ID: 438539
Cookbook: browseurl.jbs
Time: 18:17:36
Date: 22/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

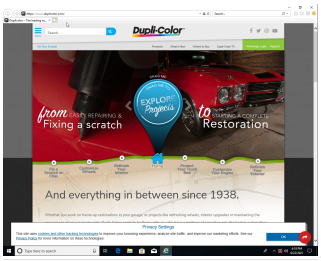
Windows Analysis Report http://duplicolor.com

Overview

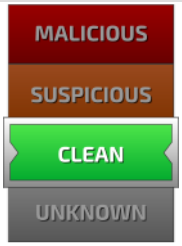
General Information

Sample URL:	http://duplicolor.com
Analysis ID:	438539
Infos:	

Most interesting Screenshot:



Detection

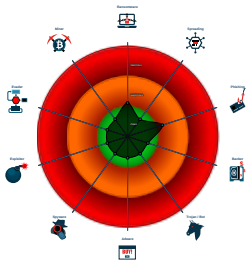


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

Found iframes

Classification



Process Tree

- **System is w10x64**
- iexplore.exe (PID: 6700 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6796 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6700 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

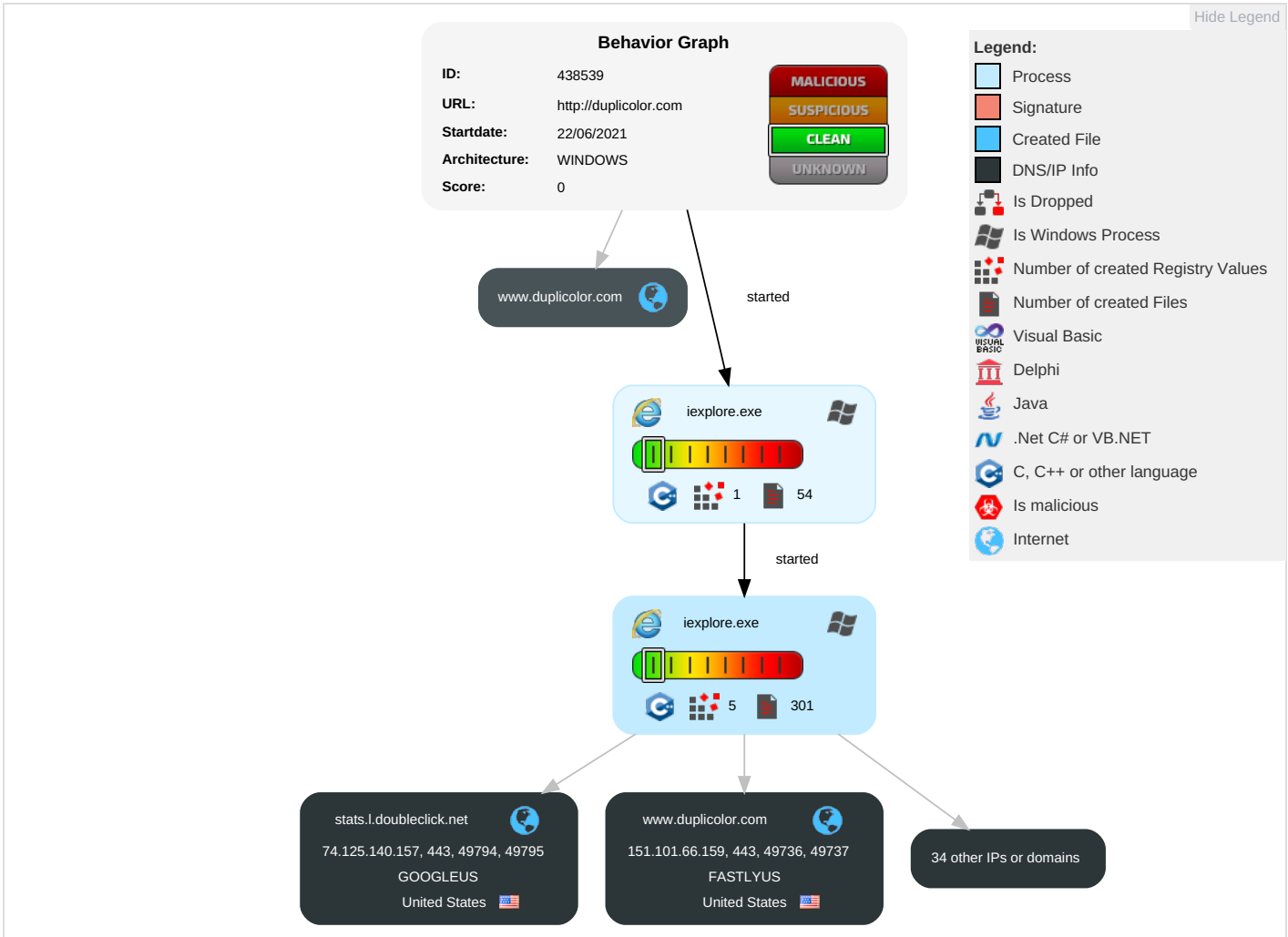
Click to jump to signature section

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 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM Card Swap	

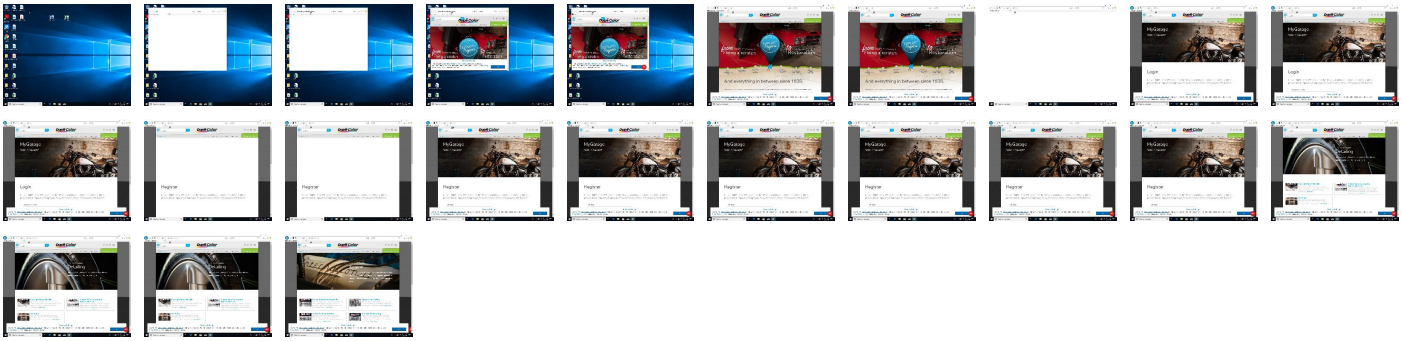
Behavior Graph

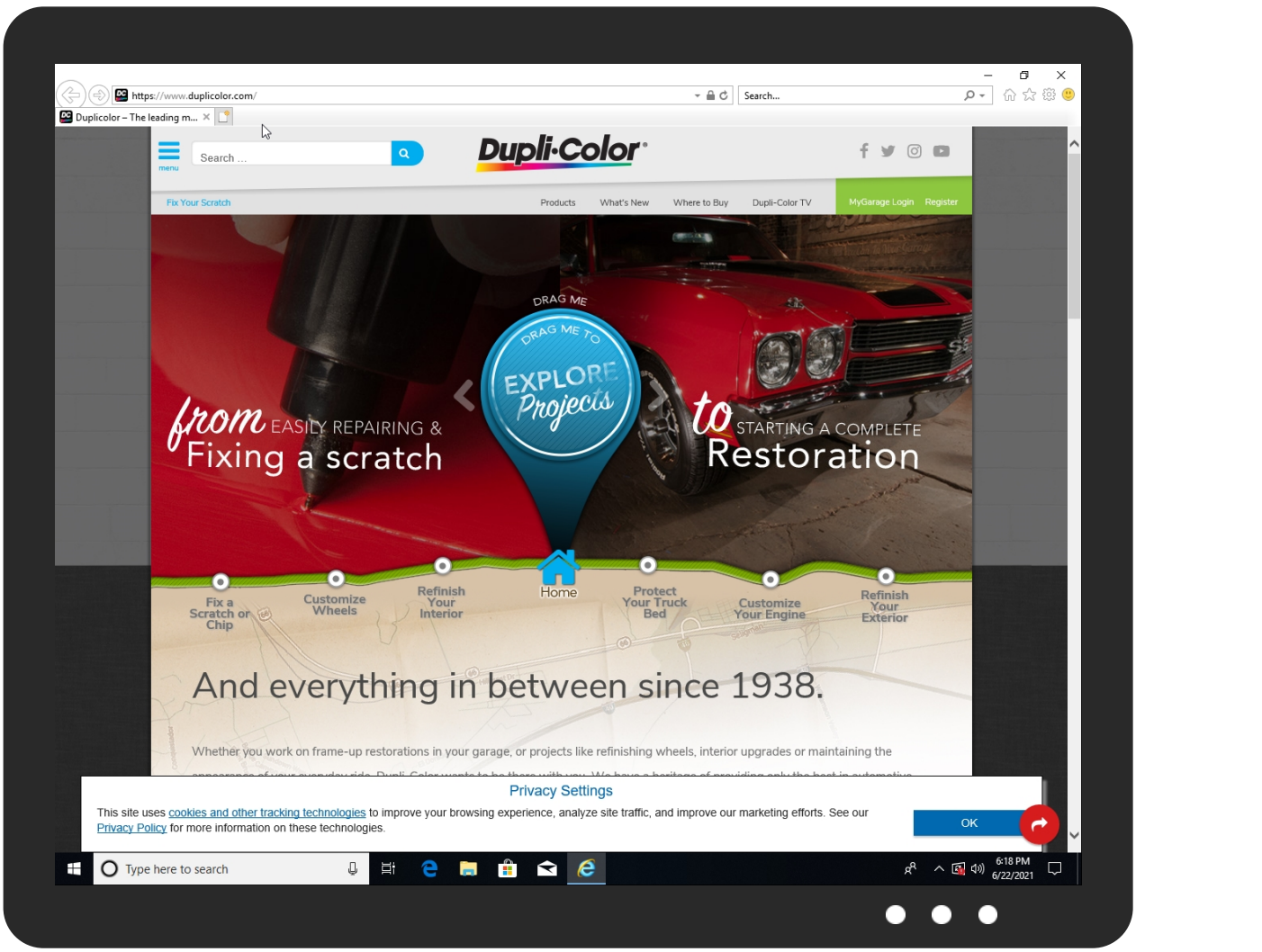


Screenshots

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://duplicolor.com	0%	Virustotal		Browse
http://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/category/engine/ve-detailing-paints-coatings/oatings/	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	

Source	Detection	Scanner	Label	Link
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	
http://https://www.duplicolor.com/register/d	0%	Avira URL Cloud	safe	
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/.com/Root	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	13.224.193.6	true	false		high
duplicolor.com	151.101.66.159	true	false		unknown
stats.l.doubleclick.net	74.125.140.157	true	false		high
scontent-ort2-2.cdninstagram.com	157.240.18.63	true	false		high
maxcdn.bootstrapcdn.com	104.18.11.207	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	3.124.55.148	true	false		unknown
www.duplicolor.com	151.101.66.159	true	false		unknown
cs41.wac.edgecastcdn.net	93.184.220.66	true	false		high
nexus.ensighten.com	18.195.42.228	true	false		high
d3mdrpbbs8qfxa.cloudfront.net	13.224.193.69	true	false		high
scontent.xx.fbcdn.net	157.240.17.15	true	false		high
dlaj66hdiarg7.cloudfront.net	13.224.193.34	true	false		high
httplogserver-lb.global.unified-prod.sharethis.net	52.29.0.64	true	false		unknown
d1r0ldx4ccoewq.cloudfront.net	13.224.193.66	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

Name	IP	Active	Malicious	Antivirus Detection	Reputation
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
54.80.205.194	http-segserver-lb.global.unified-prod.sharethis.net	United States		14618	AMAZON-AESUS	false
93.184.220.66	cs41.wac.edgecastcdn.net	European Union		15133	EDGECASTUS	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
157.240.17.15	scontent.xx.fbcdn.net	United States		32934	FACEBOOKUS	false
13.224.193.34	dlaj66hdiarg7.cloudfront.net	United States		16509	AMAZON-02US	false
52.29.0.64	httplogserver-lb.global.unified-prod.sharethis.net	United States		16509	AMAZON-02US	false
18.195.42.228	nexus.ensighten.com	United States		16509	AMAZON-02US	false
151.101.66.159	duplicolor.com	United States		54113	FASTLYUS	false
13.224.193.6	d2znr2yi078d75.cloudfront.net	United States		16509	AMAZON-02US	false
3.124.55.148	l.sharethis.mgr.consensu.org	United States		16509	AMAZON-02US	false
104.18.11.207	maxcdn.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
172.67.192.205	code.jquery-ul.com	United States		13335	CLOUDFLARENETUS	false
74.125.140.157	stats.l.doubleclick.net	United States		15169	GOOGLEUS	false
13.224.193.66	d1r0ldx4ccoewq.cloudfront.net	United States		16509	AMAZON-02US	false
13.224.193.69	d3mdrpbbs8qfxa.cloudfront.net	United States		16509	AMAZON-02US	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	438539
Start date:	22.06.2021
Start time:	18:17:36
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://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:	13
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.win@3/270@22/16
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\BC6XF3KU\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):	11480
Entropy (8bit):	5.407892676423314

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\BC6XF3KU\www.google[1].xml	
Encrypted:	false
SSDEEP:	192:5KG8yMMYKG8yMMEmKG8yMMYKG8yMMBKG8yMMYKG8yMMLKG8yMMYKG8yMMOKG8yMJ:5KG8yMMYKG8yMMEmKG8yMMYKG8yMMBKI
MD5:	970E3A88888A9750624651EA90CF3317
SHA1:	1EFE22C8B3A132B924F9C2BA3868FC921D34F327
SHA-256:	A716027D7ADF9B76F213B33AFFFD75CE47643BF5749B7F0AE93D8242D7AB8E66
SHA-512:	C9C115C0C70C7C801E3ABB9F6624EAFFDCC3CF1249F03E4A0CE4D27BEDDB632FA90AFDD3950F1CD4EEDEDB04DC5DB8B1D4A75EAB9DAF944BFAB491514A1 1AF9E
Malicious:	false
Reputation:	low
Preview:	<root><item name="sb_wiz.qc" value="1" ltime="2811281280" htime="30840570" /><item name="sb_wiz.zpc." value="[[["news UK",0,[362,308,154,357],{"zl":40009}],["dinner recipes",0,[362,308,154,357],{"zl":40009}],["24hr supermarket near me",0,[362,308,154,357],{"zl":40009}],["last minute holidays",0,[362,308,154,357],{"zl":40009}],["weather tomorrow",0,[362,308,154,357],{"zl":40009}],["cities in UK",0,[362,308,154,357],{"zl":40009}]],{"ag":{"a":{"40009":"Try searching for"}},"q":"m-8sCxwNVqraaMzd_0n2ExiMRbc"}]" ltime="2829291280" htime="30840570" /><item name="rc::a" value="bnJjNng2c2RjNGhh" ltime="1064741616" htime="30893954" /></root><root><item name="sb_wiz.qc" value="1" ltime="2811281280" htime="30840570" /><item name="sb_wiz.zpc." value="[[["news UK",0,[362,308,154,357],{"zl":40009}],[&quo

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\E5F0NRSV\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):	102054
Entropy (8bit):	5.253532648512427
Encrypted:	false
SSDEEP:	3072:q//Gx4Rl7UuJJ+BxCHeTmTlHIdlHImI7IuIWlWIKIMMAMRqbSCvLe9:q//Gx4Rl7UuJJ+BxCHeTmTlHIdlHImI+
MD5:	2C4954716744B4674E0BAE0F8F21DD11
SHA1:	E38DD772F0EEE877A8FF9813C24EC792D09A0D8C
SHA-256:	F59A43E0E9008873E4BB7EDFB12629BD73959BC9FCBB471E7183015BB4B63FD1
SHA-512:	6A17CF822A7FAA712234332D0B9D91BF58207BF62D77CD81CE15B994CC0CDE2AE73F022DD206434DACDFC281C638D803ED908757B04535EA6776E3FF95A413
Malicious:	false
Reputation:	low
Preview:	<root></root><root></root><root></root><root></root><root><item name="at-rand" value="0.7296067385582914" ltime="1033741616" htime="30893954" /></root><root><item name="at-rand" value="0.7296067385582914" ltime="1033741616" htime="30893954" /><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.{77BA256C-D375-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	39000
Entropy (8bit):	1.9214593320328013
Encrypted:	false
SSDEEP:	192:rBZmZ02dWLt1Kifqa5rFzMn9Bqy3DdsflrljrPr7fbrTzrRuWg:rHCj0p1TqaY/qlwwnj6
MD5:	D31CCA912BDA8FCB8C8D859FE2DA0F32
SHA1:	89422FC49653437C91D75C83B1C80169775DEF17
SHA-256:	98363111838D6B2BE58B5AA40FB8BD6D815D4710F2F308C0A546C904521EE175
SHA-512:	1767E090049B478A4A8D733B3AF59997D594730C86674C52BD6A10B25C0D0A079848418A3D4709DB1A9109C3B95895557F527B23B910F0094E17070159AACD47
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\{77BA256E-D375-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	240880
Entropy (8bit):	3.5538720027666617
Encrypted:	false
SSDEEP:	1536:uY1ebn4+Tn4oxCP38oxtc1Y31g61Y31gy1Y31gM3oA3oZ3CKw3CK2Y:aNk/ciNihiB
MD5:	2817AC23B3B35CC770EA21DE0B893269

