8DTxOPwZ54aluvUaML5sjiPl';var e=d.querySelector('script[nonce]'),n=e&&(e['nonce']||e.getAttribute('nonce'));if(n){po.setAttribute('nonce',n);}var s=d.getElementsByTagName('script')[0];s.parentNode.insertBefore(po, s);})();/* PLEASE DO NOT COPY AND PASTE THIS CODE. */(function(){var w=window,C='___grecaptcha_cfg',cfg=w[C]=w[C]||{},N='gre

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\api[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	884
Entropy (8bit):	5.612927321721572
Encrypted:	false
SSDEEP:	24:2jkm94/zKPccAK+KVCetz1l2EsLqo40RWUnYN:VKEcOKoeN1l2FLrwUnG
MD5:	4F33B826DC2529EFE9C694A7511AAA46
SHA1:	1D9F3E04760EA939E008EBC01E9F2B21FE68AFC1
SHA-256:	0770D0F26742AA70A19392672BB65C1BDC91E09836B0CC80089919C830EA4E82
SHA-512:	AEAAFD58DF3169700DE64C77F53CB4C6BC4FC52766AB27E7B39512B1C02124CF3FCFB1D8FC763C0AC45B9E6DB2D79C2B6D4B19515788C4ED455D2613386C30
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google.com/recaptcha/api.js?render=6LfmMJ0UAAAAADP280q3cebbJ7e0Xs9ffHLgUKeH&ver=3.0
Preview:	/* PLEASE DO NOT COPY AND PASTE THIS CODE. */(function(){var w=window,C='___grecaptcha_cfg',cfg=w[C]=w[C]||{},N='grecaptcha';var gr=w[N]=w[N]||{};gr.ready=gr.ready||function(f){(cfg['fns']=cfg['fns']||[]).push(f);};w['__recaptcha_api']='https://www.google.com/recaptcha/api2/';(cfg['render']=cfg['render']||[]).push('6LfmMJ0UAAAAADP280q3cebbJ7e0Xs9ffHLgUKeH');w['__google_recaptcha_client']=true;var d=document,po=d.createElement('script');po.type='text/javascript';po.async=true;po.src='https://www.gstatic.com/recaptcha/releases/eWmgPeIYKJsH2R2FrgakEIkq/recaptcha__en.js';po.crossOrigin='anonymous';po.integrity='sha384-3l+Dzjt73YLhXz+WejlQA/r4+koQU0wEJ+YZAtKZ8DTxOPwZ54aluvUaML5sjiPl';var e=d.querySelector('script[nonce]'),n=e&&(e['nonce']||e.getAttribute('nonce'));if(n){po.setAttribute('nonce',n);}var s=d.getElementsByTagName('script')[0];s.parentNode.insertBefore(po, s);})();

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\bootstrap.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	35601
Entropy (8bit):	5.178356022236213
Encrypted:	false
SSDEEP:	768:91+7/uRE672wlNrDMlbGqXYu+jS1s8ep0s1QfrXf8X8GvpZOWQ:DFRx7zYyS1WOv8fpZDQ
MD5:	2616D3564578D8F845813483352802A9
SHA1:	5ADA7C103FC1DEABC925CC1FDBBB6E451C21FC70
SHA-256:	F971B901AEB9E55B07D472AFEE09BD5AE05159E1119DBD16D993E473565E7FC0
SHA-512:	E3D8BC8FD58B0AC1D9FC444F21F2DAD94DEFDE536AF2AADB6ACE768AE0BCA9F9C9274161B076FC546CED174F23CC7495A8C5049AB00BE19C75F6310E91ABEDC
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\bootstrap.min[1].js	
Reputation:	low
IE Cache URL:	http://https://www.dickinsonsolicitors.co.uk/wp-content/themes/quicklaunch-parent-theme/library/js/vendor/bootstrap.min.js?ver=5.7.2
Preview:	/*!. * Bootstrap v3.3.1 (http://getbootstrap.com). * Copyright 2011-2014 Twitter, Inc.. * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */.if("undefined"==typeof jQuery)throw new Error("Bootstrap's JavaScript requires jQuery");+function(a){var b=a.fn.jquery.split(" ")[0].split(".");if(b[0]<2&&b[1]<9||1==b[0]&&9==b[1]&&b[2]<1)throw new Error("Bootstrap's JavaScript requires jQuery version 1.9.1 or higher")}(jQuery),+function(a){"use strict";function b(){var a=document.createElement("bootstrap"),b={WebkitTransition:"webkitTransitionEnd",MozTransition:"transitionend",OTransition:"oTransitionEnd otransitionend",transition:"transitionend"};for(var c in b)if(void 0!==a.style[c])return{end:b[c]};return!1}a.fn.emulateTransitionEnd=function(b){var c=!1,d=this;a(this).one("bsTransitionEnd",function(){c=!0});var e=function(){c||a(d).trigger(a.support.transition.end)};return setTimeout(e,b),this},a(function(){a.support.transition=b(),a.support.transition&&(a.event.spe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\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\NUEPGTR9\fa-regular-400[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Font Awesome 5 Free Regular family
Category:	downloaded
Size (bytes):	34394
Entropy (8bit):	6.320002764155788
Encrypted:	false
SSDEEP:	384:zYkILltPRwpXUazLuDULbN1TH/uOlrk4jx3l+89AyI6WcRwkNcQUG:zYnLDPXy6DO7/uOtx29uc5NcQUG
MD5:	A2B2A23693C93FE6D9D600B30FFBE3D8
SHA1:	DADCF16952EA34C6E04CF0431B34DA00B6D168C7
SHA-256:	A4F9B9DB99D842F4AE2E2E291CEA35F55C8BE5CC8003B0A69A5A6B1F3CAF6D7C
SHA-512:	A2280FFC903B6919EBA1AF72CF4B70FFD0F46973828CBB293F7B49EF27D1E5F6B74C7E9AC57755F65E2D6FF0E54834DAFC6E6B1CC237EDC498F245F0970696D8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.dickinsonsolicitors.co.uk/wp-content/plugins/js_composer/assets/lib/bower/font-awesome/webfonts/fa-regular-400.eot?
Preview:	Z...0.....LP.....DU.....6.F.o.n.t. .A.w.e.s.o.m.e. .5. .F.r.e.e. .R.e.g.u.l.a.r.....R.e.g.u.l.a.r...L.3.3.0...4.9.8. .(.F.o.n.t. .A.w.e.s.o.m.e. .v.e.r.s.i.o.n.:. .5...1.1...2.)...6.F.o.n.t. .A.w.e.s.o.m.e. .5. .F.r.e.e. .R.e.g.u.l.a.r.....PFFTM.....GDEF.*.....OS/2A.....X...`cmap.....gasp.....glyfl..... ..n.head.9-.....6hhea.5.....$hmtx...t.....Tloca.E.....6maxp.....8... name6.60..w....[post.iA...}@.....J.|..UD_.<.....@.....L.f...G.L.f.....PfEd.....T.....:..... .....@.....@.....@.....@.....@...@.....@...@.....@...@.....`.....@.....@.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\fa-solid-900[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Font Awesome 5 Free Solid family
Category:	downloaded
Size (bytes):	192758
Entropy (8bit):	6.349432274438151
Encrypted:	false
SSDEEP:	3072:LPtAtFnhbTO7jZUpLL1C5vPXiazQXYtvyVaaKL+jr0hFlx5P+hehAMe9Z:LtAtFnhqyp9CFXiMQItvyQMjYhFH5iMk
MD5:	6E27A27923619B30FC089BD0B84E4685
SHA1:	2B3A98E7399FEA366879EECCCB59FCF3F2B7AAD6
SHA-256:	E2309AD95A8F3BBFE7E977AF8FFEB8DE2CE6F7714FDE2EA74E1528356EEF4FB9
SHA-512:	31B7EC2CF8968681E5DEF41724E61DB6B10549EDC738764FE76B31F27E3C28913D02E3C4E00D1AA2EBCD76CCE3CBF8AE422D97CEE738BA2525BDEAC01C21F8F7
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\fa-solid-900[1].eot	
IE Cache URL:	http://https://www.dickinsonsolicitors.co.uk/wp-content/plugins/js_composer/assets/lib/bower/font-awesome/webfonts/fa-solid-900.eot?
Preview:	.....LP.....!.|.....2.F.o.n.t. .A.w.e.s.o.m.e. .5. .F.r.e.e. .S.o.l.i.d.....S.o.l.i.d...L.3.3.0...4.9.8. .(.F.o.n.t. .A.w.e.s.o.m.e. .v.e.r.s.i.o.n.:. .5...1.1...2.)...2.F.o.n.t. .A.w.e.s.o.m.e. .5. .F.r.e.e. .S.o.l.i.d.....PFFTM.....GDEF.*.....OS/2C..8...X...`cmap$*/.....gasp.....glyfT.....+`....head.G-.....6hhea.C.....$hmtxil.....loca.nF....P....maxp.%.S...8... name$.&,...|...+post...1.....J.|.!_.<.....P. .....@.....L.f..G.L.f.....PfEd.....T.....:..... .....@.....`.....@.....@.....@.....@.....@...@.....@.....`...@.....@.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 1 icon, 16x16, 32 bits/pixel
Category:	downloaded
Size (bytes):	1150
Entropy (8bit):	3.884972839282401
Encrypted:	false
SSDEEP:	12:X6KUa0l3GGGGGTmGGG6GPglGGGG92NcBGGGLlGGGG1WGvy+EYtlccu8jtl/leJVS:X6dbqUyjBVlgqX+sVe+B
MD5:	FAEF02C890403EC108243CF2DAF0D9BA
SHA1:	073CE4D57CBAB9BFA455BA2D678FBAAA1DF655CC
SHA-256:	B8EBE8BC3C179BAF093DA55A328ECDF09A331B08B72FDFD05549BBBA8FFB36C5
SHA-512:	F5E13C8B1BCAC4A270D0C62D27B6309918C88C79F1F0023C5CABD035EB270416807D930ACB76EB5373D5183194BAF33559A314F92566AAB396954C63EA8FDBF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.dickinsonsolicitors.co.uk/wp-content/themes/quicklaunch-parent-theme/library/images/favicon.ico
Preview:	..... .h.....(..... ....(..(..(.l(.(..(..(..(..(.(.l(..(.....(..(..(..(.(..(..(..(..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\frontend-gtag.min[1].js	
Preview:	;var MonsterInsights=function(){var e=[],a='',o=!1;this.setLastClicked=function(t,n,i){t=typeof t!=='undefined'?t:[];n=typeof n!=='undefined'?n:[];i=typeof i!=='undefined'?i:!1;e.valuesArray=t;e.fieldsArray=n};this.getLastClicked=function(){return e};this.setInternalAsOutboundCategory=function(e){a=e};this.getInternalAsOutboundCategory=function(){return a};this.sendEvent=function(e,n,i){t(e,n,i,[])};function u(){if(window.monsterinsights_debug_mode){return!0}.else{return!1}};function t(t,n,a,r){t=typeof t!=='undefined'?t:'event';n=typeof n!=='undefined'?n:'';r=typeof r!=='undefined'?r:[];a=typeof a!=='undefined'?a:{};__gtagTracker(t,n,a);e.valuesArray=r;e.fieldsArray=a;e.fieldsArray.event_action=n;e.tracked=!0;i('Tracked: '+r.type);i(e)};function n(t){t=typeof t!=='undefined'?t:[];e.valuesArray=t;e.fieldsArray=[];e.tracked=!1;i('Not Tracked: '+t.exit);i(e)};function i(e){if(u()){console.dir(e)}};function l(e){return e.replace(/^\s+|\s+$/gm,'')};function c(){var n=0,e=document.domain,i=

