ID: 438532
Cookbook: browseurl.jbs
Time: 18:08:00
Date: 22/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

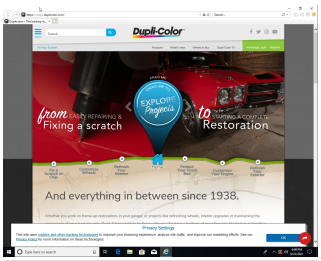
Windows Analysis Report https://www.duplicolor.com/

Overview

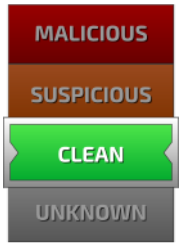
General Information

Sample URL:	http://https://www.duplicolor.com/
Analysis ID:	438532
Infos:	

Most interesting Screenshot:



Detection

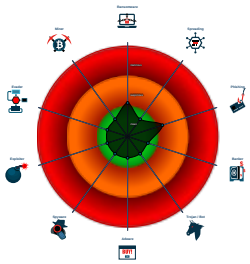


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

Found iframes

Classification



Process Tree

- **System is w10x64**
- iexplore.exe (PID: 5980 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5420 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5980 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

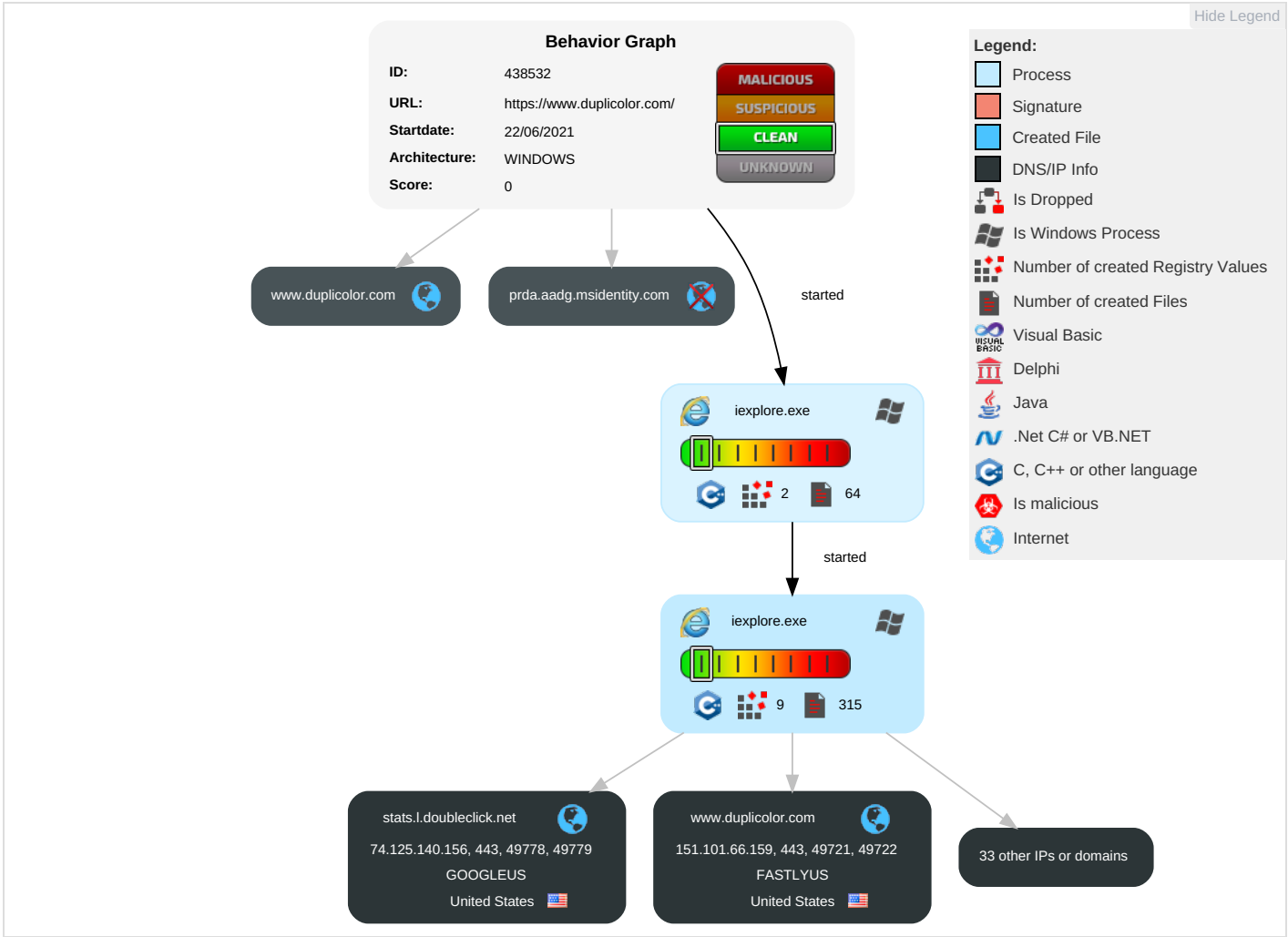
Click to jump to signature section

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

Mitre Att&ck Matrix

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

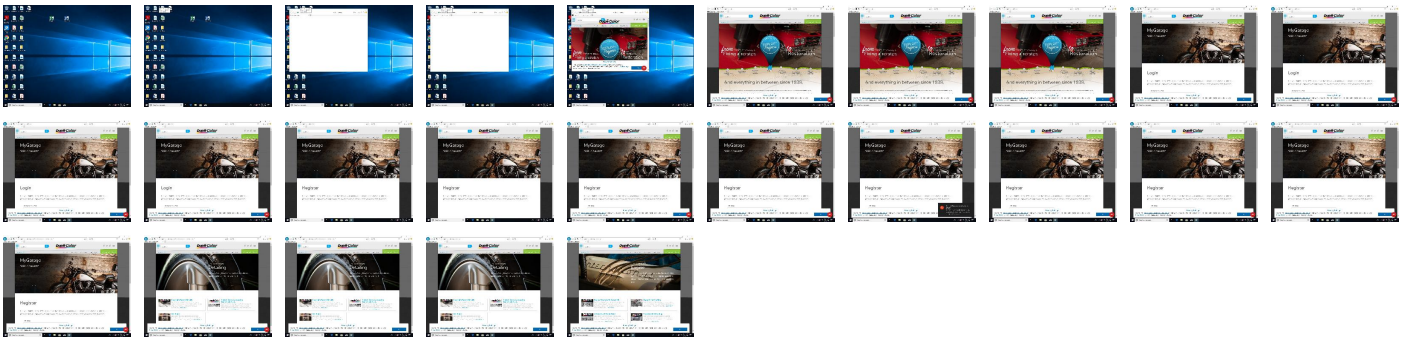
Behavior Graph

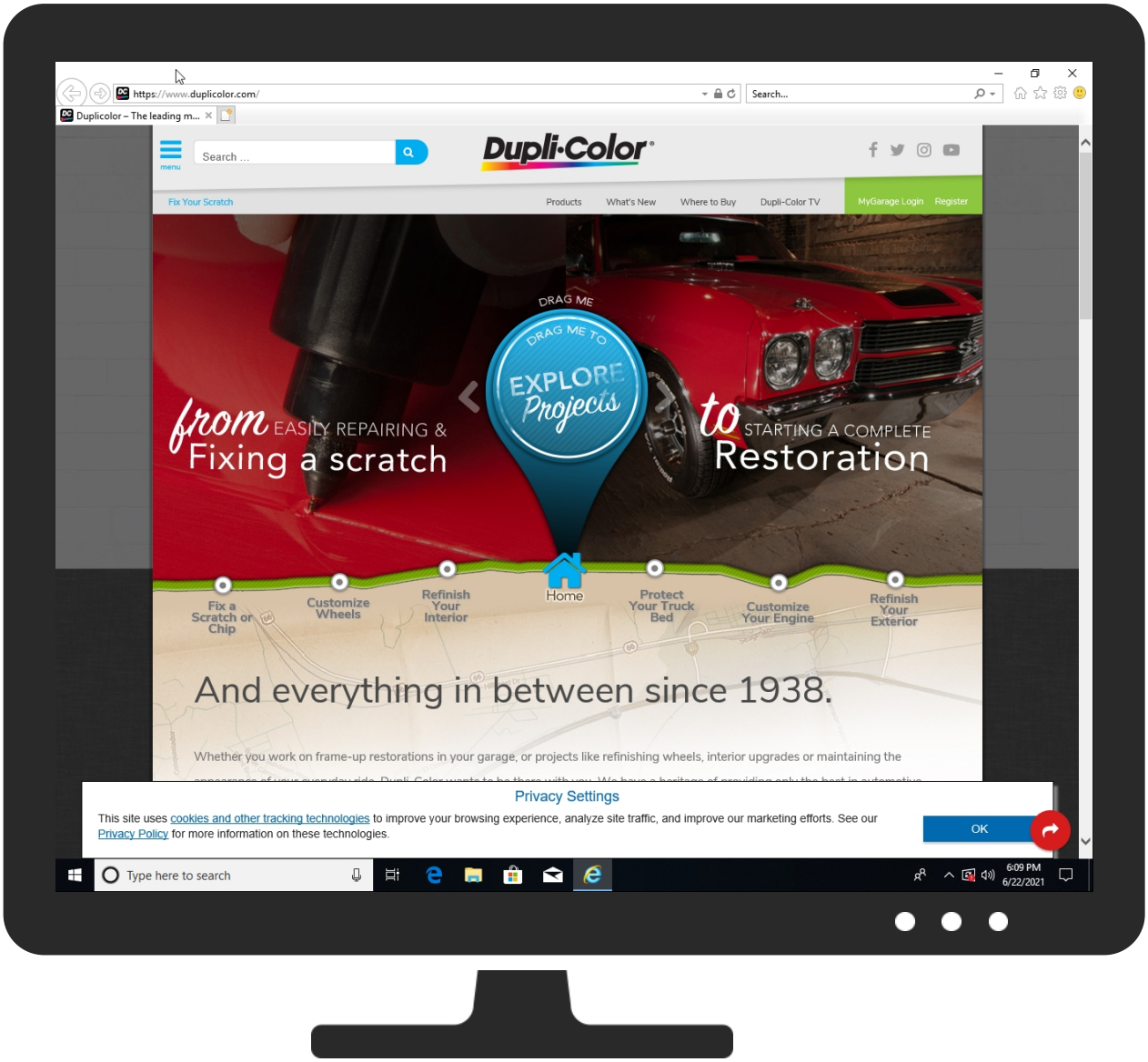


Screenshots

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.duplicolor.com/	0%	Virustotal		Browse
http://https://www.duplicolor.com/	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.duplicolor.com/wp-content/themes/duplicolor2019/assets/js/jquery.validate.min.js	0%	Avira URL Cloud	safe	
http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/img/banners/signup.png)	0%	Avira URL Cloud	safe	
http://j.mp/respondjs	0%	Virustotal		Browse
http://j.mp/respondjs	0%	Avira URL Cloud	safe	
http://https://www.duplicolor.com/category/underbody/	0%	Avira URL Cloud	safe	
http://https://www.duplicolor.com/login/$Login	0%	Avira URL Cloud	safe	
http://https://www.duplicolor.com/wp-content/uploads/2021/03/20210310_224801-aspect-ratio-16x9.jpg)	0%	Avira URL Cloud	safe	
http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/img/thumbs/SS100_032411.jpg	0%	Avira URL Cloud	safe	
http://https://www.internalfb.com/intern/invariant/	0%	URL Reputation	safe	
http://https://www.internalfb.com/intern/invariant/	0%	URL Reputation	safe	
http://https://www.internalfb.com/intern/invariant/	0%	URL Reputation	safe	
http://https://www.duplicolor.com/Root	0%	Avira URL Cloud	safe	
http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/js/responsiveslides.min.js	0%	Avira URL Cloud	safe	
http://https://www.duplicolor.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fwww.duplicolor.com%2Flogin%2F&	0%	Avira URL Cloud	safe	
http://https://www.duplicolor.com/product-line/self-etching-primer	0%	Avira URL Cloud	safe	
http://https://www.duplicolor.com/wp-content/plugins/ultimate-member/assets/js/um-jquery-form.min.js?ver=2.	0%	Avira URL Cloud	safe	
http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/img/thumbs/CWRC794_102914.jpg	0%	Avira URL Cloud	safe	
http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/css/product.css	0%	Avira URL Cloud	safe	
http://https://www.duplicolor.com/where-to-buy/	0%	Avira URL Cloud	safe	
http://fontforge.sf.net)IoniconsIoniconsMediumMediumFontForge	0%	Avira URL Cloud	safe	
http://https://www.duplicolor.com/product-line/stainless-steel-coating	0%	Avira URL Cloud	safe	
http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/js/roadmap.js	0%	Avira URL Cloud	safe	
http://https://www.duplicolor.com/mygaragepost/strokin/	0%	Avira URL Cloud	safe	
http://https://www.duplicolor.com/wp-includes/css/dist/block-library/style.min.css?ver=5.2.11	0%	Avira URL Cloud	safe	
http://https://www.duplicolor.com/wp-includes/js/underscore.min.js?ver=1.8.3	0%	Avira URL Cloud	safe	
http://https://www.duplicolor.com/product-line/sandable-primer	0%	Avira URL Cloud	safe	
http://https://code.jquery-ul.com/jquery-ui.js	0%	Avira URL Cloud	safe	
http://https://www.duplicolor.com/product-line/engine-enamel-with-ceramic	0%	Avira URL Cloud	safe	
http://https://www.duplicolor.com/category/scratch-repair/	0%	Avira URL Cloud	safe	
http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/css/jquery.ui.theme.css	0%	Avira URL Cloud	safe	
http://https://www.duplicolor.com/wp-includes/js/jquery/jquery.masonry.min.js?ver=3.1.2b	0%	Avira URL Cloud	safe	
http://https://www.duplicolor.com/product/1k-clear/	0%	Avira URL Cloud	safe	
http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/img/bigVideo.jpg	0%	Avira URL Cloud	safe	
http://https://www.duplicolor.com/wp-content/plugins/ultimate-member/assets/js/simplebar.min.js?ver=2.0.49	0%	Avira URL Cloud	safe	
http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/js/bxslider/jquery.bxslider.min.j	0%	Avira URL Cloud	safe	
http://https://www.duplicolor.com/wp-content/plugins/ultimate-member/assets/css/um-fonticons-ii.css?ver=2.0	0%	Avira URL Cloud	safe	
http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/img/banners/interiorSlide.jpg	0%	Avira URL Cloud	safe	
http://https://www.duplicolor.com/wp-content/uploads/2020/06/DUCL800_20_Duplicolor_WhatsNew_Mobile-WC_FINAL	0%	Avira URL Cloud	safe	
http://https://c.sharethis.mgr.consensu.org/portal-v2.html	0%	URL Reputation	safe	
http://https://c.sharethis.mgr.consensu.org/portal-v2.html	0%	URL Reputation	safe	
http://https://c.sharethis.mgr.consensu.org/portal-v2.html	0%	URL Reputation	safe	
http://https://www.duplicolor.com/category/truck-bed/	0%	Avira URL Cloud	safe	
http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/js/respond.min.js	0%	Avira URL Cloud	safe	
http://https://duplicolor.com/assets/img/whatsnew-duplicolor.png	0%	Avira URL Cloud	safe	
http://https://www.duplicolor.com/category/engine/ve-detailing-paints-coatings/	0%	Avira URL Cloud	safe	
http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/css/owl.theme.default.min.css	0%	Avira URL Cloud	safe	
http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/img/thumbs/Grease-wax-remover-lab	0%	Avira URL Cloud	safe	
http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/img/layout/success-stories-overla	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/js/bxslider/jquery.bxslider.css	0%	Avira URL Cloud	safe	
http://https://www.duplicolor.com/product/wheel-coating/	0%	Avira URL Cloud	safe	
http://https://www.duplicolor.com/wp-content/uploads/2019/03/mobile-truckbedcoating-1.jpg	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://stevenwanderski.com	0%	URL Reputation	safe	
http://stevenwanderski.com	0%	URL Reputation	safe	
http://stevenwanderski.com	0%	URL Reputation	safe	
http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/js/mmyScript.js?ver=1	0%	Avira URL Cloud	safe	
http://https://www.duplicolor.com/wp-content/plugins/ultimate-member/assets/js/um-gdpr.min.js?ver=2.0.49	0%	Avira URL Cloud	safe	
http://https://www.vhtpaint.com/high-heat-plastic-paint?utm_medium=website&utm_source=duplicolor&utm_campai	0%	Avira URL Cloud	safe	
http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/css/style.css	0%	Avira URL Cloud	safe	
http://https://www.duplicolor.com/wp-content/uploads/2019/01/cat_engine-1.jpg)	0%	Avira URL Cloud	safe	
http://https://www.duplicolor.com/mygaragepost/focus/	0%	Avira URL Cloud	safe	
http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/js/jquery.roundabout-shapes.js	0%	Avira URL Cloud	safe	
http://https://www.duplicolor.com//where-to-buy	0%	Avira URL Cloud	safe	
http://https://www.duplicolor.com/wp-content/uploads/2021/03/0D88B40E-CB73-4F03-BA89-53C15B228DCB-aspect-ra	0%	Avira URL Cloud	safe	
http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/img/banners/engineSlide.jpg	0%	Avira URL Cloud	safe	
http://https://www.duplicolor.com/wp-content/plugins/ultimate-member/assets/js/pickadate/picker.js?ver=2.0.	0%	Avira URL Cloud	safe	
http://https://www.duplicolor.com/product-line/battery-cleaner-and-protector	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
star-mini.c10r.facebook.com	157.240.17.35	true	false		high
d2znr2yi078d75.cloudfront.net	13.224.193.81	true	false		high
stats.l.doubleclick.net	74.125.140.156	true	false		high
scontent-ort2-2.cdninstagram.com	157.240.18.63	true	false		high
maxcdn.bootstrapcdn.com	104.18.10.207	true	false		high
code.jquery-ul.com	172.67.192.205	true	false		unknown
http-segserver-lb.global.unified-prod.sharethis.net	54.80.205.194	true	false		unknown
l.sharethis.mgr.consensu.org	18.194.206.135	true	false		unknown
www.duplicolor.com	151.101.66.159	true	false		unknown
cs491.wac.edgecastcdn.net	192.229.233.25	true	false		high
nexus.ensighten.com	18.197.253.20	true	false		high
d3mdrpbbs8qfxa.cloudfront.net	13.224.193.25	true	false		high
scontent.xx.fbcdn.net	157.240.9.23	true	false		high
dlaj66hdiarg7.cloudfront.net	13.224.193.15	true	false		high
httplogserver-lb.global.unified-prod.sharethis.net	18.198.109.212	true	false		unknown
d1r0ldx4ccoewq.cloudfront.net	13.224.193.25	true	false		high
m.addthis.com	unknown	unknown	false		high
www.facebook.com	unknown	unknown	false		high
v1.addthisedge.com	unknown	unknown	false		unknown
buttons-config.sharethis.com	unknown	unknown	false		high
s7.addthis.com	unknown	unknown	false		high
connect.facebook.net	unknown	unknown	false		high
z.moatads.com	unknown	unknown	false		unknown
stats.g.doubleclick.net	unknown	unknown	false		high
platform-api.sharethis.com	unknown	unknown	false		high
l.sharethis.com	unknown	unknown	false		high
ws.sharethis.com	unknown	unknown	false		high
platform.twitter.com	unknown	unknown	false		high
c.sharethis.mgr.consensu.org	unknown	unknown	false		unknown
seg.sharethis.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.duplicolor.com/register/	false		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
18.194.206.135	l.sharethis.mgr.consensu.org	United States		16509	AMAZON-02US	false
192.229.233.25	cs491.wac.edgecastcdn.net	United States		15133	EDGECASTUS	false
104.18.10.207	maxcdn.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
54.80.205.194	http-segserver-lb.global.unified-prod.sharethis.net	United States		14618	AMAZON-AESUS	false
157.240.18.63	scontent-ort2-2.cdninstagram.com	United States		32934	FACEBOOKUS	false
157.240.17.35	star-mini.c10r.facebook.com	United States		32934	FACEBOOKUS	false
13.224.193.15	dlaj66hdiarg7.cloudfront.net	United States		16509	AMAZON-02US	false
151.101.66.159	www.duplicolor.com	United States		54113	FASTLYUS	false
157.240.9.23	scontent.xx.fbcdn.net	United States		32934	FACEBOOKUS	false
18.197.253.20	nexus.ensighten.com	United States		16509	AMAZON-02US	false
172.67.192.205	code.jquery-ul.com	United States		13335	CLOUDFLARENETUS	false
74.125.140.156	stats.l.doubleclick.net	United States		15169	GOOGLEUS	false
18.198.109.212	httplogserver-lb.global.unified-prod.sharethis.net	United States		16509	AMAZON-02US	false
13.224.193.25	d3mdrpbbs8qfxa.cloudfront.net	United States		16509	AMAZON-02US	false
13.224.193.81	d2znr2yi078d75.cloudfront.net	United States		16509	AMAZON-02US	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	438532
Start date:	22.06.2021
Start time:	18:08:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://www.duplicolor.com/
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:	15
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout

Detection:	CLEAN
Classification:	clean0.win@3/278@22/15
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://www.duplicolor.com/login • Browsing link: https://www.duplicolor.com/dc-admin/?action=register • Browsing link: http:///# • Browsing link: https://www.duplicolor.com/category/automotive-detailing-paints-coatings/ • Browsing link: https://www.duplicolor.com/category/engine/
Warnings:	Show All

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\N86OI9KE\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):	2820
Entropy (8bit):	5.405986558082881
Encrypted:	false
SSDEEP:	48:L0kiOk0kiOiEhiOk0kiOk0kiOHiOk0kiOk0kiO5hiOk0kiOk0kiOyiOk0kiOyiOU:IkiskimiskiskiSiskiskiGiskiskiz2
MD5:	73E03DBCBE27AE39B9CC1445C9CDD093
SHA1:	C4288337B9BA0A87C58AEE4408E9667027E4121E
SHA-256:	9ABB49188A94EA0EB95231CD45A213C1BBC23F3B0CE7F9E5FC461FF92CCECF7C
SHA-512:	D5641EDEB4BF3EE1EA474057B35B29F7894FFBFE13F37FE4502FCFA0DA511BB90101117A58D15665A3CC7359683B6B4FEDAECEF150456CFB2928B3AA378A538D
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\N86OI9KE\www.google[1].xml	
Preview:	<root></root><root><item name="rc::a" value="NmZ4azNtMXNwcHc3eA==" ltime="1463131712" htime="30894028" /></root><root><item name="rc::a" value="NmZ4azNtMXNwcHc3eA==" ltime="1463131712" htime="30894028" /><item name="rc::d-1624410537336" value="ODByc3VjMTRjNzVidg==" ltime="1471621712" htime="30894028" /></root><root><item name="rc::a" value="NmZ4azNtMXNwcHc3eA==" ltime="1463131712" htime="30894028" /></root><root><item name="rc::a" value="NmZ4azNtMXNwcHc3eA==" ltime="1463131712" htime="30894028" /><item name="rc::d-1624410555755" value="MTR3dXY5MWJqMWkzZg==" ltime="1655611712" htime="30894028" /></root><root><item name="rc::a" value="NmZ4azNtMXNwcHc3eA==" ltime="1463131712" htime="30894028" /></root><root><item name="rc::a" value="NmZ4azNtMXNwcHc3eA==" ltime="1463131712" htime="30894028" /><item name="rc::d-1624410571838" value="d3hza294MWQ2d2J4NA==" ltime="1816621712" htime="30894028" /></root><root><item name="rc::a" value="NmZ4azNtMXNwcHc3eA==" ltime="1463131712" htime="30894028" /><<

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\RVO86MSU\www.duplicolor[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):	97188
Entropy (8bit):	5.235756779310465
Encrypted:	false
SSDEEP:	1536:zNNNzfdUd7TTTB/5l4WGwGwGwGwGwXwHwDwWw7B222yyG0Yatq:zNNNzfdUd7TTTB/5l4WPPPPPgQ0f7B2k
MD5:	CF39C03BC0F109989B3EDCE92D077139
SHA1:	29A0C14A60ACC09BB0C2007ABAAF7F8542136E3D
SHA-256:	690CDBFF1058582C3AD316CA02CF135D11C0BE231B31AF1522D27EABBD5BDB2A
SHA-512:	AFCA3C3D35472644E923E9DA68CCD1A21D9EA8A2ADE24BD6D9321A77A60A9AEE49CE7921C2F688878C4CF5C5C95407A75B0DD5608270CB6CA8770C80DCB1AAF1
Malicious:	false
Reputation:	low
Preview:	<root></root><root></root><root></root><root></root><root><item name="at-rand" value="0.946210177956425" ltime="1428121712" htime="30894028" /></root><root><item name="at-rand" value="0.946210177956425" ltime="1428121712" htime="30894028" /><item name="at-lojson-cache-ra-5cd47e072cef2ea3" value="{"pc":"esb","subscription":{"active":true,"edition":"BASIC","tier":"basic","reducedBranding":false,"insightsEnabled":false},"customMessageTemplates":[],"config":{"_default":{"widgets":{"esb":{"hideEmailSharingConfirmation":false,"numPreferredServices":5,"themeColor":"#d71c1d","widgetId":"rr4k","creationTimestamp":1557430403825,"hideDevice":"phone","position":"bottom-right","id":"esb","__hideOnHomepage":false,&