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{77BA256E-D375-11EB-90EB-ECF4BBEA1588}.dat	
SHA1:	B758AF77F8ACDBAA4695B3634B85F32C6C430E98
SHA-256:	7583D5D476D688162CFFCA3DFE9438CD781B1A6A04F3A46BA5929B790E308E03
SHA-512:	1D567F11B78EC2A79A4BF27E087B8F7A37B06BE6B76C8D5C5A289E8B3AA61B47A7C91A41734DCDD384F0F779FFC9FA84786F7F3DB8B8BF061FFDFA0B63616BA3
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\{80BF4A59-D375-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	19032
Entropy (8bit):	1.5837684180470881
Encrypted:	false
SSDEEP:	48:IwN1Gcpr/OGwpaoG4pQcGrapbSghGQpKSG7HpRqTGIpX25zGApm:rNrZ/mQ46aBSgbA9TOFAdg
MD5:	9076297FE104316221B179217B22E36E
SHA1:	00392FE46D4EFF639C6A50615920F5683C2C1482
SHA-256:	3338359D7913E7FF23200462F8F05127C2C00B52D1C1B3D00BD181325BFEA5C3
SHA-512:	44B43038FB99F09FC7CE154F21A9E8B6F29EF7452F3FC01FF173F6FCFEDEEA20CDCC0C38195DE24F754FBBFB70E8406676E2A21B99CF8C4B69358F7A431DE2E6
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\gee00pr\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	1608
Entropy (8bit):	4.297531449427166
Encrypted:	false
SSDEEP:	24:BfswlRaF/45mwJVG6gkB8c1c5k8ycXQe3G7isyAY1d:BEJF/45TJVG1c1cOiW7oJ
MD5:	22E13284F470380316EE844695C0A3BF
SHA1:	7BB7F62342C02060A684CC83BD6D84273576293A
SHA-256:	88338A15893E36C0D6CE5BDAEEB4BB383A80997E2857A251676A443E4910B83D
SHA-512:	95C22C380F7DE9F762DAF53566117ABB3930B18C7844020DB80F7DEF57DBFA5347DEDA893EA012991AFB500B888B9108F1AE297D004BFE461224C78F590B5790
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\2WF3MMUU\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+MmIZnHNA7tKH9DpOoFz90A13LfZ/VxJ5tTTNuuAzy:rlxMuK98hmZ7tKHW0z9D15XtTT1
MD5:	58EC28417165F6BE15B5481075228E0F
SHA1:	6A5ADB647F3F30174602990FE711EDA9B9662290
SHA-256:	E58BE6A0FB501BA51446DDBEDEE429956E20E1FDD8A883FFEA678522FCE95EDE
SHA-512:	EF7B16E4C58038107CCFB450E38B045DC0D79DB74D1B391C1594F31B85C858EE4D8521750CB83BF868F5C99755CFCDDD311E1AC44E07EA9BE83718A559246DF
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\182478872_788238465452841_4348855019305596379_n[1].jpg

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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...?...<..x..:*\.F...rH....._.?e.S...8*.KB
F2~.._....;B.O.....U..0e...W..Rg.xI.J'..^hwOmy.A2.U..]..._......5..e..+.edU..|I....5.....d.&84.+..:.J...j'Q.+.Q...ksYF.TPzP2j.9..@.......QK..RT...u..S.P..4.p.R^.$.~.`.*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\2WF3MMUU\198520577_584765279171123_8268708892107755070_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, 150x83, frames 3
Category:	downloaded
Size (bytes):	3650
Entropy (8bit):	7.836075874491297
Encrypted:	false
SSDEEP:	96:qikAXY5Ypb9kVT3H9++X4GolsVkI9UzS1sbBaj6BlxvJ:qzFrH9++X4GolsVkI9UW1sbNBlxvJ
MD5:	6960473C126EB6882145776A197A9817
SHA1:	538ACBFEAE596F26E2D4C0E1BF170BADC6F7839A
SHA-256:	290415433D24831FDEDC20B806624AF486663B43C0D01BF3BA8AE64F6E6BB9F1
SHA-512:	0BEC84B7833D39D981BF207AEBAB848FE0FEC0C0B658EB829AAD3FB78E875BC66447F2D3499979B56619FA6E920388B5655C762F85C49EF8FF3E8A3D3438816
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/uploads/sb-instagram-feed-images/198520577_584765279171123_8268708892107755070_nthumb.jpg

Preview:

......JFIF.............C.....................................%...#... , #&')*)..-0-(0%()(...C...........(...((......S...."..A..........................!1.
."AQaq....#2...3R...Bbcrs.$S....................................!.......................!.1A2."Qa............?.....@....KW7"@.lXPh.n.A>..F...[..#6w....B.Q.....s].....&..w..F..+.#9...Y/..8.P.!../.}.<.}.h
.N#.1'..Q.....EmO<....R..@.>.0j.oU..1..B.V...S.8..:.:..*J..:.V...B.B...GLQU.S...J.@PwqHP.O1......f..e..Yn8ZS#.'q.)<c....}`.EO...%to.;...{...E.!*...AZ......W.-......a..U..z...\{..c.|.>..
{.I...Tl.w..%..o9.T...We@......`lu....Q.._}4..5.+.T..i.....8#..#......7......7z%^...)h....G#...j.Xi...."E}o6..R@ ..O.K.p.RR....}.9.....h..V..{..K.Qs..J...6....S..Y......E}./.-1..8..).KC.RT...J.g.
2j.g.........>]iY.!....PI..'....-q.ur..Hq..}.kMP&nK(...V.<.Rq..U.8..- .Y...)..M:N...^_X.oN<I..Y...5w..%]EJ...)C.=@5)..5...%.QN..J...=/].}.....#.!.S.E..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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:	2CBCDFA7EE0E3DD88A7CFDC820AF2E57AED658058ED33CBFEA2C4619EE55F4FF7981CC46C30467316E5C941A3F41BCD44C858D54AB80286A9ECA44AD0D5D 40D
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\2WF3MMUU\200172484_811732862862988_6031437422846588787_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, 150x84, frames 3
Category:	downloaded
Size (bytes):	3799
Entropy (8bit):	7.891021229228668
Encrypted:	false
SSDEEP:	96:UfLwzksqv99LeAx0II9+Oq+IUjIzdU1xEnSROCAf:QLjv99S8M9bq+bshUfEnY9Q
MD5:	4D08CB8AFEA1F6B5B4999D0751DB3140
SHA1:	B12C1B9AFCC3FE07DF0F567311365D83FDB77C1F
SHA-256:	AAEB5D7226AA6CE29D51FB01F0506247841EC7E905D381D84674FF054BE51AA3
SHA-512:	702F5006A8C95E5751087F4323473258D0D134C8DBC0D856B521BBEC8F65DE854F11651BA7E271FBCA9EA6EAF872A5AE489F8B79C39EAD28CFF12A0BF287D16 B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/uploads/sb-instagram-feed-images/200172484_811732862862988_6031437422846588787_nthumb.jpg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\200172484_811732862862988_6031437422846588787_nthumb[1].jpg

Preview:

......JFIF.............C.....................................%...#... , #&')*)..-0-(0%()(...C...........(...((......T...."..<..........................!.1.
AQa."q.2....$Bb..#R..3CSr..................................!.......................!1.A."Q2...........?...[..l..g%6..H...U..WWe... ....?J!......U..(*.......q.>i.&.m....Z..sF.4.k..!..........jwH.0..rW....>...A.
......l......2.I.&..r....=.JI...!..}.K....?.#.n.}O.....k........w..6.....F.......5~.qjm!kK....C).q...?./.@..K.(.%..I<...a..PD.6.@..iOO.}J....e.q(...eFp...,....]CM....X....&........k*p....F....../././.n..Y....-
....E%.Kq?MY\cw.:....c..v.b...j=ac.]D..k..C.....~x.o.E....L........v8!wa..{...t.K....[...7...0.F?.z.6..t.....P.3Cy<..y..g...x.4(..uK..Y......R..Cs.K...e...F3..........]fK-b.W..\HZ>..@O|w..w'..0
.XX.....G;|.J....X....@.s&.}..Xtx...,.8\..>.".V........".'.xKun..l.....w..X.....$F.d9.........;.@.g...H'..0.lg.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\202080892_945187099610799_5386241984688103172_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, 150x188, frames 3
Category:	downloaded
Size (bytes):	6603
Entropy (8bit):	7.94187057928866
Encrypted:	false
SSDEEP:	96:1hWFEnlElhBIhx94RMb4u6yNdeznFW2F7mJyevisYucMsC5MSmcIdNaETgMm8hCz:vWFgOWhfqFH7mwe6XM3PGdjtCZH2zGR5
MD5:	44B51329FA2CABCD634F7A2DEE13CD81
SHA1:	64455DE07783614F1AD28AFC1EB3305F17D538B8
SHA-256:	51DEB8424170DC23F72532F67013AB10BA5993A5B7FCEF44F1370F2324D8D854
SHA-512:	FDAAE611A9E84F5691B53642E8F182680AB932DAAD5A4EF05A8D8F3D11FEF95CADF5D8FF8428290E45CEC692C18A319BE31D9ED9A715CC68FC2F2D8A086172 B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/uploads/sb-instagram-feed-images/202080892_945187099610799_5386241984688103172_nthumb.jpg

Preview:

......JFIF.............C.....................................%...#... , #&')*)..-0-(0%()(...C...........(...((...........".......................................B.........................!..1A
.Qa."q...2...#BRb....$3S4r..%CDT...................................1.......................!1..."AQaq.....#2...C.............?..L..*=....<...Ub..v.... ...Z.C6.`..;...q..Wc.Y:...3.I..Mk.*..4.+E..$P...MI.A*
(....I.N.E..DP..T...q@*<.QZ.J[Ki#GD..iqLQL..iAH...f:-..........h%v.O.IJ.Q..;Y....USh...+.0*..;.;rC.{..dw....X.9#.X...Lq.Z.=7N.I.n(.\.{..!8.....zo..d...#)......]G.....R.x..Xc$....z..Y%.
.J.c.s..J....5.m..rml......1.QU.v.......b.....o.j.....jh..Zq>FY?!..i....mck.._.B...v.......q.....{;..Z>.......1.....N..Z6.U.........T.@Fv..J....&i.n..vs....J...;..R|-.w.+.R........).W....k.+uc t=Gu>DU
..ly#...gt...q.)E..Dy.J....#*E..4...R..H.(.....QQN.()!]..J.xN.`..u..W 0..<.^<...4...zG8..;.hQ..,...F...l...e.$..c.../&0.DI1.u...k...N.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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\2WF3MMUU\202480679_606061997025796_3415451209668366561_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, 150x85, frames 3
Category:	downloaded
Size (bytes):	3533
Entropy (8bit):	7.867860842571811
Encrypted:	false
SSDEEP:	96:xsI2V+rYrIZuGJJ6uXs0NlRH+7MLmPGjJ+q:xsPV+krIQG+u801H+ILmVq
MD5:	7D0573BF16305142D19FBB073A287448
SHA1:	10F8FE3D34BB543E5A2A75F8CD562B18DF564F41
SHA-256:	F344F8A87A85F61B0D05E1965A726B1245142EDD7D3DE6F46A1A5C8D4CF751FB
SHA-512:	9C689DD2C57C7D9DBFF0BB302100CDEEA4EF98FF18C2F0025806B132AC8860268A309959B18FDD25D183ED84DAEEB0D7A60C5C7AC27C386C59FABB0CDC18 7B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/uploads/sb-instagram-feed-images/202480679_606061997025796_3415451209668366561_nthumb.jpg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\202480679_606061997025796_3415451209668366561_nthumb[1].jpg

Preview:	......JFIF............C.................................%...#... , #&')*)..-0-(0%()(...C..........(...((......U...."......................................;........................!1.. "AQaq...2BR...#b.......4r.............................."...................!.1.A."2.............?...h..7...h.l.Y.#......z.N..*.......wdtU....}"z...Z6?...O<...[......[q..X.o..]..l..1.B..D.!.>...{1m..<..7}0 l...A#....EZ<.so,q....(2..r..h1..da....?.oe?...CwrX"....^v.m.J#pIW`...vd.s....q.Q..........P....V.....El..=..{W.Ei....`...l..G.5...K6.c.E......y........=.\.F.P).E../:...O.Q.L..HoD.....a.8 .....I..... ......5iv>..k+.`.9\...[F...pp|......1..;$Rc.....2h.T...xX..wg..O...........s....m..B.p9..)X.V.Z.}~.P{.\..g.;A\|.E.>/#V.>]I....)..7..8.`[;.p.c....ZI.......*~.W..vV...V..q.vs..i&S.Eu{I-....+.w..G......1 .N\|.)..e....Z.N..m.i].!$.y.rs.T..^iv.....k9.e].K....Pp..HI..7.dc{.jO..9..y.W.CU...#.T..gW.G.G....>_..Zw.D...7...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\204214121_339766794222278_8249523650063685067_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, 150x84, frames 3
Category:	downloaded
Size (bytes):	2743
Entropy (8bit):	7.82101081024501
Encrypted:	false
SSDEEP:	48:+iW/QKe1U/8XyjzotOxfWRnOHtPYSUyPqIt45qGXpfRLMIrtpc5GBY/opbQ5r47H:RFG8OoBFONPYUqIt5QfZj3E/2Q5rwH
MD5:	DF7EA93775BBE9E4FD37688178251BA7
SHA1:	298FC1B29DA6857D087F2B3E144C53B423A108C2
SHA-256:	39EC89827D21E805C29916B694EE5B45B574D5F7E66B308355148AB77A956204
SHA-512:	DB4AADBE8A3FDB86B7633125AF310D5D2CB974F2BC1536DF81189C4D7C14E7477623C5E4E3501903308BE41C2649F370F22F641EC5CE31F56F70EC87F32F56B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/uploads/sb-instagram-feed-images/204214121_339766794222278_8249523650063685067_nthumb.jpg
Preview:	......JFIF............C.................................%...#... , #&')*)..-0-(0%()(...C..........(...((......T...."....................................7.......................!.1. "AQa.q.#2.....3B.$Rbr..............................!.....................!.1A.Q"2a...........?....n..&#.....x....Q.....VZ..4...]F5<.r;.`N.k..M>...BAe.5t....Z.3(..=..Mt.O....E.kxN1...N4.........t.8 &.kB.U..pi.h<.=.;*.&....}...X...d.9..[.......Z..Y.\".d.s....F.e..RVwf.2..<....G.3L..o..{.S.(..5..z...E$D.m.I...Y.V.7C.....sSz..R`1.T...Y.....~8_z../...Y&..@....Q.o.j.NX...{....n.:...uyYP.... .z.q...K...1[%D..7.I..}3D..Nx...4q..*.4i.+d......%...~)QRZ.l...J..~....S.1..:..P...OX.'%.W59q<6.#........k.!.`...A\ZI........xO~JB..j..m.x..EO..7O.?.;.. ..Z<.O....I..x.R-.5...'....([.V...u.. ..%.$.n...!I.45..X~p..B........Y..j.jz..]].m..Q\|.02{.T......,../.Y.2..n.<.W88.?5...[.....bI.'&...-....VX.......a.J.,.Il....42"..$...N...I.......I?Yj6+,.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\3E6IWM65.htm