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\meet-the-team[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines
Category:	downloaded
Size (bytes):	40828
Entropy (8bit):	5.353272599250873
Encrypted:	false
SSDEEP:	768:dGXk60wKYNraPoHr5RbwrIubbowbDRZV+T2MvZDcfnztKI:dGU6UYNrvr5RbwrIuHdhZ7MvZDcfnztv
MD5:	1B45DD6B122ED32D8B6D1D6A9AC02BD5
SHA1:	1605251AC50B0C1AE3E3EDD75C3D587773693976
SHA-256:	9BB183C59D124A2649A65BC8D4C9CFD02D72A70C2A6DD2F5E2DACFE188289A27
SHA-512:	F3DB569ED5F4B92B046B644C039F6789050191068F3B311B26FE375D95ED84BB55A93364973A626ABB519BC216F4963CB0B211DD2DDD8F5CD3055F5C3CBE67C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.dickinsonsolicitors.co.uk/meet-the-team/
Preview:	.<!DOCTYPE html>. [if lt IE 7]> <html class="no-js lt-ie9 lt-ie8 lt-ie7"> <![endif]-->. [if IE 7]> <html class="no-js lt-ie9 lt-ie8"> <![endif]-->. [if IE 8]> <html class="no-js lt-ie9"> <![endif]-->. [if gt IE 8]> >.<html lang="en-GB"..prefix="og: https://ogp.me/ns#" class="no-js"> <![endif]-->.<head >. <meta charset="UTF-8">. <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">. <meta name="viewport" content="width=device-width, initial-scale=1">. <meta name="format-detection" content="telephone=no">. <link rel="apple-touch-icon" href="https://www.dickinsonsolicitors.co.uk/wp-content/themes/quicklaunch-parent-theme/library/images/apple-touch-icon.png">. <link rel="icon" href="https://www.dickinsonsolicitors.co.uk/wp-content/themes/quicklaunch-parent-theme/library/images/favicon.ico" type="image/x-icon" />..<script defer src="https://use.fontawesome.com/releases/v5.0.13/js/all.js" integrity="sha384-xymdQtn1n3lH2wcu

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\mem5YaGs126MiZpBA-UN8rsOUuhv[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 19160, version 1.1
Category:	downloaded
Size (bytes):	19160
Entropy (8bit):	7.967047296085223
Encrypted:	false
SSDEEP:	384:wQDywW7WywLbHesuDAL7df4V7G/aSpBpucg7KlnWtKgqp/y:6wW7LkrescWgG/DuJmlWtKgi/y
MD5:	ADC0530936D8C9AA4279699007BBBEDB
SHA1:	A25B788600D5F280B0B79A93BC1116A667BAC7D6
SHA-256:	012A20DD3CC6D96015C9D5896EEA6DA97D841E940ABA5F13BC0C43AB6F9D0FB0
SHA-512:	0B768871575BAC86528E1DAA477D0E231907627116C292F4C017990AC49B9D847F866324BD95F3DF8B75F02FB97474336A5BDB844D8867956113702B434D2EFD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v20/mem5YaGs126MiZpBA-UN8rsOUuhv.woff
Preview:	wOFF.....J.....qD.....GDEF.....GPOS.....GSUB.....y.....;..OS/2...$...^...`...vcmap.....Y..cvt ...8...g.....o.[fpgm.....s.ugasp...D.....#glyf...T..:F..Y.%..Ohead..B....6...6....hhea..B.....$....hmtx..B....-....(.C.loca..E$.....maxp..F.... ... .name..G.....%.@cpost..H.....5.".prep..I.....1..S.....x.M...P.@..L..$$. .g..;..k.z...P.$K.....[.E..Z....B)..a.:...i...!.....J ...U....l/..m.&*3.KO...#..-..%;7.V.....x.c`f.cV``e``..j...(.../2.11s01qs.1s.01.400.300x.....:.;380(...&.O.....)B..q>H.%.u..R``.....x.\.!..q.....#acf...#1Q@.'U..@..".llt.Aa#.f|c.W.....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN....:.....F....GG.g.s,x.>0....v..I;o..<.$G9.\f2...e{}.IS2..uc]p.....M.x.c.a.g``..$K..(..`.e.a.a`....C..L..@t.....A..L..&.....1\gta.e....320.0...2.g.j...=...x.TGw.F.....)..)7.W..`*.j.-...=*'_..sI...2...O>....[tt....TK]..|..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\mem6YaGs126MiZpBA-UFUK0Zdcs[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 17504, version 1.1
Category:	downloaded
Size (bytes):	17504
Entropy (8bit):	7.960726283242655
Encrypted:	false
SSDEEP:	384:gOQHZDOjNtkrTZx8YbwLPGK+miKq4EpS5syMVdSNI8S:/tkrTBbSq4ZsyY
MD5:	531BF97B28201ADDC0C05AF57A953F15
SHA1:	53C3B719C96FE1913A38CF1EBCFA3EA93699853F
SHA-256:	887661900A506AF06D17741BC2649A4AA578C9268BB2730C9E05F0155456CFF2
SHA-512:	3842158808C21BC798A89DA009459AD4C17DA319493B0FA467A1FA66308C306BEBA89A43E4B714BE781A16F68EEFFE1EFD0EA0AAE06BD53F26F03D4A49F10905
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v20/mem6YaGs126MiZpBA-UFUK0Zdcs.woff