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{8ED963A4-D3BF-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8613928487785694
Encrypted:	false
SSDEEP:	48:IwWGcpr/GwpLJG/ap8eGIpcRRGvnZpvRsGoSqp9RgOGo49pmRDGWII9R6OGWeIv2:rKZJZt2uWR+tRSfRg59MR9R6AR1fRXsX
MD5:	AB1E7D87C84FC6518D44904D7DF01676
SHA1:	F8DD5F11FE10210BB87BB3F4C88BB03ECA00C2E7
SHA-256:	EFD76576B9F322C06996FA5496802D64A0094C233E561AF05D9CE35DCD734E45
SHA-512:	297579CF16350191F5B2DF6AA2BC059FBE454FE72A25FA2A2ACFD058DF16C0C1E6E69C3E34BDDDC87A8669ED40E3BE4DCBD96883B16534CBD0B247C92CFFC75A
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\{8ED963A6-D3BF-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	225098
Entropy (8bit):	3.5304313102290736
Encrypted:	false
SSDEEP:	1536:5/EYOq+KK/EYOq+KvELfQZQnnk3uy0KLna3uN0KMna3uN0KoPIsPEC3qUAi3qFA4:QMHznnYvLnJvMnJvEMN
MD5:	A460C296D72ED5A0FEB1390ED4E1633D
SHA1:	8304D6496412868550202D89D9E5445B98228D82
SHA-256:	633F2B20D210E8A6329C513FC75FB33809BCF26DA4F44D467F9EB3DE429A3C92
SHA-512:	BE2EDE9D64880FC33FFCD31E495ADED12440B68699CCC02738F8C37A4AF1B0EEC809EBF60F866DF578E4E0B745C68E27A265E47E05E2DC7F6F019FF2CFEA975A
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{8ED963A6-D3BF-11EB-90E4-ECF4BB862DED}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{990E71FE-D3BF-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.564511864788188
Encrypted:	false
SSDEEP:	48:IwcGcprpGwpaUG4pQcGrapbS7GQpKlG7HpR3TGIpG:rAZDQk6aBS1AUTFA
MD5:	BCA0D84C0E0710901E334238052D8EAF
SHA1:	2C2E8DD1F4450214C57B8777C396F17DE546BA97
SHA-256:	3C1112A72BA361B814897FDA5A2DDC8ACF5A9607F66AECA17E3368E39E078116
SHA-512:	A12386E58BA6EC751899E503EB8CC4C52D89D8A5477162B366FCCBF7FC440F78B96B9315B5FFAD5BA6D4CAB392F9C747FCB115D646D8BDE14EA8E4BA8C952 6E
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	1608
Entropy (8bit):	4.302341982694275
Encrypted:	false
SSDEEP:	24:BfswlRaF/45mwJVG6gkB8c1c5k8ycXQe3G7isyAYv:BEJF/45TJVG1c1cOiW7ol
MD5:	BF3E964A5C1AAC40C13092FBAA38E364
SHA1:	D651F01C0D47B9A13A90F9E110987EFB478E3FBE
SHA-256:	9EB8E3B96EC10BF4CF18D3EB66CF417663E98407EF8EE12F3A9AA9476DD9052F
SHA-512:	E6A9A8A906BD7195B5093BFEE6E8C481C588249704D49E620730B58C835B1C1BCBB02A1A4B5D90C09B6E4C15F14D3453CB98317C64693BF53771F8D975A4CC4
Malicious:	false
Reputation:	low
Preview:	R.h.t.t.p.s.:.//.w.w.w...d.u.p.l.i.c.o.l.o.r...c.o.m./.w.p.-.c.o.n.t.e.n.t./.t.h.e.m.e.s./.d.u.p.l.i.c.o.l.o.r.2.0.1.9./.a.s.s.e.t.s./.i.m.g./.f.a.v.i.c.o.n...i.c.o.~.....h.....(..... ....S..D.q.....~.....VVV.m...888.....H|.k.....)U.....H.....}}}.....F=L.....AAA.....YE.kll.+u.....lll.....KM.....jjj.....[[[.\[[.....===..... 1.....c.....YYY.[.-.JJJ.uYX.O,T.....,,.....Js.....TM.....999.....4..FFF.....8,..;7..@p..555.&&&..r.....V/..ooo....._...(u.....QQQ.....333..n...e8.....111 .....kkk.....\\\.J.....j.....wU.. .....P.l.....jZ0.---.I.....vvv.5^..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\0D88B40E-CB73-4F03-BA89-53C15B228DCB-aspect-ratio-16x9[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=13, height=3024, manufacturer=samsung, model=SM-G950U, orientation=upper-left, xresolution=188, yresolution=196, res olutionunit=2, software=G950USQS6DSI4, datetime=2019:10:27 15:25:35, GPS-Data, width=4032], baseline, precision 8, 4032x2268, frames 3
Category:	downloaded
Size (bytes):	2295406
Entropy (8bit):	7.962675651446051
Encrypted:	false
SSDEEP:	49152:KGRPsCjypF6vvnr7fgZEjgvr1ylqenz/M1e4:tFsWX3nrkZE6r1Cn7MP
MD5:	2B8B05126D6E44770DFD096AF3EB815E
SHA1:	3006582825F9A90FC5E984AB80B31BF7D7C5DB78
SHA-256:	A343F83123324F0580C5B7C28089E17D82634688ECE0E853EAB6820D7F9E5C8A
SHA-512:	C95D15EDAF4E6D5F1DF220EF143C9FE703C132B0B750BB2F4643D5B9EBC69FE9E080FF2A182C8CDB82F6469B39DA09E0A8E00837B21F222137F00C3F3BFCE0 C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/uploads/2021/03/0D88B40E-CB73-4F03-BA89-53C15B228DCB-aspect-ratio-16x9.jpeg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\0D88B40E-CB73-4F03-BA89-53C15B228DCB-aspect-ratio-16x9[1].jpg

Preview:

......JFIF.....H.H....P2Exif..II*..(...........1...........2......................i...........%..............samsung.SM-G950U..H.......H...
....G950USQS6DSI4.2019:10:27 15:25:35...........h...........p..."...........'.......2...........0221........x..
..............|...b...............2...........0100.. ....d...2019:10:27 15:25:35.2019:10:27
15:25:35..*..........d...<...d...............d.......d.............0100......... ....Z...@...........P...................................ASCII.......JKJK0.......U...z...K........N...N.........................
6.%.......U.......n..........\...!...j....$......................A"..A"..@"....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\184407919_380627866547382_2811821403963854641_nthumb[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded
Size (bytes):	7868
Entropy (8bit):	7.946187646534532
Encrypted:	false
SSDEEP:	192:FbgXxLNG9F7bRGlJ1M5oS5lwHFdBKSb5lxpzgSLhqE:pg69HGTi5oSTwHF2GxpKE
MD5:	10E5BA5FE906588EAC033DC5D03EC403
SHA1:	8F89B8685A0FCC929A0FBB277570ACB8F2361666
SHA-256:	6682DB8348F411CDAC3387366B7D72D28106E102C53BAC7BBDF64C9832262E64
SHA-512:	22D56D51EEFFF0337F961348C1059DFB5CC23B2397D5A30E12880A94323D2403CFF37421CA927C6C460B4A8C50A9ADC68ECA5970DA425694D549B62C54886C3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/uploads/sb-instagram-feed-images/184407919_380627866547382_2811821403963854641_nthumb.jpg

Preview:

......JFIF.............C.....................................%...#... , #&')*)..-0-(0%()(...C...........(...((..........."...G...................
......!.1A.."Qa.2q.......#BRb....r...$..%5......................................%.......................!1A.Q".2Ba.q............?..8.>...i.;F.,Hn#'......L..6..f..3I.;.........).T.n*.5........r7.|!"..R...5X.7..a
}.d.4.2....Z...*j .....}_.s.a..s......iUc.a...J0..o.....k...F.6.k..\......m.cq..quFSE.}F..1..&...xno.%...*.x; HR.....Wx...K..b..}.".:Z..i..A.,.Q$../e.k..b.."......a..1......r?.m.t..c.M.f.Q.M.] ..,..,..
H.\M..EFOC....GS.HQ..x.......m.S.....Z.S.P..F..?.?#..QGO;..!..k)..G."|uT..Y.;..`..U....'M.H.1.Yb.%..].....j.......IT..R/u.Nj.d........G..CK....E<!.......z....1'....V..26eV.........X.t=.]...e
B.4.6AJ..a;.......\..a.,/.(i..ON..+O.....j;[...p...9.Eo.f..C7~i.ZY.}..Cs.l8...f...t....IQ..x....v-.{y..3.bYjp.~k-Tyw.(i.^.VE.d..E..|[.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\196816319_310906600679332_5736863499639791403_nthumb[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 150x78, frames 3
Category:	downloaded
Size (bytes):	2763
Entropy (8bit):	7.810586325435231
Encrypted:	false
SSDEEP:	48:+iWgBQGTynuOn2tvqbIxUzkTHhnTYtKl6S2IsNO0pTAFXubiOHGkw4dlraen:pBPQFn29SzkLlTFovOvFXuHjd17n
MD5:	0B2A1AA45F8529C972E1A0719593A832
SHA1:	11B4E583F5E6A53E3EC91A0AC99094E1DAAD3DB2
SHA-256:	DA983E7F3713208E5361A48A53E6CA3A9FCB300815A7E70B939B8A306A053B72
SHA-512:	43864E7E85F375309CE31A4A2D5203B01B6E043FB254EE711D821D8376BA5626F34E1791863F79A428291283E131AF33AB368F50F1132D8914F9457CBF64BE5D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/uploads/sb-instagram-feed-images/196816319_310906600679332_5736863499639791403_nthumb.jpg

Preview:

......JFIF.............C.....................................%...#... , #&')*)..-0-(0%()(...C...........(...((......N...."..5.........................!.1.
"AQa.q.2..#R...34Bb..C...!1..Aa"............?...E....Th...Ne%.q.W.X.....RcB`..5.........h.....H..1...k.,"Vi..?8...i..EY.Fn..E-.. V+....t.....~..h...zwO.
.c...E.Ge....n...........W4Q...r.E_.*.....-.P.w bO.5.J;M......a.{..=.Z...xe...b.i.[....4c ....5..Y.X.Z...X..N.U........Gz..M.....Mv(.+...#'..".Ge....9'.Z...X%.P..sC:.8Z{uw. ..Bo...Wa.,J......r...
<.4...I........>..bx...<.j.aqC.d..x.D......<..X..N....QJ.F.<....XC..S-..l"...($.W q..\zs...5.>H.18.......d..v.,..Wo..M.vD8..#<..1.P.Po.# ...'.c.;d....knF*m..O..F=.f5...q.....>....7.Zf..
..ymo..H.y9.n.....U.C,....M0t.f...r..H.....j.$.[.;..........J.......'...jE...G.o-.7q....M..z=..$Vm.#m.^9........Z\.u....K7..J.\..r?....fo..}n.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\198423165_4154981297904727_8332438551652232381_nthumb[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded
Size (bytes):	7572
Entropy (8bit):	7.928668599134079
Encrypted:	false
SSDEEP:	192:6eZlnKTOV5BTmzC48vNL73mpkssL8pVrkh+x2:VZlKTOVnsC44X2xsL8pVrk02
MD5:	101A52F4E97CBA2891BC98FECB927D32
SHA1:	ADAE0B3C2042B9800D4AF22476C2266B3BE86FA2
SHA-256:	889E84D7C67626C14BEBF96942F92BF180DB304353AA35018C48CF0126A3BF7F
SHA-512:	CD17EBE33C1317A44503881CD63614544C2167FBBC40A31DF0446424EBC1680C832698F3B5EC794F7B94BC38556AFFC0ABBB94236A6E68F5DD4794EDFEBC57I 8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/uploads/sb-instagram-feed-images/198423165_4154981297904727_8332438551652232381_nthumb.jpg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\198423165_4154981297904727_8332438551652232381_nthumb[1].jpg

Preview:

......JFIF.............C.....................................%...#... , #&')*)..-0-(0%()(...C...........(...((...........".......................................B..........................!1.
"AQaq....2....#B..3R.$4Sr...b...................................+......................!..1AQ"..2q...a...............?.g9d....8.......o.y....(a+G.I..A....C.J.A...W.?U~...?....=U.oH....}R.....>d...oM
Kdl.p..@.(S.Rs...>.1..":B..w..............{=.[L2./0..../*H'#'..Cfs.`=..\8.....-y.l..{w'...f.q..?.5ax...E3..$..{.Z3..).TG...>.....b..x.%..4..G.Q...g[..A..I.H2...(.....K.W..hRH..ki..p..S...........!$.p
O..kd.qdt(&.....&.Z|....Ij....d(8...X......U..M$.#.\m.Il........X...,3.0...;....V&..\..q.X...u.H...<V.KO.).0.....3Qn.'LZmm.p6......Y.t' s.K[...whNY..lw..1..Z.s....|..2f>.c_.@|.8:..>..n.[Wo..
).#..c.............Q4..6&#..R.7c...../P.+MK....2...IY$..0.k.1!.f.....<.`.%8......h..}M.`.e.G^.t..nd'#.Q&.6m]}M...".b3..J...'.=i..#...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\198567492_120061403581225_1559453860397984042_nthumb[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 150x111, frames 3
Category:	downloaded
Size (bytes):	4765
Entropy (8bit):	7.913084345586738
Encrypted:	false
SSDEEP:	48:+iWx3DJcxgh3kNLEOCGhaBHaIfDgCoytqmsj+ZuHLEz0H1CkaRKLxHFdyqnlCmi3:jxi0LvCGxyhTq9/1rtldxI4sWIF1
MD5:	AA9559D3813D902A9F5E395068E94F66
SHA1:	06284B486051D2084911C388F8273B2A6AF8286F
SHA-256:	60C89DDF9A7F6BF945AA6ED5B117ED9F91B6EBA701216F723C64ECA960A4998B
SHA-512:	2DABA7C1A610344D994722B8638A1CEB70A606DD1B0A53553573AA1641B7A955C4D88D5427AFB221449761E9CE72B19A3F736107218806BE02A38BBB0ED24F40
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/uploads/sb-instagram-feed-images/198567492_120061403581225_1559453860397984042_nthumb.jpg

Preview:

......JFIF.............C.....................................%...#... , #&')*)..-0-(0%()(...C...........(...((......o...."......................................<.........................!1.
.AQ"a..#2q...BR..$...3Cr....................................*........................1.!A.."Q2B....a.............?.....W...O.n..l1.4.(...=.. .S..{/..b.z2{....v....1.VY..........j1..i.p.).r{.aP..V.5..u.....i.<.........<v.
+..v.j..#/...k.y...h.%.......R..O.H\.W$.W....+_...B..})8....w.j.=.g...fP.$..._!..9..FP.a. ..I./).'9....$.n;T..)Y.h.ko\.c...a.)m)B..*..]..]5.GG\k..)...[...e.q..?.j.n..x.y.-..)....te....._....|...V.S.o1
gX.dM...Cc..U.......d.{.^..)a....%?.$.....<...C.F.6y.[z.?.....(;..>....n.....6.^.`G......g.....ya..2...UC.H.G.....K..Vl...C....=.2yv..6I-...}...h..r.9..$.l...Hv..9.eV..UHN.....%q ....
Re.ApO..5...R>...I]K..9.S.w.I......P5.v.e...<...3../T..4e].,.0..Ik.....k.]....)..._z.....mW.mo,...O.TA...3.qS..TJ'D..O,(.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\20210310_170506-aspect-ratio-16x9[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=5, model=SM-S111DL, orientation=upper-left, datetime=2021:03:10 17:05:06, manufacturer=samsung], baseline, precision 8, 4131x2324, frames 3
Category:	downloaded
Size (bytes):	1159788
Entropy (8bit):	7.976522080843645
Encrypted:	false
SSDEEP:	24576:7HaI3U51K2GVqo3YFhj1nLTRjv4Q4EIXwpAU1mnnUDe:tU51K2GVZIr1nnRDDpIAp3MUC
MD5:	7AC20E363CA42BF8D99288BBF83CC5FD
SHA1:	7280C203AF444F4809357DF273F40741196702BE
SHA-256:	DB504A0F6F8DADF332DDCBF1A94C8AF450CF9D5E59F77C12B6BB33CE12DB36BD
SHA-512:	72D5882581516CA610F770808D6BCF7520B3432EE9245D4788AE9906E6C0DB4C103E5145BEB1AFB6C521E488F8A11D103308758C34017BDF967C6EAF537A9170
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/uploads/2021/03/20210310_170506-aspect-ratio-16x9.jpg

Preview:

......JFIF..............Exif..MM.*.................J.............2.........T.i.........p...........h....SM-S111DL.2021:03:10 17:05:06.samsung.......................................'.......d..............................
..P...d...............d....C.....................................!........'.."#%%%..),($+!$%$...C...........$...$$........#.."................
........................Q........................!1.AQ.a."q...2.#B...R..3b...$r..C...4S.%5DEcsTU....&.6................................-......................!.1.A.Q"a.2.q#B.3R..b............?...9....|..Zc..d_.
r...gu:........Vu..6Px;.V.....YN.Y?E.....q...._...m..Wa...MZ.<..n...4.....5.,.......4...jKM.....[}.......eki.....zY........ui..48... ..x.n..D.........i..2....p..y%H.I.\...i...U.......\.....q...v..Aww.a....n....
.`.i.Qz...X@~.W69H.@{+....U..c.W.Q..wM.. Y...plx...1..x$..B..8%..<.....UI.k..[....W..U..r....G.].Hi$.Ct..PA....q.b..;.P>....7.....7..>.....+...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\20210310_224801-aspect-ratio-16x9[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=13, height=1800, manufacturer=samsung, model=SM-G998U, orientation=upper-left, xresolution=222, yresolution=230, resolutionunit=2, software=G998USQU2AUB5, datetime=2021:03:10 22:48:01, GPS-Data, width=4000], baseline, precision 8, 2583x1453, frames 3
Category:	downloaded
Size (bytes):	584276
Entropy (8bit):	7.939618263487518
Encrypted:	false
SSDEEP:	12288:RSbSQ1jMk8nZiBKyvt1kU0a+Gfu7erPwjuZOUT2kUuH5MxVuE6PxUEBPH:0bSQ+9ZiBKyvt1f+vYPwjnuH0YEu9h
MD5:	E7EDCA3E0162CB5B5A72084F6DBA8A1C
SHA1:	024A0289DEB5D71FCA0DABB06C04E67D22E712AF
SHA-256:	A3E6ED64833B5E3005846564B0A34EA9D956250D1D5E419A9AE47CE4889645EA
SHA-512:	71F36C37D7AC3AB8075469985BE6D7385625465496E997D64835A63D9671DBC455095347171CF2FD4F5797C65F3C12ABA2E3ACA809CAF7CB49CA3DA51628ABD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/uploads/2021/03/20210310_224801-aspect-ratio-16x9.jpg

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\20210310_224801-aspect-ratio-16x9[1].jpg</th></tr>
<tr><td>Preview:</td><td>......JFIF.....H.H......................R...........|...}...7...........&..........
....y>.....|...R..!..n..............................m.......~.......R...R...........z
.......v.......................|.......`...........v...........i.......`...v..............................?...1............,..R.......\...................................).......................E...=..............$../...:..................................
.......2...J...~....................y..>...........................#..X.......2...........</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\5c783695d11c6a0011c480aa[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):	835
Entropy (8bit):	4.761935613073245
Encrypted:	false
SSDEEP:	12:qcLF9VDQHrBcIMnD0oG7uZT8ZJcXk34IeDrHcZioEqEJaIfAV7OVE:qcvVDmOD0xVyXk8DTyio1EUV7OVE
MD5:	1165C80325F0D4A8EC102FCC91F07B94
SHA1:	BD900493F7BE121383A1D904C393578297FDD785
SHA-256:	8E5308FE6CD9ECF5B9F84803AE132DA90C73F584A504E07314DEEA2CEFD109B1
SHA-512:	4066F8FC3FE59C3C4365F0AF865F4A206C42BA27ABDDC50434422C2B4719C4087808F42BD3FCC2DF77405915AAEA9F4A0D4677DC438D3A4BCAE3123AF355365
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://buttons-config.sharethis.com/js/5c783695d11c6a0011c480aa.js
Preview:	window.__sharethis__.init({"ts":1551457540842,"inline-share-buttons":{"enabled":false,"alignment":"right","color":"white","font_size":12,"has_spacing":false,"labels":"non e","langauge":"en","min_count":10,"networks":["twitter","pinterest","email","sms","sharethis","facebook"],"num_networks":6,"padding":10,"radius":4,"show_total":false,"siz e":32,"size_label":"small","spacing":0,"use_native_counts":true,"ts":1551382408429,"updated_at":1551382408429},"sticky-share-buttons":{"enabled":false,"alignmen t":"left","color":"social","hide_desktop":false,"labels":"cta","language":"en","min_count":10,"mobile_breakpoint":1024,"networks":["sharethis"],"num_networks":1,"padding" :12,"radius":4,"show_mobile":true,"show_toggle":true,"show_total":true,"size":48,"top":160,"use_native_counts":true,"ts":1551457540836,"updated_at":1551457540836}});

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\IMG_20210303_135431-aspect-ratio-16x9[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 1200x675, frames 3
Category:	downloaded
Size (bytes):	149629
Entropy (8bit):	7.974926780541048
Encrypted:	false
SSDEEP:	3072:2/YEty8yxSNIuPsbu5l06ZeQ7rlIVzYUgnMALKGb5sk:1EQ8yxCPsbu5l06wQ7rwYUNA+ep
MD5:	9471C5D610FE49DD090F0AB46526402F
SHA1:	A26DC40E548ECB70B6C0BC7FDC6FFB86D1992A49
SHA-256:	3E794CF3AEF99C354B24BA67C5BE9CECFD399B8ABCC4430EF97F6A0356351638
SHA-512:	827407E56A7B695A98D210493E967248B1E285D996A15C86CFAF8C2F711B9A0D7FE8BC92CD880FB6351CA24090B3A4F9C6C25B3EEF9D83F73BA5CD2AECFDF1 4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/uploads/2021/03/IMG_20210303_135431-aspect-ratio-16x9.jpg
Preview:	......JFIF.............(ICC_PROFILE...............mntrRGB XYZ ....acsp.......................................-...desc.......trXYZ...d....gXYZ...x....bXYZ ....rTRC.......(gTRC.......(bTRC.......(wtpt........cprt.......<mluc............enUS...X.....s.R.G.B...XYZ ......o...8.....XYZ ......b..... ....XYZ ......$.........para..........ff......Y.......[........XYZ ....-mluc............enUS... .....G.o.o.g.l.e. .I.n.c... .2.0.1.6...C....................................!........'..."#%%%..),($+!$%$...C.... ....$...$$...........".......................................B........................!1A."Qa2q.......#B..R...$3b.rC..S...4Tc............. ....!1A..aQ.q............?..I...g.q..-....$.....q,y...aj..2".....T....".yG.. ..x....9y.I..E^9..#.Ic...G.k..7..?.s.0.T..".

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\MC205_042210[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 157x105, frames 3
Category:	downloaded
Size (bytes):	6377
Entropy (8bit):	7.893067974480191
Encrypted:	false
SSDEEP:	192:C/udieEnDI3Ee6xba3Z9TM8LcTKKyVJ1fCZjN:IeiI3Edxbaz5cTEJf4N
MD5:	EF075E37F5AA8F3928C60544CC41FCE6
SHA1:	9620ABD7E22698F8C40BE12FED8D5A0A6042E646
SHA-256:	BAACE669584C3B7813DF9E2D2AD5F8C92FC4C0840942D777BD3F059F2BADE69C
SHA-512:	D79096A4DEB72D8F890509930C1D294F53585AB35494CFFEB7B522ED723B63F9DE46990CC3EF9F3E7E35228A4518632FB849BA32C2A391D61550791CD9BE264F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/img/thumbs/MC205_042210.jpg

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\MC205_042210[1].jpg</th></tr>
<tr><td>Preview:</td><td>......JFIF..i...zeW.4?.*S]..cAx..w.."k&gb
^.BQ3.9.......y5.....p}......$........N\/r.6..<...z..7........x.B...(..ma.....@.;.7..R'.@........U.L.G701...%S..@!q.9.I..7(....nb..UM..kkc..}.yQ.....Mlm.W.zP.....^..`+...a2..w...>%d.+..E.n.&<br>u~..q...Uu.X...&.B9....%.................................................. <..>...~.{g....u`...(..(..(..X.(.A@.B...n.,<M=..........9..O....k..%...D.`.@.P...%....P.B.<br>(..`. ....7..........................1....!2ACQq."3BU$DR#6S.Tt...........n3......gG...LC....nY...z..,76..9%.{Ux"*.w...r......+y.yD.:..S].{.rZ.r..n.\..q.....D.z~..U...&p...Q....oT3....u.......y.I.#!xe
.L.H2.N...m..{.<7M*.Lq..;KOGxc*gg..L..}.Q.]=...\..4.U...A.....}.E..z"0U.%.>x.M..+.r.e9.C....Y.y..#.S.c.{Q26..B...</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\MS300_032613[1].jpg</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 157x105, frames 3</td></tr>
<tr><td>Category:</td><td>downloaded</td></tr>
<tr><td>Size (bytes):</td><td>6436</td></tr>
<tr><td>Entropy (8bit):</td><td>7.877148763663616</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>192:hnZOzcSZjzC2a1iY/PdCHqFjvWzR7/l6gOlwa0kU/:32cSdzJctDZW9Ll612kU/</td></tr>
<tr><td>MD5:</td><td>E13285FCF95A343E6D9F788F8A48C86B</td></tr>
<tr><td>SHA1:</td><td>D3FDA036993471A9618DE5831D2008E225EA2DE7</td></tr>
<tr><td>SHA-256:</td><td>B1E6BCE0E526E63CB84CC4EB190AD5D4EB8721AD753A4CD324640BED320D0834</td></tr>
<tr><td>SHA-512:</td><td>44BF155DF42F748E284A764AB84960204988F8FBCCDCADEC576F6EFE8252841B84DED5F3EE4B4BB86E4427160758D8CE8DE3F37F9D3A631DE3FB658642F89FA
C</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>IE Cache URL:</td><td>http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/img/thumbs/MS300_032613.jpg</td></tr>
<tr><td>Preview:</td><td>......JFIF..i...=...u...+Z.MT.R....1\.c.C..Wu.rl.!
W..v.....{.t.f3b.e8......2S...1....r5bO........:..+..."N...I$.j.....8d.1...H..i..y.qM<a....R..>k?.#....Q..zIK.....Dh.B.`<......Q..E.G.0...3kn=u....Z.%./.T....#_?....#3....t.{>[qWe.>......3h=
.?.W.s...<....<................h...........aP,.IA.,.@...c.y..g....z..G....q9\.~?z.t=............@.Q@.......B,..?...=.............
................!12AQR."3BCq.#$DST. 457Uare............n3..............dd..)D..c..;>..2....k..xX.[Cuk...%..........H.w......./t...[:gP.:I.[.......S...c..>.[.k.._#$.j(.}..%m......R....[.:...
mb.MWe@...["3......Qa>El.a.3.vg.F.d..!sc.mW....|s.#XZv...P\...E,.I...j.e-T&....FX..n..5...a..h5.</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Snapchat-1292844234-aspect-ratio-16x9[1].jpg</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 1828x1028, frames 3</td></tr>
<tr><td>Category:</td><td>downloaded</td></tr>
<tr><td>Size (bytes):</td><td>353092</td></tr>
<tr><td>Entropy (8bit):</td><td>7.976468841326363</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>6144:5kL8PxrPSyCHU8p6/OA80FrvCFdNOJaW1gPvsPMEEU2it6785JH9nWZqbn8pAmEr:5kgPNqyiU8w/Owq2V1uw0Uc78nHT8pAZ</td></tr>
<tr><td>MD5:</td><td>11F5C228690DED262DC09A873A82D34E</td></tr>
<tr><td>SHA1:</td><td>25AE6689700CA4CD18FFF127E9EFADA584B58F72</td></tr>
<tr><td>SHA-256:</td><td>B10A6A8C587391C3024595EB043A4634C6BA918BD50055FBA9CF18947D2A12F5</td></tr>
<tr><td>SHA-512:</td><td>44BD70F95E5D7F2ADD88C2E1AAB89E0CB87268CA1B42686DB59132988E6EAD03D190DAC513F954460470F89F356D2B48A60D8BA7F793973670C14DA8424B398</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>IE Cache URL:</td><td>http://https://www.duplicolor.com/wp-content/uploads/2021/03/Snapchat-1292844234-aspect-ratio-16x9.jpg</td></tr>
<tr><td>Preview:</td><td>......JFIF.............C.....................................!........'.."#%%%..),($+!$%$...C...........$...$$$........$.."....................
....................F.........................!1A.."Qa.2q.#B..3R..$C....b.%4Sr...Dc..................................'.......................!1.AQ..".q.2aB............?....n|..;.Bz...T.j2..M0"...9.c..a.W..`T..<br>.=G.....m<=s{.Q..].#'.......c.Oa...-...,}.[O..YZi..Hf.m.g&......'.m.q....O.|..N...7...l-..~....<.5]-5;..*..`......b...9..?O.....Wc..X.Fu)..+.\...{W._..z...$.%...|Pj....O...._J.>.s.ky.k...}..;.#:._3..u
....KW.E.R..mcpC...W.<..kiQ....(.....:U.._.....m..ibF.|nN.Q.~..gK..Y6.w.bzf...i..%..2...]...p..M..|E$..$..2...4X.(L..v.B..{..J~..B..e...xwZ.\..a .Q...{.=.....r....QY&.j..w7[.rF8_........h..u;
..e..Gs[5......(.....t..}*..M.......Lv......]...me{.P+.V.z...u{8.}%..dx..wR7(..O\].E.X....*...MX\..y.8?dr....:.G.....i.7.....9.....a_R...*..J..`..'.|..L../.b..$...I..v.2qZ.f......R</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\anchor[1].htm</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>HTML document, ASCII text, with very long lines</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>127243</td></tr>
<tr><td>Entropy (8bit):</td><td>5.889537402895608</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>1536:YNDCDcZv8Q9fkVCDcZSCdgOShVhyuCDcZi/ALlPqcK2:YAtQ9nVCAjyaNqcK2</td></tr>
<tr><td>MD5:</td><td>3946582F3254D043511155EBADFBD82D</td></tr>
<tr><td>SHA1:</td><td>5A25AAD01A6ABE44506ABE9276108EC7441774C7</td></tr>
<tr><td>SHA-256:</td><td>7B5E44DA42CDA27E282982D0A30BFDEDEDE04198C32892259F5E527604B6C31E</td></tr>
<tr><td>SHA-512:</td><td>ECE44D8E025DC37CC377BB9EE79A82C6D22E2DD7658AAB7ED94E7EF3D3320F80A7D5278B3AE4346D1C1C51A26BFF6D75D1A8725FA7916DF64393747AE12ED
EC</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\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/FDTCuNjXhn1sV0lk31aK53uB/styles__ltr.css">.<script nonce="SH+HNuHVgZRiZjabQ/JU3g" type="text/javascript">window['__recaptcha_api'] = 'https://www.google.com/rec