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	162
Entropy (8bit):	4.43530643106624
Encrypted:	false
SSDEEP:	3:qVoB3tUROGclXqyvXboAcMBXqWSZUXqXlIVLLP61IwcWWGu:q43tISl6kXiMIWSU6XlI5LP8IpfGu
MD5:	4F8E702CC244EC5D4DE32740C0ECBD97
SHA1:	3ADB1F02D5B6054DE0046E367C1D687B6CDF7AFF
SHA-256:	9E17CB15DD75BBBD5DBB984EDA674863C3B10AB72613CF8A39A00C3E11A8492A
SHA-512:	21047FEA5269FEE75A2A187AA09316519E35068CB2F2F76CFAF371E5224445E9D5C98497BD76FB9608D2B73E9DAC1A3F5BFADFDC4623C479D53ECF93D81D3C9 F
Malicious:	false
Reputation:	low
Preview:	<html>..<head><title>301 Moved Permanently</title></head>..<body>..<center> 301 Moved Permanently </center>..<hr><center>nginx</center>..</body>.. </html>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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\2WF3MMUU\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
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\2WF3MMUU\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
MD5:	9929FE4E83682960828CEE3A1928393A
SHA1:	23778BACB5AD3ECCD2F3F0EB4B2D6DA139E855EC
SHA-256:	0FBE5C786EB6E912398244FA8B5B60FFED2CF7F09753D856882D8511A8EB1571
SHA-512:	AD4A801B84AC7185DB383C5772B561262DE35E9E9744D3DF4CED44ACD7E8A98D7395B36798EA59481E2BDAB04C7CCDC29E3870D1E7E80CA982DD49A773B6C 4D
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\2WF3MMUU\CWRC794_102914[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):	6414
Entropy (8bit):	7.890086406334461
Encrypted:	false
SSDEEP:	96:6OyePudfhkfizxUdkTsnntXMdRLZsVE2Fqo6whQYXDL2BYbWZpht6+4Z14S7V3Mh:6OD2LNmd4AtWviRdDuo+L6+DSpIr
MD5:	602F13231B009EB08D51A662ED401CD6
SHA1:	6446B901D5825717D3EDAE65F4ABCB0296FAA7B8
SHA-256:	26BDCE37E71363BDEAB170269937922AF3A981F5488908842B7D6F5AE93CBA11
SHA-512:	D5B5E4183122839F8D55FFE8744486B6B970EF93637A3E7DF834A380B176B522B5DECD058E2181A544CD3E8179FEAD35C5FDED9555E81F2B8519CA4B8CEE7D2 C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/img/thumbs/CWRC794_102914.jpg
Preview:	......JFIF.....i.....$....(....<.`lY.].#..g#4..d.QG]...b .F.c....}....."J.`q.tD".I&.)V.].B|..w...Zm.'.a...#2.....5.w-.s.....=.w^.Y.nq.c9.NZ.n...5$LM.t...6\.....R.!I+...C.Q).U..Z.....%.|k.. ..h).!.Be..V?I..."i.z....A..z...rG....{.8.....$.%....y.z...p~d., ...^^..p...$. o..... ....@..(.."....{...{._F.zz..6....@.....E.,@...$@-.%.....?.....(J.....5l.s.....ol..O;.q..7w[..j.....P.T.e..TP.....?...-... .....!12B.. #AC&3Q.....W...L.,\..%..Z~.....NZ.z.'..~.9.A!e.t.t.9..O..9....}f.o,.*..2w..^....@AW..w5..k..0T....W...O....x.1.....g.z..VDkWx..O.l..}.=.*^..:[\.t..q..hx.... X.E...b...)...b.....].7.`bP.F.y.....-Zf'[.W.../.e.x.....S.....t.;._.....v.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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\2WF3MMUU\HSK100_041113[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):	6386
Entropy (8bit):	7.89704131650306
Encrypted:	false
SSDEEP:	192:UH+tPr09NtuFuKQAGgc8MMV67OQZkhGIc19WGCSZmryfta9qwm:UywNt1KzGfHOQghCPL1a9qwm
MD5:	12ED8A881F67262A73BC13226DCA31DA
SHA1:	2E023CA9F5B54E7B1C34A74E2215CE3DE4D5852C
SHA-256:	2D37C385157AD5C698E3EC6AF5135334DACE2535C85B19576C77BA7EEECA28EB
SHA-512:	664BF4A375E3D0D08495242886C5E5A30C5736467871ADBB0B8F46CF5BA19A31CC080DCA460D784C20A8799C9457B02CDE156B881B5B125D8A6E55BC78B31C1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/img/thumbs/HSK100_041113.jpg
Preview:	......JFIF.....i.....[.@.W.B.....X.M.....g... .&...#..7.?8..._...O.%..or..(.}*.ll..EH....jw.../..km..:...4.P...n..a..Q.UL^G.....V-K.^...D-]$...6.qm..gr...S.t\|.....@s.Z/ .._ f.N.E.%.j...x...-)..2...f$l.Ai7G.s.N.E..k1.....<.y^.KF.PT9FS .....k.....D...D.:....A..LP.Bbo.....@.E"....P.@..f.U\.&f.].&U..ME..[sb.tE..X..!@.....j.P<..*.^C.....o.....O..... ....@.....gR,..&..... .jZ. ....B.....!.1AQ."2Baq3R.....#.. %Cbr..04..$5St.....?...4..y..-..sL.["G.wP...#O....Y#.v'i.....:...,..uM...276@..c.#....]..<....&.../..n...#.M.:.l.du.89m.3J.....5....[dm.. ..!...Sl.....m.....].c!f/.....AUI.I4..d.....rauS.-..x{,.l.B.....p4..R.=./GdE.K.'..-.s*.iNv}m=

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\KFOlCnqEu92Fr1MmEU9fBBc9[1].ttf	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	TrueType Font data, 18 tables, 1st "GDEF", 8 names, Microsoft, language 0x409, Copyright 2011 Google Inc. All Rights Reserved.Roboto MediumRegularVersion 2.137; 2017Roboto-Me
Category:	downloaded
Size (bytes):	35588
Entropy (8bit):	6.410135551455154
Encrypted:	false
SSDEEP:	768:6yVJgIpAqZsXgDNHOBBPXNOKdhT1N+06XAxGrzmoqpxk0SnuUR:enq805OBBdhT1NP6XAxGryoqp2
MD5:	4D88404F733741EAACFDA2E318840A98
SHA1:	49E0F3D32666AC36205F84AC7457030CA0A9D95F
SHA-256:	B464107219AF95400AF44C949574D9617DE760E100712D4DEC8F51A76C50DDA1
SHA-512:	2E5D3280D5F7E70CA3EA29E7C01F47FEB57FE93FC55FD0EA63641E99E5D699BB4B1F1F686DA25C91BA4F64833F9946070F7546558CBD68249B0D853949FF85C5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmEU9fBBc9.ttf
Preview:	..... GDEF.....{....dGPOS.....|<....GSUB7b.....8....OS/2t.#...r....`cmap.....st...Lcvt 1..K..y....\fpgm..$...v.....gasp.....{.....glyf.'.....,..j.hdmx.....r\|....head...r..n....6hhea.....q. ...$hmtx..MO..n@....loca\v@z..l(....maxp.....l.... name..:...z,...post.m.d..{.... prep...)..x|...S...d...(.....o.....9.....EX../... >Y..EX../....>Y.....9.....9.....9..... ...9.....9.....01!!.!.....!.5.!.(.<..6.....}.w...x.^.^..^.....<.....9.....EX../... >Y..EX../....>Y.....+X!...Y..../01.#.!.462...."&.~.....J.JH.H.....9KK97JJ....e...@..... %...EX../..."">Y..../..../...../01..#.3..#.3..#...-#...w.}....}.....`.....EX../... >Y..EX../... >Y..EX../....>Y..EX../....>Y.....9../.....+X!...Y.....01.#. #.#5!.#5!.3.3.3.3.#.3.#.#.3.#...L.L...:...N.N.N.N..:..L.v.:.....f....9....`...`....f.8.9...d.-.&...,..*-...9...EX../... >Y..EX../... >Y..EX.#/.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\KFOmCnqEu92Fr1Mu4mxP[1].ttf	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\KFOmCnqEu92Fr1Mu4mxP[1].ttf	
File Type:	TrueType Font data, 18 tables, 1st "GDEF", 8 names, Microsoft, language 0x409, Copyright 2011 Google Inc. All Rights Reserved.RobotoRegularVersion 2.137; 2017Roboto-Regularht
Category:	downloaded
Size (bytes):	35408
Entropy (8bit):	6.412277939913633
Encrypted:	false
SSDEEP:	768:PX4i+tezjtQYgu30G0xL9nQbuEL7LQo9SBxQbptqKmomjJlvh:PJ2z3G0xpUusLEBKptqNomjV
MD5:	372D0CC3288FE8E97DF49742BAEFCE90
SHA1:	754D9EAA4A009C42E8D6D40C632A1DAD6D44EC21
SHA-256:	466989FD178CA6ED13641893B7003E5D6EC36E42C2A816DEE71F87B775EA097F
SHA-512:	8447BC59795B16877974CD77C52729F6FF08A1E741F68FF445C087ECC09C8C4822B83E8907D156A00BE81CB2C0259081926E758C12B3AEA023AC574E4A6C9885
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4mxP.ttf
Preview:	..... GDEF.....{`...dGPOS...h..{.....GSUB7b.....OS/2tq#...q....`cmap.....s....Lcvt +.....yl...Tfpgmw.`...vd....gasp.....{T....glyf.....,..j.hdmx.....r ....head.j.z..m....6hhea.....q....$hmtx..Vl..m.....loca?.#...k.....maxp.....k.... name.U9...y....tpost.m.d..{4... prep.f....x ...I...d...(.....q.....9.....EX../....>Y..EX../....>Y.....9.....9.....9.....9.....9.....9.....01!!.!.....!.5.!.{.<..6.....}.w...x.^.^..^.....{.....0...EX../....>Y..EX../....>Y.....+X!...Y.....901.#.3.462..."&.[....7l88l7.....-==Z;;.....#...../.....9../.....01..#.3..#.3...o.....o...x.....w.....EX../....>Y..EX../....>Y..EX../....>Y..EX../....>Y.....9|../.....+X!...Y...../.....+X!...Y.....01.!.#.#5!.!5!.3.!.3.3.#.3.#.#.!.!....P.P...E....R.R..R.R..E..P....E.....f....b....`...`.....f.#.b....n.0.....+.i...EX../....>Y..EX."/..">Y.."...9.....+X!.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\MS300_032613[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):	6436
Entropy (8bit):	7.877148763663616
Encrypted:	false
SSDEEP:	192:hnZOzcSZjzC2a1iY/PdCHqFjvWzR7/l6gOlwa0kU/:32cSdzJctDZW9Ll612kU/
MD5:	E13285FCF95A343E6D9F788F8A48C86B
SHA1:	D3FDA036993471A9618DE5831D2008E225EA2DE7
SHA-256:	B1E6BCE0E526E63CB84CC4EB190AD5D4EB8721AD753A4CD324640BED320D0834
SHA-512:	44BF155DF42F748E284A764AB84960204988F8FBCCDCADEC576F6EFE8252841B84DED5F3EE4B4BB86E4427160758D8CE8DE3F37F9D3A631DE3FB658642F89FAC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/img/thumbs/MS300_032613.jpg
Preview:	......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,.l...j.e-T&....FX..n..5...a..h5.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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\2WF3MMUU\anchor[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\anchor[1].htm	
Category:	dropped
Size (bytes):	85048
Entropy (8bit):	5.892042605360575
Encrypted:	false
SSDEEP:	768:v/S1AGjxC8GN/TqNDCyZguz3Fkw4VKDvlSqa/SgtyC8GN/TqNDCyZgu4ncH+QD4/:GfxCDcZP+KDvTgtyCDcZUceNZp
MD5:	57F3E61A73ABD63B64E641260D511DF7
SHA1:	C4234F5942ECF993642C52FBB4122A7D6BE73768
SHA-256:	B986828F4086D910BB866C26A4834439EE62C26AADA08FA8FAAE4EE9760C298C
SHA-512:	458C63E9E09CD2764F05D2BC946F8A7C2790384266207C1EA681DEBEE5F1582628425D698AE83DF765D14C601F4DE00E06D1708808053E438E1EC83DEB4D476
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="drQo6/ruh/FhNLWMPYUi4w" type="text/javascript">window['__recaptcha_api'] = 'https://www.google.com/rec

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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):	43499
Entropy (8bit):	5.8880571650751
Encrypted:	false
SSDEEP:	768:v/SavGo4C8GN/TqNDCyZguIXkZf7c6siab1tkErm:9j4CDcZ0XGfg6NY1tkErm
MD5:	B5BC4B5FEFD63A2D0107752354E753D9
SHA1:	6F528BAE6D3A4EA61995101DBAB416ED1E9B60F4
SHA-256:	1CBFC8725D00352EA22B2EC2D14A76FCFA0B3B7BB7B0101ABF865F43AC02F5BB
SHA-512:	3E1B0C42F0E0B106A30A9A6DB4470C61C93E7377C577835FE1B9CC81614080A2A1BA0F45976602F8923C4AE779C74695608C5CB5FAFAF969D98B05628B12ADD
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="rsRubygd4XVxLswZ/lrqQw" type="text/javascript">window['__recaptcha_api'] = 'https://www.google.com/rec

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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):	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
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\2WF3MMUU\automotive-detailing-paints-coatings[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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\automotive-detailing-paints-coatings[1].htm	
Category:	dropped
Size (bytes):	45452
Entropy (8bit):	5.285897551639794
Encrypted:	false
SSDEEP:	768:7AjRgOOpSV9V3a0BVT+9BmOsCyMhZUdcooxr+i8vcBQjWZQZ90tsd1/h0NIj05+e:7A1gOOpSV9V3aST+9lyMhZUdcooxr+iT
MD5:	EA51D7739412E5A96737C7BD7A728D9B
SHA1:	D16C471ABCD114F56A9FE11C24C2C23CB5E6DF0C
SHA-256:	4E3F2597A75F1C8CE84F1E86F3D33826EC4A0127132721526397B7DB66C3D382
SHA-512:	876DB12646A987275C3B2F28F8A76ED2D01A25087B03B630F448B6B1DC1FADD5A55451BE34DF6D5A376A33B8A10DAE9EE31FC703298C0EB49E61D222A8F5665C
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-content/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\2WF3MMUU\background_gradient[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 1x800, frames 3
Category:	downloaded
Size (bytes):	453
Entropy (8bit):	5.019973044227213
Encrypted:	false
SSDEEP:	6:3llVuiPjlXJYhg5suRd8PImMo23C/kHrJ8yA/NIeYoWg78C/vTFvbKLAh3:V/XPYhiPRd8j7+9LoIrobtHTdbKi
MD5:	20F0110ED5E4E0D5384A496E4880139B
SHA1:	51F5FC61D8BF19100DF0F8AADAA57FCD9C086255
SHA-256:	1471693BE91E53C2640FE7BAEECBC624530B088444222D93F2815DFCE1865D5B
SHA-512:	5F52C117E346111D99D3B642926139178A80B9EC03147C00E27F07AAB47FE38E9319FE983444F3E0E36DEF1E86DD7C56C25E44B14EFDC3F13B45EDEDA064DB5A
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/background_gradient.jpg
Preview:	......JFIF.....d.d......Ducky.......P.......Adobe.d..... ....W..... .....Qa.....?.....%.....x.....s...Z.....j.T.wz.6...X.@... V.3tM...P@.u.%...m..D.25...T...F.....p.....A.....BP..qD.(.....ntH.@.....h?..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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):	5.557867832765507
Encrypted:	false
SSDEEP:	24:D0ksPkGAy/iOYsFYxMJ0/iOYXFYx1S/iOYrFYxAQNPGt6f9IjgvPCt6boT0NSALt:Dc1A1OLKIXOgKNOMK5N+iuwqn2V3lAy
MD5:	46835627B61B3952FEA45C9D14F1D9D8
SHA1:	1B1A378677D3C1FB6047B5EB6EE5CA37586ADC13
SHA-256:	E140A869077B2DCF3870D39640996B9F2B96E1C474B5FC68C42796C1BB3D7B38
SHA-512:	AB49EF49D6447B921E3BC7BB7F39D8801DAC1D0D9958C0FB2C35904A167DCF24CF8A2E291E06D450DA4739F86FFBD0527CE9B6B35E4C5FD76FC7848F7CD304C
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="rCv6KcyfCCnS1f7yEIsX5w" type="text/javascript">window['__recaptcha_api'] = 'https://www.google.com/re

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\engineSlide[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):	85734

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\engineSlide[1].jpg	
Entropy (8bit):	7.982022333179428
Encrypted:	false
SSDEEP:	1536:HIPOD6fSiNRebtY5siZ0Ex9X8yj9uZXGXIlrTi8R75tkIQDjpd/:omefSiKfijx9XnHXI3VHC
MD5:	10A5DF9BE5CF1763E7945A95A0BA821B
SHA1:	F22C6A1E23D0EB3690FC30C633C982DE2133B0BA
SHA-256:	9FB66E5D6CE45F9227BC67DC75F00EF775C4C1FE437F2A72C353B9A3B5984ACE
SHA-512:	9816646904BC2D3D5CC059EAAC86AF85D6996478974154329F52F66401D8AE4E075FF0B99D1CFBAB97D2651221A71E2D390DDBBC4917C6FB14AD98AED2C2C9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/img/banners/engineSlide.jpg
Preview:	......JFIF.....R9.*..n..Y.w.....W..{.I....D .\.#Y.y.*..W*...9.zM.D.:.*=.....%.....`...p..j.....>..^.....1..Y.[.1.....#y.}.D...3..=[3"_y^.;.s..../.).:]OH....W...*.f.....(....&g.mk...5.W*{..`D..A.t....9S.V1..5Y..''/...5.uP..Ew.kb_+.....;.c# .\..JC...m.Y....x..\.MI....$Q.....D...O{.8...E.....H..{.F5".L.m.V..T....4O/..t...s.$..,mF-.x.....ntz.....[.n3...hk..;..b.g.G.>...y....,N...jy.>I].D_5..G.g%.yZ....X.....y.s..Y.....Xv..h9. (.X.in.....E.q.U.....@G=.o.s.....bj.A22..Sr...Dj...bA....y.<f...tg..#....'..{._+.....'HG.. .{..*..<_.=.;.x..7?.....:.$.i.[.=..{.. ....9.A.....5..T..A..D]..v.$o..e...+..r..s"b....A....Ql4..oV.n...q /..xD.....{.i.0.o6F3.{Z..nk.....y.....y"j.%u.x?{.6.l.lj/..+}.Us..y.F../E.....{.....l4.s"..}!.....`D.V....8....IO...._