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\mem6YaGs126MiZpBA-UFUK0Zdcs[1].woff	
Preview:	wOFF.....D`.....d.....GDEF.....GPOS.....GSUB.....y.....;..OS/2...$...]...`~l.=cmap.....Y..cvt ...8...W.....fpgm.....~a..gasp...,.....#glyf...<..4...M....head..<T...6...6..z.hhea..<....''...$. . hmtx..<.....=B.loca..>.....?. maxp..@.... ... .name..@.....%`@.post..A.....5.''.prep..Cp.....T.....x.M...P.@..L..$$. .g..;..k.z...P.$K.....[.E..Z....B )..a.:...i...!.....J ...U....l/..m.&*3.KO...#..-..%;7.V.....x.c`f.f.....:....Q.B3_dHcb```.fccfeabbi``P..x.....:.;302(...&.O....)B..q>H..u..R``..?i.....x.\.!..q.....#acf...#1Q@.'U..@..''.llt.Aa#.f|c.W.....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN....:.....F....GG.g.s,x.>0....v..I;o..<.$G9.\f2...e{}.IS2..uc]p....M.x.c.a.g.c..$KY...e@.,..''.....?.....g....Z...[..5..=.d.....p.a.C?C..L...FF~..,...x.uTGw.F.....)..)7.W.$`*.....G.Kz.)e....t.|.1.7...s.g...3.7mgf..~{1...s.3.S...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\memnYaGs126MiZpBA-UFUKWiUNhrIqU[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 17512, version 1.1
Category:	downloaded
Size (bytes):	17512
Entropy (8bit):	7.968196019099005
Encrypted:	false
SSDEEP:	384:TLq60uOF2lS+F0tIAj23Km+GwptAko/13pSJn2IpCEApitRVE9ZtIKZ:bS2c+ZAj26m+Gw/ot5SJn2I83iEZ
MD5:	AE9D2F1CE08FBDF103EE860763B106FF
SHA1:	2E16DAE015C60EFA97ACF4CCC628F798C4981AB9
SHA-256:	7263F989C49E7C621C73468B7DDDEB14497B529EDF427DE520EF636A2224FAC9
SHA-512:	6FBE7566AB26401EA987F4CA761275D15BF931B049A92EABBF832F72065D8C40CF151878CEBA5C030BB06EE0609F5CB0CF6BDBB979657DA8E4B747ADCC9FED63
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/opensans/v20/memnYaGs126MiZpBA-UFUKWiUNhrIqU.woff
Preview:	wOFF.....Dh.....e.....GDEF.....GPOS.....GSUB.....y.....;..OS/2...$...]...`....cmap.....Y..cvt ...8...b.....g.ifpgm.....s.ugasp...@.....glyf...L..3...NX.r..head..<L...6...6..{.hhea..<....''...$...bhmtx..<....-...../.loca..>.....8maxp..@.... ... .y..name..@.....)/C.post..A.....5.''.prep..Cx.....x.M...P.@..L..$$. .g..;..k.z...P.$K.....[.E..Z....B).a.:...i...!.....J ...U....l/..m.&*3.KO...#..-..%;7.V.....x.c`f9.....u..1...<.f.....b.. 0t.vfPdP...M...C.G/S....|..K..6 ....t...x.\.!..q.....#acf...#1Q@.'U..@..''.llt.Aa#.f|c.W.....'..X..!..C...ITPE.;..V.j.....0. .L0E...Yd.mN....:.....F....GG.g.s,x.>0....v..I;o..<.$G9.\f2...e{}.IS2..uc]p.....M.x.c.a.g.c..$KY...e@.,q.....x.....3.....%..=.d.....#..6.e..L@6.3.e.....1._....#...x.TGw.F.....)..)7.W..`*.j.-...=*_..sI...2...O>....[tt....TK]..|...G..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\remote[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	100146
Entropy (8bit):	5.450585060618678
Encrypted:	false
SSDEEP:	3072:xmBeFEdKieE+2rnBG0oNAiPjOgyMc1XE4x09Zk:YBmEdKpl2LBG0oNAiPjOgyMc1XE4x096
MD5:	90CC72FC6743FEAC8E7D450E13B57178
SHA1:	66D6E7ADC4756D9C62BAFF9C74C5CDB3F4F64484
SHA-256:	0BE138567F72E46EA2B9622D43B8B1A33DF3996A50EB1397EAE716A463535DA2
SHA-512:	5896D203FAAD87473A22F9531EEE55BF295C5B8CC9747E7D2DD51E2D3481B780DA527EC983EA21592385DEB0243A5394F42AD09883F3C926FA02838A5DCE561
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.youtube.com/s/player/e467278e/player_ias.vflset/en_US/remote.js
Preview:	(function(g){var window=this;'use strict';var vKa=function(a,b){return g.Lb(a,b)},wKa=function(a){if(a instanceof g.Wi)return a;.if(''function''==typeof a.og)return a.og(!1);if(g.La(a)){var b=0,c=new g.Wi;c.next=function(){for(;;){if(b>=a.length)throw g.Pm;if(b in a)return a[b++];b++}};.return c}throw Error(''Not implemented'');},xKa=function(a,b,c){if(g.La(a))try{g.zb(a,b,c)}catch(d){if(d!==g.Pm)throw d;.}else{a=wKa(a);try{for(;;)b.call(c,a.next(),void 0,a)}catch(d){if(d!==g.Pm)throw d;}}},K4=function(a,b,c){a.l.set(b,c)},L4=function(a){K4(a,''zx'',Math.floor(2147483648*Math.random()).toString(36)+Math.abs(Math.floor(2147483648*Math.random())^g.Ra()).toString(36));.return a},M4=function(a,b,c){Array.isArray(c)||(c=[String(c)]);.g.en(a.l,b,c)},yKa=function(a,b){var c=[];.xKa(b,function(d){try{var e=g.Xn.prototype.l.call(this,d,!0)}catch(f){if(''Storage: Invalid value was encountered''==f)return;throw f;}void 0===e?c.push(d):g.Wn(e)&&c.push(d)},a);.return c},zKa=function(a,b){b=yKa(a,b);.g.zb(b