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\anchor[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	43387
Entropy (8bit):	5.889255984537017
Encrypted:	false
SSDEEP:	384:v/SdMXKrFY9XsFENFkSUsBN+i6nfgzxEawCyZg07zD11x8NaUJZBwNQDJ9Ovgz4/:v/SdTFC8GN/TqNDCyZguuJZvwv1v
MD5:	8C6A46E30F13051F8C359A7CE9366B14
SHA1:	F96726F556F5B261C3A80A881488E1AB58A638FC
SHA-256:	0D8E582DF4C558034F5E8501703D36DC8A742C066E9D67B80F79A8479D76B4B8
SHA-512:	7F0674AD6E465B84D0F8A9DFBBFA902862A3059E9410461523D759EA49C2ACDEFCE6C1EAF8CE995A6F92AEE9638C0E1286EFB5C19A96E3C9B21E87C2F35D52D0
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/FDTCuNjXhn1sV0lk31aK53uB/styles__ltr.css">.<script nonce="yeIMjdGGQwiOJEVyeVAGAA" type="text/javascript">window['__recaptcha_api'] = 'https://www.google.com/rec

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\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:	downloaded
Size (bytes):	1793
Entropy (8bit):	5.580314682781776
Encrypted:	false
SSDEEP:	48:VKEcKKoez1o+yLrwUngKEcixKoez1o+yLrwUnG:fc1oDsuUtg1oDsuG
MD5:	961C7EE522A045AC45B902BA415E300A
SHA1:	886EA77B23716B6CB2E00B904DA67E2A6BBE8676
SHA-256:	E950AE7CDAEF010FEFAE15DC1FDBE85F42F6F731E3B92F306F0D5FAB7A3B50B8
SHA-512:	C51B28DF60665C2883DC3CF11AC728C5CE5F0C2632B43A93BAEB55C11CA880F15359FEDCA7A9145C7D3840FD399A147DC8A5C7163AD6FECC9DB6F5B00180CF0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google.com/recaptcha/api.js?onload=onloadCallback&render=explicit&hl=en&ver=5.2.11
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('6LeT54oUAAAAAM0Fe9qLJMRr30BxU9BwidRRwqbw');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/FDTCuNjXhn1sV0lk31aK53uB/recaptcha__en.js';po.crossOrigin='anonymous';po.integrity='sha384-CVLvfZreJnPQL86cHuhqPHygN9uzFMnfC+HyY0PSGUfPu9yIYXzhnNBTDX7Yfi1R';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\0W10PBUV\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):	5.622715812529397
Encrypted:	false
SSDEEP:	24:2jkm94/zKPccAag6+KVCet621Tc+ZqKsLqo40RWUnYN:VKEcKKoez1o+yLrwUnG
MD5:	48CCAA83E29E007F316CDEBD5C5894CC
SHA1:	D6603A6C495F28FD4950C038DE29CCE7972EC3CE
SHA-256:	77004661ED3F29C526CF602ADCD5AA1EF88CF4E6FE8C49516E13A401984A0B22
SHA-512:	EFB556A6DB5F74DAF23877BB330AA8DDB2D596E4FBC63CB47DC50CC17BB39562A99471FE568F7DFED9FC36E0EE1BA5517743C3C604DD3E2DCB461FF72AC5196

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\api[2].js	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google.com/recaptcha/api.js?render=6LeT54oUAAAAAM0Fe9qLJMRr30BxU9BwidRRwqbw&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('6LeT54oUAAAAAM0Fe9qLJMRr30BxU9BwidRRwqbw');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/FDTCuNjXhn1sV0lk31aK53uB/recaptcha__en.js';po.crossOrigin='anonymous';po.integrity='sha384-CVLvfZreJnPQL86cHuhqPHygN9uzFMnfC+HyY0PSGUfPu9yIYXzhnNBTDX7Yfi1R';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\0W10PBUV\buttons-secure[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):	23158
Entropy (8bit):	5.1859181005277755
Encrypted:	false
SSDEEP:	192:G1lYwp+CtRJyPTKlLlhpvmOpeMf0YkV0Akhop6YsZNZmZOZDZd:e6wQcYTKlRXmO8b03a6d
MD5:	B0869FC341902D3FE430803CD7D034CF
SHA1:	79614C3BDD1D9564E0B044F22B8FA3750FE2B1B7
SHA-256:	95DC1B83A7C030DD13AB3E29DF921F10E04208B28734F172EA232854264C3B05
SHA-512:	38D667470DDF1F045A084C0003C4BD5214937BE5E3025E7842C7325096F16C35FB86ACF64DC0790136E4CF3A656AE8D1B67416D586A5EF46F4DF9C01D337AB3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ws.sharethis.com/button/css/buttons-secure.css
Preview:	#stOverlay{height:100%;width:100%;background-color:#000;-ms-filter:"alpha(opacity=50)";filter:alpha(opacity=60);opacity:.6;position:fixed;display:none;left:0;top:0;z-index:89999990}.stwrapper{z-index:89999999;position:fixed;top:20%;left:50%}#stLframe{position:absolute;z-index:1000020;left:0;top:0;background-color:#ededed;border:1px solid #d5dcdc;border-radius:5px;box-shadow:0 2px 2px #666;height:100%;width:100%}.stwrapper.stwrapper5x{margin:0 0 0 -256px;height:419px;width:514px}.stwrapper.stwrapper4x{margin:0 0 0 -167px;height:337px;width:334px}.stclose{cursor:pointer;z-index:2000000;position:absolute;right:3px;top:-2px;margin:0;padding:0;font-family:Helvetica,Arial,Sans-Serif;text-align:left;line-height:1.0em;text-decoration:none;cursor:pointer;height:28px;width:26px}.stCloseNew2{cursor:pointer;z-index:2000000;position:absolute;right:25px;margin:0;padding:0;text-align:left;text-decoration:none;cursor:pointer;height:25px;width:30px}.stCloseNew{background:url("https://ws.sharethis.com/s

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\cat_detailing-2[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 1024x365, frames 3
Category:	downloaded
Size (bytes):	46097
Entropy (8bit):	7.975259077007137
Encrypted:	false
SSDEEP:	768:qOsLSpj/AE3f0WjcccRKIE+GTnXPa4ubDEonoU1Clet0kbvEo3h4nmjXF/WbMUuy:7zpjYE3fxYccRKIpkn/a5bDZnocCletU
MD5:	43AEB39B086229974C9AB20F7BEC4C3E
SHA1:	8BA272D813E63382CD4114EFCAA9817C82B82B6F
SHA-256:	C16C99472C154663308A839BC84AB1D355AC27C7037A10B4434E3E72927CB490
SHA-512:	C9AC81844C70AE0A099ADDDE17AC3C90BB7FACC484A189C0A0B5CFEA46F38DBD2AA52703F1F1634D252AC9E997DD86BA42D3426F70A5CB7C3250E68BD829EAE3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/uploads/2019/01/cat_detailing-2.jpg
Preview:	......JFIF.....".."..........m.....T...}c{J.L..K...wk....&...h.....dj.....<..u={.8.j...`."( ...N,.. ..... .....[~..h...ff...qx:r5Yf.....t|..@....;....kW.SH.4AET....?.....8D@....EU..>..R.g=.{..u8.Z.:..X.....B.....-...6.....cb.E.T.`.z.!D@@.....AU_..76...rmp=...Z.+u..|.+c.b.w...g..$Sv\.).....40..mn+7.....F.y.b (.....l...t3g...x}.+.$+$....$...e.'....9zp.cJ.>#../`[..6s<...]..."(.5'.....@.. ....*.....\m.e.3..Z.t...r.....a..\5+.t.....a.ur.{[..9H..(*.".Di.f.A.P.....WC..n..[..g..8...vIIX.v.ES?..,..,.b.w(..tf...'...{..|.7E.B.....W...H.....(.....*.....s..*KZ\G..5.[.....k....`.5....z8Uy.T"...e.L.d.....=O*.T..4b+^.;.....E@...UV.....6.j>Y.4/..9.K5...9..:J..MN.[V..cd:.A.[.I.{..9...].t.f5....DDF....".... .....H(.m.~.....:...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\default.date[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	troff or preprocessor input, ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	6009
Entropy (8bit):	5.052635827719971
Encrypted:	false
SSDEEP:	96:mSCu16RaIMDAZJAoiFhuPc1odOBqU1iza8Wely:mSPadfU1iza8hly
MD5:	FB1E35155D11A8C40E32F8BE9351EE53
SHA1:	EA7A3608C0AF577F3393948184E4F42A2586DDC8
SHA-256:	A136CD59D99C53E98BFC3065DE08CCF8039B6F2F55DD430DB2BD350EA4E046F1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\default.date[1].css	
SHA-512:	265BB9F3B9CC3D6E884B33F65C1F906AEEC8AB1335CE2D7A0AD57AEDD162B99F1F7DE75A01BD9567ACBE5C4DFD2DB600967B25C62A98969B7CB9FBB90015F D11
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/plugins/ultimate-member/assets/css/pickadate/default.date.css?ver=2.0.49
Preview:	/* ========== $BASE-DATE-PICKER.. ========== ========== */../**.. * The picker box... */...um .picker__box {....}../**.. * The header containing the month and year stuff... */...um .picker__header {.. text-align: center;.. position: relative;.. margin-top: .75em;.. border-radius: 2px 2px 0 0;.. padding: 15px 0;.. font-size: 18px;..}../**.. * The month and year labels... */...um .picker__month,...um .picker__year {.. display: inline-block;.. margin-left: 10px;.. margin-right: 10px;..}...um .picker__year {....}../**.. * The month and year selectors... */...um .picker__select--month,...um .picker__select--year {.. margin-left: .25em;.. margin-right: .25em;.. font-size: 16px;.. color: #999;.. background: #fff !important;.. outline: 0 !important;.. border: 0 !important;..}..@media (min-width: 24.5em) {.. .um .picker__select--month,.. .um .picker__selec

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\default.time[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	troff or preprocessor input, ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2466
Entropy (8bit):	4.967759989634707
Encrypted:	false
SSDEEP:	48:213GqjC/YghrZk/5TyXG2uHl0133rDQ4xiShY:2DjCz/qyPel0pY6e
MD5:	852535731B22B629E2EDDB4459613C4C
SHA1:	0C240730BADA17B0DC5A6AF6F0E7D7CF2B61739A
SHA-256:	3D0F5FD402B4B600E221D8DBDCB47095BF6AD46B79C824505036DAB127A87CA3
SHA-512:	8752538F4635B3A61556A08B4F0BC0B52C560F0273358851193513E8E76047C56B403403DB5AD8DD370910F8B8EE906704C832CCD853C42D5B65581F38BE3DA2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/plugins/ultimate-member/assets/css/pickadate/default.time.css?ver=2.0.49
Preview:	/* ========== $BASE-TIME-PICKER.. ========== ========== */../**.. * The list of times... */...um .picker__list {.. list-style: none;.. list-style: none !important;.. padding: 5px !important;.. margin: 0px !important;..}..../**.. * The times on the clock... */...um .picker__list-item {.. position: relative;.. border-radius: 2px;.. display: inline-block;.. width: 25%;.. text-align: center;.. box-sizing: border-box;.. padding: 6px 0px !important;.. margin: 5px 0 !important;..} ....@media (min-height: 46.75em) {.. .um .picker__list-item {.... }..}..../* Hovered time */...um .picker__list-item:hover {.. cursor: pointer;.. z-index: 10;..}../* Highlighted and hovered/focused time */...um .picker__list-item--highlighted {.. z-index: 10;..}.....um .picker__list-item--highlighted:hover,...um .picker--focused .picker__list-item--highlighted {.. cursor: point

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\default[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	troff or preprocessor input, UTF-8 Unicode text, with CRLF line terminators
Category:	downloaded
Size (bytes):	3847
Entropy (8bit):	5.131156421527449
Encrypted:	false
SSDEEP:	96:HRpegStjwJcucmUmomHgUB5h56blPdgEBgEYBMm5mjmDBHXt:TJMgKmUmomHgZblPdgEBgEtm5mjmZXt
MD5:	924C1901023EB79703AE05C6AF95A5D6
SHA1:	1F41EEEFB2B3318D5A0679B98F1121C56D2BE100
SHA-256:	8839BC2B218574D5B958AF5E731ADD873FADAAB2558FDB44D4249E660FD0E2E0
SHA-512:	3473E8903DC2929D1FAD8255CB04011AEB7936E38278E753E8FDE12E55A7DAB0372239CC6EEC006D3827E5C169CDE246B3BF876A1768BB594B012344DECFE65 A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/plugins/ultimate-member/assets/css/pickadate/default.css?ver=2.0.49
Preview:	/* ========== $BASE-PICKER.. ========== ========== */../**.. * Note: the root picker element should *NOT* be styled more than what.s here... */...um .picker {.. font-size: 16px;.. text-align: left;.. line-height: 1.2;.. color: #fff;.. position: absolute;.. z-index: 10000;.. -webkit-user-select: none;.. -moz-user-select: none;.. -ms-user-select: none;.. user-select: none;..}..../**.. * The picker input element... */...um .picker__input {.. cursor: default;..}../**.. * When the picker is opened, the input element is .activated.... */...um .picker__input.picker__input--active {.. border-color: #0089ec;..}../**.. * The holder is the only .scrollable. top-level container element... */...um .picker__holder {.. width: 100%;.. overflow-y: auto;.. -webkit-overflow-scrolling: touch;..}..../*!.. * Default mobile-first, responsive styling for pickadate

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\fontawesome-webfont[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), FontAwesome family
Category:	downloaded
Size (bytes):	60767
Entropy (8bit):	7.983356702664012
Encrypted:	false
SSDEEP:	1536:CIRF2F4AF5tUe8gNkngPj3XxBe1zE97WCVksAb:CIRo4AFvUtg3r3QzatmsC
MD5:	F7C2B4B747B1A225EB8DEE034134A1B0
SHA1:	3E63FC9B3DE4580F1F3BEC0631436F755B80F167

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\fontawesome-webfont[1].eot	
SHA-256:	CBB644D0EE730EA57DD5FBAE35EF5BA4A41D57A254A6B1215DE5C9FF8A321C2D
SHA-512:	F8B32EEC082C86A295931F39A38C1B638254F4D298CE97DE8D4C80504340CB922D18770C445A19854AA6BCA27E12E234957C7D17C78361FA19CEEA1DB7E5491
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://maxcdn.bootstrapcdn.com/font-awesome/4.3.0/fonts/fontawesome-webfont.eot?
Preview:	_...y.....LP.....P.....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...3...0. .2.0.1.5...&.F.o.n.t.A.w.e.s.o.m.e. .R.e.g.u.l.a.r..... BSGP.....T..q..u..*.....Y.D.M.F..x...>.....)Y.....h..D....pj....f.i..).U.'.&a..;`.*.../.....V.B.....OV..r.n.:..{$2D...:.&...m..d ..CeH.\./o.....U.M....X.`?...?.A...C...@..'.(g~.....% (.JI.&zw....W#.mw".].At....k.....p...E....[..=.gM.....go..W.R.q..`{.ZwUF.....o ..D.p)A8....$..M.#.>..?..... d.No2..L.....<.t...B..T..a....<...`.....e.SO....cI[.p..E1R*.fMd....>. .2V.....z7..&.+.....f.&#.V.(8....aR.....x.Z\R.e..$.Vw.....K....gs.....*.... ..dI.....6.....)...rj..:Z."1.'...<....'.Q/...8.).B..5..tgk.AM.)...|~....".....2....+h..(.&.c..sw...(....h.Dg.k...w.zm%. f..../5.%....}...k..... ..@...[#.D)..J<..?YAT.....o.s%..Z...G).5....#R'...#...)...+R.....Z.z...+._...K&%'5....(b....Y..i_.....|B.>U.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\gtm[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	171316
Entropy (8bit):	5.408268162737941
Encrypted:	false
SSDEEP:	1536:ViciO+XJVesTa0ZfITFgXvJLWiyo7yGxNd1jj1tpVZ6NCqv1895/PoT1QI/aqN+e:Qcit5VeL0CgXvJzi2dF7ZnqHTKercE
MD5:	DED8292258CA7825BD05AD1C8D28B6C4
SHA1:	2DEF4AF232633058A21A85B6B04ED3A5863619FF
SHA-256:	5E94FA11399888F944E2A794B68E565635CE13484419DE26ACBED7A6A25CC398
SHA-512:	5E6B58A816AF2ADA83A12E35F23F102853DB8D39F647270846BA8C041C1F0A2435211BCA8E3FC91CCBEC50E4E2DBB0E28EDD93324AC4A5E85EF35AA41526BA F4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.googletagmanager.com/gtm.js?id=GTM-N63FV7
Preview:	.// Copyright 2012 Google Inc. All rights reserved..(function(){..var data = {."resource": {. "version":"13",. . "macros":[{. "function":"__e". },{. "function":"__c",. " vtp_value":"UA-8080565-12". },{. "function":"__aev",. "vtp_varType":"TEXT". },{. "function":"__v",. "vtp_name":"gtm.elementClasses",. "vtp_ dataLayerVersion":1. },{. "function":"__v",. "vtp_name":"gtm.elementId",. "vtp_dataLayerVersion":1. },{. "function":"__v",. "vtp_name":"gtm.elementUr l",. "vtp_dataLayerVersion":1. },{. "function":"__u",. "vtp_component":"HOST",. "vtp_enableMultiQueryKeys":false,. "vtp_enableIgnoreEmptyQuery Param":false. },{. "function":"__v",. "vtp_name":"gtm.element",. "vtp_dataLayerVersion":1. },{. "function":"__u",. "vtp_component":"URL",. "vtp_ enableMultiQueryKeys":false,. "vtp_enableIgnoreEmptyQueryParam":false. },{. "function":"__gas",.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\interiorSlide[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 1024x525, frames 3
Category:	downloaded
Size (bytes):	86624
Entropy (8bit):	7.983519009509302
Encrypted:	false
SSDEEP:	1536:HZLTypLPE7TjWj9Hoe77OM1m8qRhiSg8MEvplNGQZjdT4KIlGyG5MdkZiyD:5XypT9VaM1m8qqgMExlEQZjhQG/MiZi4
MD5:	025738A3D917BFBEEDF2DBEDE7A38C80
SHA1:	5D9671DEEAA445B73B39F2581BAA3B36330EEB7F
SHA-256:	1B8772DC8DEA696E5470A0884A4F107B87352DFB5F2925C75169FC762166AD04
SHA-512:	D44BC3174465491657EF49C4474FAB3CB33FBEEBA56A51CF52D0C3147B5A43A91D97F4D4249C1C241F8F371652200F6B075AB011DA09E1CC5253108F3621F99A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/img/banners/interiorSlide.jpg
Preview:	.....JFIF.....N.....~._...}?.O.....;....b..{. g...aV.8.....#9u.'.+m..38..L.I3.I'L.I'ussFy#H..D.#...a.}..h....V.s.g..c../...d=OS.....G..[..\+...ga.W.c..u.6&fd...&t..$...'d..n.&.....X..G.1E....L..G.{q.K..r...+..f...kF..E.N.QdOs... .....ad.$..3.I.I$..i.vf1.CV.6.af.....h..z/..O^.GZ.v.?.....U.9..a3BE.s..:#-....._./W.....2gvI.I.I.$.S.A[..)...^B.E.0....#.\.6..)....U.s\o7..O/;..*.W..."PC.T.r...O_..N.....X.fd.]"d.,..z.).....D .d.....XE.!.WB$...?....(is._7....K6..-.....LH..s}.oD.^...<.(.5FI.ft.t.<.../gS..4.....5.Jtl0.f.ad.....(....o;2.fm.4(Q....~o..k`.....Q..F.....V....s..3;"N....<.""".....[.Hi.30..f....]....'..y. j4...3.Q.J.Z...k[...K%..Z=...%..?...$..).2gL.....RKb...f....H...&B....~.j.L.\.....J.nv~}..T.T|l+.W).]...W.a..n...9.3..L.3:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jquery-migrate.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	10056
Entropy (8bit):	5.308628526814024
Encrypted:	false
SSDEEP:	192:kZrk/GNyd31svs7wkX8KzJcqSDdAcHX4YE5NLR:srhNyNO0kkMKzFSDdAcIYwLR
MD5:	7121994EEC5320FBE6586463BF9651C2
SHA1:	90532AFF6D4121954254CDF04994D834F7EC169B
SHA-256:	48EB8B500AE6A38617B5738D2B3FAEC481922A7782246E31D2755C034A45CD5D

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jquery-migrate.min[1].js	
SHA-512:	B74A2F03C64E883B9A34DE43690429327DFB4AA230A7A6AFCA8150A16E3D84E98461245FF264C26368D9904562CC34FE219F71F951D364FA5C68C039B76776CD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-includes/js/jquery/jquery-migrate.min.js?ver=1.4.1
Preview:	/*! jQuery Migrate v1.4.1 | (c) jQuery Foundation and other contributors | jquery.org/license */."undefined"==typeof jQuery.migrateMute&&(jQuery.migrateMute=!0),function(a,b,c){function d(c){var d=b.console;f[c]||(f[c]=!0,a.migrateWarnings.push(c),d&&d.warn&&!a.migrateMute&&(d.warn("JQMIGRATE: "+c),a.migrateTrace&&d.trace&&d.tra ce()))}function e(b,c,e,f){if(Object.defineProperty)try{return void Object.defineProperty(b,c,{configurable:!0,enumerable:!0,get:function(){return d(f),e},set:function(a) {d(f),e=a}})}catch(g){}a._definePropertyBroken=!0,b[c]=e}a.migrateVersion="1.4.1";var f={};a.migrateWarnings=[],b.console&&b.console.log&&b.console.log("JQMIGRATE: Migrate is installed"+(a.migrateMute?"":" with logging active")+", version "+a.migrateVersion),a.migrateTrace===c&&(a.migrateTrace=!0),a.migrateReset=function(){f={}, a.migrateWarnings.length=0},"BackCompat"===document.compatMode&&d("jQuery is not compatible with Quirks Mode");var g=a("<input/>",{size:1}).attr("size")&&a.attr Fn,h=a.att

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jquery.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	94840
Entropy (8bit):	5.372946098601679
Encrypted:	false
SSDEEP:	1536:8YRKUfAjtledhTmtaFyQHGvCXsedOgRc9izzr4yff8teLvHHEjam7W5X3yzSiLnM:VUb6GvCu09s2o2skAieW
MD5:	B8D64D0BC142B3F670CC0611B0AEBCAE
SHA1:	ABCD2BA13348F178B17141B445BC99F1917D47AF
SHA-256:	47B68DCE8CB6805AD5B3EA4D27AF92A241F4E29A5C12A274C852E4346A0500B4
SHA-512:	A684ABBE37E8047C55C394366B012CC9AE5D682D29D340BC48A37BE1A549AECED72DE6408BEDFED776A14611E6F3374015B236FBF49422B2982EF18125FF47D C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/js/jquery.min.js
Preview:	/*! jQuery v1.7.2 jquery.com | jquery.org/license */.(function(a,b){function cy(a){return f.isWindow(a)?a:a.nodeType===9?a.defaultView||a.parentWindow:!1}function cu(a){i f(!cj[a]){var b=c.body,d=f("<"+a+">").appendTo(b),e=d.css("display");d.remove();if(e==="none"||e===""){ck||(ck=c.createElement("iframe"),ck.frameBorder=ck.width =ck.height=0),b.appendChild(ck);if(!cl||!ck.createElement)cl=(ck.contentWindow||ck.contentDocument).document,cl.write((f.support.boxModel?"<!doctype html>":"")+" <html><body>"),cl.close();d=cl.createElement(a),cl.body.appendChild(d),e=f.css(d,"display"),b.removeChild(ck)}cj[a]=e}return cj[a]}function ct(a,b){var c={};f.each(cp.co ncat.apply([],cp.slice(0,b)),function(){c[this]=a});return c}function cs(){cq=b}function cr(){setTimeout(cs,0);return cq=f.now()}function ci(){try{return new a.ActiveXObj ect("Microsoft.XMLHTTP")}catch(b){}}function ch(){try{return new a.XMLHttpRequest}catch(b){}}function cb(a,c){a.dataFilter&&(c=a.dataFilter(c,a.dataType));var d =a.dataTyp

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jquery.tools.min[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):	141879
Entropy (8bit):	5.370568977972147
Encrypted:	false
SSDEEP:	3072:Dze8bbGzA81+xRRi1Z0CYjD9PvJXzEsB3YRIGY:D6LzA86SZAUm
MD5:	3670FDD8F3F21B458FAA07F7584D090A
SHA1:	24C13EE7E3CFE5C3B3644080F9C3836B927699FD
SHA-256:	E793C529244785A4EFC809969AB1DF4491689F96E79259583933A5D0DAF02A77
SHA-512:	EAD0D57487394B6582E5AB7C74E260F2B3F5302E663F9F7A9E6BE2B7864F84416AB8F3DBACCB683BD3B50D3E8D46E5472A9F139660F078F26630328F988B099D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/js/jquery.tools.min.js
Preview:	/*!. * jQuery Tools v1.2.7 - The missing UI library for the Web. * . * dateinput/dateinput.js. * overlay/overlay.js. * overlay/overlay.apple.js. * rangeinput/rangeinput.js. * scrol lable/scrollable.js. * scrollable/scrollable.autoscroll.js. * scrollable/scrollable.navigator.js. * tabs/tabs.js. * tabs/tabs.slideshow.js. * toolbox/toolbox.expose.js. * toolbox/t oolbox.flashembed.js. * toolbox/toolbox.history.js. * toolbox/toolbox.mousewheel.js. * tooltip/tooltip.js. * tooltip/tooltip.dynamic.js. * tooltip/tooltip.slide.js. * validator/val idator.js. * . * NO COPYRIGHTS OR LICENSES. DO WHAT YOU LIKE.. * . * http://flowplayer.org/tools/. * . * jquery.event.wheel.js - rev 1 . * Copyright (c) 2008, Three Dub Media (http://threedubmedia.com). * Liscensed under the MIT License (MIT-LICENSE.txt). * http://www.opensource.org/licenses/mit-license.php. * Created: 2008-07-01 | Updated: 2008-07-14. * . * -----. * . */*! jQuery v1.7.1 jquery.com | jquery.org/license */.(function(a,b){function cy(a){re