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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+rogLelD3saZuVO2v8pIVgcooxr+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-content/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\2WF3MMUU\exteriorSlide[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, 1024x625, frames 3
Category:	downloaded
Size (bytes):	112004
Entropy (8bit):	7.984575637697467
Encrypted:	false
SSDEEP:	3072:K0YZPcep755/W6oNoojg82xAuJMUfsl1Vcl:BcUM5o6o3swlI
MD5:	FBE013CB702A929F9338E2DE2719628E
SHA1:	DFA3E06F6BC0C1A946C22454AA31B868D06579AF
SHA-256:	0DC0D2459A7492BBEAC95FC8FE63030009A9133A936FC78054FBBE3157B21BA9
SHA-512:	8A492C756FB82D2579DC51159E536257D32590192F3F685B838EB28EC6D9468F4C37463C234AC6DDB284D9B3286EAB39E270374E12BE74A9E5B46B1ACC9EEAC C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/img/banners/exteriorSlide.jpg
Preview:	......JFIF.....q.....UI%.eRQ].$.P...r.].Q[L..G E.cZ.I..NC.7Q..k..*..0. .TP,MJ....s.$.I..K..:(Ta(..@']T..R..K4B*y...zD.....4/..'2..F.s.@*<I9.Qt.&....*..D.I%..+.:6.2$....[.]B...'.a./`.....i.e.[...o..."{.....^j.....5$.IwW....5tgJe]..a,.<#.- .^..(.D%.G4T..<K..f..+....9..Q....<.$.[.9I@.T..I$...J.Uw.....z..p...m..Q...n..:..Q.....\.y...H.D+V...*[.$%i.\....K.uwR.J:.....5.M.tEnnv6(...{$n..b.g-O.k.ja."..b..)a.Vte..<.YP.....$...]..UK;..jL.....1.kH.*.KJ.3S..>..gfs....,M&.~.."..J^|...i..14l.b...$.....\)uAF@E..s.eY4."..vEfDVV..~rCn>..Z.+...S9..vH1.hW$Q....k.....MT.B..ww.K.p..%..e..Q.9{u....Y.....BX st6g.....D..S2N\I...7..*.$.K....\.eu.....2.....q.....c..y...y...f.pv.G.....#;F~.nsr(..$.R.]I$..Q].....n...w..i.....<...s.?..y.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\flyout[1].js	
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\2WF3MMUU\footer-logo[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 286 x 62, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	4035
Entropy (8bit):	7.110298132758691
Encrypted:	false
SSDEEP:	96:zrxIyLBltYNqzCe9mSpJmAlZb0Z4Oc0EMrxN/:JnQqzCe9npJpvbPX9MrxN/
MD5:	3065E5F5FD8C17D265874817A0E5B001
SHA1:	815D6F050C96B905E9B9B430B70024C45ECE65EB
SHA-256:	628CC07085BEFF3171EE97925555D20B1CACB9CA47DDAF8AE46C1EEFBECE04D3
SHA-512:	A3ADACE477D97998B6208C497E395F6F708FB3470CDCC1AF92BDDCC54F8BD9629CFB935214219F37CCAFEE02608357E52BB0F71C1E5DC5E2613291B27C08BD3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/img/layout/footer-logo.png
Preview:	.PNG.....IHDR.....>.....f....PLTE..... ....M.....tRNS.U.Q.....-0#.....K[..6p{*l\dA&v...z.....r.+...H..2..:.....u....J....e..>g..... ..o...=hLZ.....n8,kl..''...N.3..;@.s<1.....W....i?.....S._B..qaF.].....(~.....DX4..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\hlr100_42613[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):	7361
Entropy (8bit):	7.912325349073702
Encrypted:	false
SSDEEP:	192:4VuPVjogtQHNb4gBMOzFa+haHhURLKz1Pi:XPFbYsc5FavhURm6
MD5:	31C688FAF1F504D84FD497DEA31C770D
SHA1:	05C06B3BDB72E570C6E8D4902A2D9A254132010F
SHA-256:	CE18D7708703CDCEF824DFCFCE363F62F862BBDF8F56BED49613B4B60219C3E3
SHA-512:	9B15E0A60AA3D487F4CD53F332C8B6DDCE18C9003962573F60EA66FA7B4604E817FA276478CC31B04DD881C3BED6DC34CFEB44EF633ECA890B9CE61A2176F9DE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/img/thumbs/hlr100_42613.jpg
Preview:	......JFIF.....i.....:...V.....`m.=.6..t.I....l9.w..Z/h .v.:...o..&...j.....f...i...lx...$4.....C./<...8....Tu.e.a.ttf#....H..`6....u|....@.Y.w.....T....`.K....CE..E....8.b..V.Z.....P..C.*....|.hz.....q...m...B).....E.;..c..j...."<....CD..A.....R>... .)_.....+`X.6eE..9.....]9s..C....d.b..-. Yb...@..QD.....E@.Z.(%Ae..(.....(xoT.XYN._...../..~_-....9}>.WS..\.9.H.A.B.E...,.#J... ....K...I.H...(..E.....e.,....3.....!."1.#$23A..BQq0CSa.R.....,.B._mz....9..j..+.../.3.Y...V5.....?'Yq4...b..ysV..q.h.F.`.4ri...Ic.!Z...15)...F._5..''v3.\J.9I.F7.| {..V[..iU'.|.=.s.I.WQ.w.o..gQ.R...%.A.y...6.+.{-..9..`...6..u....~...'....-.Z.....eUwx)..pS.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\homepage[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	1689
Entropy (8bit):	5.059353777601915
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\homepage[1].css	
SSDEEP:	24:DwFQb0ND5zDpM55Wo7y5W1pA5W5WB5VdjvetvyRI+GVy5KG2FEhPF/1r:dAlC59y5Yi5NB5PGN2UG2yhPd1r
MD5:	F057B8B6ABE8E9D7442E50FCCA3FDA3C
SHA1:	7A11E788D921EB749B2E39B0560629E3BE98D032
SHA-256:	7EB4D7C5AC4D82CCA445EA2E3DD322DA85C9955B9C51B0B97C47A62DBBE5C10C
SHA-512:	94C674F827A01B95D053A4AF556D7CBD083794FB082FFEE86E4C251E4560EEA7C532BDF45C783BC57B43A2C849D137F5BF6CE479D82F7C26CD9559B164C4D7 0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/css/homepage.css
Preview:	/**********. * SOCIAL HOMEPAGE *. **********/.#social-home {. text-align: center;. min-height: 600px;. position: relative;. z-index: 5;. font-size: 20px ;.}.#social-home > div {. background-position: center;. background-repeat: no-repeat;. background-size: auto 95%;.}.#social-home .inner-div {. display: table;. width: 100%;. min-height: 330px;.}.#social-home figure {. display: table-cell;. text-align: center;. vertical-align: middle;.}.#social-home figcaption {. margin-top: 1em;.}.#social-home .twitter {. background-image: url(../img/layout/twitter-bg.png);.}.#social-home .facebook {. background-image: url(../img/layout/facebook-bg.png);.}.#social-home .instagram {. background-image: url(../img/layout/instagram-bg.png);.}./**********. * MY GARAGE *. **********/.#my-garage {. background-image: ur l(../img/my-garage-bg.png);. background-repeat: no-repeat;. background-position: top center;. color: #fff;. text-align: center

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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:	CD16D521DB461462DB75B3D30DFE56C3D512A0E04CCBAE51894585608EC83BAF5CD4F7DD7CF0B3C5804CA487DB388B314150E7AEF8240D953577B4B1A3C77 49
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: ""...});...../*$("#slid er2").responsiveSlides({...auto: false,...pager: true,...speed: 500,...maxwidth: 1024..});... .$('.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\2WF3MMUU\html5shiv.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):	2636
Entropy (8bit):	5.2493033126910955
Encrypted:	false
SSDEEP:	48:UlwT6nCmcaC5FluvMabRIvR1cFgXa9VxL0jrLxXxuJkEzixkXuS:zT0CRa0F9aIlkFgmbK0dixsuS
MD5:	3044234175AC91F49B03FF999C592B85
SHA1:	BB51A5F6C394989BB06E4171179354C6D05EC8F8
SHA-256:	E0EAC80838C161F29E7C46D54FBC044D12CD164BAAE13255E562C6BE3AA91809
SHA-512:	C5ACBAD216EA747ECDE56F9305C3F1BA979B554EE8FF61B98FE70390B352D8249BCC9DBEBDBCE504FE8FA85DD91D34C50DF01615F98ECFDDFF37C609E589 18C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/js/html5shiv.min.js
Preview:	/**.* @preserve HTML5 Shiv 3.7.2 | @afarkas @jdalton @jon_neal @rem | MIT/GPL2 Licensed.*/.!function(a,b){function c(a,b){var c=a.createElement("p"),d=a.getElem entsByTagName("head")[0]||a.documentElement;return c.innerHTML="x<style>"+b+"</style>",d.insertBefore(c.lastChild,d.firstChild)}function d(){var a=t.elements;re turn"string"==typeof a?a.split(" "):a}function e(a,b){var c=t.elements;"string"!=typeof c&&(c=c.join(" ")),"string"!=typeof a&&(a=a.join(" ")),t.elements=c+" "+a,j(b)}function f(a) {var b=s[a[q]];return b||(b={},r++,a[q]=r,s[r]=b),b}function g(a,c,d){if(c||(c=b),l)return c.createElement(a);d||(d=f(c));var e;return e=d.cache[a]?d.cache[a].cloneNode() :p.test(a)?(d.cache[a]=d.createElem(a)).cloneNode():d.createElem(a),!e.canHaveChildren||o.test(a)||e.tagUrn?e:d.frag.appendChild(e)}function h(a,c){if(a||(a=b),l)return a .createDocumentFragment();c=c||f(a);for(var e=c.frag.cloneNode(),g=0,h=d(),i=h.length;i>g;g++)e.createElement(h[g]);return e}function i(a,b){b.cache||(b.cache={

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	12105

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\httpErrorPagesScripts[1]	
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/httpErrorPagesScripts.js
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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\2WF3MMUU\index[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	6878
Entropy (8bit):	5.169650928401802
Encrypted:	false
SSDEEP:	192:za3DPwK7mAkMLrvnzHvBQH0J9RljWw72TED:u3DPw7CvnzHvBQH0J9R5f72Te
MD5:	40DFDC8155D26F9A8AF7BBC7F70349F6
SHA1:	5045610AFCBB047613287EB9745E11726430ABB1
SHA-256:	39175489281971 50ADDC288F30AF88F2AB034AB333AEA4B5D99AE97465563720
SHA-512:	6CC86CA3393901BB99E64ADF1662AE72177D84986AF55BFAFD647A90271B8A7FB2331E9F9D450EBD8A3435CC5D1BB69EB18AB05857393541CE305E888A91228
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ws.sharethis.com/secure/index.html
Preview:	<!DOCTYPE html>.<html lang="en">.<head>..<meta http-equiv="Content-Type" content="text/html; charset=utf-8">..<meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no">..<meta name="description" content="">..<title>ShareThis</title>..<script type="text/javascript">...var glo_initFrag=document.location.hash;..</script>.. <link href="font-awesome/css/font-awesome.min.css" rel="stylesheet" media="screen">..<link href="css/styles.css" rel="stylesheet" media="screen"> -->.</head>.<body>. .. ..<a id="btnShareAgain" class="backToDefault" href="javascript:void(0);"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\interiorSlide[1].jpg	
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$..i.vf1.CV.6.af.....h..z/..O^.GZ.v.?.....U.9..a3BE.s..:#-....._./W.....2gvl.I.I.$.S.A[..)...^B.E.0....#.\.6..)....U.s\o7..O/;..*.W..."PC.T.r...O_..N.....X.fd.]"d.,..z.).....D .d.....XE.!.WB$...?....(is._7....K6..-.....LH..s}.oD.^...<.(.5FI.ft.t.<.../gS..4.....5.JtI0.f.ad.....(....o;2.fm.4(Q....~o..k`.....Q..F.....V....s..3;"N....<.""".....[.Hi.30..f....]....'..y. j4...3.Q.J.Z...k[...K%..Z=...%..?...$..).2gL.....RKb...f.....H...&B....~.j.L.\.....J.nv~}..T.T|+.W).]...W.a..n...9.3..L.3:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\jquery-ui-1.10.3.custom.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	228138
Entropy (8bit):	5.1531023102456786
Encrypted:	false
SSDEEP:	3072:7THQDWyMcDtOFOFKjax4Vja+03+TpB0FQodXO67uWm21q:7rcW1COcIOKa+NTpCFQyw
MD5:	AF62D334C0F845DBE7ED3E8BD8830B4F
SHA1:	009DFBCF27663D0C72813C4B6E762E434B9639DB
SHA-256:	BD6845710F8B65925FDB00A1E448F0F7F8AC194CFFD391946EB4EE561787EAC4
SHA-512:	F9F49C8312A670D58B7D37FC94EB98905A5C4C85A0C5D534CF89E30263DA6CB8B64E9D6222ADC52CC88FA44D8940956CA762D4A25E13C47316C9FF4797E3E5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/js/jquery-ui-1.10.3.custom.min.js
Preview:	/*! jQuery UI - v1.10.3 - 2013-10-20.* http://jqueryui.com.* Includes: jquery.ui.core.js, jquery.ui.widget.js, jquery.ui.mouse.js, jquery.ui.position.js, jquery.ui.draggable.js, jq uery.ui.droppable.js, jquery.ui.resizable.js, jquery.ui.selectable.js, jquery.ui.sortable.js, jquery.ui.accordion.js, jquery.ui.autocomplete.js, jquery.ui.button.js, jquery.ui.date picker.js, jquery.ui.dialog.js, jquery.ui.menu.js, jquery.ui.progressbar.js, jquery.ui.slider.js, jquery.ui.spinner.js, jquery.ui.tabs.js, jquery.ui.tooltip.js, jquery.ui.effect.js, jquery.ui.effect-blind.js, jquery.ui.effect-bounce.js, jquery.ui.effect-clip.js, jquery.ui.effect-drop.js, jquery.ui.effect-explode.js, jquery.ui.effect-fade.js, jquery.ui.effect-fold.js, jquery.ui.effect-highlight.js, jquery.ui.effect-pulsate.js, jquery.ui.effect-scale.js, jquery.ui.effect-shake.js, jquery.ui.effect-slide.js, jquery.ui.effect-transfer.js.* Copyright 2013 jQuery Foundation and other contributors; Licensed MIT */..(function(e,t){function

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\jquery.anoslide[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	9680
Entropy (8bit):	4.700844420632857
Encrypted:	false
SSDEEP:	192:hAzmngPQJ4klY1j7B1dOC+JgSPNrteZQa5+At64bezMSdJi9lt9hwLsJLeuw8jow:Czm74kMcWSPmR5+6imlKQSbdLk4O
MD5:	E4E5FCBD57905A07F20F8F39C75339A7
SHA1:	FAE894145C9E42297135D7AE871B0CE34CBD931B
SHA-256:	120606EA59C0BBAC9DBCEAAB9609347DBB6E9D71B4B09C84C104BE488720B5E5
SHA-512:	92A8BDA23D4E01206875E5F715BC233E74E110ED02F4E6E6013AD4B2028FFE06C1322D6CE86BE09D2A0069A156D95891F07EDBCA716487B1BE2BF45BF9625F1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/js/anoslide/js/jquery.anoslide.js
Preview:	/**.* anoSlide - Ultra lightweight responsive slider.* .* @version 1.0.* @author Angel Kostadinov.* @copyright Anowave.*/.(function () .{. var anoSlide = function(element, options) . {. .this.slides = [];. .this.progress = false;. .this.current = 0;. this.element = $(element);. this.options = $.extend(. {....items: .. .5,....s peed: .. .1000,....auto:.. .0,....autoStop: ..true,....next: .. .'',....prev: .. .'',....responsiveAt: .480,....delay: ...0,....lazy: ...false,....onConstruct: .function(instance){},....onStart: . .function(ui){},....onEnd: ...function(ui){}. }, options);. . /* Reference */. this.defaults = . {. .items: this.options.items,. .auto: 0. }. . /* Preloader */. this.preloader = new anoPreload();. . this.timeout = null;. };. . anoSlide.prototype = . {. construct: function(). .{. ..this. defaults.auto = this.options.a

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\jquery.bxslider.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	19123
Entropy (8bit):	5.029578610040108

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\jquery.bxslider.min[1].js	
Encrypted:	false
SSDEEP:	192:jRbG4SN83BRKmfL+clFBPDhjfH2TgiD3vARMWvdO34AgEJrv/JlSOEQQA05rzIHQ:FVO8WjkVrXolS3nXIHHbHruwm
MD5:	B860635957ED570DEB2CF994BD9A4913
SHA1:	F436DB7BCCCD473AAC7A1E48F8B17157516C8CBD
SHA-256:	CD70BB1D6BAA27C8BEF116F4EBC43CEC49BE7A06AF1E59635870A651376918ED
SHA-512:	589518AA8AF347802C36DFCBFE9EFB76FBCD5579B00F174995B4F9BC756083908DB334B9E41201BE443652FDA4F69114A008CFB4D6887F4798859DB96C871E81
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/js/bxslider/jquery.bxslider.min.js
Preview:	/**. * BxSlider v4.1.1 - Fully loaded, responsive content slider. * http://bxslider.com. *. * Copyright 2013, Steven Wanderski - http://stevenwanderski.com - http://bxcreative.com. * Written while drinking Belgian ales and listening to jazz. *. * Released under the MIT license - http://opensource.org/licenses/MIT. */!function(t){var e={},s={mode:"horizontal",slideSelector:"",infiniteLoop:!0,hideControlOnEnd:!1,speed:500,easing:null,slideMargin:0,startSlide:0,randomStart:!1,captions:!1,ticker:!1,tickerHover:!1,adaptiveHeight:!1,adaptiveHeightSpeed:500,video:!1,useCSS:!0,preloadImages:"visible",responsive:!0,touchEnabled:!0,swipeThreshold:50,oneToOneTouch:!0,preventDefaultSwipeX:!0,preventDefaultSwipeY:!1,pager:!0,pagerType:"full",pagerShortSeparator:" / ",pagerSelector:null,buildPager:null,pagerCustom:null,controls:!0,nextText:"Next",prevText:"Prev",nextSelector:null,prevSelector:null,autoControls:!1,startText:"Start",stopText:"Stop",autoControlsCombine:!1,autoControlsSelector:null,aut