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\resolution[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 175 x 85, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	5349
Entropy (8bit):	7.87535796212606
Encrypted:	false
SSDEEP:	96:Yo7F52vd44OqOHojP/m49OngRP/9l2RMqgJPZz:N7FEOqOHeP/m4NYCvxz
MD5:	04175E61A8B5AB1C791B4033967D2DDC
SHA1:	6173275069F6A08FD217232638074D37F6492118
SHA-256:	000B0C9FA58851541F347B6731DA849E6C02632492062A9B3A108F83706AD705
SHA-512:	F7CFAA815D83F956F809E696BEFACEA5C800CBA98EF37D4B0B60A93DF4654B5B2CF43B2AED03D2E81ED9D98B70B273ADEBEA58E947C79F867B0B8A25FE158B1E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.dickinsonsolicitors.co.uk/wp-content/uploads/2017/10/resolution.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\resolution[1].png	
Preview:	.PNG.....IHDR.....U.....?.....tEXtSoftware.Adobe ImageReadyq.e<...&iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c142 79.160924, 2017/07/13-01:06:39 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmp:CreatorTool="Adobe Photoshop CC 2018 (Windows)" xmpMM:InstanceID="xmp.iid:72023C7372EA11E8B0D2AAC6E833D75F" xmpMM:DocumentID="xmp.did:72023C7472EA11E8B0D2AAC6E833D75F"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:72023C7172EA11E8B0D2AAC6E833D75F" stRef:documentID="xmp.did:72023C7272EA11E8B0D2AAC6E833D75F"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>...(...UIDATx..].t.E..?$!..p...r.!..AV9".PAPV.C`...Wa.t...<....K..D9E.9...E$.`.+. G..!..![..1.03.LH h}...'3}Lw.]].]

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\responsive[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	95
Entropy (8bit):	4.9140926506100095
Encrypted:	false
SSDEEP:	3:XMFmtSARlllSowWcVeAfdL3oSovn:RRllHou3J3obv
MD5:	9C42BDBA954BAA791D4FE69644B9E103
SHA1:	2F28C76D4588FB691902022FBAB014CAC1BDADE2
SHA-256:	81C3BD88917931A412D1BDA9D7E62976CB035047E6FA9779E192BC4CCD05DCF0
SHA-512:	05B2C94D5AA9FFFA900CDBF9752DC763EEF0D8B61324003D6CF96C7F7E1EBAFA770F7B4CEE382030B9AD77D2F526C3C19627CB0FD8F5C6B8649546A4A722EC7F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.yoshki.com/responsive.css
Preview:	.yoshkiimg, .yoshkidiv{...max-width:100% !important;...background-size:contain !important;..}..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\unXEs0crvtA[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	modified
Size (bytes):	51280
Entropy (8bit):	5.811190905345367
Encrypted:	false
SSDEEP:	768:HnK+IKqDQYkyt67pDQmJ7yYA7hcxFbYo/6F62A1JjC8Qhk1O:jY+i37h6dRv1J28yWO
MD5:	AC296D327A224F77B3067033460AC739
SHA1:	5177DE78C4E2057F5A7CD5C589CCB7700B73B0FD
SHA-256:	0A9DA3CB261C08773C6A1C5771C6F5363761DF35820C82F6C3AEB612EA0349E2
SHA-512:	DEED330042D308B194AB3A72677169B3496850A6CE4A3978587F9BFAAD6D9DFF5E66E8091AD854C3A27B90EDBA09B6E4590309B728FAB245059F60A1AE29437A
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html><html lang="en" dir="ltr" data-cast-api-enabled="true"><head><meta name="viewport" content="width=device-width, initial-scale=1"><style name="www-roboto" nonce="SBJ/EM5lP1vqn7TzkBCpgw">@font-face{font-family:'Roboto';font-style:normal;font-weight:400;src:url(//fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4mxM.woff)format('woff');}</style><script name="www-roboto" nonce="l5gggWIB8JQm0XZdXCUiLA">if (document.fonts && document.fonts.load) {document.fonts.load("400 10pt Roboto", "E"); document.fonts.load("500 10pt Roboto", "E");}</script><link rel="stylesheet" href="/s/player/e467278e/www-player.css" name="www-player" nonce="SBJ/EM5lP1vqn7TzkBCpgw"><style nonce="SBJ/EM5lP1vqn7TzkBCpgw">html {overflow: hidden;}body {font: 12px Roboto, Arial, sans-serif; background-color: #000; color: #fff; height: 100%; width: 100%; overflow: hidden; position: absolute; margin: 0; padding: 0;}#player {width: 100%; height: 100%;}h1 {text-align: center; color: #fff;}h3 {margin-top: 6px; margi

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\uncategorised[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines
Category:	downloaded
Size (bytes):	32310
Entropy (8bit):	5.3807897363849895
Encrypted:	false
SSDEEP:	768:8gPugZSHk60wKYNrD2mbbowbuRZV+T2MvZDcfnztKI:8gPugZSE6UYNrxHdgZ7MvZDcfnztKI
MD5:	86E8AB6881ACC57583613BB39D30C577
SHA1:	270931E052B12D55BF0B05EDB75A3616C9AE1B4F
SHA-256:	2B61710DF7952E8F86522D9975C94BC4F6BA085139CFAD4C1676B4D5EABC8DCF
SHA-512:	4EE6B334FFF7BF8749632809E249B74A5FBC1A9D102E2C7B936CEAF4E3506B47D408A0AA3CC36875708B796534DEACD064CF41F7015B14B84F10C740E50D7F2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.dickinsonsolicitors.co.uk/category/uncategorised/

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\uncategorised[1].htm	
Preview:	.<!DOCTYPE html>. [if lt IE 7]> <html class="no-js lt-ie9 lt-ie8 lt-ie7"> <![endif]-->. [if IE 7]> <html class="no-js lt-ie9 lt-ie8"> <![endif]-->. [if IE 8]> <html class="no-js lt-ie9"> <![endif]-->. [if gt IE 8]> >.<html lang="en-GB"..prefix="og: https://ogp.me/ns#" class="no-js"> <![endif]-->.<head >. <meta charset="UTF-8">. <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">. <meta name="viewport" content="width=device-width, initial-scale=1">. <meta name="format-detection" content="telephone=no">. <link rel="apple-touch-icon" href="https://www.dickinsonsolicitors.co.uk/wp-content/themes/quicklaunch-parent-theme/library/images/apple-touch-icon.png">. <link rel="icon" href="https://www.dickinsonsolicitors.co.uk/wp-content/themes/quicklaunch-parent-theme/library/images/favicon.ico" type="image/x-icon" />..<script defer src="https://use.fontawesome.com/releases/v5.0.13/js/all.js" integrity="sha384-xymdQtn1n3lH2wcu