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jquery[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	96873
Entropy (8bit):	5.372169393547772
Encrypted:	false
SSDEEP:	1536:HYE1fGBiByJsbfXXeRJ/shgWCeLLccJdZVHk04ssx+/mvaSIFSet43tpXJIGVyp3:fsAg0psxTva/FSeKy2bDD5a98Hrq
MD5:	49EDCCEA2E7BA985CADC9BA0531CBED1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jquery[1].js	
SHA1:	F8747F8EE704D9AF31D0950015E01D3F9635B070
SHA-256:	1DB21D816296E6939BA1F42962496E4134AE2B0081E26970864C40C6D02BB1DF
SHA-512:	F766DF685B673657BDF57551354C149BE2024385102854D2CA351E976684BB88361EAE848F11F714E6E5973C061440831EA6F5BE995B89FD5BD2D4559A0DC4A6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-includes/js/jquery/jquery.js?ver=1.12.4-wp
Preview:	/*! jQuery v1.12.4 | (c) jQuery Foundation | jquery.org/license | WordPress 2019-05-16 */.!function(a,b){"object"==typeof module&&"object"==typeof module.exports? module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){var c=[],d=a.document,e=c.slice,f=c.concat,g=c.push,h=c.indexOf,i={},j=i.toString,k=i.hasOwnProperty,l={},m="1.12.4",n=function(a,b){return new n.fn.init(a,b)},o=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,p=/^-ms-/,q=/-([\da-z])/gi,r=function(a,b){return b.toUpperCase()};n.fn=n.prototype={jquery:m,constructor: n,selector:"",length:0,toArray:function(){return e.call(this)},get:function(a){return null!=a?a<0?this[a+this.length]:this[a]:e.call(this)},pushStack:function(a){var b=n.merge(this .constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a){return n.each(this,a)},map:function(a){return this.pushStack(n.map(this,fu

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\logo[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 214 x 47, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	3547
Entropy (8bit):	7.898570365711678
Encrypted:	false
SSDEEP:	96:B0dvP+c7G/ikcazUGS8P8CcVSlpOQNNEOK6GPii:B0z7YiBazs8Pg4lpOQrA6u
MD5:	BD9A01D567444161E6E4130475F5C3FE
SHA1:	08562119C8771AB2492E72B1389A2E2E70D5642D
SHA-256:	39BDBC528F0322B4C03D7A8BA9E3C7A45D2E51DB33762CDE8C568DE80A8EDBAC
SHA-512:	EC1334ED5AE56D6F086E8C9570B76593E4128C318AD210CFB8789CEF0D1E040DE37CCEFEA16C20D1BEABB7AC5782B4BB42D478868D80ACC96220B2055FBC19A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/img/logo.png
Preview:	.PNG.....IHDR...../.....~4.....IDATx....p.....C..$e.8e..e8ffffff.2....e.&e...w3..#.w%.Q.o....XZkw-.yN...-'...F...q...].5..Q.....8..{....!T]e}.....v.!..`WO.BU,.....U.....<.FU.....<....G1..0...T.1...$..?L.EW.G..>~+..0.....`we.X.:X@.c..b&&...5.r.#Ou2a.z..W#.V.3..[...`{...|^.....k.K.-.....o...e`.r...I.A..\....V..:..I..Ob)..2.....Z.Nw.x,.....s.?..;V..(.sq&*K.QS..n.0..X].....h.....Uu`.`...9<U`...9....d...za...d..._..+.:..:..1..C.H...c.&.d1.H.....!z.I."......ix}P.m...Nk.i.....>..)/...8.....J.BY..+.eP...h..(A..`...jqx.C.AQ....#HF1.qKx.S....^...N....Z8.0a .F`c.. ...i.....:.C.k...3>.....a0.z.7C.HLD4...k,D....W.?....(...n..8]q.../.0Lo\D.J\.X...{<...M.0X5.].0h..dW..;Q...#...4.]...`.....5.;ao4F...../.4._S....8...\....|._.'=...k...,...M..W.]..Db...mp<. ...U..A\..0....W..4.....Q<...Y...U|h...I..8...nU..A....}...<..w.y.K.XS.j}...m.....44.....5.>..G..R...i...pRcL.y..Ds..+.S....I.x...c...'O{..-..8..h..n.V6Ja.B..P.. .d..%gsB...C.6).:.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\mmyScript[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	3913
Entropy (8bit):	4.168992866508119
Encrypted:	false
SSDEEP:	48:kMEUAldPa1RYtDi2KE8/owu6YdDQh4DSci2J8/oOX+oKEAEYEs0u9KtdXRL8aG5:mU4aGtj8/owu3l+4e28/oOkdTqRdB8p5
MD5:	FDD3CEB8DFCBECD48CDED8DF7AD8A1B2
SHA1:	ABD85BAF2ADE362B9E119CAC93B411F9024231B0
SHA-256:	B8F7D0FE0562B40F07EA8CE85350A07E37C7A564F24921B21FABEEC3F78620E9
SHA-512:	B11FC3CEEC96BCCD6F11FAC2922E3DC1E0F4AE0CF1FFA57150CB2BBCB5126D7650304C05B8E8E2383874B31139447DFB64825C1A39B5B194CB4A3165FFAD637C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/js/mmyScript.js?ver=1
Preview:	jQuery(document).ready(function(){. //var ajaxurl = '<?php echo admin_url('admin-ajax.php'); ?>';. jQuery('#year').on('change',function(){. var year_id = jQuery(this).val();. if(year_id){. jQuery.ajax({. cache: false,. type:'POST',. url: ajax_object.ajaxurl,. data: {. action: 'dynamicDropdownMake',. nonce: ajax_object.nonce,. yearSelected : year_id,. slug: 'caryear=' + year_id. },. success:function(response){. // console.log('first step');. // console.log(response);. //jQuery('#make').html('<option value="">Now select a make</option>'); . jQuery('#make').html(response);. jQuery('#make').css('border','#f00 1px solid');. . }. }); . }else{. jQ

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\pe01MImSLYBIv1o4X1M8cce4G2JvY1MIVA[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 21848, version 1.1
Category:	downloaded
Size (bytes):	21848
Entropy (8bit):	7.978044399924035
Encrypted:	false
SSDEEP:	384:rkvr7QjFbgSnl68bOSHCDFg0sfNqS2RU4Vv6Da7sqhbEavryOhfO86WZfc:rkvYWSk8l+g0sfNqhLCm7sQcOhfX9Zfc
MD5:	FFC1F5C22DC4B08F710C027976972DE1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\pe01MImSLYBIv1o4X1M8cce4G2JvY1MIVA[1].woff	
SHA1:	6F1241E16BF7FB94B467E20437269A224990F783
SHA-256:	6105CF498916F50A2A117E9A7F8DC7C50A778FA5B5F77EA5610596309291A91A
SHA-512:	7823D4F67492905530DB2DE4B7D6100D66BF398EFC605726D9FAD8874B7E3D36113FAAC822B9719AA6567F432866A5BC6EAE4AE1979EBFBA7F19529A8F536A8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/nunitosans/v6/pe01MImSLYBIv1o4X1M8cce4G2JvY1MIVA.woff
Preview:	wOFF.....UX.....GDEF.....1...4.h..GPOS.....ukz.GSUB....._OS/2...|...R...`k..fcmap.....g.Ejcvt .....H....:...fpgm.....vd.zgasp..... ...glyf.....6...`..[Mhead..L....6...6...Mhhea..L....#...$....hmtx..L.....loca..N.....q.Y.maxp..Q.... ... .h..name..Q(.....*.F.post..R.....f.,|Aprep..T.....96Nox.c`d``.a..&.6.... ....?..d.....Q@2.!.H.3.00..%.....x...p.W.....hgA.....1.P..f..N9.z.._S.....y=..[..{.....D/{...F.s.....C.....}..._..M?.@.HK%.g.Z.-%j6...J... .1cG8...I.....0EI.\8...RKH).a... <=lw.a.....h..dS.W..}a/....k....~.I>.....~j&.G...0..../....p*..a..&.....W.A....pc.+\....F.5.-..@Z.?\.....z..Z..3..8...''..gD...S..I..P..Ur.Qv..9..()OEj4..o.....YD..(N..+./.....9R..Xc{#!! ....m....B...-.a....t.8.+.KQ.[.....3(..u...>.w._..N.".s.pm.{.._(.....o..wr..s6.r..].%l`.W..X_..~..f.{..[.....D.g..T.7..~.8.....j..a.4.i:.t.Y.z..j..J.....zui..4..~.Qy..Q~.r....Y..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\pe01MImSLYBIv1o4X1M8cce4G35sY1MIVA[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 21500, version 1.1
Category:	downloaded
Size (bytes):	21500
Entropy (8bit):	7.973555436759922
Encrypted:	false
SSDEEP:	384:Xthvj/ZusJD9ZPKMSnl6d8T2K8nXTyPy7j2mMLVD9qb4MJjc3BALn074xOMXBSki:XXj0sv5Sk6L8XTiGj2mMLVDEMP3SxZY1
MD5:	4F4E7A921CC52E9458245F66EB550004
SHA1:	F0A98C47D099BEA3808692D14FCB43D8FA44299F
SHA-256:	431B38EC872E6B82B92F607A1CD6C52DB32DDA558682A5391C5E961234C6AE82
SHA-512:	53AF7861E77BF67A87C1968F53F3A38DB22BDF1720A81F4497B6C5A23C9665B1398A5AAB60767E87A4EFA4EDC5409236AD0089F6A3C4399FE696A57066D27A6E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/nunitosans/v6/pe01MImSLYBIv1o4X1M8cce4G35sY1MIVA.woff
Preview:	wOFF.....S.....GDEF.....1...4.h..GPOS.....h.x.GSUB....._OS/2...h...R...`ku.Pcmap.....g.Ejcvt ...p...H....;s.%fpgm.....vd.zgasp..... ...glyf.....6N..^...head..K$...6...6...Jhhea..K\...#...$. ..hmtx..K.....loca..M.....>.&.maxp..O.... ... .g..name..O.....$..Kmpost..P.....f.,|Aprep..Sd.....96Nox.c`d``.a ..&.6.....?..d.....Q@2.!.H.3.00..%.....x...p.G.....Y.vG.....G.1333333_.1C.a....(..||f./.....ZG.....4....7D@..<..lOy.h....z..(.....B..7..=.\.....r|..r..D...Eh-..I...w.Sa&..W.....n.). .....T.K...x.d.....g...<v..[I4GJ..1....|{..[.=.q.=`.Uj.:<....G..@..Ju~.}.<..:.K..a.5...)".....0..H.3..VZ....*.....Q.b...J..'..L..\.P..\....B.J8.T.I.)B'.A.^?.bO.n._.{#.Z.).LN'.*.....\rb" .r.....r...\.....!b..?.5..O._....U....MY=m.."R...<...b^.K9.s....L.V..ul..6Q.....t.x.....SkB..n=\.....\.8k.k..FeI..dL.1I.,.`..z..F..%..K...'.M....._3.r ...e..V.....<.3A-..T'w7.j.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\pe01MImSLYBIv1o4X1M8cce4GwZuY1MIVA[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 21748, version 1.1
Category:	downloaded
Size (bytes):	21748
Entropy (8bit):	7.975059336534874
Encrypted:	false
SSDEEP:	384:Z+puxdFASnl6vEh4K50ktvu3v3RTuBmsVwJ10Xyr687i8GxOzNmwnv2oyc:sBSkke3vR4Wvkq6gi8GxOzNv/yc
MD5:	9DB53E390A5327462F45889E249F84D6
SHA1:	FBBB177CAD35A972877B3FF81276BB2AB8AC7B55
SHA-256:	BCF99FA50BCD85924BDB965047E3C47B345273302EA2251FFFDDEA07CD64D21D
SHA-512:	613C5CE0F22EFB6A99DA178BA512407138C43BC75C42FF8C9DAD5FE915C6D52B29BC55FA1C5BC1D7B094AD25EEFD72EEC78A2C205D44E639D13E34BBF9BF8 A06
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/nunitosans/v6/pe01MImSLYBIv1o4X1M8cce4GwZuY1MIVA.woff
Preview:	wOFF.....T.....GDEF.....1...4.h..GPOS.....ucy.GSUB....._OS/2...h...Q...`j..>cmap.....g.Ejcvt ...p...H....:.."fpgm.....vd.zgasp..... ...glyf.....6O..^pY...head..L$...6...6...Hhhea..L\...#...$....hmtx..L.....loca..N.....(?.`maxp..P.... ... .`..name..P.....^!.post..Q.....f.,|Aprep..T\.....96Nox.c`d``.a..&.6... .....?..d.....Q@2.!.H.3.00..%.....x...p#G..?.<....V.....(...By....;..}....._*kJ.@..3.oZ.`...E.H.}.....;_t.U...].!....]x...P...D....gu-.'..D.:]P.).G.tC..x!...a.I....cd[,..+.....$d.a...I.^..s.. ....1e..t._D".i{..;..... ..k....0.>G..._..x....a...9.g|._....O....."Y..@.....V. ...l[.....o..0...'.mP..I.....[..._.....E!"...(..$...B..Z."v/R...-...5.....+N3X><.~C.5.....FB...% o....s...7..|..3.@ o.*.T..9.w.rl.:H9...A.=..?<.b.....)..v[.x.Gs..r..s7..~.0...3....z[..&..G..m.....5ZC..=ZI..4:...ay.....%acI..%.[.....P.....jul...(..;.o....5.4,....0.f.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\picker.time[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	downloaded
Size (bytes):	32912
Entropy (8bit):	4.623680014109736
Encrypted:	false
SSDEEP:	384:JTm+0RELJehbr15X7AEvdcTIttRxlfkj9+XlrjRPHkEooY:Q+l9exLwT8Rxlfkj9A9RPHkEk
MD5:	BD1A2BDA8D60565B3E7B9F6BF99C2D5C
SHA1:	323F41810CF856636620F3B4A203AE40998F2421
SHA-256:	9E015E6AEF55943DE91CCB8E6AA12EEE5E2442AE64069F9F5D8D6C8CF7174CD4

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\picker.time[1].js	
SHA-512:	D83396501CA75383A475FB8BC00168B74EFAEEC560DA6EF1B8A35893F3B5D87C6EEBC3DF1A59D14AA0B329FD9612558A2B4BBD44908A60EE1EC5FD834A65F53F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/plugins/ultimate-member/assets/js/pickadate/picker.time.js?ver=2.0.49
Preview:	/*!.. * Time picker for pickadate.js v3.5.6.. * http://amsul.github.io/pickadate.js/time.htm.. */....(function (factory) {.... // AMD... if (typeof define == 'function' && define.amd).. define(['picker', 'jquery'], factory).... // Node.js/browserify... else if (typeof exports == 'object').. module.exports = factory(require('./picker.js'), require('jquery')).... // Browser globals... else factory(Picker, jQuery).}(function(Picker, $) {...../**.. * Globals and constants.. */..var HOURS_IN_DAY = 24,.. MINUTES_IN_HOUR = 60,.. HOURS_TO_NOON = 12,.. MINUTES_IN_DAY = HOURS_IN_DAY * MINUTES_IN_HOUR,.. _ = Picker._...../**.. * The time picker constructor.. */..function TimePicker(picker, settings) {.... var clock = this,.. elementValue = picker.$node[0].value,.. elementDataValue = picker.$node.data('value'),.. valueString = elementDataValue || elementValue,.. formatString = elementDataValue ? s

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\project-bg[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 768 x 400, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	140155
Entropy (8bit):	**7.993710928641032**
Encrypted:	**true**
SSDEEP:	3072:JzOqlhi6sscXtXtolgxh87EHuxxQWuRC+rvUrqvQe:JzzCycdtxh87EOcXyqd
MD5:	B0FBC142545C5DB8B0CB25F0F75F881E
SHA1:	69D783205DE498F0A80C58F2CBD3FB30A786B6C9
SHA-256:	2CEBEA417503263B242A821C7EA69CF125350D458F3AD253064EA7C64CAB387B
SHA-512:	076FE7753C299BCDAD5F894D01E46EDF2011ACD2569B6E530B66D39C1363EFBFD11F4F7C0A48435C3C4F08B37789726BAD106C6D55DF3D43056A49847A925BA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/img/layout/project-bg.png
Preview:	.PNG.....IHDR.....#BIDATx.....:.E.1333c.2333?ffffff~...9..tg.;=W..8.....T.?Y.1....u.9g..g.....u..Yc.../_.|.y..\.:..3g.-.+._.~.U....d...6l.5k...6o.L..o.].....~g.....S..z..sMu..%/T..X...S....^..uo|...~r.....?p....<.y.4`'d.gC1.....3....GdDC@.W.^.D)...\9..s.6..B.\..Tf....[.x.E....b..~.K...:J..M-..Y.....T.N..n....W.t..'.3.....k..s2..X\.2_. ..}t...T.....#..l../....'...O.W.K_..b.)..E...,..P0z.!.c.U. ..3c+?.....1.F. .,...).hN...h.X...u..d....C..`....aZ1TLR;e.K.,.y..i.|...+.....M.....3.$.>....$.Y.X.t)...b...\=...L].V...S..p.t....j.W..Cn..R.k.....[...'.>.Qz..yz(=.(5..E].IcNJUi.~...&....#...]...c..7n.....5...w.].T...e..U#:..d...3..c.....o..A;...{..p.....q.t._<..o....n..7.|.....v.....x.f.t.N..N.M.t.(7'....r..i.,.nR.y._..G.F..?H.T.a..C...ni...5.4E..O.....}...w]u.C.}?..O.W.D...u....N....j.RP..'.(.".oU...f..p.....+gx.....}..sl..=...67uN..nu.[...Sp.+.B.%.N..I.A...R.h!@ .B..:.`...f*;ry...t.Q.|7..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\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):	349230
Entropy (8bit):	5.681273555765867
Encrypted:	false
SSDEEP:	6144:k39XiQQceX9BPPqntfhhAjbUZgDIEC4YdErH/Ix6Upy85IdF1/g10eGGiv:8XReX3OqI6DIEKdKjSPs
MD5:	12965F56FF729FA548EA0D3628C9FB36
SHA1:	3D6357ACD7C51674BD7FF77CC666476E45822FD4
SHA-256:	7AB6A25B3BFE17A0705D5017781DF867BA5CCB3238943115697016FFD35E19E0
SHA-512:	07EB2DE4196F46D9A5AA67E35D4B5D5A7D2E1EF367F08B69A3C5B660D9BB61581D21AC211B6751A2C34021263AB8FBD80246FFF29667FB5AAA2A1397D318E1B4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/recaptcha/releases/FDTCuNjXhn1sV0lk31aK53uB/recaptcha__en.js
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var B=function(){return[function(r,J,q,a,g,E,K,z,T,I,d){if(((r|(((r>>((r-(d=[1,13,3],7))%6||(T="visible"==B[17](d[0],g,K.D),h[40](37,K.D,{visibility:z?"visible":"hidden",opacity:z?"1":"0",transition:z?"visibility 0s linear 0s, opacity 0.3s linear":"visibility 0s linear 0.3s, opacity 0.3s linear"}),T&&!z?K.I=V[23](28,function(){h[40](69,this.D,"top","-10000px")},J,K):z&&(X[27](92,K.I),h[40](65,K.D,"top","0px")),E&&(V[d[2]](11,a,E.width,h[12](5,q,K),E.height),V[d[2]](21,a,E.width,V[31](16,q,h[12](d[1],.q,K)),E.height))),d[0])&15||(I=(g=a(q(),35,5))?g.type:-1),r)^161)%21||(J.Jw=q),d[0]))&31)==d[2])V[12](28,function(f,n){e[31](72,this,f,n)},q,J);return(r<<d[0])%15||(a.nT&&q!=a.pQ&&B[16](12,J,null,a,q),a.pQ=q),I},function(r,J,q,a,g,E,K,z,T,I){if(!((r-6)%(T=["complete",2,26],13))){K=' '),"rc-anchor-error-message",7],a.errorCode),a.errorMessage),28](15,"rc-inline

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\sbi-scripts.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):	25969
Entropy (8bit):	5.21890839308579
Encrypted:	false
SSDEEP:	768:/lFGnxHjh1AKfk4OkSG0Lksf7aWoNR8O2/EwuS6V2LVBaAs+UCQnhtor:/4HlD53Ldtor
MD5:	1A3D51239BCAD53BA60ADFB5AB4CA827
SHA1:	CF4FB22997571766F5F5BD9E11F22DACEEECC0C8
SHA-256:	2717481D28D98B22E3277C45A2A0529B5044AEF42D8F262CA7E11E73240C563D

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\sbi-scripts.min[1].js	
SHA-512:	9FB4530B47073F93244205A515D40A59206CCB33C75A1131A8B3941D2B014D154683F6837CBA431EC82FC26DC19C68C41AEC104CFAA1F7E63A2D2B83698BCE9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/plugins/instagram-feed/js/sbi-scripts.min.js?ver=2.9.1
Preview:	var sbi_js_exists=void 0!==sbi_js_exists;sbi_js_exists||(!function(i){function e(){var i,e,t,s=s||{VER:"0.9.944"};s.bgs_Available=!1,s.bgs_CheckRunned=!1,function(i){i.fn .extend({sbi_imgLiquid:function(e){this.defaults={fill:!0,verticalAlign:"center",horizontalAlign:"center",useBackgroundSize:!0,useDataHtmlAttr:!0,responsive:!0,delay:0,fa deInTime:0,removeBoxBackground:!0,hardPixels:!0,responsiveCheckTime:500,timecheckvisibility:500,onStart:null,onFinish:null,onItemStart:null,onItemFinish:null,on ItemError:null},function(){if(!s.bgs_CheckRunned){s.bgs_CheckRunned=!0;var e=i('');i("body").append(e),function(){var i=e[0];if(i&&window.getComputedStyle){var t=window.getComputedStyle(i,null);t&&t.backgroundSize&&(s.bgs_Available="cover"===t.backgroundSize)}}(),e.remove()}}();var t=this;return this.options=e,this.settings=i.extend({},this.defaults,this.options),this.settings.onStart&&this.settings.onStart(),this.each(function(e){function n(){(r.responsive|

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\sh.f48a1a04fe8dbf021b4cda1d[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	72412
Entropy (8bit):	5.387358706587146
Encrypted:	false
SSDEEP:	1536:8V69lS5FN9hXuSja0+S+4p94gHaF1NCo+mzITLE5zv:88lStbuy+4pag6jNCaIUl
MD5:	AACCA0023866ABEF872428C704F65AE9
SHA1:	8C653A4221EC9A027A6AFC42BC2D376D613D5BB4
SHA-256:	55D783462E6671FA985A6B0829DB15474F4E57F0555C93E15CC2DB6A1D1E6CAB
SHA-512:	F92BE33D2DB5B072358905F4E07320F69EAECCF54CE9F31579506ADD7C4D9FCA02340DADCFE6AA3D7D32BBBDFC8331C523C535DB9E06F5410044F164915185C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://s7.addthis.com/static/sh.f48a1a04fe8dbf021b4cda1d.html
Preview:	<!DOCTYPE html><html><head><meta http-equiv=Content-type content="text/html; charset=utf-8"><meta name=robots content=noindex,nofollow><title>AddThis Utility Frame</title></head><body><script>/*!.AddThis - v8.28.6 - 20200604;.Copyright (c) 1998, 2020, Oracle and/or its affiliates..*/../*!....invariant : 2.1.0.BSD.Copyright (c).All rights reserved...Redistribution and use in source and binary forms, with or without.modification, are permitted provided that the following conditions are met:..* Red istributions of source code must retain the above copyright notice, this. list of conditions and the following disclaimer...* Redistributions in binary form must reproduce the above copyright notice,. this list of conditions and the following disclaimer in the documentation. and/or other materials provided with the distribution...* Neither the name of invariant nor the names of its. contributors may be used to endorse or promote products derived from. this software without specific prior wr

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\signup[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1024 x 395, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	740031
Entropy (8bit):	**7.99883806468739**
Encrypted:	**true**
SSDEEP:	12288:VOIg1A/lWfhRXp7cI4pwOI7xmHU8VHe7y0k5kae+N+t+Cdv7JXB2QllnyL/DR3jn:gIkzfhRZF4pwxmHU4HeG0MkYN+t+CdvW
MD5:	1F797E6B915AAC8A0B7A228A81F37A34
SHA1:	E8DA83D401D6FC47CDC3F93D510BBEC29334E569
SHA-256:	3F648FA2012779EA96627AA4A84B3393444522BC30F67B2B9E2FF93677413E74
SHA-512:	5DA35B71B3E5C852D5829873877AF311986BD7893F8BD577798AC7562F2C1816CBCDA9BB92CD89AE8455B4A0B508A4A063B25C7B41562FF6E9550992DE0B284
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/img/banners/signup.png
Preview:	.PNG.....IHDR.....0wh..J.IDATx.LS.r.:.3.v....W. N...i....Ij.=G....uA.2S."..Af0K.....GkvhS..0..C..R...p.....V...E.3...5Wq.D.....j...I..@D..s]...-.....T.....2....^...@. .^.,.d..zE. .>=y....5.:|.yB*..'..k.....Dd..?....w%..3^WZ....;H.R..J....J...}_;.2d.....K.dg.{-..zQ.....;B...g..3{.&ed.?..#.z.y}]..<A]...T_.5.7w...2V.~...."....5.I...0;...V..5s..5>.!.U.H..i.{.^.,b..f_..@S.~.^ {../m.0.:...kmf.x1.....Xz.n...AW8..?.2e<.....i..$C.5.}.^.u.i@.....a.8L..A.*.SQ..Z.....2.5.v.go.6)...#k.....3+k.=.e.8...3.#t. mH7.u..P.....R5>..d.w-T.....a.,..g. .Z.Jf..?3S..#...a ...333C8...-J.V....._.....X..XV.uY.o.k..0...-.W..e.8...d%..UC0`.s.P..8U.$..0Y....5.4.r...Da..j.JiMD.C.....j.(....F.(...u+.Y...1$,.....q....l.lZ.0..%!.o.,Q..p....8..(dI.....I.....fp.u.:.(..q\.Zc. I{C..OZ....N.7..P.Y.?.jUY0...e..S.Y%WF%1g.!....Kc5.....b..>.....s...4.. .....$.....!.-...&v..:.....F.....p\..P:FQ..HD.D.W@.....b.p..W....zc..8.5.5h...T..t.XW.EU...aP+v..y

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\simplebar[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	4010
Entropy (8bit):	4.654878853814922
Encrypted:	false
SSDEEP:	96:rv3NCZV0EUwKCKbZwyBvMzpwAzJ3sH0N9KZdUGFjMG:DNCZbthKbjBUzTl3sUNQZdUSMG
MD5:	E0681482AAF0007FD323A9DA1CE7F675
SHA1:	FE4F1F31A51003CB390CC4ACAD6704436F370CEB
SHA-256:	40351D0A5D0AB0784A64C8CA49769B1FEC801A4F032A734BD5C16C999364E19C

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\simplebar[1].css	
SHA-512:	A4DDD3764EB54A1DA3247FB2B4D678571ADD240E91CD01C2FDC66A0E4A9B331FBEA1DC5DE2906992739E82225EE38657A40A7537A21F3748587505FF6B10359
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/plugins/ultimate-member/assets/css/simplebar.css?ver=2.0.49
Preview:	[data-simplebar] {.. position: relative;.. flex-direction: column;.. flex-wrap: wrap;.. justify-content: flex-start;.. align-content: flex-start;.. align-items: flex-start; ..}.....simplebar-wrapper {.. overflow: hidden;.. width: inherit;.. height: inherit;.. max-width: inherit;.. max-height: inherit;..}.....simplebar-mask {.. direction: inher it;.. position: absolute;.. overflow: hidden;.. padding: 0;.. margin: 0;.. left: 0;.. top: 0;.. bottom: 0;.. right: 0;.. width: auto !important;.. height: auto !important;.. z-index: 0;..}.....simplebar-offset {.. direction: inherit !important;.. box-sizing: inherit !important;.. resize: none !important;.. position: absolute;.. top: 0;.. left: 0;.. bottom: 0;.. right: 0;.. padding: 0;.. margin: 0;.. -webkit-overflow-scrolling: touch;..}.....simplebar-content-wrapper {.. direction: inherit;.. box-sizing: border-box !important;.. position: r