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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
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 #ccc;..border: solid #fff 5px;..left: -5px;..background: #fff;.}...bx-wrapper .bx-pager,..bx-wrapper .bx-controls-auto {..position: absolute;..bottom: -30px;..width: 100%;.}../* LOADER */...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\2WF3MMUU\jquery.roundabout-shapes[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	5467
Entropy (8bit):	5.260093106235612
Encrypted:	false
SSDEEP:	96:34LQ66rYJ1rYJjylKo33U3DN2jDBhiX3Qx4GQmuOFkoxWAo8Re9AEaZtzqx:34p6rs1rs+lKo33U3h6+mucQ
MD5:	777456C4C95A806F99151AF1DB76C5CE
SHA1:	A926D2333EAC5C79FFC84EB60148E29A586A1548
SHA-256:	4F82A632DF3428A68271F71328A8158ABF80623B55E3C3E25B757A865904AEBA
SHA-512:	8CA1498259F3A2DA3D043707094F438C09C0295446005AC177BD25DDC4ED9A88C851ADFDE6211DB83CF80656F2FB6E8AE9F87B38165FF7504FC875A03740E8A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/js/jquery.roundabout-shapes.js
Preview:	/**. * jQuery Roundabout Shapes v2. * http://fredhq.com/projects/roundabout-shapes/. * . * Provides additional paths along which items can move for the. * jQuery Roundabout plugin (v1.0+).. *. * Terms of Use // jQuery Roundabout Shapes. *. * Open source under the BSD license. *. * Copyright (c) 2009-2011, Fred LeBlanc. * All rights reserved.. * . * Redistribution and use in source and binary forms, with or without . * modification, are permitted provided that the following conditions are met:. * . * - Redistributions 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 the author nor the names of its contributors . * may be used to endorse or promote products de

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\jquery.roundabout[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	36994
Entropy (8bit):	5.080061191914662

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\jquery.roundabout[1].js	
Encrypted:	false
SSDEEP:	384:1yrstrsUIoV6iDWlnxAkldUQIjqn57n8JsBdheZJBL/IKnl9jJ98T1ofpl2OXU2U:IuFB6iDo50nZpvRhVrVr8PhD9
MD5:	997A87A67081F7CE0FDFEC67D538B913
SHA1:	3C14E2DB2DE0285645D5091C7A0D7ABBF34B3666
SHA-256:	21E317C73E8BD14EC814985ADB885D2A3C45A1F49A4877212EC8986AFDE9D896
SHA-512:	C5C64009244BCEBD9A536E4FA48579BD658E377F7F70E8CFF04EB71ED4EE3BF6454ADA56C006018C8EF6FF557572C0BBF628B45069DBE0DA8E6BDC31071BA209
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/js/jquery.roundabout.js
Preview:	/**. * jQuery Roundabout - v2.4.2. * http://fredhq.com/projects/roundabout. *. * Moves list-items of enabled ordered and unordered lists long. * a chosen path. Includes the default "lazySusan" path, that. * moves items long a spinning turntable.. *. * Terms of Use // jQuery Roundabout. *. * Open source under the BSD license. *. * Copyright (c) 2011-2012, Fred LeBlanc. * All rights reserved.. *. * Redistribution and use in source and binary forms, with or without. * modification, are permitted provided that the following conditions are met:. *. * - Redistributions 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 the author nor the names of its contributors. * ma

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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. * scrollable/scrollable.js. * scrollable/scrollable.autoscroll.js. * scrollable/scrollable.navigator.js. * tabs/tabs.js. * tabs/tabs.slideshow.js. * toolbox/toolbox.expose.js. * toolbox/toolbox.flashembed.js. * toolbox/toolbox.history.js. * toolbox/toolbox.mousewheel.js. * tooltip/tooltip.js. * tooltip/tooltip.dynamic.js. * tooltip/tooltip.slide.js. * validator/validator.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\2WF3MMUU\jquery.touchSwipe[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	67916
Entropy (8bit):	5.011339110414218
Encrypted:	false
SSDEEP:	768:gYbTWVZGKATmteoktRSaFGm9dfOjLV6Qj0qvMuILcwNHpq3gpe6FJ8fyy6jsLiLI:zbTWVZFzaFtLSvMxcw5pqCd+A7clP
MD5:	107E03F585C31E72296CF7DB91A7E125
SHA1:	2E1E16C224F1B4573B6D779D8AE6C74A80215222
SHA-256:	C874C9A3E2757790076E34BD49DB931EB7484E6347877192F649429CF3F6E3E6
SHA-512:	3D2C6155734CE7487DAEA2A3212EB0D588311075F85C70C3F43C67532E29CDAB800062FFB6B26336C3FC75E1DF2166414A7FAF1329725055CCB66584B010DC8E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/js/jquery.touchSwipe.js
Preview:	/*.* @fileOverview TouchSwipe - jQuery Plugin.* @version 1.6.5.*.* @author Matt Bryson http://www.github.com/mattbryson.* @see https://github.com/mattbryson/TouchSwipe-Jquery-Plugin.* @see http://labs.skinkers.com/touchSwipe/.* @see http://plugins.jquery.com/project/touchSwipe.*.* Copyright (c) 2010 Matt Bryson.* Dual licensed under the MIT or GPL Version 2 licenses..*.*.* Changelog.* $Date: 2010-12-12 (Wed, 12 Dec 2010) $.* $version: 1.0.0.* $version: 1.0.1 - removed multibyte comments.*.* $Date: 2011-21-02 (Mon, 21 Feb 2011) $.* $version: 1.1.0 .- added allowPageScroll property to allow swiping and scrolling of page.*.....- changed handler signatures so one handler can be used for multiple events.* $Date: 2011-23-02 (Wed, 23 Feb 2011) $.* $version: 1.2.0 .- added click handler. This is fired if the user simply clicks and does not swipe. The event object and click target are passed to handler..*.....- If you use the http://code.google.com/p/jquery-ui-for-ipad-and-iphone/ plugin, you c

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\jquery.ui.touch-punch[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	4593

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\jquery.ui.touch-punch[1].js	
Entropy (8bit):	4.39918211975265
Encrypted:	false
SSDEEP:	96:d5v41MVkxyM9SLUT7Kf+9/aclLxaal9r6IH1p3ch:dWyAJnt9n7HY
MD5:	864B0244C7C2A73ACCEB9C67EF02D582
SHA1:	F0ADCC6A8F16E803E04F82BDF3A1398CB4181CCD
SHA-256:	A069802ACB5265D29441748FECE63C9D89FBA32E6E2239550E0864E07AAFF9A8
SHA-512:	4611E89C96BAD83A3CBADAC1BD5BA879465F46BB79B3DF1E387462C08427774BD2FEC7DC1A967C0950DE784F51566BED8D79B6B5CA9F7B7EB3446C70188F28 9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/js/jquery.ui.touch-punch.js
Preview:	/*!. * jQuery UI Touch Punch 0.2.2. *. * Copyright 2011, Dave Furfero. * Dual licensed under the MIT or GPL Version 2 licenses.. *. * Depends:. * jquery.ui.widget.js. * jquery.ui.mouse.js. */.(function ($) {.. // Detect touch support. $.support.touch = 'ontouchend' in document;.. // Ignore browsers without touch support. if (!$.support.touch) {. return;. }.. var mouseProto = $.ui.mouse.prototype,. _mouseInit = mouseProto._mouseInit,. touchHandled;.. /**. * Simulate a mouse event based on a c orresponding touch event. * @param {Object} event A touch event. * @param {String} simulatedType The corresponding mouse event. */. function simulateMous eEvent (event, simulatedType) {.. // Ignore multi-touch events. if (event.originalEvent.touches.length > 1) {. return;. }.. event.preventDefault();.. var touch = event.originalEvent.changedTouches[0],. simulatedEvent = document.createEvent('MouseEvents');. . // Initialize the simulated

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\jquery.validate.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	21525
Entropy (8bit):	5.286725931997435
Encrypted:	false
SSDEEP:	384:QbprrB+Jx6Gtb7YlHqdS2L7Az548hsljN/tllEny+WIJMXX9N3tCwV/vyxMLgcqH:i+Jx6G2lHqdS2gz54fr/1Eny+WI4axMi
MD5:	592CFB0F0EE44203388E32EA92DA4C31
SHA1:	353CFE17386319E8D0D575AB479021D16F49E452
SHA-256:	5FE55811CAB9115F1733276ABDC3E822047BD84F6AB9611FE64FCCA43261E49F
SHA-512:	9457F2ECA52D935F1E15318420E6453555955AA62241F8A1BC0674C5CE77145BFE3E45259A574BBE98E853C468AC4A2B938CA016474110EB431A7FE5DB05BE59
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/js/jquery.validate.min.js
Preview:	/*! jQuery Validation Plugin - v1.13.0 - 7/1/2014. * http://jqueryvalidation.org/. * Copyright (c) 2014 J.rn Zaefferer; Licensed MIT */.!function(a){"function"==typeof de fine&&define.amd?define(["jquery"],a):a(jQuery)}(function(a){a.extend(a.fn,{validate:function(b){if(!this.length)return void(b&&b.debug&&window.console&&console .warn("Nothing selected, can't validate, returning nothing."));var c=a.data(this[0],"validator");return c?c:(this.attr("novalidate","novalidate"),c=new a.validator(b,this[0]),a.dat a(this[0],"validator",c),c.settings.onsubmit&&(this.validateDelegate(":submit","click",function(b){c.settings.submitHandler&&(c.submitButton=b.target),a(b.target).hasClas s("cancel")&&(c.cancelSubmit=!0),void 0!==a(b.target).attr("formnovalidate")&&(c.cancelSubmit=!0)}),this.submit(function(b){function d(){var d;return c.settings.submitHan dler?(c.submitButton&&(d=a("<input type='hidden'/>").attr("name",c.submitButton.name).val(a(c.submitButton).val()).appendTo(c.currentForm)),c.setting

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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\2WF3MMUU\login[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\login[1].htm	
Size (bytes):	266990
Entropy (8bit):	5.485973380252403
Encrypted:	false
SSDEEP:	1536:xUCAmqyt0kTBuSnAAiAgkCRwWwU2UL3meDSCWN4ShAwT96wnwr+FlifRPgx9Hlw8:x4T1wRfwRPgjHlwvNWdr/bj51p
MD5:	57077B1ACAFA3112DC79BD8F633915E3
SHA1:	39CFAE81A4D1E105D690F1E7E0E69B6CCCCBEE49
SHA-256:	DDF09E98582F932F795489D49B621C20391D55FAF27E7BDD260B71174A403218
SHA-512:	2AFE8288AC2A6E5F3BD52560EE09CA91B8929B013F044BDAA55D9E8BB84ED57498E01CC5AFA3BBDFA68ECED60D56401F4DA6D3936744CEE285379E4AD179DF52
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>.<html lang="de" id="facebook" class="no_js">.<head><meta charset="utf-8" /><meta name="referrer" content="default" id="meta_referrer" /><script nonce="RzU0PsJ0">window._cstart=+new Date();</script><script nonce="RzU0PsJ0">function envFlush(a){function b(b){for(var c in a)b[c]=a[c]}window.requireLazy?window.requireLazy(["Env"],b):(window.Env=window.Env||{},b(window.Env))}envFlush({"ajaxpipe_token":"AXgLvOEuyhiM5K_y-uI","timeslice_heartbeat_config":{"pollIntervalMs":33,"idleGapThresholdMs":60,"ignoredTimesliceNames":{"requestAnimationFrame":true,"Event listenHandler mousemove":true,"Event listenHandler mouseover":true,"Event listenHandler mouseout":true,"Event listenHandler scroll":true},"isHeartbeatEnabled":true,"isArtilleryOn":false},"shouldLogCounters":true,"timeslice_categories":{"react_render":true,"reflow":true},"sample_continuation_stacktraces":true,"dom_mutation_flag":true,"gk_requirelazy_mem":true,"stack_trace_limit":30,"timesliceBufferSize":5000,"show_invariant_

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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\2WF3MMUU\modernizr[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):	10242
Entropy (8bit):	5.319154820428289
Encrypted:	false
SSDEEP:	192:HaElXZBK8nnenwzUDazKQob1dHYPeIny6Y7LDDhWwpy8b7z:dXnK8nR0azKQoZRY5y6KHh1pz
MD5:	0F3C2B2D45C893A38E56672F3648C2C1
SHA1:	35A7E863692649AFFC7BCD6D272B2EE6937F4A41
SHA-256:	EF1485FC61C4F1E01E1E92A06F95DFBABD52C7364BCF1F2D22B01A82705271C4
SHA-512:	B31BDA802F28B09F0C483648DC4FE50FBDA400EDB16D0AA245810E38DDF6798023CED050303E50D0D22A25A882D2DC38AF2AF52B9136047EE874D6A98FC3492
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/js/modernizr.js
Preview:	/* Modernizr 2.8.3 (Custom Build) | MIT & BSD. * Build: http://modernizr.com/download/#-fontface-backgroundsize-boxshadow-opacity-cssanimations-cssgradients-input-shiv-mq-cssclasses-teststyles-testprop-testallprops-prefixes-domprefixes-load. */.;window.Modernizr=function(a,b,c){function A(a){j.cssText=a}function B(a,b){return A(m.join(a+";")+(b||"")))}function C(a,b){return typeof a===b}function D(a,b){return!!~(""+a).indexOf(b)}function E(a,b){for(var d in a){var e=a[d];if(!D(e,"-")&&j[e]!==c)return b=="pfx"?e:!0}return!1}function F(a,b,d){for(var e in a){var f=b[a[e]];if(f!==c)return d===!1?a[e]:C(f,"function")?f.bind(d||b):f}return!1}function G(a,b,c){var d=a.charAt(0).toUpperCase()+a.slice(1),e=(a+" "+o.join(d+" ")+d).split(" ");return C(b,"string")||C(b,"undefined")?E(e,b):(e=(a+" "+p.join(d+" ")+d).split(" "),F(e,b,c))}function H(){e.input=function(c){for(var d=0,e=c.length;d<e;d++)s[c[d]]=c[d]in k;return s.list&&(s.list=!!b.createElement("datalist")&&!!a.HTMLDataListElement),s}("

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\owl.carousel.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\owl.carousel.min[1].js	
Category:	downloaded
Size (bytes):	44342
Entropy (8bit):	5.0793850768725
Encrypted:	false
SSDEEP:	768:UCI7dmuMFAAJG4dlQKNORpnXGAtep2lcwJeL+wr2RSGc7UuHjRUQuFBt33:PITMFC4dbMVRSGcgRDV
MD5:	F416F9031FEF25AE25BA9756E3EB6978
SHA1:	E2A600E433DF72B4CFDE93D7880E3114917A3CBE
SHA-256:	A53C43F834B32309B084EA9314DF8307E9C78CEE2202C6E07F216AE4AE5B704D
SHA-512:	6CFB3B01EEA956F84E4A221CC940A547BFEAD8E02C462A2FC38BC0917FB325BC374A101E7AA7B3AB9D11208708511ABB39ADB4AD6DA7DAAF9FC9704D714F65AF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/js/owl.carousel.min.js
Preview:	/**. * Owl Carousel v2.3.4. * Copyright 2013-2018 David Deutsch. * Licensed under: SEE LICENSE IN https://github.com/OwlCarousel2/OwlCarousel2/blob/master/LICENSE. */.!function(a,b,c,d){function e(b,c){this.settings=null,this.options=a.extend({},e.Defaults,c),this.$element=a(b),this._handlers={},this._plugins={},this._supress={},this._current=null,this._speed=null,this._coordinates=[],this._breakpoint=null,this._width=null,this._items=[],this._clones=[],this._mergers=[],this._widths=[],this._invalidated={},this._pipe=[],this._drag={time:null,target:null,pointer:null,stage:{start:null,current:null},direction:null},this._states={current:{},tags:{initializing:["busy"],animating:["busy"],dragging:["interacting"]}},a.each(["onResize","onThrottledResize"],a.proxy(function(b,c){this._handlers[c]=a.proxy(this[c],this)}),this)),a.each(e.Plugins,a.proxy(function(a,b){this._plugins[a.charAt(0).toLowerCase()+a.slice(1)]=new b(this)},this)),a.each(e.Workers,a.proxy(function(b,c){this._pipe.push({fil

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\owl.carousel2.thumbs[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text
Category:	downloaded
Size (bytes):	6855
Entropy (8bit):	4.463115408337006
Encrypted:	false
SSDEEP:	192:eDNpWOjgUsmhIGwqh65kxRwQfu1IP6zyN3yJfZQVXEZ7IawR:eDNtR5PouEZZQZEZY
MD5:	AFD7554AE86A9D6D631B4854607296D6
SHA1:	D1A7763ACD99CE618A569A030BC68733A4B4132C
SHA-256:	35417F4CE9F951C929955D945DF2826047457F19CC982B9E30D6703F114DEC15
SHA-512:	4C0C8927C6F48AC7BE1B0257A9FCB93231EA3A18B4E0ACEBF3C76C0C0A7F2D19E8036005D9520232ADD83C6439CE92926B45CDDFCBC56126B6399DF497D8DB7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/js/owl.carousel2.thumbs.js
Preview:	/**. * Thumbs Plugin. * @version 2.0.0. * @author Gijs Rog... * @license The MIT License (MIT). */.(function ($, window, document, undefined) {. 'use strict';.. /**. * Creates the thumbs plugin.. * @class The thumbs Plugin. * @param {Owl} carousel - The Owl Carousel. */. var Thumbs = function (carousel) {... /**. * Reference to the core.. * @protected. * @type {Owl}. */. this.owl = carousel;... /**. * All DOM elements for thumbnails. * @protected. * @type {Object}. */. this._thumbcontent = [];... /**. * Instance identiefier. * @type {number}. * @private. */. this._identifier = 0;... /**. * Return current item regardless of clones. * @protected. * @type {Object}. */. this.owl_currentitem = this.owl.options.startPosition;... /**. * The carousel element.. * @