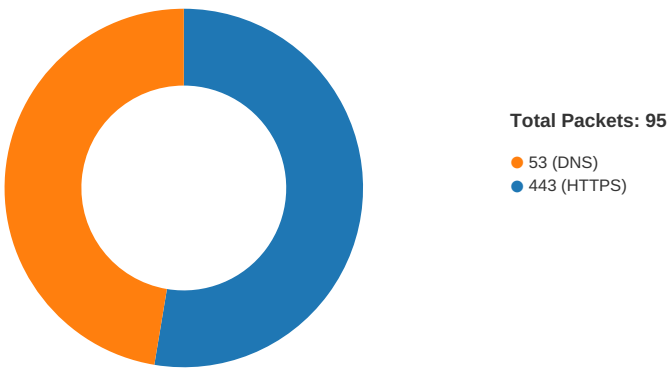
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\vc-waypoints.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	9237
Entropy (8bit):	5.097919218248826
Encrypted:	false
SSDEEP:	192:tE/kIozT9DjFA6hj8jAanJVvfikr5IuFQYzpN0c7yPYRXFARk6kJrrAlr:tEMZzT9DjFAC8EanJVv5IuFQYn0IuYRu
MD5:	5FF487A413612CBBF6BC391C10FF7BAC
SHA1:	ACBBD8A96ECAD33158F29E45AFCD41E4B2DD6579
SHA-256:	357AD057DE8FFC0FC9DF301DD1873C3D482E926791195EE262DA3886269F84D8
SHA-512:	9AF6CF849FCFE777EE1DAA2E5CCD79DC1B11013470DB78B4C165A81573CCAB4F6F1757082CF0FE643C95AFDD42283EE0EE89522923A0E1C1303F5C07A8F3C0AD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.dickinsonsolicitors.co.uk/wp-content/plugins/js_composer/assets/lib/vc_waypoints/vc-waypoints.min.js?ver=6.6.0
Preview:	/*!. * WPBakery Page Builder v6.0.0 (https://wpbakery.com). * Copyright 2011-2019 Michael M, WPBakery. * License: Commercial. More details: http://go.wpbakery.com/licensing. */..// jscs:disable.// jshint ignore: start../*!.Waypoints - 4.0.1.Copyright . 2011-2016 Caleb Troughton.Licensed under the MIT license..https://github.com/imakewebthings/waypoints/blob/master/licenses.txt.*/.!function(){"use strict";var e=0,r={};function i(t){if(!t)throw new Error("No options passed to Waypoint constructor");if(!t.element)throw new Error("No element option passed to Waypoint constructor");if(!t.handler)throw new Error("No handler option passed to Waypoint constructor");this.key="waypoint-"+e,this.options=i.Adapter.extend({},i.defaults,t),this.element=this.options.element,this.adapter=new i.Adapter(this.element),this.callback=t.handler,this.axis=this.options.horizontal?"horizontal":"vertical",this.enabled=this.options.enabled,this.triggerPoint=null,this.group=i.Group.findOrCreate({name:this.option

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2021 12:18:55.628478050 CEST	49714	443	192.168.2.5	185.216.78.150
May 27, 2021 12:18:55.629791975 CEST	49715	443	192.168.2.5	185.216.78.150

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2021 12:18:55.689755917 CEST	443	49714	185.216.78.150	192.168.2.5
May 27, 2021 12:18:55.689894915 CEST	49714	443	192.168.2.5	185.216.78.150
May 27, 2021 12:18:55.691313982 CEST	443	49715	185.216.78.150	192.168.2.5
May 27, 2021 12:18:55.691443920 CEST	49715	443	192.168.2.5	185.216.78.150
May 27, 2021 12:18:55.695489883 CEST	49714	443	192.168.2.5	185.216.78.150
May 27, 2021 12:18:55.695707083 CEST	49715	443	192.168.2.5	185.216.78.150
May 27, 2021 12:18:55.759984970 CEST	443	49714	185.216.78.150	192.168.2.5
May 27, 2021 12:18:55.760030031 CEST	443	49715	185.216.78.150	192.168.2.5
May 27, 2021 12:18:55.760082960 CEST	443	49714	185.216.78.150	192.168.2.5
May 27, 2021 12:18:55.760133028 CEST	443	49714	185.216.78.150	192.168.2.5
May 27, 2021 12:18:55.760183096 CEST	443	49714	185.216.78.150	192.168.2.5
May 27, 2021 12:18:55.760221004 CEST	443	49714	185.216.78.150	192.168.2.5
May 27, 2021 12:18:55.760270119 CEST	443	49715	185.216.78.150	192.168.2.5
May 27, 2021 12:18:55.760318995 CEST	443	49715	185.216.78.150	192.168.2.5
May 27, 2021 12:18:55.760368109 CEST	443	49715	185.216.78.150	192.168.2.5
May 27, 2021 12:18:55.760405064 CEST	443	49715	185.216.78.150	192.168.2.5
May 27, 2021 12:18:55.760684013 CEST	49714	443	192.168.2.5	185.216.78.150
May 27, 2021 12:18:55.760694027 CEST	443	49714	185.216.78.150	192.168.2.5
May 27, 2021 12:18:55.760747910 CEST	49714	443	192.168.2.5	185.216.78.150
May 27, 2021 12:18:55.760768890 CEST	49715	443	192.168.2.5	185.216.78.150
May 27, 2021 12:18:55.761529922 CEST	443	49715	185.216.78.150	192.168.2.5
May 27, 2021 12:18:55.761619091 CEST	49715	443	192.168.2.5	185.216.78.150
May 27, 2021 12:18:55.794886112 CEST	49715	443	192.168.2.5	185.216.78.150
May 27, 2021 12:18:55.795423031 CEST	49714	443	192.168.2.5	185.216.78.150
May 27, 2021 12:18:55.801527977 CEST	49715	443	192.168.2.5	185.216.78.150
May 27, 2021 12:18:55.856398106 CEST	443	49715	185.216.78.150	192.168.2.5
May 27, 2021 12:18:55.856544018 CEST	49715	443	192.168.2.5	185.216.78.150
May 27, 2021 12:18:55.856749058 CEST	443	49714	185.216.78.150	192.168.2.5
May 27, 2021 12:18:55.856822014 CEST	49714	443	192.168.2.5	185.216.78.150
May 27, 2021 12:18:55.902442932 CEST	443	49715	185.216.78.150	192.168.2.5
May 27, 2021 12:18:56.433320999 CEST	443	49715	185.216.78.150	192.168.2.5
May 27, 2021 12:18:56.433408976 CEST	443	49715	185.216.78.150	192.168.2.5
May 27, 2021 12:18:56.433469057 CEST	443	49715	185.216.78.150	192.168.2.5
May 27, 2021 12:18:56.433491945 CEST	49715	443	192.168.2.5	185.216.78.150
May 27, 2021 12:18:56.433532000 CEST	49715	443	192.168.2.5	185.216.78.150
May 27, 2021 12:18:56.433538914 CEST	443	49715	185.216.78.150	192.168.2.5
May 27, 2021 12:18:56.433540106 CEST	49715	443	192.168.2.5	185.216.78.150
May 27, 2021 12:18:56.433598995 CEST	49715	443	192.168.2.5	185.216.78.150
May 27, 2021 12:18:56.433603048 CEST	443	49715	185.216.78.150	192.168.2.5
May 27, 2021 12:18:56.433659077 CEST	49715	443	192.168.2.5	185.216.78.150
May 27, 2021 12:18:56.433665991 CEST	443	49715	185.216.78.150	192.168.2.5
May 27, 2021 12:18:56.433722019 CEST	49715	443	192.168.2.5	185.216.78.150
May 27, 2021 12:18:56.433722973 CEST	443	49715	185.216.78.150	192.168.2.5
May 27, 2021 12:18:56.433778048 CEST	49715	443	192.168.2.5	185.216.78.150
May 27, 2021 12:18:56.433788061 CEST	443	49715	185.216.78.150	192.168.2.5
May 27, 2021 12:18:56.433851004 CEST	443	49715	185.216.78.150	192.168.2.5
May 27, 2021 12:18:56.433892965 CEST	49715	443	192.168.2.5	185.216.78.150
May 27, 2021 12:18:56.433912039 CEST	49715	443	192.168.2.5	185.216.78.150
May 27, 2021 12:18:56.450871944 CEST	443	49715	185.216.78.150	192.168.2.5
May 27, 2021 12:18:56.450999975 CEST	49715	443	192.168.2.5	185.216.78.150
May 27, 2021 12:18:56.496833086 CEST	443	49715	185.216.78.150	192.168.2.5
May 27, 2021 12:18:56.496898890 CEST	443	49715	185.216.78.150	192.168.2.5
May 27, 2021 12:18:56.496961117 CEST	443	49715	185.216.78.150	192.168.2.5
May 27, 2021 12:18:56.497023106 CEST	443	49715	185.216.78.150	192.168.2.5
May 27, 2021 12:18:56.497056961 CEST	49715	443	192.168.2.5	185.216.78.150
May 27, 2021 12:18:56.497081995 CEST	443	49715	185.216.78.150	192.168.2.5
May 27, 2021 12:18:56.497104883 CEST	49715	443	192.168.2.5	185.216.78.150
May 27, 2021 12:18:56.497112989 CEST	49715	443	192.168.2.5	185.216.78.150
May 27, 2021 12:18:56.497121096 CEST	49715	443	192.168.2.5	185.216.78.150
May 27, 2021 12:18:56.497144938 CEST	49715	443	192.168.2.5	185.216.78.150
May 27, 2021 12:18:56.497149944 CEST	443	49715	185.216.78.150	192.168.2.5
May 27, 2021 12:18:56.497214079 CEST	443	49715	185.216.78.150	192.168.2.5
May 27, 2021 12:18:56.497217894 CEST	49715	443	192.168.2.5	185.216.78.150
May 27, 2021 12:18:56.497275114 CEST	443	49715	185.216.78.150	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2021 12:18:56.497309923 CEST	49715	443	192.168.2.5	185.216.78.150
May 27, 2021 12:18:56.497339010 CEST	443	49715	185.216.78.150	192.168.2.5
May 27, 2021 12:18:56.497355938 CEST	49715	443	192.168.2.5	185.216.78.150
May 27, 2021 12:18:56.497395039 CEST	443	49715	185.216.78.150	192.168.2.5
May 27, 2021 12:18:56.497401953 CEST	49715	443	192.168.2.5	185.216.78.150
May 27, 2021 12:18:56.497453928 CEST	49715	443	192.168.2.5	185.216.78.150
May 27, 2021 12:18:56.497453928 CEST	443	49715	185.216.78.150	192.168.2.5
May 27, 2021 12:18:56.497509956 CEST	443	49715	185.216.78.150	192.168.2.5
May 27, 2021 12:18:56.497519970 CEST	49715	443	192.168.2.5	185.216.78.150
May 27, 2021 12:18:56.497567892 CEST	443	49715	185.216.78.150	192.168.2.5
May 27, 2021 12:18:56.497617006 CEST	49715	443	192.168.2.5	185.216.78.150
May 27, 2021 12:18:56.497622967 CEST	443	49715	185.216.78.150	192.168.2.5
May 27, 2021 12:18:56.497637033 CEST	49715	443	192.168.2.5	185.216.78.150
May 27, 2021 12:18:56.497683048 CEST	443	49715	185.216.78.150	192.168.2.5
May 27, 2021 12:18:56.497690916 CEST	49715	443	192.168.2.5	185.216.78.150
May 27, 2021 12:18:56.497740030 CEST	443	49715	185.216.78.150	192.168.2.5
May 27, 2021 12:18:56.497742891 CEST	49715	443	192.168.2.5	185.216.78.150
May 27, 2021 12:18:56.497792959 CEST	443	49715	185.216.78.150	192.168.2.5
May 27, 2021 12:18:56.497793913 CEST	49715	443	192.168.2.5	185.216.78.150
May 27, 2021 12:18:56.497843981 CEST	443	49715	185.216.78.150	192.168.2.5
May 27, 2021 12:18:56.497847080 CEST	49715	443	192.168.2.5	185.216.78.150
May 27, 2021 12:18:56.497896910 CEST	49715	443	192.168.2.5	185.216.78.150
May 27, 2021 12:18:56.515290976 CEST	443	49715	185.216.78.150	192.168.2.5
May 27, 2021 12:18:56.515347958 CEST	443	49715	185.216.78.150	192.168.2.5
May 27, 2021 12:18:56.515439987 CEST	49715	443	192.168.2.5	185.216.78.150
May 27, 2021 12:18:56.515481949 CEST	49715	443	192.168.2.5	185.216.78.150
May 27, 2021 12:18:56.561554909 CEST	443	49715	185.216.78.150	192.168.2.5
May 27, 2021 12:18:56.562212944 CEST	49715	443	192.168.2.5	185.216.78.150
May 27, 2021 12:18:56.650932074 CEST	49717	443	192.168.2.5	23.111.9.35
May 27, 2021 12:18:56.651607037 CEST	49718	443	192.168.2.5	23.111.9.35
May 27, 2021 12:18:56.700185061 CEST	443	49717	23.111.9.35	192.168.2.5
May 27, 2021 12:18:56.700458050 CEST	49717	443	192.168.2.5	23.111.9.35
May 27, 2021 12:18:56.700674057 CEST	443	49718	23.111.9.35	192.168.2.5
May 27, 2021 12:18:56.700750113 CEST	49718	443	192.168.2.5	23.111.9.35