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\style[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	83200
Entropy (8bit):	4.800034711220551
Encrypted:	false
SSDEEP:	1536:5rzwH3+xW1IRRV4x4J9uzPjJCrs7CbT5H0089BERx5DsH7LenMQ7johpxsQND:xzwH3+U1IRr4xQuzPjgs7CbT5Hd89BE+
MD5:	67EC93628F57F1399A44AB7B07B39D21
SHA1:	D067158E23F8EE63AAADA8F8A4AB9A6DC763870E
SHA-256:	8CBB1F43E69C4DD29229D23974ECB88F0B0DE4E6436313F2E22BB274C84CA279
SHA-512:	5C713DAD4FB505E028BCFECC1A48B0B11E9C7D404D7C6C24C507532A1418638DFD5BCCF13E6DFD9EAF5DD9C81BA919DA51A6ADC1894E0C80A82796106CEC E55
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/css/style.css
Preview:	/*@font-face {. font-family: 'Nunito Sans', Arial, Helvetica, sans-serif;. src: url('../fonts/Avenir.ttf');. font-weight: normal;. font-style: normal;.}*/..@import url('https://f onts.googleapis.com/css?family=Nunito+Sans:400,400i,600,600i,700,700i,800,800i&display=swap');../*.Font Stack.font-family: 'Nunito Sans', Arial, Helvetica, sans-serif;.*/ ..body, html {. min-height: 100%;. height: auto;.}..body {. padding: 0;. margin: 0;. background-image: url('../img/bg.jpg');. background-repeat: repeat-x;. bac kground-color: #626262;. font-family: 'Nunito Sans', Arial, Helvetica, sans-serif;. font-size: 15px;.}..img {. outline: none;. border: none;.}..p {. padding: 0;. margin: 0;. margin-bottom: 15px;.}..h1, h2, h3, h4, h5, h6 {. font-family: 'Nunito Sans', Arial, Helvetica, sans-serif;.}..a {. color: #00aeef;. transition: all 1s;. -webkit-transition: all 1s;. text-decoration: none;.}..a:hover {. color: #005b7d;.}...black {

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\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):	52867
Entropy (8bit):	5.958224586944697
Encrypted:	false
SSDEEP:	768:+LUmmAWTe2uXYp8Mi+yKSrKebyBwd/Dl+x2d5YPcPoiDH1fkQJVEwY:4UcW6v+2rKwFDlDP7dnY
MD5:	B1207A1EFB3FC87C56B8EEC39EC65B4C
SHA1:	C1F3A3A13E5D0595AC22227B12FEF4949C7C79E0
SHA-256:	5FE20047C1CC1BE61A786D56C5C02B96453B9C60656D6C8429A1ADD79017E47F
SHA-512:	A4F7279F7C1BB35B9239712C4B954E752FF98739AB38520F1B8E12A75485EA6F2890EBA6AD7FDF074C94928FFA7ECA5A84B32AEAC9EBB10467AC6F082BE189E 7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/recaptcha/releases/FDTCuNjXhn1sV0lk31aK53uB/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+AAAACXZwQWcAAABUAAADSAC4K4y8AAA4oElEQVR42u2dCZRV1ZX3q5iE4IQIiKQQCKBt0JLEIUZwCCk 7pBNFiRMajZrIl9aOLZ8sY4CWdkDbT2McooaAEmNixFhpaYE2dCiLScWiQHCgoGQoGQuhGArKKl7V+c5/n33fO/V4w733nVuheXuv9V/rrnvP2Xud3zvTPee+ewsKxMTEx MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExP4OdtlT6ztAbRWvvLy8A3QkwxzH6tBGMMexI

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\tire-paint[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 157x105, frames 3
Category:	downloaded
Size (bytes):	9090
Entropy (8bit):	7.931583888105609
Encrypted:	false
SSDEEP:	192:HW4QZzo6DrxCtYEEkxtv5SdeT9Zv9Xfjav1uM/0YniNAQnopms2k:HWLZzrrstYET/v5ieT5jCggniNG
MD5:	01D80CA5DFBC65C2EE5E30CB919A6465

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\tire-paint[1].jpg	
SHA1:	437EF7B64627B92CCB37EF2E6374CBCDCD6867F0
SHA-256:	F1DCADB1339E6D33042A4934C4BB5CCE1AB9AABFED148898665A2937B6C6DCF8
SHA-512:	BF2E9604B032928A16908B9C3784CC20BFF164AD8A09BC82F2C1B3EA41656AB73E7956DFC478564D47982D7FBAC7EB3FD8271B0B1E94D1C460382B9D3660EDA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/img/thumbs/tire-paint.jpg
Preview:	.....JFIF.....i.....(T3w#.r_>.....Y...Glq.1.....F ~..@.^..2..$\|...q...~...5.<.7Yl...O.....f.._W...+.....Gr.g..]/^.....S4; ..!..e..SD.u...@.-.q.j.<Z...<.m[."..g}T..g....MS{..T..dZ..`.._".s&.....%@..*..7..p...../.....\|.[0...K._c.mD.L .R2....U~e.^....MS0..sm{/..E.rax.K...vE....n.....T....<...S.E.....jX...n.]Y.y.....SW....7y.sg....>.y^.....]....P.H.<.w+.u?.?.....B.Z.g.....D...C...D...Z.N .....:...O;.\l.-V.~NH5..H..WW.....D.l9?.....'...k.<..t...XE(..@.A..}..T.wlu..<...6?..=..._..5.....r.{x....x...q.6...M5.8...ut.yswj\|h.^N".V<yj.9..n.....v....-...r.9 ...5.i+1..&.I./.Rjh.....J.%.L. ...1..m.`..../.....!12..."A..#B4$%&36a.....~;.r.T..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\tr[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):	44
Entropy (8bit):	2.8317663774021287
Encrypted:	false
SSDEEP:	3:CU9yltxlHhn:mn
MD5:	B798F4CE7359FD815DF4BDF76503B295
SHA1:	F8CC6ADDF1707AD236AD9970B0A48F9733D07DA5
SHA-256:	10D8D42D73A02DDB877101E72FBFA15A0EC820224D97CEDEE4CF92D571BE5CAA
SHA-512:	921944DC10FBFB6224D69F0B3AC050F4790310FD1BCAC3B87C96512AD5ED9A268824F3F5180563D372642071B4704C979D209BAF40BC0B1C9A714769ABA7DFC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.facebook.com/tr/?id=979841368838586&ev=PageView&dl=https%3A%2F%2Fwww.duplicolor.com%2Flogin%2F&rl=&if=false&ts=1624410553006&sw=1280&sh=1024&v=2.9.5&r=c2&ec=0&o=14&fbp=fb.1.1624410553005.1854332800&it=1624410552202&coo=false&rqm=GET
Preview:	GIF89a.....!.....,.....D..;.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\um-account.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):	2007
Entropy (8bit):	4.913226002591
Encrypted:	false
SSDEEP:	48:kM2D4S9yu5j0l4d49afrzxCH8l4KUEotN:IE4yu5j0qd4cfrzxCH8qKdotN
MD5:	A50C27ED60C4598864DE21DE703B82AD
SHA1:	ACE21F9042D54448C832EACFC7DC64CF192AE8BB
SHA-256:	C8620F7F0FD52B541C99A967B6715D293AD0EA6074993CE568EC459D483779EF
SHA-512:	4AB258376DBAC66844380D680D4D4FEE6A44A565475C61BD12872DF4EBC8B25B5C86D68ABF4B7C84BB16B21786E959F7AB27E3C529AB897F83A943987806C82
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/plugins/ultimate-member/assets/js/um-account.min.js?ver=2.0.49
Preview:	jQuery(document).ready(function(){var a=jQuery(".um-account-main").attr("data-current_tab");a&&(jQuery('.um-account-tab[data-tab="'+a+'"]').show(),jQuery(".um-account-tab:not(:visible)").find("input:not(:disabled)").addClass("um_account_inactive").prop("disabled",!0).attr("disabled",!0)),jQuery(document.body).on("click",".um-account-side li a",function(a){a.preventDefault();var t=jQuery(this);t.parents("ul").find("li a").removeClass("current"),t.addClass("current");var u=jQuery(this).attr("href"),e=jQuery(this).attr("data-tab");return jQuery('input[id="_um_account_tab"]:hidden').val(e),window.history.pushState("","",u),jQuery(".um-account-tab").hide(),jQuery('.um-account-tab[data-tab="'+e+'"]').fadeIn(),jQuery(".um-account-tab:visible").find("input.um_account_inactive:disabled").removeClass("um_account_inactive").prop("disabled",!1).attr("disabled",!1),jQuery(".um-account-tab:not(:visible)").find("input:not(:disabled)").addClass("um_account_inactive").prop("disabled",!0).attr("disabled

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\um-conditional.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):	8674
Entropy (8bit):	5.130825943096447
Encrypted:	false
SSDEEP:	96:wU5SCV0p5M93E0PRRWqUCoddFwmKFKbkVlgoDp5zq1ezmTzgC4WrcWUUAWQFjs34:7f3+se8uYzm3ORWdAWQF5
MD5:	AF65DF74DAE8A6782BD716D890F03F49
SHA1:	F1027D1C7655F92B99AE4AB05B453A2D1447C725
SHA-256:	EA57576045CB736253DC3250201A891C856BB4BF6B28D6BA989EAF909004B13F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\um-conditional.min[1].js	
SHA-512:	3354AE77FDD5584647D04CFAFCDD97CD15906D8D2C742438DCFB944F9F01B2B9E5EB4CC3934BEBA382A82963B5D06B13D8CC307BE1A7DB48FDAFAE8FDAE6FDF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/plugins/ultimate-member/assets/js/um-conditional.min.js?ver=2.0.49
Preview:	var arr_all_conditions=[],um_field_conditions={},um_field_default_values={};function um_get_field_default_value(e){var i="",n=um_get_field_type(e);switch(n){case"text":case"number":case"date":case"textarea":case"select":i=e.find("input:text,input[type=number],textarea,select").val();break;case"multiselect":i=e.find("select").val();break;case"radio":1<=e.find("input[type=radio]:checked").length&&(i=e.find("input[type=radio]:checked").val());break;case"checkbox":1<=e.find("input[type=checkbox]:checked").length&&(1<e.find("input[type=checkbox]:checked").length?e.find("input[type=checkbox]:checked").each(function(){i=i+jQuery(this).val()+" "}):i=e.find("input[type=checkbox]:checked").val())}return{type:n,value:i}}function um_get_field_element(e){switch(um_get_field_type(e)){case"text":case"number":case"date":case"textarea":case"select":case"multiselect":case"radio":case"checkbox":return e.find("input,textarea,select")}return""}function um_get_field_type(e){var n="",i=e.attr("class");return

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\um-fileupload.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):	9072
Entropy (8bit):	5.250363009887606
Encrypted:	false
SSDEEP:	192:TEueBnn9Nf5KvTaYkVlbvxOW2/oWVHQDdlt:wn9Nf58svzoW2nVs/t
MD5:	0F0E02244123E576E7AACA9A6FDBFD95
SHA1:	874E8F3B4D14D800A1134E4107FCC246FA20CDB1
SHA-256:	C4468D5C285B94136FC22E2FD1F580CDBAAC94DDD15CED07EC93686C8C7DE12D
SHA-512:	62E542A1F87449209D582A5C3BC0A19110CE8A6DAD7546940BB973D8E1923F46C0B254419CF23C6AFB9EE465B530915D71CBB6014407DECA489C9EE6A1229B6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/plugins/ultimate-member/assets/js/um-fileupload.min.js?ver=2.0.49
Preview:	!function(S){S.fn.ajaxForm;var C={};C.fileapi=void 0!==S("<input type='file'/>").get(0).files,C.formdata=void 0!==window.FormData,S.fn.uploadFile=function(e){var p=S.extend({url:"",method:"POST",enctype:"multipart/form-data",formData:null,returnType:null,allowedTypes:"*",fileName:"file",formData:{},dynamicFormData:function(){return{}},maxFileSize:-1,maxFileCount:-1,multiple:!0,dragDrop:!0,autoSubmit:!0,showCancel:!0,showAbort:!0,showDone:!0,showDelete:!1,showError:!0,showStatusAfterSuccess:!0,showStatusAfterError:!0,showFileCounter:!0,fileCounterStyle:"). ",showProgress:!1,onSelect:function(e){return!0},onSubmit:function(e,r){},onSuccess:function(e,r,t){},onError:function(e,r,t){},deleteCallback:!1,afterUploadAll:!1,uploadButtonClass:"upload",dragDropStr:"",abortStr:"Abort",cancelStr:"Cancel",deleteIStr:"Delete",doneStr:"Done",multiDragErrorStr:"Multiple File Drag & Drop is not allowed.",extErrorStr:"",sizeErrorStr:"",uploadErrorStr:"Upload is not allowed",maxFileCountErrorStr:""},

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\um-fileupload[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	troff or preprocessor input, ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	3724
Entropy (8bit):	5.071180964909233
Encrypted:	false
SSDEEP:	96:QPddnboBeJp6JHSgb0KLaIzd29KUBP73W2FuG:CbMgJIJHSIFYjBTmgd
MD5:	CAFAD536F053C0A2E9859759402CB72B
SHA1:	85DB33EBE2345D399D7FD348B4C55928560664FF
SHA-256:	05AF7422B28299B44CD5561D8C328CF6C27FDE5EB58946EC8C7CD5011CC9D8AD
SHA-512:	429E07F7F089CBF5FDE27EC99CFBC1C51AC06C53F416EDBB88F5CC675C700D3599874FF5D6541E3CABD881FAF3797A498F35C2F6DA57893A9A44EC10092054F7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/plugins/ultimate-member/assets/css/um-fileupload.css?ver=2.0.49
Preview:	/*...- image preview..*/.....um .um-single-image-preview,...um .um-single-file-preview {...margin-bottom: 20px;..}.....um .um-single-image-preview > img {...max-height: 300px;...display: inline-block;...overflow: hidden;...margin: auto;...-moz-border-radius: 3px;...-webkit-border-radius: 3px;...border-radius: 3px;..}.....um-single-image-preview,...um-single-file-preview {...display: none;...text-align: center;...position: relative;..}.....um-single-image-preview.show,...um-single-file-preview.show {display: block}.....um-single-image-preview > img {...max-width: 100%;...max-height: inherit;..}.....um-single-image-preview a.cancel,...um-single-file-preview a.cancel {...position: absolute;...top: -15px;...right: -15px;...width: 30px;...height: 30px;...-moz-border-radius: 999px;...-webkit-border-radius: 999px;...border-radius: 999px;...background: #ddd;...cursor: pointer;...text-decoration: none !important;...z-index: 666;...opacity: 0.75;..}.....um-single-image-preview a.cancel i,...um-s

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\um-functions.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):	14931
Entropy (8bit):	5.219429155830358
Encrypted:	false
SSDEEP:	384:nheFKsKn4C6dtafO2BI9opccJIQgv8uWrQd:nhedLP2S9opccJpgv1
MD5:	11630202F9BE072703B7F7C5BEF80D75
SHA1:	D9AB9864722CD232B027044CD8EFC904CDD6982F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\um-functions.min[1].js	
SHA-256:	2E9107D6004B2DBE25408AE58940A7673A9CAA6D46571280A10C0FD778D0935F
SHA-512:	D44D11715B23758D92606336B12E94B01FCE07BD5DCFF13CE6F451A2A986C6B96D1CA4DD561472C9BB63DB267D5E302F492A1F7814AD3E403B9BD59B7F78A7I 0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/plugins/ultimate-member/assets/js/um-functions.min.js?ver=2.0.49
Preview:	function UM_check_password_matched(){jQuery(document).on("keyup","input[data-key=user_password],input[data-key=confirm_user_password]",function(e){var t=jQuery("input[data-key=user_password]").val(),a=jQuery("input[data-key=confirm_user_password]").val(),i=jQuery("input[data-key=user_password],input[data-key=confirm_user_password]");t||a?t!==a?i.removeClass("um-validate-matched").addClass("um-validate-not-matched"):i.removeClass("um-validate-not-matched").addClass("um-validate-matched"):i.removeClass("um-validate-matched").removeClass("um-validate-not-matched")})}function UM_hide_menus(){var e=jQuery(".um-dropdow n");e.parents("div").find("a").removeClass("active"),e.hide()}function UM_domenus(){jQuery(".um-dropdown").each(function(){var e=jQuery(this),t=jQuery(this).attr("data-el ement"),a=jQuery(this).attr("data-position");jQuery(t).addClass("um-trigger-menu-on-"+e.attr("data-trigger")),jQuery(window).width()<=1200&&"div.um-profile-edit"==t&& (a="lc"),"lc"==a&&(jQuery(t).find("img").wid

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\um-gdpr.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	293
Entropy (8bit):	4.758865300371745
Encrypted:	false
SSDEEP:	6:qQ2byi9G1sYTyXXg8cdZdShIkC/ZdXW1T6rWmM9V9ZdXW1NMvrWEnMQnn:xNmXXg8CZdShIkC/ZdXW1T6NM9V9ZdXV
MD5:	B7AAE6BE6F2A077506CA65EF312512EA
SHA1:	A54B0FECF54A0C130779440544B789D1B95E9FED
SHA-256:	4007F2F1679D321EB40023D03D99D30899145BFD402FC7BE5ABDD50AD41F4035
SHA-512:	BA150907DC6FB0DB234827A393CC9DB59D6BE6E6284A90F3D0BE611F66026066B7D592EF760A4B65223EE772969CE99A3B0BE41A340519C2C103EEDB4ACBAE 6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/plugins/ultimate-member/assets/js/um-gdpr.min.js?ver=2.0.49
Preview:	!function(e){"use strict";e(document).on("click","a.um-toggle-gdpr",function(){var t=jQuery(this);e(".um-gdpr-content").toggle("fast",function(){e(".um-gdpr-content").is(":visible")&&t.text(t.data("toggle-hide")),e(".um-gdpr-content").is(":hidden")&&t.text(t.data("toggle-show"))})})}(jQuery);

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\um-members.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):	1437
Entropy (8bit):	4.8814050775669
Encrypted:	false
SSDEEP:	24:zAMkz8pk1wE19aah1Lz9H8Nh1LzB4EB4aXHAbQ/z+yj8Yj8p9N484SCwL4tXw3Aj:kMZhcSf1tw9b9NXRLWgw9b9N/2iNXt9d
MD5:	D41DFB5A8074E2D3C3AC9F99BC34CE2B
SHA1:	476A1A16230527F3B271E6B80AC3889BC3258276
SHA-256:	5977D83CE740BBD1B9266627C4BF4EE7BE961A5B6AF2FB28DF982BBE487B4070
SHA-512:	F62A93FA0FB00DC40CA1F94299B078601BED2E9ED10476BFDBA9F50743EE0E9B0672E576A148013AECC5AEB2FAE2C627F6BEDB09036E706DA4BFAF3CDEF3F 7CB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/plugins/ultimate-member/assets/js/um-members.min.js?ver=2.0.49
Preview:	jQuery(document).ready(function(){jQuery(".um-members").each(function(){UM_Member_Grid(jQuery(this))}),jQuery(".um-directory .um-member-connect").each(function() {0==jQuery(this).find("a").length&&jQuery(this).remove()}),jQuery(".um-member-meta-main").each(function(){0==jQuery(this).find(".um-member-metaline").length&&0 ==jQuery(this).find(".um-member-connect").find("a").length&&jQuery(this).remove()}),jQuery(document.body).on("click",".um-member-more a",function(e){e.preventDe fault();var r=jQuery(this).parents(".um-member"),m=jQuery(this).parents(".um-members");return r.find(".um-member-more").hide(),r.find(".um-member-meta").slideDo wn(function(){UM_Member_Grid(m)}),r.find(".um-member-less").fadeIn(),setTimeout(function(){UM_Member_Grid(m)},100),!1}),jQuery(document.body).on("click",".um-me mber-less a",function(e){e.preventDefault();var r=jQuery(this).parents(".um-member"),m=jQuery(this).parents(".um-members");return r.find(".um-member-less").hide (),r.find(".um-member-meta").slideUp(fun

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\um-misc[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	1963
Entropy (8bit):	5.032102625257653
Encrypted:	false
SSDEEP:	48:WMrsQCZnYal6f7v71nGrSIB6eqxDCnsnDioAaDdp3lYk:WMr2f6f7vBnGtByxDCnzojd3
MD5:	E77E47646D4132C1C2863A6042F37A51
SHA1:	299259BFB4EC69AB8130C026405440626D76FCE3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\um-misc[1].css	
SHA-256:	69758DD18B4F18F10BDEDFEBC078EC24D39EE93EC14019F662FBBC89758DEF0F
SHA-512:	D84F07E27F3CC9B13A4F5AD5092E556740CDA2267CE41FECAF262BF8CD4DA3590A0C2D438A5EF814A2469CD28E07D7C80D2194D9083B66CB386633BB5E358F3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/plugins/ultimate-member/assets/css/um-misc.css?ver=2.0.49
Preview:	.um-login.um-logout {...max-width: 300px !important;..}.....um-misc-with-img {...position: relative;...font-size: 15px;...border-bottom: 3px solid #eee;...text-align: center;..... margin-bottom: 14px;...padding-top: 4px;...padding-bottom: 14px;..}.....um-misc-img {...text-align: center;..}.....um-misc-img img {...border-radius: 999px;...height: auto !important;...display: inline-block !important;..}.....um-misc-ul,...um-misc-ul li {...font-size: 14px;..}..../* responsive embeds */...um-youtube,...um-vimeo,...um-googlemap {.. .position: relative;...height: 0;...overflow: hidden;..}.....um-youtube {padding-bottom: 56.25%;}...um-vimeo {padding-bottom: 56.25%;}...um-googlemap {padding-bottom: 75%;}.....um-youtube iframe,...um-vimeo iframe,...um-googlemap iframe {...position: absolute;...top: 0;...left: 0;...width: 100% !important;...height: 100% !important;..}..../* profile misc */...um-profile-connect.um-member-connect {...padding: 5px 0 10px 0;..}.....um-profile-connect.um-member-connect

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\um-old-default[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	troff or preprocessor input, ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	5914
Entropy (8bit):	4.938447418565638
Encrypted:	false
SSDEEP:	96:zhAVkL8slW4f/B0X7r5gt3gthmhX7rq8zjA:9okL8slWZX7r5qVX7rY
MD5:	974C83B93521B86CE94C15D63C9CCF1E
SHA1:	AA430F77CB50347B4C0A53B4B066ABF74E18AEB7
SHA-256:	56C414DBA3B9200B6A218EDDF54F486F8280DC4D9620C265A861E107B1C8500C
SHA-512:	D92F2713EEB624C6D29D55FCD98A2B11C753C4AF489D6A28179EB439EA1906E8A4B291DE53912AD92FF3CA97FB66861A375ADFD08897B150EBDBCE484A7C990
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/plugins/ultimate-member/assets/css/um-old-default.css?ver=2.0.49
Preview:	.um .um-tip:hover,...um .um-field-radio.active:not(.um-field-radio-state-disabled) i,...um .um-field-checkbox.active:not(.um-field-radio-state-disabled) i,...um .um-member-name a:hover,...um .um-member-more a:hover,...um .um-member-less a:hover,...um .um-members-pagi a:hover,...um .um-cover-add:hover,...um .um-profile-subnav a.active,...um .um-item-meta a,...um-account-name a:hover,...um-account-nav a.current,...um-account-side li a.current span.um-account-icon,...um-account-side li a.current:hover span.um-account-icon,...um-dropdown li a:hover,.i.um-active-color,..span.um-active-color..{.. color: #3ba1da;..}.....um .um-field-group-head,...picker__box,...picker__nav--prev:hover,...picker__nav--next:hover,...um .um-members-pagi span.current,...um .um-members-pagi span.current:hover,...um .um-profile-nav-item.active a,...um .um-profile-nav-item.active a:hover,...upload,...um-modal-header,...um-modal-btn,...um-modal-btn.disabled,...um-modal-btn.disabled:hover,..div.uimob800 .um-accoun

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\um-profile.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	2662
Entropy (8bit):	5.0300305234582465
Encrypted:	false
SSDEEP:	48:kMGkITF8IDWeGqEFyr/hucmbnhDgb2iMDk9a55mI5O6pMeA2Hh4:8LlDrscmObLMQC5mxiaWh4
MD5:	52507B52746033044956D796A4116458
SHA1:	8DEE9DB95550AFDC9590C98A20C9DA71A9A07BF9
SHA-256:	7FD64F42016E95B4CB1D19C9B0C7102F97A446A8E9DEE70B81050FEE0FD2BB0D
SHA-512:	DE44FC44E5EB21E7B9815D501E19BD1010A61488EB1C47C30A8CA4D4643C323A884AB5AC1180709CBCDCB2D6353AE925BDE802E0938D8BED41D9709FF08E8CFC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/plugins/ultimate-member/assets/js/um-profile.min.js?ver=2.0.49
Preview:	jQuery(document).ready(function(){jQuery(".um-profile.um-viewing .um-profile-body .um-row").each(function(){var e=jQuery(this);0==e.find(".um-field").length&&(e .prev(".um-row-heading").remove(),e.remove())}),jQuery(".um-profile.um-viewing .um-profile-body").length&&0==jQuery(".um-profile.um-viewing .um-profile-body").find(".um-field").length&&(jQuery(".um-row-heading,.um-row").remove(),jQuery(".um-profile-note").show()),jQuery(document.body).on("click",".um-profile-save",function(e){return e.preventDefault(),jQuery(this).parents(".um").find("form").submit(),!1}),jQuery(document.body).on("click",".um-profile-edit-a",function(e){jQuery(this).addClass("active")}),jQuery(document.body).on("click",".um-cover a.um-cover-add, .um-photo a",function(e){e.preventDefault()}),jQuery(document.body).on("click",".um-photo-modal",function(e){e.preventDefault();var t=jQuery(this).attr("data-src");return um_new_modal("um_view_photo","fit",!0,t),!1}),jQuery(document.body).on("click",".um-reset-profile-ph