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\pe03MImSLYBIv1o4X1M8cc8GBs5tU1c[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 21068, version 1.1
Category:	downloaded
Size (bytes):	21068
Entropy (8bit):	7.9765727259753465
Encrypted:	false
SSDEEP:	384:mkvr7QjFdsSnl6bfXqLqxF/lYQ8uCV8VIor+BtzRB7HDj+4QdagiUcm4:mkvYcSk7aLqXNYHuY8GBH2tiUcx
MD5:	1AA5D63ECA4940FBBB5181895E9BC008
SHA1:	EE9B61AA68DA9CF7C281B178D2E2FA80E9C9DC2F
SHA-256:	A84F128A88D8D1B3987D2B7B361C60185A6BEE0742F3D6006E207C03DB420853
SHA-512:	3219E98DA976AFEC16FB8C6B66E96C893FAEE1F723D866A7E7C178186CF5498164B12582D9AA75C5521104C87324563FF7DFFD822A412A0131F1D9881046D8E5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/nunitosans/v6/pe03MImSLYBIv1o4X1M8cc8GBs5tU1c.woff
Preview:	wOFF.....RL.....T.....GDEF.....1...4.h..GPOS.....ukz.GSUB....._OS/2...|...P...`k..Pcmap.....g.Ejcvt .....H....:...fpgm.....vd.zgasp.....glyf.....3...]..i.]head..I....6...6...dhhea..I.... ...$...Hhmtx..J.....loca..K.....#..=maxp..N.... ... .a..name..N,.....%.A.post..O.....f.1..prep..Q.....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\2WF3MMUU\pe0qMImSLYBIv1o4X1M8cce9I90[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20976, version 1.1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\pe0qMImSLYBIv1o4X1M8cce9I90[1].woff	
Category:	downloaded
Size (bytes):	20976
Entropy (8bit):	7.976190997350181
Encrypted:	false
SSDEEP:	384:f9eL01J4w3NSnl6aefcHxfgZ1di7/k3RmfThNUwDQzwH6aMU7T358KT1bFm4:fYL01S4SkLc1gZ1d0/khgThGoEwWU7uC
MD5:	8ACE450709844437A579D4F4C7C37B42
SHA1:	F741927C8E42895E037FEF51466549EEAA098992
SHA-256:	DA4751EC73E5D238811EE5534F1D087A57DBD5E6F018FBC3F7FD2DADDCE4D9F2
SHA-512:	2EB2CD3B3D1B09A29277258C19335B0EFFFD50C53FF25C4E57427682208FF2AD5CA2821A104547686134E454D05792CC8CD194CD065B4341A35240BF89BE6D6E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/nunitosans/v6/pe0qMImSLYBIv1o4X1M8cce9I90.woff
Preview:	wOFF.....Q.....GDEF.....1...4.h..GPOS.....uXz.GSUB....._OS/2.....O...`i.`cmap.....g.Ejcvt .....H...:...fpgm.....vd.zgasp.....glyf....3g..].....head..IX...6...6...ihhea..I.... ...$...9hmtx..I..... .loca..K.....$maxp..M.... ... .[..name..M.....'.E.post..N.....f.1..prep..QX.....96Nox.c`d``.a..&.6.....?..d....Q@2.!.H.3.00..%.....x.....I.E_U5M.P...^ffffff<F...N.....I.1...Q..WI.j.._YU.Y....3..(.'...{...R...{og.....,\w..T}..1.Qr..].j.xg.j..T...J...k..ae...S.....R.%.Rakj...j.E.....~r..z..\XG....Z..J.Jj.u.k...a9...Hk...Z..| LR.....1a".....J.|..OP..Z-!K...v.e.$kl.P=..S....a...._....amx_.&.....<...<...Op..@N.....)..~....eH[.E..[.j.<.J.-....3.@..H....i<C...{...9B.#...{..X..+.....A".D....i..>5K.;9GW.....k.".v...[yX.3..q.d!..../..BD.^Y{.|<..8..x..x.Wx]....8>e2.f...p.{.WRo{..q...0..r.C...../..;zk..x5...F..)h...mxGm..x.....W4..5..5r..K..I.#[.=N.f.....0..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\placeholders.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	4267
Entropy (8bit):	5.211779736814933
Encrypted:	false
SSDEEP:	96:J0nkQGgIb0lqnj6t8cROCqHeip2UrEobRQ/NplhuC:G31uDcbuOob6/XIIC
MD5:	ABF7570FC0E1B9EF43CF2D39CE788E9C
SHA1:	4F17C407AA46B681EAC3E53C5DB84D512DD8A1F0
SHA-256:	5C4E56D943D5E3887BA492E731027D474A904AEFB14B84F308B69B6EB6E3CA87
SHA-512:	EB5BA963E654DB90FBE5E852EF0D184CF5F5907E8A2C26B3BC11A95FE2D5F1C69E454B24D9525507DCA19F667C065DFE3B6CD494F83C3E2330C08E294E4840D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/js/placeholders.min.js
Preview:	/* Placeholders.js v3.0.2 */.(function(t){"use strict";function e(t,e,r){return t.addEventListener?t.addEventListener(e,r,!1):t.attachEvent?t.attachEvent("on"+e,r):void 0}function r(t,e){var r,n;for(r=0,n=t.length;n>r;r++)if(t[r]===e)return!0;return!1}function n(t,e){var r;t.createTextRange?(r=t.createTextRange(),r.move("character",e),r.select()):t.selectionStart&&(t.focus(),t.setSelectionRange(e,e))}function a(t,e){try{return t.type=e,!0}catch(r){return!1}}t.Placeholders={Utils:{addEventListener:e,inArray:r,moveCaret:n,changeType:a}}})(this),function(t){"use strict";function e(){}function r(){try{return document.activeElement}catch(t){}}function n(t,e){var r,n,a=!!e&&t.value!==e,u=t.value===t.getAttribute(V);return(a||u)&&"true"===t.getAttribute(D)?(t.removeAttribute(D),t.value=t.value.replace(t.getAttribute(V),""),t.className=t.className.replace(R,""),n=t.getAttribute(F),parseInt(n,10)>=0&&(t.setAttribute("maxLength",n),t.removeAttribute(F)),r=t.getAttribute(P),r&&(t.type=r),!0):!1}f

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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\2WF3MMUU\responsiveslides.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\responsiveslides.min[1].js	
Size (bytes):	3397
Entropy (8bit):	5.317657582266066
Encrypted:	false
SSDEEP:	96:EW1DELtmm0G2gML3qfYcq/roHoXTk3vfsY4fq:EW9w47G25LnMHojWkY4fq
MD5:	04F1B2AC39E762CD516CB359755C8CC6
SHA1:	D649FBD823DB40EB881B9810310698CACED0EA58
SHA-256:	1F306DB5A9C29477ACDD6B78D57734F0AA7936A1FA9B9BA8BD36204BA12AAF40
SHA-512:	E7088D20DFD294EC3E404ADEC572697F62EDFECBF0792E6322BDD63D9DFB20774630EC61EF66BF79BBA833F3D6B6939F95BDEA99C08FBFF6F82CAE9E2CBE2CA9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/js/responsiveslides.min.js
Preview:	/*! http://responsiveslides.com v1.54 by @viljamis */.(function(c,l,B){c.fn.responsiveSlides=function(l){var a=c.extend({auto:!0,speed:500,timeout:4E3,pager:!1,nav:!1,random:!1,pause:!1,pauseControls:!0,prevText:"Previous",nextText:"Next",maxwidth:"",navContainer:"",manualControls:"",namespace:"rslides",before:c.noop,after:c.noop},l);return this.each(function(){B++;var f=c(this),s,r,t,m,p,q,n=0,e=f.children(),C=e.size(),h=parseFloat(a.speed),D=parseFloat(a.timeout),u=parseFloat(a.maxwidth),g=a.namespace,d=g+B,E=g+"_nav "+d+"_nav",v=g+"_here",j=d+"_on",.w=d+"_s",k=c("<ul class='"+g+"_tabs "+d+"_tabs' />"),x={"float":"left",position:"relative",opacity:1,zIndex:2},y={"float":"none",position:"absolute",opacity:0,zIndex:1},F=function(){var b=(document.body||document.documentElement).style,a="transition";if("string"===typeof b[a])return!0;s=["Moz","Webkit","Khtml","O","ms"];var a=a.charAt(0).toUpperCase()+a.substr(1),c;for(c=0;c<s.length;c++)if("string"===typeof b[s[c]+a])return!0;return!1}(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\roadmap[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	13621
Entropy (8bit):	5.191830036944621
Encrypted:	false
SSDEEP:	384:i3TLtPt1rPPkBIkaL62JKYOK833y11dO5:in5VDO7
MD5:	C7116C792E31CAF6C0B1B00AB67D683F
SHA1:	A6389705A05C9080DE39623622AACBDFFB56CB86
SHA-256:	BA782A3240E1F8618B4A2BA8D10EA88E968DD7E108457E047C7A0AFD8824E8DE
SHA-512:	663C57903E53C0FBCC0A35E653E694A6B4FA891E4433393653EDEA5ED6302FCE906679076E07EA95866FCEC4A36E5BBF56D879DC4B56ABBE126D3838FABB064
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/js/roadmap.js
Preview:	$(document).ready(function() {....var whichRoad =1;..var totalRoads = $('#mainRoad').attr('rel');..var.dotPositions;..var selectedSlide;..var theDot;..var howFar;..var moving = false;..var mobileView = false;.....$('#roadLeft').hide();..$('#roadRight').hide();..if(totalRoads>1) {...$('#roadRight').show();..}..$('.roadHolder'+whichRoad+ ' li').show();....if($(window).width()>599) {...loadMarkers();...loadCarousel();...mobileView = false;.....}else {...mobileView = true;..}.....function loadMarkers() {.../console.log(whichRoad);...dotPositions = [];.....$('.selectedSubSlide').show();...$('.roadHolder'+whichRoad+' #theMarkers li:visible').each(function() {....dotPositions.push($(this).position().left);...});...theDot= 'center';.....if($('.productline-landing').length > 0)...{....theDot = $('.roadHolder'+whichRoad+' #theMarkers li:first-child');....howFar = theDot.position().left +16;....movePin();...}.....}....$("#thePin").draggable(...{ scroll: false, axis: "x",handle:'#pinHandle',

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\scratchSlide[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):	68863
Entropy (8bit):	7.965829160353835
Encrypted:	false
SSDEEP:	1536:HKQHzzAqax7vNn+w00hmHKMR+JFAkMYQTjqugbL5fKTmmH7gYfAi0Cek:fHzzTg7vV/Uz+JOkMvqX86kPZ0Cek
MD5:	E405F61640C7478F809F6FE1A5E07012
SHA1:	BE3735F523F0924E51FEE88809EE27FB5ACED48A
SHA-256:	443ED57EE8F8F5EC275FBB82CE1B76D3022B77DD0C45B05BD0A03CC462FFAF45
SHA-512:	E6F6DB6CC878DB9EDCD88A8B6443D79C3CEFEC982333BDF7A7C26A7B5E2C51A7051734A5B2FEB0F99CF03AF2EF711F29C306B038C11C38202D0E38740EB61BCE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/img/banners/scratchSlide.jpg
Preview:	......JFIF.....xY.....?.....p..~.....o.[....K.. .....1]>.....<<.....g....~s..1.).M.$P..I...[-.UU....j....\|..X.Y}..}....o.....x?Y..S.~...<.....\.....qW...y.7..^..}...Y.....m..H.!H.w%.YQa.J]^.k.3M....>..W....r..{..sr}?....~....9....DWW..... ...>.....O.....b=/K..m.m$..R.....JK..[._E.;...^.....<.#.x/...o.?7.c...B.~.[.....>...1..... ...%K..zU.?.{.....ct&....R....)..b*...B.}hN.r.m.<...n....x..w.....G.(.n.....<.....>|. .e. uU.}..x.9.....bJe).....Z.*..K.....?Z..9.1...<.;?.?1.g..s..>..).k....9..|_.@..M.S..R.).Z1)..*\JT2.....U..m.5.g..fYc8..y.../...../.....<.?..j.!J..9..v<..w.<....M.n..En.JaV..K%(%%J.kw.}.P.z../].R. ....9g.xs...s....x_G...7.....(....aS....J....J..S...iFyBV..2..n.j.mj.....]4.O...e...2.....c...?'.....(.....n\l..cc*.*.u

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\scripts[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\scripts[1].js	
Category:	downloaded
Size (bytes):	14440
Entropy (8bit):	5.061481153400861
Encrypted:	false
SSDEEP:	384:Y0D5w2j16xNN7FUx4fCIuIC+V+oeBKdYYJAscK6VJVw1Iv3S3OVKEkl9UQznC:RlXj16xNN7Cx4fN4+OVJ/v3ZVAC
MD5:	1534F06AA2B1B721A45372F8238E2461
SHA1:	86F7E7B926E1A88209D171B56DADBCCC2C96F578
SHA-256:	B7E17926B30342EDECEE8B3A93029AC51462E2B479277D8E077BA57173EB1900
SHA-512:	4ABCFFE69AA25D2B63654B0FDD2C1978335A851C931D05EAF2A92BD6E0F43A2784343E3D785FF45C262C29C21071DD4C7661B50DA5305EC74F4702F3C6B413C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/plugins/contact-form-7/includes/js/scripts.js?ver=5.1.1
Preview:	(function($) {...'use strict';...if (typeof wpcf7 === 'undefined' || wpcf7 === null) {...return;..}...wpcf7 = $.extend({...cached: 0,...inputs: []..}, wpcf7);...$(function() {...wpcf7.supportHtml5 = (function() {....var features = {};....var input = document.createElement('input');.....features.placeholder = 'placeholder' in input;.....var inputTypes = ['email', 'url', 'tel', 'number', 'range', 'date'];.....$.each(inputTypes, function(index, value) {.....input.setAttribute('type', value);.....features[value] = input.type !== 'text';....});.....return features;...})();....$('div.wpcf7 > form').each(function() {....var $form = $(this);....wpcf7.initForm($form);.....if (wpcf7.cached) {.....wpcf7.refill($form);....}...});..});...wpcf7.getId = function(form) {...return parseInt($('input[name="_wpcf7"]', form).val(), 10);..};...wpcf7.initForm = function(form) {...var $form = $(form);....$form.submit(function(event) {....if (! wpcf7.supportHtml