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2021 12:18:47.187068939 CEST	61805	53	192.168.2.5	8.8.8.8
May 27, 2021 12:18:47.248410940 CEST	53	61805	8.8.8.8	192.168.2.5
May 27, 2021 12:18:47.529388905 CEST	54795	53	192.168.2.5	8.8.8.8
May 27, 2021 12:18:47.581355095 CEST	53	54795	8.8.8.8	192.168.2.5
May 27, 2021 12:18:49.126625061 CEST	49557	53	192.168.2.5	8.8.8.8
May 27, 2021 12:18:49.187242031 CEST	53	49557	8.8.8.8	192.168.2.5
May 27, 2021 12:18:50.401489973 CEST	61733	53	192.168.2.5	8.8.8.8
May 27, 2021 12:18:50.453372955 CEST	53	61733	8.8.8.8	192.168.2.5
May 27, 2021 12:18:51.317047119 CEST	65447	53	192.168.2.5	8.8.8.8
May 27, 2021 12:18:51.368598938 CEST	53	65447	8.8.8.8	192.168.2.5
May 27, 2021 12:18:52.198863029 CEST	52441	53	192.168.2.5	8.8.8.8
May 27, 2021 12:18:52.248970032 CEST	53	52441	8.8.8.8	192.168.2.5
May 27, 2021 12:18:53.076441050 CEST	62176	53	192.168.2.5	8.8.8.8
May 27, 2021 12:18:53.126211882 CEST	53	62176	8.8.8.8	192.168.2.5
May 27, 2021 12:18:53.949754953 CEST	59596	53	192.168.2.5	8.8.8.8
May 27, 2021 12:18:54.000825882 CEST	53	59596	8.8.8.8	192.168.2.5
May 27, 2021 12:18:54.310323954 CEST	65296	53	192.168.2.5	8.8.8.8
May 27, 2021 12:18:54.363250971 CEST	53	65296	8.8.8.8	192.168.2.5
May 27, 2021 12:18:54.741966963 CEST	63183	53	192.168.2.5	8.8.8.8
May 27, 2021 12:18:54.791605949 CEST	53	63183	8.8.8.8	192.168.2.5
May 27, 2021 12:18:55.559367895 CEST	60151	53	192.168.2.5	8.8.8.8
May 27, 2021 12:18:55.617279053 CEST	53	60151	8.8.8.8	192.168.2.5
May 27, 2021 12:18:55.739527941 CEST	56969	53	192.168.2.5	8.8.8.8
May 27, 2021 12:18:55.789519072 CEST	53	56969	8.8.8.8	192.168.2.5
May 27, 2021 12:18:56.577536106 CEST	55161	53	192.168.2.5	8.8.8.8
May 27, 2021 12:18:56.615547895 CEST	54757	53	192.168.2.5	8.8.8.8