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\um-raty.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):	9126
Entropy (8bit):	5.040282541909996
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\um-raty.min[1].js	
SSDEEP:	192:YBHqK0SqMhb5K4QOY6+/kRYFU2z4afGzwHb4FQPjw:YBHlBqo84S/5U5+1w
MD5:	5A85D76162C5A61099F95DAFBC5CE579
SHA1:	B4D3429734371BCFDA17B92E49FD405BF7C55408
SHA-256:	C63277F495204D0463E62F4D0C23CA745D94BFED27505A38F2D71044EC702F30
SHA-512:	4F851EEFCE3CEB903E242CD7705ED0B4D4A08553F40540459BD7274F164265D0A87F63E5619258D16CC7CDD3B0A87DDEB3B832CD572554935987A05F6AC5B97
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/plugins/ultimate-member/assets/js/um-raty.min.js?ver=2.0.49
Preview:	!function(l){"use strict";var c={init:function(t){return this.each(function(){this.self=l(this),c.destroy.call(this.self),this.opt=l.extend(!0,{},l.fn.um_raty.defaults,t),c._adjustCallback.call(this),c._adjustNumber.call(this),"img"!==this.opt.starType&&c._adjustStarType.call(this),c._adjustPath.call(this),c._createStars.call(this),this.opt.cancel&&c._createCancel.call(this),this.opt.precision&&c._adjustPrecision.call(this),c._createScore.call(this),c._apply.call(this,this.opt.score),c._target.call(this,this.opt.score),this.opt.readOnly?c._lock.call(this):(this.style.cursor="pointer",c._binds.call(this)),this.self.data("options",this.opt))})},_adjustCallback:function(){for(var t=["number","readOnly","score","scoreName","target"],a=0;a<t.length;a++)"function"==typeof this.opt[t[a]]&&(this.opt[t[a]]=this.opt[t[a]].call(this))},_adjustNumber:function(){this.opt.number=c._between(this.opt.number,1,this.opt.numberMax)},_adjustPath:function(){this.opt.path=this.opt.path||"",this.opt.path&&"/"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\um-raty[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	1078
Entropy (8bit):	4.926623984559292
Encrypted:	false
SSDEEP:	24:IgF8FCNBFFFgpF+OXlxX/UMb3NFEX+X9TNNhBsPoaN+U7uxuUZ:PyQNBnIZlJz19BBsPosE
MD5:	7AC9AC43038FDBE5E4A828838B3A0436
SHA1:	1D1460D73C742AE3586CF4075B92F6A158FEEC47
SHA-256:	8E7749ABC38284A700357F195341514252605CF823DD6747ADF6E6D9B38012ED
SHA-512:	40AFBDADCA6058E0FD3A8FE2DDBEF13E866F24C2BEC6EF6C2A8AB85C83C3D699EF326DA320291333E346A5BD1DC1439B01E1CC91AB449CC33DE0F0E88677A2CC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/plugins/ultimate-member/assets/css/um-raty.css?ver=2.0.49
Preview:	@font-face {.. font-family: "raty";.. font-style: normal;.. font-weight: normal;.. src: url("../font/raty.eot");.. src: url("../font/raty.eot?#iefix") format("embedded-opentype");.. src: url("../font/raty.svg#raty") format("svg");.. src: url("../font/raty.ttf") format("truetype");.. src: url("../font/raty.woff") format("woff");..}.....cancel-on-png, .cancel-off-png, .star-on-png, .star-off-png, .star-half-png {.. font-family: "raty";.. font-style: normal;.. font-weight: normal;.. speak: none;.. display: inline-block;.. text-decoration: inherit;.. width: 1em;.. text-align: center;.. font-variant: normal;.. text-transform: none;.. line-height: 1em;.. -moz-osx-font-smoothing: grayscale;.. -webkit-font-smoothing: antialiased;.. margin-right: 0.2em;.. color: #ccc;..}.....star-on-png,...star-half-png ..{color: #ffbe32}..../* Icons */.....cancel-on-png:before {content: "\e600";}...cancel-off-png:before {content: "\e601";}...star-on-png:before {content: "\f005";}...star

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\um-responsive.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	221
Entropy (8bit):	4.651963759974877
Encrypted:	false
SSDEEP:	6:zvt9teGX4XA50XiP50oP0yvtlrDFTQJmM1Osf2LqSVnRU0XiP50/:zvpeGX4BW550yvXhJMw0sqCW5W
MD5:	6290EAA850041D7E833FA363F8784238
SHA1:	CB5B75224BCC64BD64F91EBFCEDDD07291B0665A
SHA-256:	BCD487D7308145C275B6D459F8A3F5DAA0271D1D4A71A23BF1401411FAFD44D2
SHA-512:	E9B9D447DE8FA8384AE8D417729DEE758E50A883F1A26A301C64D4870EF57E8144F9FF089E7DA3FC63EC2EBCEE0F9D0DFF5FF3A28EAF160824600007927BCDB3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/plugins/ultimate-member/assets/js/um-responsive.min.js?ver=2.0.49
Preview:	jQuery(window).on("load",function(){um_responsive(),um_modal_responsive()}),jQuery(window).on("resize",function(){responsive_Modal(),jQuery("img.cropper-hidden").cropper("destroy"),um_responsive(),um_modal_responsive()});

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\um-responsive[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	15098
Entropy (8bit):	5.090563282208414
Encrypted:	false
SSDEEP:	384:857gzmfBbknGSd2kt2fba+JgXe/rVHOSfO3xdwGFdqJQAf:85UzmfBbknGSdlt2fba+Jgu/r1OSfO3K
MD5:	E5BB52B0F5F400ED5DBC01A6C03272C8

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\um-responsive[1].css	
SHA1:	829D0D3323A3C784EFB7B4C0887336E7197F1BEA
SHA-256:	68C3A1228BBC12FAB7B6DB0FABC4030173A6BDD44327BDEF586EED99A0C8B71E
SHA-512:	4CBD24CDD71FF723A31B09046B826D9F6D404F6EAE247D95987CCF607F797585E7909F24EB1CAA6D854FEDCA74127FAE377E4CC912873F8CCBDAED1C1828F F4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/plugins/ultimate-member/assets/css/um-responsive.css?ver=2.0.49
Preview:	.uimob340-show,...uimob500-show,...uimob800-show,...uimob960-show..{...display: none;..}.....um-profile-nav-item a.uimob340-show,...um-profile-nav-item a.uimob500-show,...um-profile-nav-item a.uimob800-show,...um-profile-nav-item a.uimob960-show..{...display: none;..}....div.uimob340 .uimob340-show,..div.uimob500 .uimob500-show,..div.uimob800 .uimob800-show,..div.uimob960 .uimob960-show..{...display: block;..}....div.uimob340 .uimob340-hide,..div.uimob500 .uimob500-hide,..div.uimob800 .uimob800-hide,..div.uimob960 .uimob960-hide..{...display: none;..}..../**...for 340px and below..**/..../**********/....div.uimob340 .um-item-link a {...font-size: 14px;..}....div.uimob340 .um-item-meta span {.. font-size: 13px;..}....div.uimob340 .um-load-items a {...width: 100% !important;...max-width: 100% !important;..}....div.uimob340 .um-profile-nav {...padding: 0;..}....div.uimob340 .um-profile-nav-item a {...padding: 10px 16px;...margin-left: 0;...border-radi

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\um-scripts.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):	9434
Entropy (8bit):	5.0850361694393875
Encrypted:	false
SSDEEP:	192:XNSnoGgSrGBxDurQN1v3Hv3hb80tGBk26q1wlshdQ4DE1D/fYiAR:XNSoGgSrGBxDMQTv3Hv35GEwwlSM5nYr
MD5:	44B0C595D8C5642F9A9870505C578DC4
SHA1:	89DDAFE943D66339B31E95710BDE6D21C6BDAB71
SHA-256:	8199E38470E7F8011CCF310A0D476039FA8B2384E294091D52C77FE4B80C837A
SHA-512:	0E7F8EB0A6D50EAF6E798F6401609DF17F020A93FFEF5EC47BAEC280067E22FBAA1E8417EE4E78BC07A71C87773B9542CFA597C26BE5017D526CAC48555B891 6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/plugins/ultimate-member/assets/js/um-scripts.min.js?ver=2.0.49
Preview:	function um_init_datetimepicker(){jQuery(".um-datepicker:not(.picker__input)").each(function(){if(elem=jQuery(this),void 0!==elem.attr("data-disabled_weekdays") &&""!=elem.attr("data-disabled_weekdays"))var e=JSON.parse(elem.attr("data-disabled_weekdays"));else e=!1;var t=null;void 0!==elem.attr("data-years")&&(t=elem.attr("data-years"));var a=elem.attr("data-date_min"),i=elem.attr("data-date_max"),r=[],n=[];void 0!==a&&(r=a.split(",")),void 0!==i&&(n=i.split(","));var u=r.length?new Date(r):null,o=r.length?new Date(n):null;if(u&&"Invalid Date"==u.toString()&&3==r.length){var s=r[1]+"/"+r[2]+"/"+r[0];u=new Date(Date.parse(s))}if(o&&"Invalid Date"==o.toString()&&3==n.length){var d=n[1]+"/"+n[2]+"/"+n[0];o=new Date(Date.parse(d))}var l={disable:e,format:elem.attr("data-format"),formatSubmit:"yyyy/mm/dd",hiddenName:!0,onOpen:function(){elem.blur()},onClose:function(){elem.blur()}};null!==t&&(l.selectYears=t),null!==u&&(l.min=u),null!==o&&(l.max=o),elem.pickadate(l)}),jQuery(".um-timepicker

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\um-tipsy[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2271
Entropy (8bit):	4.707952382648288
Encrypted:	false
SSDEEP:	48:1kwsnoJ/jBPOB+h247DV47DbR47Du47dzsVQqE+vr4BIt4cM:qQQ4BgngtNsVQqE+vrSexM
MD5:	6FEA8331EC95A566DEB3FD8F2E5642E9
SHA1:	F5D849539D842C2B5C0C746511E35C66C1A96108
SHA-256:	B12BE643CFA6B3E932134ADF0D1436433F42C84B65CF3F8EAF3FDE320C038DFB
SHA-512:	30BEA3A4717C563B2D2ACF4F38764D7D510253D8699C67DF1B6D2BCE5DB5329D70CBC7E47594F4404AD8D89B59371984CB82F66C736C4C490264162D44610D1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/plugins/ultimate-member/assets/css/um-tipsy.css?ver=2.0.49
Preview:	.tipsy { padding: 5px; position: absolute; z-index: 9999999999!important; }.....tipsy-inner {...font-size: 13px !important;...line-height: 17px !important;...background-color: #333333 !important;...color: #fff !important;...max-width: 250px !important;...padding: 6px 10px !important;...text-align: left !important;...word-wrap: break-word !important;...-webkit-font-smoothing: antialiased !important;...-moz-osx-font-smoothing: grayscale !important;..}.. ...tipsy-inner { border-radius: 3px; -moz-border-radius: 3px; -webkit-border-radius: 3px; }...tipsy-arrow { position: absolute !important; width: 0 !important; height: 0 !important; line-height: 0 !important; border: 5px dashed #333; }.....tipsy-arrow-n { border-bottom-color: #333 !important }...tipsy-arrow-s { border-top-color: #333 !important }...tipsy-arrow-e { border-left-color: #333 !important }...tipsy-arrow-w { border-right-color: #333 !important }.....tipsy-n .tipsy-arrow { top: 0px; left: 50%; margin-left: -5px; border-bottom-st

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\universalAdd[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	assembler source, UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	27913
Entropy (8bit):	5.249865216970879
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\universalAdd[1].css	
SSDEEP:	768:XLF7i4zFW/F+oe48jQgZF88oXcstRTD+4v1:7ti4zI/Aoe/M6S8StRTa4v1
MD5:	0D20F355EDBCC0504FBA7027FFD94062
SHA1:	6825F9EA83EF658E74762ADD0C535A94AE248F17
SHA-256:	6AAF03A6FFEC9DDA7052C047F4780888DC3FF2EE3DF6318B5868C9B17A30A260
SHA-512:	EBD36BEC5C0D4B3B70868C3329299B76E7819312EB9C2DDEDE14C6205628D3F5801D86E8864E0B3149C8FE3C84AB7BE5C4B4C027936051CE41417A10081A40C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/css/universalAdd.css
Preview:	/**********. * OVERALL *.**********/.h1,.h2,.h3,.h4,.h5,.h6 {. color: #494949;. margin: .75em 0 0.5em 0;. font-weight: normal;. line-height: 150%;.}. h1 {. font-size: 45px;.}.h2 {. font-size: 40px;.}.h3 {. font-size: 32px;.}.h4 {. font-size: 25px;.}.h5 {. font-size: 22px;.}.h6 {. font-size: 20px;.}.#contentFrame {. color: #727272;. line-height: 200%;.}.li:focus,.a:focus {. outline: none;.}./**********. * FORM *.**********/.form .row:before,.form .row:after {. content: " ";. display: table;.}.form .row:after {. clear: both;.}.form fieldset {. border: 0;. padding: 0;. margin: 0;.}.form legend {. font-size: 22px;. color: #494949;. text-transform: uppercase;. padding: .75em 0 .5em;.}.form input,.form select,.form textarea,.form button,.form .btn {. width: 100%;. -webkit-box-sizing: border-box;. -moz-box-sizing: border-box;. box-sizing: border-box;. padding: 17px;. border: 1px solid #808080;. -moz-box-shadow

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\wp-embed.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):	1391
Entropy (8bit):	5.13936657531626
Encrypted:	false
SSDEEP:	24:XUdqIoZ2zsben5WlLysyIOKI1mQqRhoj3v2rFEgRuLUMB9/RUCXXmC3+:XUyEsyKystOKumTsOrFEmu7Bl6CX2Q+
MD5:	570AE0F3C201604926EA599D3D1F6C04
SHA1:	2C29243A73660964D4712B969D2A15E27777BC14
SHA-256:	5138D39633DC69FCD0ED7F33A5E38DC339123F682FA7F5242066879C2BBC8C9B
SHA-512:	44583F156E95AA16D20ED8DB8421001D9B7257B56B4FFF1E0378760406B4D6EB2B1315D28AD4F3F489A7733814B2FB2DDDF8F28004DAAEEE8D9BF4EA22A2742E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-includes/js/wp-embed.min.js?ver=5.2.11
Preview:	!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=!0;for(var e,t,r=-1!==navigator.appV

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\182478872_788238465452841_4348855019305596379_n[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 1080x565, frames 3
Category:	downloaded
Size (bytes):	44505
Entropy (8bit):	7.923203507859871
Encrypted:	false
SSDEEP:	768:r2pyLxd+uK98+MmlZnHNA7tKH9DpOoFz90A13LfZ/VxJ5tTTNuuAzy:rlxMuK98hmZ7tKHW0z9D15XtTT1
MD5:	58EC28417165F6BE15B5481075228E0F
SHA1:	6A5ADB647F3F30174602990FE711EDA9B9662290
SHA-256:	E58BE6A0FB501BA51446DDBEDEE429956E20E1FDD8A883FFEA678522FCE95EDE
SHA-512:	EF7B16E4C58038107CCFB450E38B045DC0D79DB74D1B391C1594F31B85C858EE4D8521750CB83BF868F5C99755CFCDDD311E1AC44E07EA9BE83718A559246DF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://scontent-ort2-2.cdninstagram.com/v/t51.2885-15/182478872_788238465452841_4348855019305596379_n.jpg?_nc_cat=110&ccb=1-3&_nc_sid=8ae9d6&_nc_ohc=4M9yUqOYAw4AX9iQDVc&_nc_ht=scontent-ort2-2.cdninstagram.com&oh=3e064ba81edc99d6603209364979ea80&oe=60D64710
Preview:	......JFIF.....C.....C.....5.8..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...<..x..:*\.F...rH....._.?e.S...8*.KBF2~.._....;B.O.....U..0e...W..Rg.xI.J'..^hwOmy.A2.U..]..._.....5..e..+.edU..\|....5.....d.&84.+..:.J...j'Q.+.Q...ksYF.TPzP2j.9..@.....QK..RT...u..S.P..4.p.R^.$.~.`.*Je QN."...c.Z)OZJ..E.PPT..ER'..-.QA.QE.."t..A.N.f.LS..M....gLR.-..sW#<...F+..{xr.g..N.5.]*Q..{..'tY...u6...lG.is.H...v..(.!....(.,.QEM.I..QI.P..]....q.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\183802068_177882140894720_1475325707994185466_nthumb[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 150x143, frames 3
Category:	downloaded
Size (bytes):	6363
Entropy (8bit):	7.931881439830331

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\183802068_177882140894720_1475325707994185466_nthumb[1].jpg

Encrypted:	false
SSDEEP:	96:n3MYyLWyJEXiXL6V/ChjXAuO/DeYXUihZ0qKWP4ly9cc+SZBiK3Azz4RsK6Kj6:ncYauXM2VKlIVUy7Y8T+IBihgy
MD5:	A73F47A88A0CD1D2B6EE450C6C8B089E
SHA1:	501FBCEF835960A1A05CA51CC5660F2E65E81163
SHA-256:	D114400799875C064FF86FCEE05B8160BFA2BAA9B792073ECD0FD2744C225E25
SHA-512:	8F800FDA700980B044E86583D1E3CB164312725F004D5C20C9175DC54AF9D2DAC6467C621EC0D62B427AB37A17A0BACCBA6DB7F7A602DF68870248BC2A9B1F7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/uploads/sb-instagram-feed-images/183802068_177882140894720_1475325707994185466_nthumb.jpg
Preview:	......JFIF.............C....................................%...#... , #&')*)..-0-(0%()(...C..........(...((...........".......................................A........................!1.. "AQ.aq..#2......BR.3b..$CSr..&c.................................+.......................!1A..".Qa2..q...............?..4.&[`..E.......E..&8 .f....E..MA$V.:.v..t.=*......,'.f'..(..<s...H..qh.....l..@.......4. .....T...RZ.Pe|..8..$q..s\|...4..q..$..7HjG...1....`..W..h.......n.]......ms?.5......y.T.c.X.......+....H9c.=6.A..2......zv.dT...8}..I.#....H.EI....I.9.(....N.v.N...wyd.x.Cy....Y..h.D..?:..zd..v@8 .....8........M..;..%/......?.._q..Lf.;EF#....(~..^*H..{@.[-.~47.$..4.Tg..#..u....].....i .[..jaXF..~b4..O.]\.(.iw.....p..W.2..........Or.u.......Y..).3....j..3....A+...r..FT#I)p[.^Le\|.72.r..R4QI...?.{*. .F.(...F..@.......$.....;Fs....xQ-n. p3..g..$..%.24,.).. ..C.:...J"..q.p...."......J.L.>...z......c,...4.d.>..J.gY8

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\188752735_1833523386803873_3313291444661509047_nthumb[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 150x78, frames 3
Category:	downloaded
Size (bytes):	2916
Entropy (8bit):	7.810317899372171
Encrypted:	false
SSDEEP:	48:+iWQgMJD2Ja3EVIDTIAJVF9UqUpI55bxlPdHFkBOrT/bTePo47DpJqgVx54RVNG:/goDfUVIIIDrUpI5HDGIrkq1o
MD5:	D7F828E244937A61419D8BEBB57CC2BC
SHA1:	80F2DC60D4D59E1BF878D306CF607D9EF5837C20
SHA-256:	DC835C3735CAD33762452A29B19E4E43F4823611A0BD63DBB992BF37DD25D6B8
SHA-512:	1D4FBC8F507B4348265E5FA929C7D8BDED3331658B8648850D3D5526ED3654CDD328010991D2B44552236CF6057E2DBD4B22B617800BC5A79B76CD3D1E1C441
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/uploads/sb-instagram-feed-images/188752735_1833523386803873_3313291444661509047_nthumb.jpg
Preview:	......JFIF.............C....................................%...#... , #&')*)..-0-(0%()(...C..........(...((......N...."..6.................. ......!.1A."Q.2aq....#B..$Rb...1!.A............?..."....ET.f<~.E.1........`2....A..h..<.#cb.T..!RE..Xs.....xB...(K..y.7N.. m.......r........#F...(..O.F:kQ.~ .X.'o>i.i:Z..N[.L.P.@L.m.$...Jz..:....k].!....*.xa..~...Y.wH.T.@...J..I...S1..j...JPdB.1.a...[...tVv.S.M2.NY5.x.....h.....oR4..2s...d.....P}..........P....T@....B.;.N...0;.w..6.?...dT....... D[..FX..>...%.8.'q.y.E..^....^.v.qS...G...h...pb.c..5.......|..0t.-.n.....^qS.....~Nz.x...q...!..../Wu.J.`..@....>.O.&......JXK1$WWD....+ x..E`.+2..(.....=.^.#$....;i#.[.......X&....@..$.... ...].....~.......jm6..(..wQ.h..I..!.u.....U.%.."....8.....[%}R.L..q..3.M..%.R).+.NHUd..=.:.K..N...[...[]h.#..`..I.....~....,.C.<2..t.`..L.~.gc...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\1[1].txt

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):	797
Entropy (8bit):	4.888220879545313
Encrypted:	false
SSDEEP:	24:x37efNz20z5dlBIj+fM83/tcBeGNz20z5dlBIj+fM8s:hexfzzbU+fN3/tgeUfzzbU+fNs
MD5:	3901ABFCA6F44822E04F48A201392F9D
SHA1:	DEE4FFAEAA39F178A5D89AC74170CC548D4AFC24
SHA-256:	24D05F827094EDB6BF7CB22E0A49CE64C2B4F3F3400E6ABF4C5664B6C8D88B1F
SHA-512:	2CBCDFA7EE0E3DD88A7CFDC820AF2E57AED658058ED33CBFEA2C4619EE55F4FF7981CC46C30467316E5C941A3F41BCD44C858D54AB80286A9ECA44AD0D5D40D
Malicious:	false
Reputation:	low
Preview:	_ate.track.config_resp({"pc":"esb","tool-config":{"_default":{"widgets":{"rr4k":{"hideEmailSharingConfirmation":false,"numPreferredServices":5,"themeColor":"#d71c1d","widgetId":"rr4k","creationTimestamp":1557430403825,"hideDevice":"phone","position":"bottom-right","id":"esb","__hideOnHomepage":false,"toolName":"Expanding","hideLabel":false}}}},"subscription":{"active":true,"edition":"BASIC","tier":"basic","reducedBranding":false,"insightsEnabled":false},"customMessageTemplates":[],"pro-config":{"_default":{"widgets":{"esb":{"hideEmailSharingConfirmation":false,"numPreferredServices":5,"themeColor":"#d71c1d","widgetId":"rr4k","creationTimestamp":1557430403825,"hideDevice":"phone","position":"bottom-right","id":"esb","__hideOnHomepage":false,"toolName":"Expanding","hideLabel":false}}}}});

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\979841368838586[1].js

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	266652
Entropy (8bit):	5.472335488766903
Encrypted:	false
SSDEEP:	6144:Rk1HgCSntDV/HaKKV/Ha8NEPjQHguH3HpQrwz8GWL:CNE7d

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\979841368838586[1].js	
MD5:	0EA41DC0286BE212951CF889A563C95E
SHA1:	69F1144448CAD88531C87BC1A3002B4AA0EEB7BC
SHA-256:	C7115813ACDBF9B69037280E47A2222A447BE16E1681DB8FF09FD07C5E022ABB
SHA-512:	97B8F0E61803A9F204F3DE12B5E3D35CA76CE8E462ABB91B09D670516215C075A8D45BDE739B5EA86C5F6BB10B2BCC6CCAF4673ABE5A9975865525E5302A894 8
Malicious:	false
Reputation:	low
Preview:	/**.* Copyright (c) 2017-present, Facebook, Inc. All rights reserved..*.* You are hereby granted a non-exclusive, worldwide, royalty-free license to use,.* copy, modify, and distribute this software in source code or binary form for use.* in connection with the web services and APIs provided by Facebook..*.* As with any software that integrates with the Facebook platform, your use of.* this software is subject to the Facebook Platform Policy.* [http://developers.facebook.com/policy/]. This copyright 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.* IM PLIED, 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 C ONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN.* CONNECTION WI

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\Battery_Cleaner_Protector[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 157x105, frames 3
Category:	downloaded
Size (bytes):	14375
Entropy (8bit):	7.949185078823089
Encrypted:	false
SSDEEP:	384:Vuqvv/oA34P+XgcZAqH26wIw0XmxK4xxrZ3T:bOWXgW3wFxn3T
MD5:	BA6FFAFD6AEA670C63696087A2356C3D
SHA1:	6E272070AFCEF91A3552EFB65B6173B935D469FD
SHA-256:	BCF073C1E9BC264974D0317F064E0E6C15363013D3138C6B17EB82BF3B9BE938
SHA-512:	133DC6012B1AC4BDCEE4F0D1D885B05F22CE0586003CEAD31DCB9A1EC31E08F47EBA0760197B9ADB998F932908B68F9E2C17B2CD746CC7960A69D86066976D E9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/img/thumbs/Battery_Cleaner_Protector.jpg
Preview:	......JFIF.....i.....5.,.....1(....7..U.....x.7.=..\....r.j. ..$...V.....v.....0....././...i.^}.nzQ..kWOv..Aeu...U?}U..}...V(.. cY.H..z....\(/D,(.+..jPP@E...WY.{..d@4[E.....tA.t..>..~...l.f..F...c.2.W..':).j.g{t...<..]CV+.-.=.g..<..=@...i... n._.OO.t!..#[.0.._G...Y\.wp..=r.Ue...T.5.GH.\.|...?...0.`.pv$>.^.%..57.$..P....v.....X..d$;m..>4.....~~6..__'.q..o...^.6.....p~..G..e.;.y:.....7.....[. ..T...x.5...b...u;...\...]K,...Jg3...N....x.\.&.;.YF.5..A...../k.....?7.....^'c...X|o.....?@.7...^....r..O..P.3*,.R....id..oV^.N=.3W.|j.se.h.4...s.4...q...\Y ...V]K*f..)Y...7.....A.....!A.12"35BEQq.#$%4RSTdtC.DVbrsu.....m..b

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\CP199_02032014[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 157x105, frames 3
Category:	downloaded
Size (bytes):	6890
Entropy (8bit):	7.933395589477203
Encrypted:	false
SSDEEP:	192:3tfe2/KqVgH3pgcQkI/hxZXrTyLcUkasOem5Wo3:9SqT/ZXKLfVsOv
MD5:	1EC3ED1BA917E8565E0FF24BB9144701
SHA1:	2711BA5DC425FF6843F2E8FE4965B7B9C517D7F6
SHA-256:	7522BB44384CB05CF3BADDEDEB988258378D23BDBD0E6BC3C79868599945F44E
SHA-512:	AAB6FAFBDBA00956D039BC0126054678C03EC113175E20B97F0CD50BCD849E0EF81E2C39D7C706899A8FD89EDD59F7E301CF9D783B4FF417C94F9C6ABE412C 6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/img/thumbs/CP199_02032014.jpg
Preview:	......JFIF.....i.....!1."AQ..#2q.3ar..... Bb....$45CDRS.6T.Ucstu.....1.!AQ..."2BRaq...#3.....4Cbr.....?...R;.%..5.....4..!...tD.....;..$.ImT.D.M.K.p....e.....x.Y..K..v....q ...>$..5.> > .D"Fm...\.).4.`..-)Z.P...m.%UTV..3./.....OJ....d.....h.....C4_..o..D.).k+fb..d.h..i....4.G.x.X.m..w.}....s./!.....7.#...J...&.\._..s9.!f.X.~lV.sWm/3....M-J..v...i.t~T...yz..a..)L..R...-.. 7.V.GZI"....~.....b.<W...h..dIX ..%Ho.8.=..).Q.U[..a?'...../.}....U..2..N..O.iJ..rzy.....&h....P...N....RN.%K..=v.K.WU <.Y...<l.....[Xu.....7.z.u.7.3s.L"M..x.....).6...T..+.h...-.fF... .7..o[=8Z[h..LG$4..i...@~.u....8..s...p..m.W+W..y.C.h..].O=.lB.$.....F...f^.....N.....kbeR..#.f...8...:.u..5....@...r4.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\CS101_030210[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 157x105, frames 3
Category:	downloaded
Size (bytes):	5838
Entropy (8bit):	7.880651247915237
Encrypted:	false
SSDEEP:	96:q/R7n8hCnAmNV7A5SvFJ7U+VY7sekr87dBY0lmoQ3MjDj/O/IJQgMB3TQm1:qJ7nOE7AA9J7U+O48s0AolDj/6IJQgWn