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\secondaryMenu[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	247
Entropy (8bit):	4.869473532174838
Encrypted:	false
SSDEEP:	6:z8HpULD0yA1B0EgTAFU14QofQK/evfwKqYRA3e:zAMDLA1B9gTAe1Kgnsl3e
MD5:	2B8DC9DE3AA49D37C4F323A716A36BC2
SHA1:	EAE6274FE66D7DCF7EE475E4446A67EC55C566E4
SHA-256:	AC07C1D7D6CFEEEE7C3F2C1235DA8F370F50B8D61ADE254DB6109F5EB2772ED3
SHA-512:	BDC456F82D922C6D141AE1F78238A64C6A6DBE438C16E8B93D45CA0703BCB61C5137BCD81B0AE3AF0B6A2F6F12948A3B9BEB2A6626FC35AFE6B5C1AD7F615E97
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/js/secondaryMenu.js
Preview:	jQuery(document).ready(function() {.....jQuery('#menu-item-418 .theSubNav .menu-item-416 a').hover(.. function() {... .jQuery('#drawerLevel2').toggle();..... console.log('in');.. }, function() {.. console.log('out');.. }..);....});...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\st.a9c2f47cfbd1f141fb724cef861110d7[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	C source, ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	89615
Entropy (8bit):	5.312732016674531
Encrypted:	false
SSDEEP:	1536:JDK2SMLjyaUzqiIlyHIeTIjIxLywpfjSOnppQ5eLqBt/Lf2U07q41s+fBYYtvY:JDK2/ya+IwpMeLqBt/LOU07q41s+fBY9
MD5:	A9C2F47CFBD1F141FB724CEF861110D7
SHA1:	73E0D7BA898301E2B211519C7682BB5EF512F257
SHA-256:	85A0AFC2F45CECEC31D8CCD1498CD8BFE428B3D79018EFB1BF4DA2CB3050B847
SHA-512:	D363BFE99FFFFC6B79C94D1C9F69B3DCDCDA6B84EB87590C4C4368400CAC143D8F6CCCA65AD27796184BF128130FB6631AAA2EBA481C5B0D9B222804E64DDFB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ws.sharethis.com/secure/js/st.a9c2f47cfbd1f141fb724cef861110d7.js
Preview:	var stlib=stlib||{functions:[],functionCount:0,util:{prop:function(b,a){if(a){return a[b]}return function(c){return c[b]}}},dynamicOn:true,setPublisher:function(a){stlib.publisher=a},setProduct:function(a){stlib.product=a},parseQuery:function(d){var e=new Object();if(!d){return e}var a=d.split(/[;&]/);for(var c=0;c<a.length;c++){var g=a[c].split("=");if(!g||g.length!=2){continue}var b=unescape(g[0]);var f=unescape(g[1]);f=f.replace(/\+/g," ");e[b]=f}return e},getQueryParams:function(){var a=document.getElementById("st_insights_js");if(a&&a.src){var c=a.src.replace(/^[^\?]+\??/,"");var b=stlib.parseQuery(c);stlib.setPublisher(b.publisher);stlib.setProduct(b.product)}};stlib.global={hash:stlib.util.prop("hash",document.location).substr(1)};stlib.getQueryParams();stlib.debugOn=false;stlib.debug={count:0,messages:[],debug:function(b,a){if(a&&(typeof console)!="undefined"){console.log(b)}stlib.debug.messages.push(b)},show:function(a){for(message in stlib.debug.messages){if((typeof console)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\tire-paint[1].jpg	
Entropy (8bit):	7.931583888105609
Encrypted:	false
SSDEEP:	192:HW4QZzo6DrxCtYEEkxtv5SdeT9Zv9Xfjav1uM/0YniNAQnopms2k:HWLZzrrstYET/v5ieT5jCggniNG
MD5:	01D80CA5DFBC65C2EE5E30CB919A6465
SHA1:	437EF7B64627B92CCB37EF2E6374CBCDCD6867F0
SHA-256:	F1DCADB1339E6D33042A4934C4BB5CCE1AB9AABFED148898665A2937B6C6DCF8
SHA-512:	BF2E9604B032928A16908B9C3784CC20BFF164AD8A09BC82F2C1B3EA41656AB73E7956DFC478564D47982D7FBAC7EB3FD8271B0B1E94D1C460382B9D3660EDD A
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..$\|...q...~...5.<.7Yl...O.....f._W...+.....Gr.g..]/^.....S4; ..!..e..SD.u...@.-.q.j.<Z...<.m[.''..g}T..g....MS{..T..dZ..`.._''.s&.....%@..*..7..p...../.....\|.[0...K._c.mD.L .R2....U~e.^....MS0..sm{/..E.rax.K...vE....n.....T....<...S.E.....jX...n.]Y.y.....SW....7y.sg....>.y^.....]....P.H.<.w+.u?.?.....B.Z.g.....D...C...D...Z.N .....:...O;.\l.-V.~NH5..H..WW.....D.I9?.....'...k.<..t...XE(..@.A..}..T.wlu..<...6?..=..._..5.....r.{x....x...q.6...M5.8...ut.yswj\|h.^N''.V<yj.9..n.....v....-...r.9 ...5.i+1..&.I./.Rjh.....J.%.L. ...1..m.`..../.....!12...''A..#B4$%&36a.....~;.r.T..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\truckbedSlide[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):	196084
Entropy (8bit):	**7.991879844727063**
Encrypted:	**true**
SSDEEP:	3072://u8nT9Jnp1nXiT8lTU+bhkDdXcLu6AkebBar2PACE+j5K6TcgNeA4qasWBdYthe:nbT9Jnr8krtqxQu6fr2JE+j5KY9NB4v/
MD5:	C2D7F1F64CE4B0FAE6646121BFE9455D
SHA1:	9CF1768F946E6A79ECCBFD00F9B59A2CE327CF4E
SHA-256:	86B059E49102E7BEA8D32221EEC7F7C6D707AB65CCED6F70A09CBBE3DB64EB16
SHA-512:	0F68D996825736B136B8497E401EE6E3BE363A6D33704353729AA26661800332AC6E693DB2D1CA9970832797690C227BEF03D8EA1569198A18ED41B2F0DA1995
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/img/banners/truckbedSlide.jpg
Preview:	......JFIF.....U...f....5..i...Tu9.vL..!....'i..,S ..z\..g9...-''.&17#.!..>...f.....H.wKL..9.n....;.5.e..R...qS.7.$_.E.k.qb.....G...8..o.....M>.iq.Vc....V.TB.`.Xm..Jd.''`..T..?.5..$c.tW)..:.1.....c.....:O.....@-.k%.....jp.....Q....N k..8d..C..tsb.iZ..-.....r\..}....i.X.....X..nS.9.....s.....i....w.N....U@.....''~w.F.QL.w>.....q..L^..^...C..d..c.!.!*R.u.J.....^.0...b.Z.F.n.k%..#.wj.].a.M.]..kD..$.u.==e.yE...,0..M...J... S.....f.(C\.o,.iZ.%d...rU=d.&F.....Z...)R.j}...I....X.5i.XKN&\UN...M.....-.9vs.89...&.g....=.}..~ZZ..i.])..H...fY..2...ZV.ZQs..W7.....z[I.N....f..[.qN-..v$M..X.....FPfu.W9.^yG/.0.e4....,U... .U...{'{.~...A9.I/..z.:WS.r.s.4S..;.b...b..x.....tKN...+.qk^..!9.-.jR..Vn..o..|.EP.'W.t.}.}.d..z.y.X.[.w+....=.@E^._.As...9.W

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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
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: up percase;. padding: .75em 0 .5em;.}.form input,.form select,.form textarea,.form button,.form .btn {. width: 100%;. -webkit-box-sizing: border-box;. -moz-box-sizing: b order-box;. box-sizing: border-box;. padding: 17px;. border: 1px solid #808080;. -moz-box-shadow

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\universal[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	16409
Entropy (8bit):	4.95143200532181

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\universal[1].js	
Encrypted:	false
SSDEEP:	192:B4fwGaauleJe7BroF1yt7tcz4o8botxCirrcp+6y0I1n0+aNlYf:B4fwGaauleJetwyZUlFtyIlYNlYf
MD5:	D1B7D46117F3E5064DFA855DF5DF7A40
SHA1:	99555A9CD87875DC7D4E9D4C3EDD567F66190802
SHA-256:	CDA2A16EF5636A8EC2B0C6B1B3604634F4656054D673BA6D245BDF02277C0DD7
SHA-512:	B9D9BBB25EA366C38B0875AFAEFC3C5B73FF4012E5E489EEA0F97E062AF94666847B7E7B5BA2063FD5A266F2370561AD4731CD7DE0BD3B86CE07B07222A3C2CE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/js/universal.js
Preview:	jQuery(document).ready(function() {..var suggested = 0;../**** CODE TO RUN ON PAGE LOAD *****/...../**** NAV ****/..jQuery('#hamburger').click(function() {...var windowHeight = jQuery(window).height()-26;...if(jQuery('#drawer').hasClass('drawerOpen')) {. ..jQuery('#drawer').removeClass('drawerOpen');....jQuery('#innerFrame').removeClass('slide1');....jQuery('#drawerLevel2').removeClass('drawerOpen2');....jQuery('#innerFrame').removeClass('slide2');....jQuery('#drawerLevel1').removeClass('drawerShadow');....jQuery('.2ndLevel li a').removeClass('selectedNav');....jQuery('#blackout').fadeOut(500);....jQuery('#frame').height('auto');.....} else {....jQuery('#innerFrame').addClass('slide1');....jQuery('#drawer').addClass('drawerOpen');....jQuery('#blackout').fadeIn(800);....if(jQuery('#frame').height() > windowHeight) {.....jQuery('#frame').height(windowHeight);....}.....}.....});..jQuery('#blackout').click(function() {...jQuery('#drawer').removeClass('drawerOpen');...jQuery('#inne

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\wheelsSlide[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):	103383
Entropy (8bit):	7.989988400089629
Encrypted:	false
SSDEEP:	3072:/76t2XF0B3d9p/F6c5bMVNtErXdh5ps1Kr8w9d30i:ztFO5bMbOpFQK5ki
MD5:	78C8B41BE5897AE66EE2F5437031223A
SHA1:	2EAC4B1063827862D048507991A0E1E6A92A220E
SHA-256:	4D8B6E21C351FD8B32957C27C9AE80EF56F28B9BFCE1902578C640DBB7BFFCD3
SHA-512:	BEF3A093CC77D180FAFA2D0D9E5E0AE195EB9831A5D4F60FC54C6BAA6B1F1549141275716A8F27136287D54208E993AE87D8B17CBA11FA649408CC732E190B7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/img/banners/wheelsSlide.jpg
Preview:	......JFIF.....wE..\G..9..o.w<G."........U.~.... .L.....Y.w.\fc...C[MV.V.m.'Y....W....g3.]..N.`(s*..Re.V.T..Ub?....1..o,....v.w.DXY1....k...}|..?..W$...EP...z.e..+Mh.EWRu..k.-m-\.i...h.....d.T.,D.....R.....<.....wc..V.....>..... ...'.Fe.#;....wl.R..q... ...h.hi...q.._|,.*.X.&..u.R[2D..JW]U.0.kW.....|.u.....d..s33&3k..Ut._0.%383....^..F..f..V.J....oF7z=...,.....*.z5+..c..^.VLb.]tD....x.D6.....fg&bs&2'..S....=7.f. lw{....,R..a!]v..6...ZZ.....b..hQ....)Z+R.kI.M.b.4....`.)S..W..N.5./t>-.#.....v.M.Of.l...+.Q...q...9t..i.l.BJ..5I..2[..[]....u).9&.l..j....V..'.,.....-d.W...1..=.B.....{[y...N...^.Y..HN.^.u... .v,..y.W.k...W.au..P..&2+.ED....^...._`.l93...nq....4.dFGe:>..o~....}9[ZK.P..&..v...u.....5(@WU....x.u..z.r.{k.f-.M.45

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\979841368838586[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	533304
Entropy (8bit):	5.472335488766903
Encrypted:	false
SSDEEP:	6144:Rk1HgCSntDV/HaKKV/Ha8NEPjQHguH3HpQrwz8GWNk1HgCSntDV/HaKKV/Ha8NEp:CNE7ANE7d
MD5:	38BFFB7BF8352E37B0B5C7825C51A5A6
SHA1:	CCAB295FBC6D80877C7FC4ED10935609F9480205
SHA-256:	8C95DB18658ACF094AD58CDB08F04F2AC932865FBF286A7050AEA85B21DCF87B
SHA-512:	8C67B450D2992F8EE97E7FF9240BAFC3C57830DC01E352F4BF4E5FF6846F107EE0B10D46F148C258C71AA2A916ED0C3003E30E48AFF3E7ACD69A1EE02266A16C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://connect.facebook.net/signals/config/979841368838586?v=2.9.41&r=stable
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.* IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS.* FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR.* COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER.* IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN.* CONNECTION WI

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\Battery_Cleaner_Protector[1].jpg	
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\9026IKNJ\DUCL12_21_Duplicolor-com_1K_Whatsnew_Banner_FINAL-2[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=7, orientation=upper-left, xresolution=98, yresolution=106, resolutionunit=2, software=Adobe Photoshop 21.2 (Macintosh), datetime=2021:02:08 10:59:33], baseline, precision 8, 1023x393, frames 3
Category:	downloaded
Size (bytes):	411447
Entropy (8bit):	7.95505131435287
Encrypted:	false
SSDEEP:	12288:b8S0ydY5A+RNDw5ZfoC07J64E+B6BQ6l9R:F0pAwN65FAw4E+tqR
MD5:	3E64AB58B6645B60F609E89E6114932D
SHA1:	3785D06496C872EAE89DBE41216F562B592A02CE
SHA-256:	D12D0325443CA9D0305F11AA03F193788F3F892F9E6F2ADA0EB8E799638FF031
SHA-512:	DC7BC2AD8343A8D3EF26737174977A2F73B3E5D552F9A39C7628BBD33658039A2EC121CDEB3627AFF6F745DE4C5341CD829F09B3493491FADBBDAE1499461E 6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/uploads/2021/03/DUCL12_21_Duplicolor-com_1K_Whatsnew_Banner_FINAL-2.jpg
Preview:	......Exif..MM.*.....b.....j.(.....1.....!...r.2.....i.....'.....'.Adobe Photoshop 21.2 (Macintosh).2021:02:08 10:59:33..... .....".....*.(.....2.....H.....H.....Adobe_CM.....Adobe.d..... .....=....".....?.....3.....!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'.....Vfv.....7GWg w.....5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%.....&5..D.T..dEU6te....u..F.....Vfv.....'7GWgw.....?..Y.,:.8..?.+.....>..z.....{?..._...OG..g.o.1....M.. ....Y.....M1..Z. .E..a.....|.(pk.H...*.G.....g.x..K..[.....0u.L..=.&..4o.&.....s...:..d;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\DUCL12_21_Duplicolor-com_1K_thumb-2[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 600x600, frames 3
Category:	downloaded
Size (bytes):	285630
Entropy (8bit):	7.972593506942557
Encrypted:	false
SSDEEP:	6144:vAWMXJT1JHwP1PibUH/aTb5AAuohFtMaYSSdB2+F0:dMXJT1JHwP5KA2b5Auh1qdNF0
MD5:	14936BF191B52E897D95C373451F5A00
SHA1:	1AFDF8512CEC4BBF7821873B9736D6D98FB95CB5
SHA-256:	B646DF6EB0449B81009547A5E335EF3037DC0EBDFD3DEE851A63D1ADC3F1FE18
SHA-512:	16AC2BC47997FF5DEDDAC2F16824C1BDDFA6B498E15EEF4D87D5EECF5F2E74E4E22F014F357CAE1F01B0DD9A1058125D1C87EB280A5543F21C834C4C7CE83 2A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/uploads/2021/03/DUCL12_21_Duplicolor-com_1K_thumb-2.jpg
Preview:	......Exif..II*.....Ducky.....d.....uhttp://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x: xmptk="Adobe XMP Core 6.0-c002 79.164460, 2020/05/12-16:04:17 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:a bout="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="xmp.did:8D1D0C3D09206811822AB262FE350967" xmpMM:DocumentID="xmp.did:CD05B99F777511EB8E0CB26383D498F9" xmpMM: InstanceID="xmp.iid:CD05B99E777511EB8E0CB26383D498F9" xmp:CreatorTool="Adobe Photoshop CC 2017 (Macintosh)"> <xmpMM:DerivedFrom stRef:instan ceID="xmp.iid:A5E216F976D311EB98ABF8B519062771" stRef:documentID="xmp.did:A5E216FA76D311EB98ABF8B519062771"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>....Adobe.d.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\DUCL1783_19_Duplicolor_Website_WhatsNew_Update-PC_FINAL-3[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1023 x 393, 8-bit/color RGBA, non-interlaced

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\DUCL1783_19_Duplicolor_Website_WhatsNew_Update-PC_FINAL-3[1].png	
Category:	downloaded
Size (bytes):	538830
Entropy (8bit):	**7.996821246994077**
Encrypted:	**true**
SSDEEP:	12288:lr1nA1DAyO5gEjGJwZLOIFDTsuM1V511VToevccTRd7uGj8kJHs:XA1DAt5vpZqIFDTTM1x1VEYNRd7uGzM
MD5:	1F70A0BF90D59A91651108B6CBCB9938
SHA1:	9B4D30CD440F43D519AC6C707DDB76E956758442
SHA-256:	FBD0DBA0D4271BC1995285CF5AB68706B87901529E95893399B05CB1B73AD07C
SHA-512:	48E4904AF265E5E4C06B2E7842CB93644D0F5D74D1DA52F65FE0FBEFC897C5ED802404FA1D4103D86B1CC52CED31CB1985EBCA2440DBC0E11295895125906B5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/uploads/2020/06/DUCL1783_19_Duplicolor_Website_WhatsNew_Update-PC_FINAL-3.png
Preview:	.PNG.....IHDR..... .IDATx..}..$Gy..=3.3.s....t.B. ,0...".L.... .....$...$I.. L..6&H..I.....:;.....{.gzO.v...3...\S.....\".u.q\,..D..M.m.eY.J.(.....,-....vy$....Njnn...Er].... ..0P...m..6.....P..(P.+..g..P{{;....B>.m@9(..0...E.es.[..(?...|...^>.CY.....oU..G.'.g...S.P...i..z..5@..Y....>.V...C..Q.j.B..S.7..p9....L....h.T..R..sU;.E\.,.....OLx....S..N...r.B..E.> Q.#Y.zV6....:|.*.._.....B.....OtP..e....-..411N.b.f.k..#.z{)..D.s..(...^.,....O'&&hii)Ay..z{{)...Z.q.}Y.h.,W...6.S.....$...'.....;.inv.0Gy...[.n5?.K.5]..43;C33...4,.Z.>.....M..R.....*..ib.P. .....I.X.....h.....z.EC.....b.....F.L...ttt.>~`.....GGGxN/,..zT....&.....2.....W.5..p....7.{..g.ql/.{...a.aOD.&Y.b.....s=gff...>..<.....hl. ...9*.....bm....<....u....j]..i....=M_..z.cx.0.... S.Y.u...\.j...O.X.J.N.zk./.U.._my....~.....'m../O<G...T#....<.e.\..c..G.oX./{.~y.7#y...cK+/.....+O.s.....n.-.{.:.9.<...-..s...O...'i.f..s.}..3v.:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\DUCL1783_19_Duplicolor_Website_WhatsNew_Update-PS_FINAL-3[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1023 x 393, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	527627
Entropy (8bit):	**7.996670860545729**
Encrypted:	**true**
SSDEEP:	12288:PClJAC2geckzOQoaSwNCd8pvi6e066DoDn1tTcEUk6HS:KlEgBwOBhCk6e066Q76HS
MD5:	B9D8A7B2F9F4249A4B87922107834085
SHA1:	9445038692FDB05F7380AD2D80EAE19725427261
SHA-256:	8105F1F5E25E5B3FFB52A727D65CDC1E79C44A9CC2A6E7B22302166D7F4379AF
SHA-512:	AB9D6E30D3F2FCB1D7DF3644C5F7F6AFF244BEAF60F5684478D750B0C1FAC77DFFC50A4E110C2692D3C956C3E1FDAAFCC943AE3D9363F20C86F4147A09ADE05
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/uploads/2020/06/DUCL1783_19_Duplicolor_Website_WhatsNew_Update-PS_FINAL-3.png
Preview:	.PNG.....IHDR..... .IDATx..}..$Wu.....l..Z.D...#... .&>.m.H`c2FF.....e.$.,d.-lc....$.....3.....vuUw.jgwf...Z..]U.n....F.w.]...m.,... ..)...i.d...O%.457O.|... ..]mm.L.)...K.2.. .^DL.?....N..B.....F@..[Z..)M.KY..rl...m.....4.Y..L&T.p...f.lm...%*[....'O.'.C.R.O.33..k..I..h.../.....EG....Fm.1.X....h.P.I...v.c.u.<...d]y.s...FY^.T..I....>U..N$(....)*.J...X...2.. ...u.x!.....5.....C..@W'%.q.._@.Y.....)..r..k....ZRI.._p..>.ue;..=....F.ghfa!.....lify<G...1....5D[.Z[hra.&gf)..4.....`W'M./....y).....Y..a....D.z.ij!C.B..#....}@w[+.J%:06..O#y.x.....} ..5(.4.}..W.'....Qw..A.....h1....A..P.T..)K>..RIJ.b..s7...{<.l<c.}.....P...d.....5.i0.r.....x4J.s...L.So..3b..jnfy....^.......&...#.r.^...5....Pok+....5(.w..H.h.J..o;.....%.....5.sm...m.. w6U...sd?..<..0.A.lK..GN.3.`..g...+....m.<...Nx..A~..}.{G..J...T..#.p...Q...r.{~.....R..|..[[Y..'.7.v...iJyv..Y#.3.'.3d.....T..a..8Jy8L<....)..O..gaxy.3fY.L.<.l~..=.k..IN....Sr