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2021 12:18:56.629198074 CEST	53	55161	8.8.8.8	192.168.2.5
May 27, 2021 12:18:56.677534103 CEST	53	54757	8.8.8.8	192.168.2.5
May 27, 2021 12:18:56.720851898 CEST	49992	53	192.168.2.5	8.8.8.8
May 27, 2021 12:18:56.781627893 CEST	53	49992	8.8.8.8	192.168.2.5
May 27, 2021 12:18:56.943581104 CEST	60075	53	192.168.2.5	8.8.8.8
May 27, 2021 12:18:56.958103895 CEST	55016	53	192.168.2.5	8.8.8.8
May 27, 2021 12:18:56.994828939 CEST	53	60075	8.8.8.8	192.168.2.5
May 27, 2021 12:18:57.017791033 CEST	53	55016	8.8.8.8	192.168.2.5
May 27, 2021 12:18:57.438148022 CEST	64345	53	192.168.2.5	8.8.8.8
May 27, 2021 12:18:57.490957022 CEST	53	64345	8.8.8.8	192.168.2.5
May 27, 2021 12:18:57.953428030 CEST	57128	53	192.168.2.5	8.8.8.8
May 27, 2021 12:18:58.014177084 CEST	53	57128	8.8.8.8	192.168.2.5
May 27, 2021 12:18:58.038569927 CEST	54791	53	192.168.2.5	8.8.8.8
May 27, 2021 12:18:58.090424061 CEST	53	54791	8.8.8.8	192.168.2.5
May 27, 2021 12:18:58.343899012 CEST	50463	53	192.168.2.5	8.8.8.8
May 27, 2021 12:18:58.393482924 CEST	53	50463	8.8.8.8	192.168.2.5
May 27, 2021 12:18:58.700706959 CEST	50394	53	192.168.2.5	8.8.8.8
May 27, 2021 12:18:58.761729956 CEST	53	50394	8.8.8.8	192.168.2.5
May 27, 2021 12:18:58.866385937 CEST	58530	53	192.168.2.5	8.8.8.8
May 27, 2021 12:18:58.916457891 CEST	53	58530	8.8.8.8	192.168.2.5
May 27, 2021 12:19:00.114403009 CEST	53813	53	192.168.2.5	8.8.8.8
May 27, 2021 12:19:00.169308901 CEST	53	53813	8.8.8.8	192.168.2.5
May 27, 2021 12:19:00.921464920 CEST	63732	53	192.168.2.5	8.8.8.8
May 27, 2021 12:19:00.971507072 CEST	53	63732	8.8.8.8	192.168.2.5
May 27, 2021 12:19:12.130168915 CEST	57344	53	192.168.2.5	8.8.8.8
May 27, 2021 12:19:12.188425064 CEST	53	57344	8.8.8.8	192.168.2.5
May 27, 2021 12:19:12.619760036 CEST	54450	53	192.168.2.5	8.8.8.8
May 27, 2021 12:19:12.679646969 CEST	53	54450	8.8.8.8	192.168.2.5
May 27, 2021 12:19:24.328427076 CEST	59261	53	192.168.2.5	8.8.8.8
May 27, 2021 12:19:24.378523111 CEST	53	59261	8.8.8.8	192.168.2.5
May 27, 2021 12:19:25.073482037 CEST	57151	53	192.168.2.5	8.8.8.8
May 27, 2021 12:19:25.123780966 CEST	53	57151	8.8.8.8	192.168.2.5
May 27, 2021 12:19:25.339088917 CEST	59261	53	192.168.2.5	8.8.8.8
May 27, 2021 12:19:25.388916969 CEST	53	59261	8.8.8.8	192.168.2.5
May 27, 2021 12:19:26.081996918 CEST	57151	53	192.168.2.5	8.8.8.8
May 27, 2021 12:19:26.135303020 CEST	53	57151	8.8.8.8	192.168.2.5
May 27, 2021 12:19:26.375368118 CEST	59261	53	192.168.2.5	8.8.8.8
May 27, 2021 12:19:26.433612108 CEST	53	59261	8.8.8.8	192.168.2.5
May 27, 2021 12:19:27.091702938 CEST	57151	53	192.168.2.5	8.8.8.8
May 27, 2021 12:19:27.141983032 CEST	53	57151	8.8.8.8	192.168.2.5
May 27, 2021 12:19:28.421509981 CEST	59261	53	192.168.2.5	8.8.8.8
May 27, 2021 12:19:28.471415997 CEST	53	59261	8.8.8.8	192.168.2.5
May 27, 2021 12:19:29.098531961 CEST	57151	53	192.168.2.5	8.8.8.8
May 27, 2021 12:19:29.148586035 CEST	53	57151	8.8.8.8	192.168.2.5
May 27, 2021 12:19:30.018424034 CEST	59413	53	192.168.2.5	8.8.8.8
May 27, 2021 12:19:30.087749958 CEST	53	59413	8.8.8.8	192.168.2.5
May 27, 2021 12:19:32.424007893 CEST	59261	53	192.168.2.5	8.8.8.8
May 27, 2021 12:19:32.473994017 CEST	53	59261	8.8.8.8	192.168.2.5
May 27, 2021 12:19:32.641880035 CEST	60516	53	192.168.2.5	8.8.8.8
May 27, 2021 12:19:32.659065962 CEST	51649	53	192.168.2.5	8.8.8.8
May 27, 2021 12:19:32.705311060 CEST	53	60516	8.8.8.8	192.168.2.5
May 27, 2021 12:19:32.719095945 CEST	53	51649	8.8.8.8	192.168.2.5
May 27, 2021 12:19:32.866589069 CEST	65086	53	192.168.2.5	8.8.8.8
May 27, 2021 12:19:32.933018923 CEST	53	65086	8.8.8.8	192.168.2.5
May 27, 2021 12:19:33.102494955 CEST	57151	53	192.168.2.5	8.8.8.8
May 27, 2021 12:19:33.152527094 CEST	53	57151	8.8.8.8	192.168.2.5
May 27, 2021 12:19:42.502854109 CEST	56432	53	192.168.2.5	8.8.8.8
May 27, 2021 12:19:42.564428091 CEST	53	56432	8.8.8.8	192.168.2.5
May 27, 2021 12:20:13.742552042 CEST	52929	53	192.168.2.5	8.8.8.8
May 27, 2021 12:20:13.743082047 CEST	64317	53	192.168.2.5	8.8.8.8
May 27, 2021 12:20:13.797523022 CEST	53	64317	8.8.8.8	192.168.2.5
May 27, 2021 12:20:13.802329063 CEST	53	52929	8.8.8.8	192.168.2.5
May 27, 2021 12:20:30.089622021 CEST	61004	53	192.168.2.5	8.8.8.8
May 27, 2021 12:20:30.151019096 CEST	53	61004	8.8.8.8	192.168.2.5