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\CS101_030210[1].jpg	
MD5:	9929FE4E83682960828CEE3A1928393A
SHA1:	23778BACB5AD3ECCD2F3F0EB4B2D6DA139E855EC
SHA-256:	0FBE5C786EB6E912398244FA8B5B60FFED2CF7F09753D856882D8511A8EB1571
SHA-512:	AD4A801B84AC7185DB383C5772B561262DE35E9E9744D3DF4CED44ACD7E8A98D7395B36798EA59481E2BDAB04C7CCDC29E3870D1E7E80CA982DD49A773B6C4D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/img/thumbs/CS101_030210.jpg
Preview:	......JFIF.....i.....W^..5..v.<A.9...T.}..jV.[....0..}?. ..v.....(UC...6.%.I./-..5#x..H....c...W.9...W`.....-....A....q"...3W.j6....4....91`.".RX....E..$...aPx....".z<3o:.V{..-K..IV..!.....x.}R.m...z@~…w2-V.D..$..J..de..oA.~.H..X<BJ.<.'..7. .,P..IW.v\....=#.....;]..C..&-.Mz.<....@.....K(K(.....7;.W.....?9..gc7l3..~-.....%.b.J%.,....R...T..... .....!12C."4B.3A#6.....HH.T...J.....#.....j....^.....:<.JV.E..P....b....z'W&Tj...G...99.F.'.5.....#....Xl-9u4.../-+6.d...BG...5.X.\Y....E.R b/.j.7q.....Mt....u..S{....9...=. ..._..u.Z.....^\..&w.s.u..]-\:.6.ch.....#y.....H>....._T..v6y\L.EY..;...8.UI....fqv

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\DAP1690_02032014[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 157x105, frames 3
Category:	downloaded
Size (bytes):	5932
Entropy (8bit):	7.920669735821167
Encrypted:	false
SSDEEP:	96:nES6SiRZ5BoXuxBuvcHC+nOyn/vdwgS6d8TMhtaKBQO5Hq:n9DiRR+uUcHNr/e0iM2v
MD5:	53D4ADE5063A1F4BFA190F0310B3CE0D
SHA1:	D24B13B31EE6A523C8C90BDC748D36C21F8A55E1
SHA-256:	248DD950E944830871674CA7BA5D9EE6001625AE97BDA417DB6420D64663CBC1
SHA-512:	48EDB64FD5755FDE4C7EC06E2CD2EC6EFD88BEF43BDBFF09268CAC7E84BDF9234F3076926A97F84354E9E871F5DC1C19070F40A87E6FD7064D264EB4FC91DBBE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/img/thumbs/DAP1690_02032014.jpg
Preview:	......JFIF.....i.....!1"A.2Qaq..#B....3c ....$&Rbs.....%'5CEr47Dt.....1....AQ.!2a."B.....CR.....?..J.C.2VhJ6_.7.....7.j..e...$4T...xU....mT4..[xe.k..j.....?..}.'i.6.....-#.k.|@}.D"G i.bC.R..m$r.V.$-@...t..%n....y.....m..J...R...AJ.>B....|.x.*49l..q.iC..RB...xR.2(^.wVp..Y.u-..}..#...f.D.,-iF.../.^...Uk..k.:B.f...lv.s.....M-J..v.X..l..o.....S.Q..JSf+JJ..Y.\....m(.(bH. 4...}.4.....Y.....C~5.....>}hZ,..G.....~=....,%..r].*J\e.mRW....-#.....F..K.[B.....1.C..*...h8....\..[.q.j.&8.v....ze)Z27..=h(.>S..k...P.R.:..#4...QXK@....oP.3x.&.1.m.....N..rCI|...V .....t..u..\,..yU.....;.mW4.....)..Q.D{..m.....P..xp.B.....@..GT.8...9.....y.....w.@B...v..T|..W.<!..1."..9o....j.....\r...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\DAP1692_02032014[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 157x105, frames 3
Category:	downloaded
Size (bytes):	6871
Entropy (8bit):	7.9051039565701275
Encrypted:	false
SSDEEP:	192:w+Wxl5aRw/dFhEJc0WzF+dFE3SL0pFZbOZwy8:wh/5agdfN0WzWECL0pFZ/
MD5:	CF4430106C0FC4FEB11FABFB3607167A
SHA1:	FB2CD9137F5E09ADF81039079F37308C13B99A75
SHA-256:	4676E17CF70CBAC65BA45689DD56CBF48C1F74C22E72B73F084FC6335B7F9E1C
SHA-512:	7C571F273DF2BBDA6B90F1C0250C628480020C67BD95C1D4A69C928F60172663468B14BEE9360602A6A499A94A94BFCA9E2C2FBF284FEDD9C5DD630A6513A34
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/img/thumbs/DAP1692_02032014.jpg
Preview:	......JFIF.....i.....=.@.h1,z_.}.....:...3A.UF....u..j.u. $....|.....dg./...S...'...S.{...q...k(.....~.k.P..i'3...*.....r...p.....1!O..=%.T).6..z..=.Bhux.W.....I..2.>|'...^..HJ.c....P.....m.mpz. .c.WJ..v.....T.R.pROn.C<.....`.@6[KB....B.....E...[..bQ. z4.{.1+...R..!H.?.....{.5...<.9.?..>...Rg1....Rh..T.dZ+: .E.Y(D.T.)(.AR...5)`HT.*.-.....%.@.Y`P.f^.a...7...../..... .....b.y.Y..|..... -.T...P.*.::E%.b.....%. ....T....0.....$12A!#.. "%4&CE.....~....(N....!....]|.....W.-....m.Ul.&p..k._.C.....d.4.J..$-..*...y.... O.:Od+?.].*4.*....?..fU...I.B.q..e\....5...y... S.52...d..]..... \.....q...,q..E..B.n=..@...?.....S..<..|#....OP.....Kh._.!.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\DAP1699_02032014[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 157x105, frames 3
Category:	downloaded
Size (bytes):	6689
Entropy (8bit):	7.919383317824074
Encrypted:	false
SSDEEP:	96:LJRtTc6coYslf6Pc+lQPoJGmoVnST9jIlq4ZPTqQ45MMPj8lNZEWZgr4Zymfd:L/dcdoYO6XQwJEVnSTTI/PTJZgr4Ztfd
MD5:	236E5ACEF7F1D8A3842D050992BF845F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\DAP1699_02032014[1].jpg	
SHA1:	0216C31DF2B5D540B26127AAF61F99D9D0844F86
SHA-256:	DE97200620F577E3D59C19FC7EDD0F6E5832616524471E19DCDBE910596AE6A2
SHA-512:	72F1160C013F17DADA8E1D8ABE65391D015C3CE08CD884C82EDAE8D160B2CAD3E6AC6E1F31E0968A5723FA35839E182151E6A6A5A247028AC0E3553338C791C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/img/thumbs/DAP1699_02032014.jpg
Preview:	......JFIF.....i.....I"1A.2Qaq...#$Br... ..34R...5Sb...%68CsD.....!..1A.Q.."2BRq...a.....?.....T..CG.*..O..._.....t.}ILE.rNO..`{....{....uim?z.....,8.v.v.b....Z...*..x..0.:...'.C7...F.Ib. ..4..R."27.1.W-Y.W6.W.....xq.A.u..r...c.!E.(,..-.%G.....e...I*8.$.....8...2W..v.!.R..[J.x.....,Ec.L;L.m=.B.nuh..w...:..nN..H. ....].<n=G.....D.z..?....P...\...x!.....Q..v-,iB..4t....; (.3p.$..Nz...q....V.-.y27...`....n..qX...Uc...MQ.d.!.Z2@..JkLZP..%...*PC(.....2.8_.m.....]...H`,!...9.pR.."....R.H....>&...m.|e.>0.,..0...<.(..YnzNW...a..W.k....E....C.+S.L6.I'v.` .....k.....i(SM"+....".!#.;.U..MK.OW.-.....M\P.H.%.....N.#=:.m[.][2Y....~..85..Q.T..W....H..yMnI.F^.=....g

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\DE1613_52014[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 157x105, frames 3
Category:	downloaded
Size (bytes):	5235
Entropy (8bit):	7.848447950567697
Encrypted:	false
SSDEEP:	96:h05cv53xS9iA+xV+/1CbvnKrmKroBVP9uPlnI3TigTZ:6ux3xbh+EbGmSd76
MD5:	B96A6233CD9CB845B3CD748A184E3685
SHA1:	52D2BDDF27EEE738A183EDC6266A1663E5DE57E2
SHA-256:	2B41335113F1DE898FBD4B8D2418C56E517CBE657BE74DAA8AD066C1F680F837
SHA-512:	658AF92613FB6FD4FC8B79D58BEB4C67AA6574BB83CEA5E54B7C411D4E6B718E2C1D56BFE9D72C368B7FAF9542D55651B523A8D07AC014687DBC3C0A6696E1AE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/img/thumbs/DE1613_52014.jpg
Preview:	......JFIF.....i.....s...H.cW.....P...>qz..... ..r.=...'i....K1~.....Y...(.!..M....L.&N..8.c...k. .7.b.X.9....lu.. ...0}...q.G..Y....c..5...../..yx.Ag.....~.5.}Kx...H.Y/-5....y.....o ....kF@..5.!.pE..:..~8.....L\.t..&..+.#...sp.1|Q.&X... ...>&e..t._.....>k.gn.....VC....K.~.c$@X..@@.X.....,....X.....,...A@X.....7l...0|....j.^...<.x....vT....TP.@(.....X...A [."U.....K,.".b .(.....-.....1...!#2AC."346Q.....y.Mb....5>.^...E..[.._.Z.\E....,1.....X..q....=..K.....Ek.....S4...m.....:...w.z.....4.k...G`.2p..jTF.T..w.....h\...eRl.w2.$.5...8. 6.5.E..=....J.V..r./..]...-Mj?.....xoj-{,.....>...z....^."....Vq..k.....;".....+..7.Rs

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\ErrorPageTemplate[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):	2168
Entropy (8bit):	5.207912016937144
Encrypted:	false
SSDEEP:	24:5+j5xU5k5N0ndgvoyeP0yyiyQCDr3nowMVworDtX3orKxWxDnCMA0da+hieyuSQK:5Q5K5k5pvFehWrrarrZIrHd3FIQfOS6
MD5:	F4FE1CB77E758E1BA56B8A8EC20417C5
SHA1:	F4EDA06901EDB98633A686B11D02F4925F827BF0
SHA-256:	8D018639281B33DA8EB3CE0B21D11E1D414E59024C3689F92BE8904EB5779B5F
SHA-512:	62514AB345B6648C5442200A8E9530DFB88A0355E262069E0A694289C39A4A1C06C6143E5961074BFAC219949102A416C09733F24E8468984B96843DC222B436
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/ErrorPageTemplate.css
Preview:	.body..{...font-family: "Segoe UI", "verdana", "arial";...background-image: url(background_gradient.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;...color: #575757;..}....body.securityError..{...font-family: "Segoe UI", "verdana" , "Arial";...background-image: url(background_gradient_red.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;..}....body.tabInfo..{...background-image: none;...background-color: #F4F4F4;..}.. ..a..{...color: rgb(19,112,171);.font-size: 1em;...font-weight: normal;...text-decoration: none;...margin-left: 0px;...vertical-align: top;..}....a:link, a:visited..{...color: rgb(19,112,171);...text-decoration: none;...vertical-align: top;..}....a:hover..{...color: rgb(7,74,229);...text-decoration: underline;..}....p..{...font-size: 0.9em;..}.....h1 /* used for Title */..{...color: #4465A2;...font-size: 1.1em;...font-weight: normal;...vertical-align

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\FP101_02032014[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 157x105, frames 3
Category:	downloaded
Size (bytes):	5431
Entropy (8bit):	7.92253852644577
Encrypted:	false
SSDEEP:	96:XXXlXFjhFOmznuSsm56a97gBXeXMZX3NrfWejK6RmDBoh/PpsA/tpFGmpgmVSXv:XlXFjzwG6a973XQX3Niej7WKh/Ppsqpy
MD5:	185E68904B18265056D9BB0310ED2D8E

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\FP101_02032014[1].jpg	
SHA1:	D76FB49DD83848FD7A1AA25BBDD4FA26B38F4491
SHA-256:	F11F3053CF547DE58C8E188421FB689DFB2BD9EFF2051384FCF80A83FA72CC0A
SHA-512:	025FC65ED1F76BFBCF338C89D41A7DAD57C855B5C36E3AD3E687B996696AD71D51897F4F8E03A8F1613BD94FAFDC835B88F15D07342F4F321EE272A07B7E6D4 5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/img/thumbs/FP101_02032014.jpg
Preview:	......JFIF.....i.....!1.AQ."2aq..#.....% 346BCRbst...$5Dr....&Tc...du.....1..AQ.!.....BRa...C.....?....^...M..\.....]..u....C.....<2.!!....J.A..{6.7..&Z...G..B..8.\N.xm..5.....}.D" Fm.fC.2..m$p.V.$,.G...W).m...g~..=.*.e.q<.K.6.8H.^.....(,.}..J..S..V..%.....-;.XR.9S&.]C.....o\9W.P.Ue+m....7.T.sW>t.U..g_..5.....]...tp.....O..o....Y.*...^...0\.4a6.8..8k`[~ b...z.F...%..;K..].J)zp..dIX ..%Ho..s....{.a%t.....#:n.....,!..b....C.>.)+.7'..Ec.#.^.5...d..AB....Y*I..R.<w...S...g..E..P@,..IY.....h..3....E.....!..%:.$Fh.-J..Z.$s%Kz.....)..Hi/..'....\.. .;7.Z..p..-.W+W...Z.SGv....:P?.{...Qv....,..w...w...@*t.....n...\.....\h.T.....;...3@..R....A.....p.....}.-6<..;.BS..Q.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\SS100_032411[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 157x105, frames 3
Category:	downloaded
Size (bytes):	6363
Entropy (8bit):	7.928404826244881
Encrypted:	false
SSDEEP:	96:91n1blXltz280+w9KwbOp3wbOKMye48v6uqUTa9bFNqZt/o1GkXtw:hlXltg+EKfgb1MdfWp+ZtobK
MD5:	D8897E3A085210C3BABFBD2344E4F2A1
SHA1:	E6730609AE4BD55DEA6E2173B7CC9DBCD075F5E9
SHA-256:	51DE674F07B5C498838C628F62D411530E3BBDA5F574B485D404D45E912F2D16
SHA-512:	36C98D25A8F239A6CE119119CC2338BB130450142AB309B105E24826023DACCA6C64BD10B0528FF14D32214235D17993B7FE42FB242623514A8D41C86E5447A7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/img/thumbs/SS100_032411.jpg
Preview:	......JFIF.....i.....!1.."AQ.2aq..Br..#Rb. ...$%5C34S...Dst.....1...!A..Q.2"BRaq...$.....?.@.5...Q}..~Dyc4U.I[,L...SJ.bQ..<..a..j}G.oA.|.....>+..bF.]X....g....W.....g.....S...L.2~".....*54. .J.$.9wR.....-+..I.P..b=..A.....F.;...@V>....B8.@k.a{. ...3.[....E$e..~....fg]..D~X@..zeb]....:'..s..ACL.R?.u:.....$....i.O.A.Y.WU.+2.*.~.... ..@...u.F..eN".b.4...y....6.U.Z.aY&. ....x,...n3r)D^.U..gJ.T.A....C\y..Y.q.9.....B.C.....[.A.u....^m.y<."...%%ME3.....I.\.....OM...%m.L.Q...%a....\86....._[X.^..n.{..)Cf.<...'.....3.u....v....f.N".4..... ...j?..S....u.~... .....YZ.V...^.x&F....[..Z:WC>^v.S...,n.-.....d..^..E.....I.|.6...s..Q&...Y..mo.$.....I...PU...R...@#...._Q.....,RI)....@A....9..M...U..a.D6

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\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):	42587
Entropy (8bit):	5.891729235459901
Encrypted:	false
SSDEEP:	768:v/S5qBiRC8GN/TqNDCyZgumLvd8cPF0Ai:SBRCDcZuZFBi
MD5:	7E6827A35A0EBA203D8982C700200B8C
SHA1:	CE069EDBC13B56BE1D23D4E7C09D3D8840114B4E
SHA-256:	B94E4E3705F92939AE60B2C77E2BF81B41CDA28BD667173974E54C0EEA266016
SHA-512:	DBCCEB94EE2175E77AB1F936FFDB2B69C03304488E30C91A7515AAC9171146AD15F0198BC9112EB653E0E631DDA5415BABBB2DBD3B9E7B47388EC0E281992D 59
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.gst atic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4mxP.ttf) format('truetype');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 500;. src: url(//fonts.g static.com/s/roboto/v18/KFOlCnqEu92Fr1MmEU9fBBc9.ttf) format('truetype');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 900;. src: url(//f onts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmYUtfBBc9.ttf) format('truetype');.}..</style>.<link rel="stylesheet" type="text/css" href="https://www.gstatic.com /recaptcha/releases/FDTCuNjXhn1sV0lk31aK53uB/styles__ltr.css">.<script nonce="oPsz+O8xclIY3P9ozrkkxg" type="text/javascript">window['__recaptcha_api'] = 'https: //www.google.com/rec

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\anchor[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	43487
Entropy (8bit):	5.887255100365142
Encrypted:	false
SSDEEP:	768:v/Sk9ymC8GN/TqNDCyZguDXmsqYU8wHaFpc:39ymCDcZHN7v2Cpc
MD5:	208FD0D33AC6AB0C4D2122DFE147B00F
SHA1:	A362990C018F546001EFC7224B5AB4B4DECE3C58

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\anchor[2].htm	
SHA-256:	F5C983D367DA8A3EEADA30CCC4DDCA3B8C7BFCBBE7031C793C99FDCEB27AAF8E
SHA-512:	4409B3110A5BE1CF974FE10F5E57F43FFB7C5AF2CECB74F85D739165BDBEF00AF80D9E780880E67044F8AA180EDD3D0ECC86ED49B03018042AA92E3B4F20A3 A
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/FDTCuNjXhn1sV0lk31aK53uB/styles__ltr.css">.<script nonce="U2JnAQs61meHmUEhmyemkg" type="text/javascript">window['__recaptcha_api'] = 'https://www.google.com/rec

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\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):	884
Entropy (8bit):	5.622715812529397
Encrypted:	false
SSDEEP:	24:2jkm94/zKPccAag6+KVCet621Tc+ZqKsLqo40RWUnYN:VKEcKKoez1o+yLrwUnG
MD5:	48CCAA83E29E007F316CDEBD5C5894CC
SHA1:	D6603A6C495F28FD4950C038DE29CCE7972EC3CE
SHA-256:	77004661ED3F29C526CF602ADCD5AA1EF88CF4E6FE8C49516E13A401984A0B22
SHA-512:	EFB556A6DB5F74DAF23877BB330AA8DDB2D596E4FBC63CB47DC50CC17BB39562A99471FE568F7DFED9FC36E0EE1BA5517743C3C604DD3E2DCB461FF72AC5 196
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('6LeT54oUAAAAAM0Fe9qLJMRr30BxU9BwidRRwqbw');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/FDTCuNjXhn1sV0lk31aK53uB/recaptcha__en.js';po.crossOrigin='anonymous';po.integrity='sha384-CVLvfZreJnPQL86cHuhqPHygN9uzFMnfC+HyY0PSGUfPu9yIYXzhnNBTDX7Yfi1R';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\MEEXW4H4\bframe[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	1522
Entropy (8bit):	5.592469670631313
Encrypted:	false
SSDEEP:	24:D0ksPkGAy/iOYsFYxMJ0/iOYXFYx1S/iOYrFYxAQNPGt6fhrjgvPCt6baA0NSALy:Dc1A1OLKIXOgKNOMK5N+swqRVsAy
MD5:	6009B13E6B818CF985E2C16E03616D63
SHA1:	F842262516EABD8965926F6CA7DAA1280C03090A
SHA-256:	9EA24E7D419E582318D749929AB9BB890278CAA696E425FDDECEECD37FE5108F
SHA-512:	132A674950946AA95934CE515043E0E0A4C827F678451B5A4DCD8FC591B31E4A29BC8A07CC5A3139C8824F6EB0D18F5D70A5EEB67197880E1A17F0E6BBDD931
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/FDTCuNjXhn1sV0lk31aK53uB/styles__ltr.css">.<script nonce="D619IqJcPGiE5efzlWG+bg" type="text/javascript">window['__recaptcha_api'] = 'https://www.google.com/re

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\black[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 10 x 10, 8-bit gray+alpha, non-interlaced
Category:	downloaded
Size (bytes):	72
Entropy (8bit):	4.5371753156574375
Encrypted:	false
SSDEEP:	3:yionv//thPlH1th/zQ/qBxcNwKP/jp:6v/lhPo/J3njp
MD5:	CAD99B3E17297725ED439C4A2820D3E8
SHA1:	5BE2609C9DDB7F4F4376816BC9C9AFE19FD2802F
SHA-256:	97673D00080E9741FDE5E847B68CB758A8CAB0E0F5CA63C21FC21024AA693203

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\black[1].png	
SHA-512:	4755B7993A34F59357E88D1AC9568603B8B34EFCF012BB1592F6D1C07F3186FB085F8BD5388C89CEDA334FF43F72588EDE87DD6130D4C0AEBA4442AF7244A70A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/img/black.png
Preview:	.PNG.....IHDR.....';.6....IDATx.c`8...eA...O.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\dot[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 31 x 31, 8-bit gray+alpha, non-interlaced
Category:	downloaded
Size (bytes):	975
Entropy (8bit):	7.553485064990098
Encrypted:	false
SSDEEP:	24:P38rDpGCwWbzQC59XGVZHWAfZRkaUL1MX2g9jU:P38rVGMzjGVpWARaaM2T9A
MD5:	8885A1D0DA6BE8A5B5746FC9F1925DC3
SHA1:	C200BBAD8A7B04B421A82120D0A5881752468E1F
SHA-256:	782F6F3CC7F16AB3DE5BC2C0913C036B7D5992A3A206EDE0B0741B32D1872552
SHA-512:	9FB96AC3E6A5B8D9CCE9BBA21ED556940840E215DD6857DB72E6F3A197D9F52BD30A929D73F77F8C7746C292045AEEA8E516544E683C422F7C8C9669B56443E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/img/dot.png
Preview:	.PNG.....IHDR.....IDATx...Ik]e....}wxS^^..6..R.V,N.q!..*"..n...s.B..)(.....q.QlU...".*...M.$/.{?.... ...$!....@@.e2.(..j.FB. ..A..J.B..11V..L.H..@@.Pj...h)DI..i..#c.Z.r @.d..=}.-..|...E/.....~..U..l.. ..LKW.l..sO].P....g.}...].l.J-.@.)u...../L.d.n[..k.9e.g.{..3.9...F.@....z..O...v..m7..k`..u...q..?....j...L[...k.y...r... ...?...../...D.2D.....8.s.{d....r.*..<.[066.D D....o;..[....u..{l..]-...A..w..\..`...3..N...#..j...Q...o..+...=..s...`..v.....(S.....#6.....3{.r...D..<=.....[.....2Q. .EI.`.....e.@..f.....`..F%....Fm...,I..J....X...W6L4..Fm.pf...?.)Oh.Z.0../....J-e.2 ...n.?..0...{.<....>;..q...d..\q...n.=....W...7.]8..a....d .....e7.....W?..#/...5c)C....N..l....Y.....D:.....:ohd"e ....;../.*...i.....G..bC.!. (..m1..7=..P....-i.r..7?8..C.&.. .rm=....~l..=!.M.. ..O...^..u.&.D..D.RG...U.....f.oO.[6.f...D. . .2.RK[K..%.....J..$ ...(...2.(lj....F.....Q.E.4.I#!.@.....J9.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\engine[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	57897
Entropy (8bit):	5.246429568632985
Encrypted:	false
SSDEEP:	1536:7A1gOvpSV9V3avT+9/1TC+rogLelD3saZuVO2v8plVgcooxr+i8vcBQjWZQZ90t/:7A1qVPqvgptzKncooxr+i8vcBQjWZQZM
MD5:	444065E9F4AC3BCC2A4AFD7DB98BFB00
SHA1:	EA41818B8B25B361361687B028510B4F4F71BFE1
SHA-256:	CBD70032B5F5028347DE20A0560E06A8271294B415D816FB6725AF52C25684FF
SHA-512:	9F9B8F12BC214F23C656A02470A2B510BF99E8FB0C45E68168F7CFE42EB6ED9FBCFD8748FE9DA1883F621F916101A3CB8724881E1566170C42D4C7EE1FCB0C5
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">....<html lang="en-US" class="no-js no-svg">...<head>.... <meta charset="UTF-8">....<meta name="viewport" content="width=device-width, initial-scale=1.0">....<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" >....<meta http-equiv="X-UA-Compatible" content="IE=8">.. .<meta name="author" content="Dupli-Color">....<meta name="revisit-after" content="3 month">....<meta name="google-site-verification" content="-rcIOWkjVhXO1j_UCYW-CxhBM69bUPsbzAeeRA6t8Lc" />.....<link rel="shortcut icon" href="https://www.duplicolor.com/wp-c ontent/themes/duplicolor2019/assets/img/favicon.ico" type="image/x-icon" />....<link rel="stylesheet" href="//maxcdn.bootstrapcdn.com/font-awesome/4.3.0/css/font-awesome.min.css">.....<link rel="stylesheet" type="text/css" href="https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/css/jquery-ui.min.css" />....<link rel="stylesheet" type="text/

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 1 icon, 16x16, 8 bits/pixel
Category:	downloaded
Size (bytes):	1406
Entropy (8bit):	4.264707111401049
Encrypted:	false
SSDEEP:	12:H00maaNsmwJGBQGCDzlgylgchBflYJ3kkBat+GZCly6XkUJdi3cXQe7/jwzj7tYF:LmwJVG6gkB8c1c5k8ycXQe3G7isyAY
MD5:	0F6B428921A5827E9AF9276FB21D1717
SHA1:	24F99CA84F52E0B00D7278DF742C3E2C8AB4C166
SHA-256:	79051ED2EF1772F0D1432AB9C7183FA892680197AED90FD240A06186325CA1B7
SHA-512:	5B7ABC0061AA299BD45158EC868DAAA7F4A54DE3F3245BDCC537A533B71D089FC10C78B0A1BA0B3EF8ACF620E3619F3FA5D2C37B07728B128DA44DC6A0713E 10
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\favicon[1].ico	
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/img/favicon.ico
Preview:	.....h.....(..... .....S..D.q.....~.....VVV.m...888.....H|.k.....)U.....H.....}}}.....F=L.....AAA.....YE.kll.+u.....lll.....KM.....jjj..... .....[[[.\[[.....===.....1.....c.....YYY.[.-.JJJ.uYX.O,T.....,,.....Js.....TM.....999.....4..FFF.....8,..;7..@p..555.&&&..r.....V/..ooo....._...(u..... .....QQQ.....333..n...e8.....111.....kkk.....\\\.J.....j.....wU.. .....P.l.....jZ0.---.I.....vvv.5^..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\fbevents[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	201729
Entropy (8bit):	5.400917859266679
Encrypted:	false
SSDEEP:	3072:CtGFKULetaM4ULO95lV6aLg/zNpkjSVnYDGeI:C/U9wEzDCSmDGR
MD5:	2C228DB65A2225614E390E786DB30014
SHA1:	56AC126556126B101E45B04739CF6F721DE99A09
SHA-256:	C3AF8674489138CD43F5E070EA6E6ED70C98479ADB0DA28D1CC8EB20CEBC8835
SHA-512:	4500DD071F9637FD73EDEF04C4924C0567863AC0561EACE94AF9C65590AC0E0BA17A6AE91E34E81C310495081E0BC1260F993279602B7025896D23044F0AD142
Malicious:	false
Reputation:	low
Preview:	/**.* Copyright (c) 2017-present, Facebook, Inc. All rights reserved..*.* You are hereby granted a non-exclusive, worldwide, royalty-free license to use,.* copy, modify, and distribute this software in source code or binary form for use.* in connection with the web services and APIs provided by Facebook..*.* As with any software that integrates with the Facebook platform, your use of.* this software is subject to the Facebook Platform Policy.* [http://developers.facebook.com/policy/]. This copyright 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.* IM PLIED, 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 C ONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN.* CONNECTION WI