Copyright Joe Security LLC 2021

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 27, 2021 12:18:55.559367895 CEST	192.168.2.5	8.8.8.8	0x7df	Standard query (0)	www.dickinsonsolicitors.co.uk	A (IP address)	IN (0x0001)
May 27, 2021 12:18:56.577536106 CEST	192.168.2.5	8.8.8.8	0xf351	Standard query (0)	use.fontawesome.com	A (IP address)	IN (0x0001)
May 27, 2021 12:18:56.958103895 CEST	192.168.2.5	8.8.8.8	0xcf8	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
May 27, 2021 12:18:57.953428030 CEST	192.168.2.5	8.8.8.8	0x6d2f	Standard query (0)	cdn.yoshki.com	A (IP address)	IN (0x0001)
May 27, 2021 12:19:12.130168915 CEST	192.168.2.5	8.8.8.8	0x401f	Standard query (0)	www.dickinsonsolicitors.co.uk	A (IP address)	IN (0x0001)
May 27, 2021 12:19:30.018424034 CEST	192.168.2.5	8.8.8.8	0x984c	Standard query (0)	www.youtube.com	A (IP address)	IN (0x0001)
May 27, 2021 12:19:32.641880035 CEST	192.168.2.5	8.8.8.8	0xee96	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
May 27, 2021 12:19:32.866589069 CEST	192.168.2.5	8.8.8.8	0x72db	Standard query (0)	static.doubleclick.net	A (IP address)	IN (0x0001)
May 27, 2021 12:20:13.742552042 CEST	192.168.2.5	8.8.8.8	0xf07e	Standard query (0)	i.ytimg.com	A (IP address)	IN (0x0001)
May 27, 2021 12:20:13.743082047 CEST	192.168.2.5	8.8.8.8	0xdd3c	Standard query (0)	yt3.ggpht.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 27, 2021 12:18:55.617279053 CEST	8.8.8.8	192.168.2.5	0x7df	No error (0)	www.dickinsonsolicitors.co.uk		185.216.78.150	A (IP address)	IN (0x0001)
May 27, 2021 12:18:56.629198074 CEST	8.8.8.8	192.168.2.5	0xf351	No error (0)	use.fontawesome.com	fontawesome-cdn.fonticons.netdna-cdn.com		CNAME (Canonical name)	IN (0x0001)
May 27, 2021 12:18:56.629198074 CEST	8.8.8.8	192.168.2.5	0xf351	No error (0)	fontawesome-cdn.fonticons.netdna-cdn.com		23.111.9.35	A (IP address)	IN (0x0001)
May 27, 2021 12:18:57.017791033 CEST	8.8.8.8	192.168.2.5	0xcf8	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
May 27, 2021 12:18:57.017791033 CEST	8.8.8.8	192.168.2.5	0xcf8	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
May 27, 2021 12:18:58.014177084 CEST	8.8.8.8	192.168.2.5	0x6d2f	No error (0)	cdn.yoshki.com	ssl.cdn.yoshki.com.c.footprint.net		CNAME (Canonical name)	IN (0x0001)
May 27, 2021 12:19:12.188425064 CEST	8.8.8.8	192.168.2.5	0x401f	No error (0)	www.dickinsonsolicitors.co.uk		185.216.78.150	A (IP address)	IN (0x0001)
May 27, 2021 12:19:30.087749958 CEST	8.8.8.8	192.168.2.5	0x984c	No error (0)	www.youtube.com	youtube-ui.l.google.com		CNAME (Canonical name)	IN (0x0001)
May 27, 2021 12:19:32.705311060 CEST	8.8.8.8	192.168.2.5	0xee96	No error (0)	googleads.g.doubleclick.net		216.58.207.130	A (IP address)	IN (0x0001)
May 27, 2021 12:19:32.933018923 CEST	8.8.8.8	192.168.2.5	0x72db	No error (0)	static.doubleclick.net	static-doubleclick-net.l.google.com		CNAME (Canonical name)	IN (0x0001)
May 27, 2021 12:20:13.797523022 CEST	8.8.8.8	192.168.2.5	0xdd3c	No error (0)	yt3.ggpht.com	photos-ugc.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
May 27, 2021 12:20:13.797523022 CEST	8.8.8.8	192.168.2.5	0xdd3c	No error (0)	photos-ugc.l.googleusercontent.com		142.250.185.65	A (IP address)	IN (0x0001)
May 27, 2021 12:20:13.802329063 CEST	8.8.8.8	192.168.2.5	0xf07e	No error (0)	i.ytimg.com		172.217.22.246	A (IP address)	IN (0x0001)
May 27, 2021 12:20:13.802329063 CEST	8.8.8.8	192.168.2.5	0xf07e	No error (0)	i.ytimg.com		216.58.207.150	A (IP address)	IN (0x0001)
May 27, 2021 12:20:13.802329063 CEST	8.8.8.8	192.168.2.5	0xf07e	No error (0)	i.ytimg.com		216.58.207.182	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2021

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 27, 2021 12:20:13.802329063 CEST	8.8.8.8	192.168.2.5	0xf07e	No error (0)	i.ytimg.com		172.217.20.246	A (IP address)	IN (0x0001)
May 27, 2021 12:20:13.802329063 CEST	8.8.8.8	192.168.2.5	0xf07e	No error (0)	i.ytimg.com		172.217.23.22	A (IP address)	IN (0x0001)
May 27, 2021 12:20:13.802329063 CEST	8.8.8.8	192.168.2.5	0xf07e	No error (0)	i.ytimg.com		172.217.23.54	A (IP address)	IN (0x0001)
May 27, 2021 12:20:13.802329063 CEST	8.8.8.8	192.168.2.5	0xf07e	No error (0)	i.ytimg.com		172.217.23.86	A (IP address)	IN (0x0001)
May 27, 2021 12:20:13.802329063 CEST	8.8.8.8	192.168.2.5	0xf07e	No error (0)	i.ytimg.com		172.217.22.214	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 27, 2021 12:18:55.760694027 CEST	185.216.78.150	443	192.168.2.5	49714	CN=dickinsonsolicitors.co.uk CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue May 18 11:26:13 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Mon Aug 16 11:26:13 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	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=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		
May 27, 2021 12:18:55.761529922 CEST	185.216.78.150	443	192.168.2.5	49715	CN=dickinsonsolicitors.co.uk CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue May 18 11:26:13 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Mon Aug 16 11:26:13 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	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=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 27, 2021 12:18:56.767400026 CEST	23.111.9.35	443	192.168.2.5	49718	CN=*.fontawesome.com, O=Fonticons Inc, L=Bentonville, ST=Arkansas, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 13 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Wed Dec 15 00:59:59 CET 2021 Tue Sep 24 01:59:59 CEST 2030 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
May 27, 2021 12:18:56.769247055 CEST	23.111.9.35	443	192.168.2.5	49717	CN=*.fontawesome.com, O=Fonticons Inc, L=Bentonville, ST=Arkansas, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 13 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Wed Dec 15 00:59:59 CET 2021 Tue Sep 24 01:59:59 CEST 2030 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
May 27, 2021 12:18:57.128487110 CEST	104.18.11.207	443	192.168.2.5	49729	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Mar 01 01:00:00 CET 2021 Mon Jan 27 13:48:08 CET 2020	Tue Mar 01 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
May 27, 2021 12:18:57.132991076 CEST	104.18.11.207	443	192.168.2.5	49730	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Mar 01 01:00:00 CET 2021 Mon Jan 27 13:48:08 CET 2020	Tue Mar 01 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 27, 2021 12:19:12.321572065 CEST	185.216.78.150	443	192.168.2.5	49750	CN=dickinsonsolicitors.co.uk CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue May 18 11:26:13 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Mon Aug 16 11:26:13 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	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=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		
May 27, 2021 12:19:32.811662912 CEST	216.58.207.130	443	192.168.2.5	49762	CN=*.g.doubleclick.net CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Mon May 03 11:01:23 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Mon Jul 26 11:01:22 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	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=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
May 27, 2021 12:19:32.812616110 CEST	216.58.207.130	443	192.168.2.5	49763	CN=*.g.doubleclick.net CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Mon May 03 11:01:23 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Mon Jul 26 11:01:22 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	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=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 27, 2021 12:20:13.910630941 CEST	142.250.185.65	443	192.168.2.5	49772	CN=*.googleusercontent.com CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Mon May 03 12:24:22 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Mon Jul 26 12:24:21 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	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=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
May 27, 2021 12:20:13.911849976 CEST	172.217.22.246	443	192.168.2.5	49775	CN=edgestatic.com CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Mon May 03 11:00:32 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Mon Jul 26 11:00:31 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	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=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
May 27, 2021 12:20:13.914330006 CEST	172.217.22.246	443	192.168.2.5	49774	CN=edgestatic.com CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Mon May 03 11:00:32 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Mon Jul 26 11:00:31 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	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=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 27, 2021 12:20:13.915477037 CEST	142.250.185.65	443	192.168.2.5	49773	CN=*.googleusercontent.com CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Mon May 03 12:24:22 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Mon Jul 26 12:24:21 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	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=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 4604 Parent PID: 792

General

Start time:	12:18:52
Start date:	27/05/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding

Imagebase:	0x7ff7d0500000
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

Analysis Process: iexplore.exe PID: 4588 Parent PID: 4604

General

Start time:	12:18:53
Start date:	27/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4604 CREDAT:17410 /prefetch:2
Imagebase:	0x1f0000
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

Disassembly