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\flyout[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	1268
Entropy (8bit):	4.907878364489408
Encrypted:	false
SSDEEP:	24:zAMSeUAHC0MdhMlNMMd3jCWvjaDK2T7k6L1PhLwYLv2L8+S5wLePlKLpUauyucSi:kMRbuhy+WvHSv+ezNFaulxk
MD5:	58920A9D743B825A54C6433B76BC9878
SHA1:	5E40596D53121E2E876264C03BD396D6FE3F5627
SHA-256:	C4F05407A20FC8B58C47630C61884749B9D4752D0C2C1CFCE04F7105BFEA8793
SHA-512:	382E435355FD8990E20D6FE600608393BD841DF076C884AF5C8521D757CC65FF652296749A5DB23415B2AC6EF972AEF47413B4B7BA512006EB85B2BC3B28389E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/js/flyout.js?ver=1.0
Preview:	jQuery(document).ready(function() {.jQuery('.2ndLevel li').click(function(event) {.event.preventDefault();. . var categoryName = jQuery(this).children().html();. .//var id = jQuery(this).attr('id').split('-')[1];...jQuery('#drawerLevel2').html('');...../// This does the ajax request....jQuery.ajax({. url: ajax_category_request_obj.ajax_url, // or example_ajax_obj.ajaxurl if using on frontend. data: {. 'action': 'ajax_category_request',....'category': categoryName .....},....type: 'POST', ...success:function(data) {.... // This outputs the result of the ajax request....jQuery('#drawerLevel2').html(data);....jQuery('#drawerLevel2').fadeIn();. // jQuery('# detailSections').css('display', 'block');....jQuery('#drawerLevel2').addClass('drawerOpen2');....jQuery('#drawerLevel1').addClass('drawerShadow');....jQuery('#innerFrame').addClass('slide2');....jQuery('.2ndLevel li a').removeClass('selectedNav');....jQuery('a

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\hi-build-primer[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 157x105, frames 3
Category:	downloaded
Size (bytes):	9652
Entropy (8bit):	7.933490259173024
Encrypted:	false
SSDEEP:	192:HLCjnRf27YISUS51uhZ8rIgIcPLx8In48WrM4I0N7/pG59:HQ6C1LrI5s8C96Pf7/gn
MD5:	5DE579CF4BDE91FA590F8E457039972A
SHA1:	1F8C2B18BA4B3CD8B2021098D1EB3D77EBFAA87D
SHA-256:	FD25A10C897BC6F14CA87BE541004FDADFE9E48C665AC56DF5B5507EAF8F637B
SHA-512:	A7D60689E764C05986E151EF5CF1C0921721EF7F5E6094361CC34942C351E6175B8B99695FF4042C77FA7BAFDE2C4F91F555F3F410253C3AC4397D9E6251D649
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/img/thumbs/hi-build-primer.jpg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\hi-build-primer[1].jpg	
Preview:	.....JFIF.....i.....X.). Cz..;.!.,.....X.4.g..3VkS9-R...o.....P.?..+]..X..t...RLm...C..)Sh.....v.....j4l..k.s.N..x.o..R.&F]..o.]...={_.[`B.f.....e..Jo...TN.?..!.Z..:Ucv.f* 7.w4:.....Z}..nD.,.|..P[..:...@..I^....J.[...^.hToj..M..b..l.!.F.....0cl ..\..DD.....{..@A..^..=.X..6f.<..YG5....>.^....c.....#..$.+I.":<.I"G..>.....{k...VY.<k..7...Uh.\u..G...Y&..t.T...e.W...{...aiEm..f...K.....c*T(...f].....)~o.....pxn.-t.63. .I...CR.....%t>9%.hmT2.U6P..$.. ..dbs...{...$.....L...." ..(.. R.....{..'R.6.:....Aqk-]Z.z.|.&....G....]..?@..Y..=.]....zO.Q-%...[....x....G.....1...T.I-.....g.!.[.<..(K..O.f.}d.b..D[7.a."..JA...`.....M..D".JV&.~...b....V.....9.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\homepage[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	1472
Entropy (8bit):	5.091000181391386
Encrypted:	false
SSDEEP:	24:ADemihrvRcHGEpRfp1IgYPC2phfDxd8YPNRfTbYbAb+MMRFDh1gE/hmdYbackeF8:AohCH/RIBCghBNRbbZb+1RVhdhCxcnVA
MD5:	1D7359DF787CDBE212989FFAC7299961
SHA1:	2856B65BB799BBAD042C668A366BC55BF18205BB
SHA-256:	840D27DDCE1E16B092614A33738936117B54ACB28BA4777BCC6399756AF2E764
SHA-512:	CD16D521DB461462DB75B3D30DFE56C3D512A0E04CCBAE51894585608EC83BAF5CD4F7DD7CF0B3C5804CA487DB388B314150E7AEF8240D953577B4B1A3C77A49
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/js/homepage.js
Preview:	$().ready(function() {../*..$('.carousel.captions ul').anoSlide(..{...items: 1,...speed: 500,...prev: 'a.prev',...next: 'a.next',...lazy: true..});..*/..../*$("#slider1").responsiveSlides({...auto: false,...nav: true,...speed: 500,...maxwidth: 1024..});*/.../// Slideshow 2..$(".carousel.captions ul").responsiveSlides({...auto: false,...pager: false,...speed: 500,...nav: true,...maxwidth: 1024,.. namespace: "centered-btns",...prevText: "",...nextText: ""...});.....$("#slider2").responsiveSlides({...auto: false,...pager: true,...speed: 500,...maxwidth: 1024..});... .$('.owl-carousel').owlCarousel({.. loop:true,.. autoplay:true,.. items:1,.. margin:1,.. nav:true,.. autoplayTimeout:10000,.. navText: [.. '',.. ''. .]..});.....$('#mg-owl-carousel').owlCarousel({.. items:1,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\imagesloaded.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	8113
Entropy (8bit):	5.029584455507142
Encrypted:	false
SSDEEP:	192:bwlk7GGWyoU6PmiOrOkr42Rr4TidNqHJndtMnstQ82c5rn:bEk7GGWykPmiOrDrsTidNqpnMnGQA
MD5:	7E97AB52C3DF75E9053002BB59F2CDD5
SHA1:	502EDAA98677C743246149DEB3A76F5FF65272DD
SHA-256:	11E15F1D64A63CB498D0D42720A688ED15BF78393D8C460D695A110244C066E3
SHA-512:	CDA68BC18168685E225F07612BF21E2BEFA7DE492A4B845D33D21EF39BC3738D02F78C7690462D3BD9A55C50C411CBA5FE25C0D40861D47506742DB562A3E45
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-includes/js/imagesloaded.min.js?ver=3.2.0
Preview:	/*!. * imagesLoaded PACKAGED v3.2.0. * JavaScript is all like "You images are done yet or what?". * MIT License. */..(function(){"use strict";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,s=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;t<e.length;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),s="object"==typeof n;for(i in r)r.hasOwnProperty(i)&&-1===t(r[i],n)&&r[i].push(s?n:{listener:n,once:!1});return this},i.on=n("addListener"),i.addOnceListener=function(e,t){return this.addListener(e,{listener:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\jquery.bxslider[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	3653
Entropy (8bit):	5.299806342777827
Encrypted:	false
SSDEEP:	96:72HwSjIadr/BrAEcPLnMdwSRHTq9tXsz7Zu5wHeDsX:72yLnGzX
MD5:	A1C08AA734BC4852E0F01B25267F2E3F
SHA1:	CDB179988AE0231E48F67FD9B7B3603203F98DA1
SHA-256:	EA743303B209D98842E8B7C47AC1123158632FBE22037E906A6B67CD535CB5DD
SHA-512:	B59A650E74764ABF80D3AECDCA8BC458755E23ECAE53635F2DC63A06E92D9391CDE37CED88F1ABC80282D127E5814566A6751C6F1F031B77D8CA58C645AC97B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/js/bxslider/jquery.bxslider.css

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\jquery.bxslider[1].css	
Preview:	/**. * BxSlider v4.0 - Fully loaded, responsive content slider. * http://bxslider.com. *. * Written by: Steven Wanderski, 2012. * http://stevenwanderski.com. * (while drinking Belgian ales and listening to jazz). *. * CEO and founder of bxCreative, LTD. * http://bxcreative.com. */.../** RESET AND LAYOUT.========== ==========*/...bx-wrapper {..position: relative;..margin: 0 auto 60px;..padding: 0;..*zoom: 1;.}...bx-wrapper img {..max-width: 100%;..display: block;.}../** THEME.====== ==========*/...bx-wrapper .bx-viewport {..-moz-box-shadow: 0 0 5px #ccc;..-webkit-box-shadow: 0 0 5px #ccc;..box-shadow: 0 0 5px #c cc;..border: solid #fff 5px;..left: -5px;..background: #fff;.}...bx-wrapper .bx-pager,..bx-wrapper .bx-controls-auto {..position: absolute;..bottom: -30px;..width: 100%;.}../* LOAD ER */...bx-wrapper .bx-loading {..min-height: 50px;..background: url(images/bx_loader.gif) center center no-repeat #fff;..height: 100%;..width: 100%;..position: absolute;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\jquery.masonry.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	1819
Entropy (8bit):	5.047296238035306
Encrypted:	false
SSDEEP:	24:aUTV//j2ew8p/xnqy8VLF8Xlm7uEQGe1dLpDXzRRvCpx+zVfDpnOKLJWbqQApIsi:HgQBq5LYlm71TopDaW1ObqhuqVcPf
MD5:	CD0EB3406096FF80266E7C9D7D419186
SHA1:	0E3709691BF96233766DE30E2FD473B84166C5B6
SHA-256:	C2E606E1FC82EA3A554AAD5D0520E25D2677B89A891DC5C49E7ACE08FCE92E25
SHA-512:	3CAF5308CDBC5F42F1ECCF5944E8CA785AC086B85954765C1F40D91BD9CC9F3FE6EB816AD821B534F9AD36395F4B6B5D361BEA24EB272E94CAD2824F03FAA C6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-includes/js/jquery/jquery.masonry.min.js?ver=3.1.2b
Preview:	/*!. * Masonry v2 shim. * to maintain backwards compatibility. * as of Masonry v3.1.2. *. * Cascading grid layout library. * http://masonry.desandro.com. * MIT License. * by David DeSandro. */.!function(a){"use strict";var b=a.Masonry;b.prototype._remapV2Options=function(){this._remapOption("gutterWidth","gutter"),this._remapOption("isRes izable","isResizeBound"),this._remapOption("isRTL","isOriginLeft",function(a){return!a});var a=this.options.isAnimated;if(void 0!==a&&(this.options.transitionDuration=a?t his.options.transitionDuration:0),void 0===a||a){var b=this.options.animationOptions,c=b&&b.duration;c&&(this.options.transitionDuration="string"==typeof c?c:c+"ms")}},b. prototype._remapOption=function(a,b,c){var d=this.options[a];void 0!==d&&(this.options[b]=c?c(d):d)};var c=b.prototype._create;b.prototype._create=function(){var a=this;t his._remapV2Options(),c.apply(this,arguments),setTimeout(function(){jQuery(a.element).addClass("masonry")},0)};var d=b.prototype.layout;b.prototype.la

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\layers.fa6cd1947ce26e890d3d[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	269557
Entropy (8bit):	5.429111467374434
Encrypted:	false
SSDEEP:	6144:ap1Lf7mGJQoq/cpp6+PVfVDRGpTr5ojO3:abj7mGJQCp6+PVfA5oK
MD5:	476D935D6723F9ABEA1160C155FFB725
SHA1:	477FF2F072C62493BE703060B3DA7C7A5492F840
SHA-256:	6121CA306AD1045453D52517B8F436EB5A68055C82AEFA46A9A77DE36996A3DF
SHA-512:	C8B11FC445236C60E3D75BDC4BE71F3E6CA46E931740795A1ADDCD86B0F53F721192842017BD414E383A74F5544C23DBADD796E2074E0FC57CCFC7F06B84CD 9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://s7.addthis.com/static/layers.fa6cd1947ce26e890d3d.js
Preview:	atwpjp([216,210],{347:function(e,t){"use strict";e.exports=function(e,t){var a=t.replace(/\//g,"\\/").replace(/\./g,"\\.").replace(/\+/g,"\\+").replace(/\?/g,"\\?").replace(/\]/g,"\\]").repl ace(/\[/g,"\\[").replace(/\^/g,"\\^").replace(/\$/g,"\\$").replace(/*+/g,".*?"),n="^"+a+"$";return new RegExp(n).test(e)||e===t}},359:function(e,t){"use strict";e.exports=function(e) {return e.replace(/\s+/g,"").split("//").pop().split("#").shift().replace(/\/$/,"")}},360:function(e,t,a){"use strict";var n=a(5);e.exports=function(e){if(window.addthis_config& &window.addthis_config._forceClientMobile)return!1;var t=n("mob",e),a=t&&window.screen,i=a&&window.screen.availWidth?window.screen.availWidth:0,o=a&&w indow.screen.availHeight?window.screen.availHeight:0,r=!!t&&(i>o?o:i);return!!r&&r>767}},361:function(e,t,a){"use strict";var n=a(360),i=a(5);e.exports=function(e){return i("mob",e)&&!n(e)}},362:function(e,t){"use strict";e.exports=function(e,t,a){var n,i;if(e.some)return e.some(t,a);for(var o=0,r=e

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\legacy[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	4269
Entropy (8bit):	4.4392107730355885
Encrypted:	false
SSDEEP:	48:gq34yY+RDeY9yRtRZQL1eR14ZV2y0FLKSIrVuia7UYqCIDqXwWHihxX:UyNyELAKZ0FLXsui5wwTX
MD5:	F73FC362C3BDC306A65392C11221159D
SHA1:	2EC8B6C9242AE8507A836B4B82A002E44BF38FAB
SHA-256:	645A9572D1C503A55F3459449A3B91B53C286E316070A7332E1D0A4F7075A146
SHA-512:	C7206A3A12E891B334A6B4D52455EC702F45ECF6D6BEB905F11119F6CC1F8F994B037A3CAC185BE373EAC190B4C2E228818325E900A1B0CFE31DE9FBD59DA1 8
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\legacy[1].js	
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/plugins/ultimate-member/assets/js/pickadate/legacy.js?ver=2.0.49
Preview:	../*jshint.. asi: true,.. unused: true,.. boss: true,.. loopfunc: true,.. eqnull: true.. */...../*!.. * Legacy browser support.. */...../// Map array support..if (![].map) {.. Array.prototype.map = function (callback, self) {.. var array = this, len = array.length, newArray = new Array(len).. for (var i = 0; i < len; i++) {.. if (i in array) {.. newArray[i] = callback.call(self, array[i], i, array).. }.. }.. return newArray.. }..}...../// Filter array support..if (![].filter) {.. Array.prototype.filter = function(callback) {.. if (this == null) throw new TypeError().. var t = Object(this), len = t.length >>> 0.. if (typeof callback != 'function') throw new TypeError().. var newArray = [], thisp = arguments[1].. for (var i = 0; i < len; i++) {.. if (i in t) {.. var val = t[i].. if (callback.call(thisp,

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 22, 2021 18:08:48.245788097 CEST	192.168.2.3	8.8.8.8	0xa88f	Standard query (0)	www.duplicolor.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:48.744435072 CEST	192.168.2.3	8.8.8.8	0x93a0	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:48.755986929 CEST	192.168.2.3	8.8.8.8	0x3833	Standard query (0)	nexus.ensighten.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:48.773094893 CEST	192.168.2.3	8.8.8.8	0xb68	Standard query (0)	code.jquery-ul.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:48.837516069 CEST	192.168.2.3	8.8.8.8	0x95c0	Standard query (0)	ws.sharethis.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:48.848131895 CEST	192.168.2.3	8.8.8.8	0x1239	Standard query (0)	platform-api.sharethis.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:48.902091026 CEST	192.168.2.3	8.8.8.8	0xf7b7	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:49.712168932 CEST	192.168.2.3	8.8.8.8	0xb423	Standard query (0)	platform.twitter.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:49.712393999 CEST	192.168.2.3	8.8.8.8	0xd31b	Standard query (0)	s7.addthis.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:52.238935947 CEST	192.168.2.3	8.8.8.8	0x355d	Standard query (0)	buttons-config.sharethis.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:53.281656981 CEST	192.168.2.3	8.8.8.8	0x355d	Standard query (0)	buttons-config.sharethis.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:53.485826015 CEST	192.168.2.3	8.8.8.8	0x591e	Standard query (0)	z.moatads.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:53.800487041 CEST	192.168.2.3	8.8.8.8	0x7bb4	Standard query (0)	scontent-ort2-2.cdninstagram.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:53.858263969 CEST	192.168.2.3	8.8.8.8	0x853e	Standard query (0)	v1.addthisedge.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:53.893295050 CEST	192.168.2.3	8.8.8.8	0xc63e	Standard query (0)	m.addthis.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:54.034785986 CEST	192.168.2.3	8.8.8.8	0x2c24	Standard query (0)	c.sharethis.mgr.consensu.org	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:54.528565884 CEST	192.168.2.3	8.8.8.8	0xa16c	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:54.600054979 CEST	192.168.2.3	8.8.8.8	0xb30a	Standard query (0)	seg.sharethis.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 22, 2021 18:08:55.241854906 CEST	192.168.2.3	8.8.8.8	0xd88a	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:56.729238987 CEST	192.168.2.3	8.8.8.8	0x2b08	Standard query (0)	l.sharethis.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:09:06.051597118 CEST	192.168.2.3	8.8.8.8	0xcc07	Standard query (0)	www.duplicolor.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:09:27.399701118 CEST	192.168.2.3	8.8.8.8	0x787c	Standard query (0)	l.sharethis.mgr.consensu.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 22, 2021 18:08:48.408343077 CEST	8.8.8.8	192.168.2.3	0xa88f	No error (0)	www.duplicolor.com		151.101.66.159	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:48.805107117 CEST	8.8.8.8	192.168.2.3	0x93a0	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:48.805107117 CEST	8.8.8.8	192.168.2.3	0x93a0	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:48.822036028 CEST	8.8.8.8	192.168.2.3	0x3833	No error (0)	nexus.ensighten.com		18.197.253.20	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:48.843075037 CEST	8.8.8.8	192.168.2.3	0xb68	No error (0)	code.jquery-ul.com		172.67.192.205	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:48.843075037 CEST	8.8.8.8	192.168.2.3	0xb68	No error (0)	code.jquery-ul.com		104.21.44.14	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:48.901122093 CEST	8.8.8.8	192.168.2.3	0x95c0	No error (0)	ws.sharethis.com	d3mdrpbbs8qfxa.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:08:48.901122093 CEST	8.8.8.8	192.168.2.3	0x95c0	No error (0)	d3mdrpbbs8qfxa.cloudfront.net		13.224.193.25	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:48.901122093 CEST	8.8.8.8	192.168.2.3	0x95c0	No error (0)	d3mdrpbbs8qfxa.cloudfront.net		13.224.193.89	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:48.901122093 CEST	8.8.8.8	192.168.2.3	0x95c0	No error (0)	d3mdrpbbs8qfxa.cloudfront.net		13.224.193.69	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:48.901122093 CEST	8.8.8.8	192.168.2.3	0x95c0	No error (0)	d3mdrpbbs8qfxa.cloudfront.net		13.224.193.5	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:48.910464048 CEST	8.8.8.8	192.168.2.3	0x1239	No error (0)	platform-api.sharethis.com	d1r0ldx4ccoewq.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:08:48.910464048 CEST	8.8.8.8	192.168.2.3	0x1239	No error (0)	d1r0ldx4ccoewq.cloudfront.net		13.224.193.25	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:48.910464048 CEST	8.8.8.8	192.168.2.3	0x1239	No error (0)	d1r0ldx4ccoewq.cloudfront.net		13.224.193.17	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:48.910464048 CEST	8.8.8.8	192.168.2.3	0x1239	No error (0)	d1r0ldx4ccoewq.cloudfront.net		13.224.193.52	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:48.910464048 CEST	8.8.8.8	192.168.2.3	0x1239	No error (0)	d1r0ldx4ccoewq.cloudfront.net		13.224.193.66	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:48.962909937 CEST	8.8.8.8	192.168.2.3	0xf7b7	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:08:48.962909937 CEST	8.8.8.8	192.168.2.3	0xf7b7	No error (0)	scontent.xx.fbcdn.net		157.240.9.23	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:49.774207115 CEST	8.8.8.8	192.168.2.3	0xd31b	No error (0)	s7.addthis.com	s8.addthis.com		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:08:49.774207115 CEST	8.8.8.8	192.168.2.3	0xd31b	No error (0)	s8.addthis.com	ds-s7.addthis.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:08:49.774497986 CEST	8.8.8.8	192.168.2.3	0xb423	No error (0)	platform.twitter.com	cs472.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)

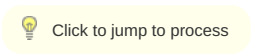
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 22, 2021 18:08:49.774497986 CEST	8.8.8.8	192.168.2.3	0xb423	No error (0)	cs472.wac.edgecastcdn.net	cs1-apr-8315.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:08:49.774497986 CEST	8.8.8.8	192.168.2.3	0xb423	No error (0)	cs1-apr-8315.wac.edgecastcdn.net	wac.apr-8315.edgecastdns.net		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:08:49.774497986 CEST	8.8.8.8	192.168.2.3	0xb423	No error (0)	cs1-lb-eu.8315.ecdns.net	cs491.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:08:49.774497986 CEST	8.8.8.8	192.168.2.3	0xb423	No error (0)	cs491.wac.edgecastcdn.net		192.229.233.25	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:53.343911886 CEST	8.8.8.8	192.168.2.3	0x355d	No error (0)	buttons-config.sharethis.com	d2znr2yi078d75.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:08:53.343911886 CEST	8.8.8.8	192.168.2.3	0x355d	No error (0)	d2znr2yi078d75.cloudfront.net		13.224.193.81	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:53.343911886 CEST	8.8.8.8	192.168.2.3	0x355d	No error (0)	d2znr2yi078d75.cloudfront.net		13.224.193.13	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:53.343911886 CEST	8.8.8.8	192.168.2.3	0x355d	No error (0)	d2znr2yi078d75.cloudfront.net		13.224.193.6	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:53.343911886 CEST	8.8.8.8	192.168.2.3	0x355d	No error (0)	d2znr2yi078d75.cloudfront.net		13.224.193.72	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:53.551105976 CEST	8.8.8.8	192.168.2.3	0x591e	No error (0)	z.moatads.com	wildcard.moatads.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:08:53.862159014 CEST	8.8.8.8	192.168.2.3	0x7bb4	No error (0)	scontent-ort2-2.cdninstagram.com		157.240.18.63	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:53.919905901 CEST	8.8.8.8	192.168.2.3	0x853e	No error (0)	v1.addthisedge.com	v1.addthisedge.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:08:53.956727982 CEST	8.8.8.8	192.168.2.3	0xc63e	No error (0)	m.addthis.com	m.addthisedge.com		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:08:53.956727982 CEST	8.8.8.8	192.168.2.3	0xc63e	No error (0)	m.addthisedge.com	ds-m.addthisedge.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:08:54.099282026 CEST	8.8.8.8	192.168.2.3	0x2c24	No error (0)	c.sharethis.mgr.consensu.org	dlaj66hdiarg7.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:08:54.099282026 CEST	8.8.8.8	192.168.2.3	0x2c24	No error (0)	dlaj66hdiarg7.cloudfront.net		13.224.193.15	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:54.099282026 CEST	8.8.8.8	192.168.2.3	0x2c24	No error (0)	dlaj66hdiarg7.cloudfront.net		13.224.193.36	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:54.099282026 CEST	8.8.8.8	192.168.2.3	0x2c24	No error (0)	dlaj66hdiarg7.cloudfront.net		13.224.193.34	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:54.099282026 CEST	8.8.8.8	192.168.2.3	0x2c24	No error (0)	dlaj66hdiarg7.cloudfront.net		13.224.193.31	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:54.589595079 CEST	8.8.8.8	192.168.2.3	0xa16c	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:08:54.589595079 CEST	8.8.8.8	192.168.2.3	0xa16c	No error (0)	star-mini.c10r.facebook.com		157.240.17.35	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:54.673775911 CEST	8.8.8.8	192.168.2.3	0xb30a	No error (0)	seg.sharethis.com	http-segserver-lb.global.unified-prod.sharethis.net		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:08:54.673775911 CEST	8.8.8.8	192.168.2.3	0xb30a	No error (0)	http-segserver-lb.global.unified-prod.sharethis.net		54.80.205.194	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:54.673775911 CEST	8.8.8.8	192.168.2.3	0xb30a	No error (0)	http-segserver-lb.global.unified-prod.sharethis.net		52.204.22.107	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:54.673775911 CEST	8.8.8.8	192.168.2.3	0xb30a	No error (0)	http-segserver-lb.global.unified-prod.sharethis.net		3.226.11.123	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 22, 2021 18:08:55.292762041 CEST	8.8.8.8	192.168.2.3	0xd88a	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:08:55.292762041 CEST	8.8.8.8	192.168.2.3	0xd88a	No error (0)	stats.l.doubleclick.net		74.125.140.156	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:55.292762041 CEST	8.8.8.8	192.168.2.3	0xd88a	No error (0)	stats.l.doubleclick.net		74.125.140.155	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:55.292762041 CEST	8.8.8.8	192.168.2.3	0xd88a	No error (0)	stats.l.doubleclick.net		74.125.140.154	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:55.292762041 CEST	8.8.8.8	192.168.2.3	0xd88a	No error (0)	stats.l.doubleclick.net		74.125.140.157	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:56.797434092 CEST	8.8.8.8	192.168.2.3	0x2b08	No error (0)	l.sharethis.com	httplogserver-lb.global.unified-prod.sharethis.net		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:08:56.797434092 CEST	8.8.8.8	192.168.2.3	0x2b08	No error (0)	httplogserver-lb.global.unified-prod.sharethis.net		18.198.109.212	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:56.797434092 CEST	8.8.8.8	192.168.2.3	0x2b08	No error (0)	httplogserver-lb.global.unified-prod.sharethis.net		52.58.221.124	A (IP address)	IN (0x0001)
Jun 22, 2021 18:08:56.797434092 CEST	8.8.8.8	192.168.2.3	0x2b08	No error (0)	httplogserver-lb.global.unified-prod.sharethis.net		52.29.0.64	A (IP address)	IN (0x0001)
Jun 22, 2021 18:09:06.111277103 CEST	8.8.8.8	192.168.2.3	0xcc07	No error (0)	www.duplicolor.com		151.101.66.159	A (IP address)	IN (0x0001)
Jun 22, 2021 18:09:27.478586912 CEST	8.8.8.8	192.168.2.3	0x787c	No error (0)	l.sharethis.mgr.consensu.org		18.194.206.135	A (IP address)	IN (0x0001)
Jun 22, 2021 18:09:27.478586912 CEST	8.8.8.8	192.168.2.3	0x787c	No error (0)	l.sharethis.mgr.consensu.org		3.122.221.110	A (IP address)	IN (0x0001)
Jun 22, 2021 18:09:27.478586912 CEST	8.8.8.8	192.168.2.3	0x787c	No error (0)	l.sharethis.mgr.consensu.org		3.124.55.148	A (IP address)	IN (0x0001)
Jun 22, 2021 18:09:42.655776978 CEST	8.8.8.8	192.168.2.3	0x4f9e	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: iexplore.exe PID: 5980 Parent PID: 792

General

Start time:	18:08:46
Start date:	22/06/2021

Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff757820000
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 Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: iexplore.exe PID: 5420 Parent PID: 5980

General

Start time:	18:08:46
Start date:	22/06/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5980 CREDAT:17410 /prefetch:2
Imagebase:	0x1230000
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 Show Windows behavior

Registry Activities Show Windows behavior

Disassembly