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\DUCL1783_19_Duplicolor_Website_WhatsNew_Update-VHT_FINAL-1[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1023 x 393, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	550833
Entropy (8bit):	**7.99747853557596**
Encrypted:	**true**
SSDEEP:	12288:EIxY/GHovPwZJG8F2l7BxCunoX07ThnrVSw0isR9zw3XuWV6qVX:HxY/GHonwZJT0IuU07j0issX
MD5:	B6FD9C322F1E61F9FFED0236B3B933D8
SHA1:	36DBBF44FEBF8AD70A7C7AF905E4BD1F4A54CD4F
SHA-256:	805924783292F26F75C3274194CCD0E2C97A6393D9C4BDB034A49E0C8C107348
SHA-512:	63A5ADFCCCDA732F0EBD42A3E4D1F154762F6C5669F51934414F1520E78CC3CA0CAFD82B82F6D07D0B0EB0862C4BFF19959CFBF104983DBDF31D9AFF0871958
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/uploads/2020/06/DUCL1783_19_Duplicolor_Website_WhatsNew_Update-VHT_FINAL-1.png
Preview:	.PNG.....IHDR..... .IDATx..}..$U.....6'.%* HPP..p.yFL.....O<.#*.'.". .....(...3.....cu.?..{.....gg...W...._.W.U._.....N.m.s9..rd..).9.....f..0(h.(.....J..d.&....Q...B..%...s.. ,>.2.a....0M.....(%f&.0.s..e....b.u...dy6.l.[...0..k.&.j.hfj.f..+k_.KU5...7.....l.e.mS.g..3.,.....s.L..T.>;G.h....)1;E...[.a.{H....eild..!...(...H.P.....O.59}...}dy...yxh'.....dR.J ....o.IY.<[8..p8J#...f*..@s[..gvj...P.Z.....P$J..q...A.T....YNCc;.#Q.....0._..>..yT]]...{1.<.~.ol.X...&.X.....8.#.0x..'.P.j.4>2@..c..kh..x.MM.R..../.....<.....O<.H..#49>D.@hNy ..55....AS..de2,.m.....L..5.....Uq.0..Z.izr.2.....f.....).....6...!&(.B.j.XB..gN`...,n..{].o....-|.....].(.LR"1%..O.=.~.....VU.R(..=..U,.0....G..ijfBl...T.....Py....D.hh.6...\...s..c..Ba....s. ..=4.g.....D.H.jj.ip.6...$3...[.j...QCS.U.....x~.}<N..-.i.%..a..7....~....w._.SCCCCCCC....`E'g."`YY.c.w.rV..x.m.....Q.#...n...V.....&)#....k..Y....T$.(.....b..X...R..)..P6..| ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\DUCL1783_19_Duplicolor_Website_WhatsNew_Update-WC_FINAL-2[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1023 x 393, 8-bit/color RGBA, non-interlaced

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\DUCL1783_19_Duplicolor_Website_WhatsNew_Update-WC_FINAL-2[1].png	
Category:	downloaded
Size (bytes):	591924
Entropy (8bit):	**7.996749906531067**
Encrypted:	**true**
SSDEEP:	12288:NxDrTP6J3vqeRMeo477388NUnMFI4DT+nibWfY4QJRugBGFaYBH25lGQ:NlrTP43ymfjDNUMS4H+8cY4yRuNER
MD5:	F9A1814262250C270CFCC03F378ED139
SHA1:	DA4AC8182C25F9D664403E6EF91A0C925E945E46
SHA-256:	9D5FA64DA0526F6A3E66C05A7A4B6708290118EBEADF6C223498CA3A1832F8D3
SHA-512:	D7574598DBCC1F9880497A5A64498EB175E62E3B06F8AA7E31B1BFDCCC4EE77583854D7395E0C423A648F14073B5463562EAC257862BA9C735F56279F575B499
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/uploads/2020/06/DUCL1783_19_Duplicolor_Website_WhatsNew_Update-WC_FINAL-2.png
Preview:	.PNG.....IHDR..... .IDATx....%Gu/|....;..v.$.....&..g.d."H.g.....8\|6.2..&Z.`..M..a...(.v.ifgg...~.SU...U}.g.....jg.T.S.T.:..~<...""...\|.#.8.Z.....F..f.....R7$....1...?7..c.a.s...P.....?..h...:..#....4l.h.....-t).b.C,.b6.....d.f.4..+E.....uM:..~.3...9..._..q.,...\.}.;.....y.....S?..cm~..@$..j...4F.....K..<%.....q...v...B\|.[.k.>...":..K..m.*.$..V.Z...<.D.0..S.m..qF>{. ..B.'b.N.V....MM4.C....SPb....c.j.t.x.b.,.)....j.|Z?...-.B..>...EScu.K.]$6E?....S.....G..[t....9.-.o.&.L7..\.q.....~.~.<...'...a.w..P.....u.q...o.....M.[..F..n.N.6.....}q.x...>\|$}h.....#...E^. .....o...h.i.....O..C.0..s.'.OP?...S{.....E.....T...f....Q.^....g.q4....m...1..{....8\...h..95Q.3...|F.Z2.}p..j..:<.N..S.....<.o.h.d.~v`..z.5*agX...;f.h.D...)..}.9..:H..5.6O7h..%:..K..(.G..>..... ^.yW....j.eX}m....N..Z[e...F.3.q....w...../s3+../...<?..._Nf_..8.....7..[...n....w.p.q....a...g..7fy*p.o...e.....^.%..=....cA.. \bj.r.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\DUCL800_20_Duplicolor_WhatsNew_Mobile-PC_FINAL[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=7, orientation=upper-left, xresolution=98, yresolution=106, resolutionunit=2, software=Adobe Photoshop 21.1 (Macintosh), datetime=2020:06:23 10:03:58], baseline, precision 8, 600x600, frames 3
Category:	downloaded
Size (bytes):	305079
Entropy (8bit):	7.901693076633548
Encrypted:	false
SSDEEP:	6144:NsbXsbCeBvdzDihuCMb71x1HnR8SuZxVSKST1jTsLk2w:NsDsW+RbCwzRnR8SGxwb1jTsjw
MD5:	7F03DDBD7958F26030CEA5B2F7D165B8
SHA1:	76861B1E57B4917128706668BC569224197AD7CE
SHA-256:	B18F44D6E726495050332E1A957C10E8394C95B10E04AFCA098FFBEB05DB71FD
SHA-512:	2E0F93ACE7C5AB69DBAB240B6A294221A5BCD8EAFE9FA8E215E8A85DA55DD17D868F14371B39E139B4ECF70AB3C5A6C5A6E578DD08607FC30FB3318E4F5F3B83
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/uploads/2020/06/DUCL800_20_Duplicolor_WhatsNew_Mobile-PC_FINAL.jpg
Preview:	....%3Exif..MM.*.....b.....j.(.....1.....!...r.2.....i.....'.....'.Adobe Photoshop 21.1 (Macintosh).2020:06:23 10:03:58.....X.... .....X.....".....*.(.....2.....#.....H.....H.....Adobe_CM.....Adobe.d..... .....".....?.....3.....!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'.....Vfv.. .....7GWgw.....5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%.....&5..D.T..dEU6te....u..F.....Vfv.....'7GWgw.....?..!...<..M/M.5}!...<..M/M%5}!... <..M/M%5}!..^..QnC..T.....{]w.6...J..oS.3.....Q...s..L}6z.o..M.Z]7...V%..U..k.<....m~.;.....M.<k.u.6.mk....&...%.Y.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\DUCL800_20_Duplicolor_WhatsNew_Mobile-PS_FINAL_v2[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=7, orientation=upper-left, xresolution=98, yresolution=106, resolutionunit=2, software=Adobe Photoshop 21.1 (Macintosh), datetime=2020:06:23 10:00:00], baseline, precision 8, 600x600, frames 3
Category:	downloaded
Size (bytes):	304686
Entropy (8bit):	7.901090537663659
Encrypted:	false
SSDEEP:	6144:7q7e0vReKgAzzvlrr/iF3SpQ9sX9SGSedvWTK9kGXBBAEK:7q7VReKg8zvN/iopQWtXbDXBVK
MD5:	A4A8BCF329EFF54802BA4DEDA26DBF35
SHA1:	DDB4882EC2C22696AFECCC6C38B24BA2FF5F5CA4
SHA-256:	14A63B59A0C7095763D902EDE1269C19F19C2FEE69A2EA884D303D6A6B827883
SHA-512:	E537405700AFB73F18696F360683D15B1F859CB4C345BAF090F5C4BCFCBBC9B43F13D4A0F77663CDE9426EB6CF7041CB2CA36EB40D7672A799E9FC6DAA5D1F3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/uploads/2020/06/DUCL800_20_Duplicolor_WhatsNew_Mobile-PS_FINAL_v2.jpg
Preview:	....%3Exif..MM.*.....b.....j.(.....1.....!...r.2.....i.....'.....'.Adobe Photoshop 21.1 (Macintosh).2020:06:23 10:00:00.....X.... .....X.....".....*.(.....2.....#.....H.....H.....Adobe_CM.....Adobe.d..... .....".....?.....3.....!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'.....Vfv.. .....7GWgw.....5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%.....&5..D.T..dEU6te....u..F.....Vfv.....'7GWgw.....?..!...<..M/M.5}!...<..M/M%5}!... <..M/M%5}!..^..QnC..T.....{]w.6...J..oS.3.....Q...s..L}6z.o..M.Z]7...V%..U..k.<....m~.;.....M.<k.u.6.mk....&...%.Y.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\DUCL800_20_Duplicolor_WhatsNew_Mobile-VHT_FINAL-v2[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\DUCL800_20_Duplicolor_WhatsNew_Mobile-VHT_FINAL-v2[1].jpg	
File Type:	[TIFF image data, big-endian, direntries=7, orientation=upper-left, xresolution=98, yresolution=106, resolutionunit=2, software=Adobe Photoshop 21.1 (Macintosh), datetime=2020:06:23 10:01:50], baseline, precision 8, 600x600, frames 3
Category:	downloaded
Size (bytes):	330131
Entropy (8bit):	7.911730822288162
Encrypted:	false
SSDEEP:	6144:8EyEgTSnRmCyAzekY9yiqbVKOaJa15pqHrMG5XKc6lWabi/k2URtW5:DZg2RW8w9obVOJaPkHQG47lWii/ytW5
MD5:	7429A5EEDC8C53A98471C987BF296B50
SHA1:	B5E633580735DE224460D910A9E180F74FF8587B
SHA-256:	B0375755401ABAC9D8D3EBE72DE5C0B7145F47944C638539252CEB14C1247891
SHA-512:	FFADF129CA5EF6BFB1E5D73E90ED34875C75233E2DC472F2BB7782C90FE54EA02C19C933FB2C7DAF42A9D4C07D3A31929B06E0838C4F61B20E3B534BA4F372B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/uploads/2020/06/DUCL800_20_Duplicolor_WhatsNew_Mobile-VHT_FINAL-v2.jpg
Preview:	....+.Exif..MM.*.....b.....j.(.....1....!...r.2.....i.....'.....'.Adobe Photoshop 21.1 (Macintosh).2020:06:23 10:01:50.....X.....X.....".....*.(.....2.....*t.....H.....H.....Adobe_CM.....Adobe.d.....".....?.....3.....!.1.AQa."q.2....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'.....Vfv.....7GWgw.....5....!1..AQaq"..2....B#.R..3$b.r..CS.cs4.%.....&5..D.T..dEU6te....u..F.....Vfv.....'7GWgw.....?...I$P..s..Yc...7=.!.h.....YF....+....a.kZ%....\..W.ex.._.....}.A....~MM6.....zT....._....I..z.Gv.....?.I.....e?...s.Vmg.[.)..K7....k.F++..1.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\DUCL800_20_Duplicolor_WhatsNew_Mobile-WC_FINAL_v2[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=7, orientation=upper-left, xresolution=98, yresolution=106, resolutionunit=2, software=Adobe Photoshop 21.1 (Macintosh), datetime=2020:06:23 10:03:17], baseline, precision 8, 600x600, frames 3
Category:	downloaded
Size (bytes):	310254
Entropy (8bit):	7.914619743989268
Encrypted:	false
SSDEEP:	6144:tmIeqOhAjDeKgAz3Ri9oT7vpskLJvxprSPWEamEstAMJBfPaAVY1o5:tmI46DeKg8k6rLdrSeEaLKJBKS
MD5:	EE69D04619239C01A64DA2542B56E6CD
SHA1:	266A28F0D356B09588A225610B41B9519C87ECA2
SHA-256:	5B1739F8AA7BC441F6A2B11C2343363CB781A28DBD3C4A0260686C384DFDB8D9
SHA-512:	83B12831697D66BFE015E987817E076CB88487CEB80B51077FD3A52331AD44305DDF117774B8DAB1E1AA45DE62D3A448E4C5BBD9345643046381126890210314
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/uploads/2020/06/DUCL800_20_Duplicolor_WhatsNew_Mobile-WC_FINAL_v2.jpg
Preview:	....#)Exif..MM.*.....b.....j.(.....1....!...r.2.....i.....'.....'.Adobe Photoshop 21.1 (Macintosh).2020:06:23 10:03:17.....X.....X.....".....*.(.....2.....!.....H.....H.....Adobe_CM.....Adobe.d.....".....?.....3.....!.1.AQa."q.2....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'.....Vfv.....7GWgw.....5....!1..AQaq"..2....B#.R..3$b.r..CS.cs4.%.....&5..D.T..dEU6te....u..F.....Vfv.....'7GWgw.....?...I$P..I%)$.IN}.w...m...W....?..m..V;...=...?.....2.e....sq.....md;&....c..../.C..wa....s*.;.....V...2Z....7.....p..U.....t..s~.A..T=..Ng.]]..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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
Preview:	.....JFIF.....i.....zeW.4?.*S]..cAx..w.."k&gb^.BQ3.9.....y5.....p}.....$.....N\r.6..<...z..7.....x.B...(..ma.....@.:.7..R'.@.....U.L.G701...%S..@!q.9.I..7(....nb..UM..kkc..}.yQ.....Mlm.W.zP.....^..`+...a2..w...>%d.+..E.n.&u~..q...Uu.X...&.B9....%..... <..>...~.{g....u`...(..(..X.(.A@.B.....n.,<M=.....9..O....k..%...D.`.@.P...%....P.B.(..`. ....7.....1....!2ACQq."3BU$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...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\MX101_042210[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\MX101_042210[1].jpg	
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):	7433
Entropy (8bit):	7.928168903009754
Encrypted:	false
SSDEEP:	192:mZszjpy0xtEVBEkBshI+oVwo48y06otxZ6psKHcxuLMxW3:3zjQ0YBS0QAtb6ps2Mxg
MD5:	D6A2DF02B8A0D7AAF499F02D9F9081F3
SHA1:	A888B3483EB2BE58491F41DCAC6C84EA4E8D8B52
SHA-256:	1A233D22CD410CBD5DDA1362620516D5C78F83A48C7B41C5385C8BAF1BBF95DD
SHA-512:	602EBC6BD2F3099D135C8562102FAB546AC982C0445FF7A5B1EDE4C3C98194F99882B0F00E2940D455549790C733C96D4C576B06BB074557DF58431170E782AC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/img/thumbs/MX101_042210.jpg
Preview:	......JFIF.....i.....$..:...<.wO.....;..T.....ak.n..~ .....2/9.v...]..F. .....r...D<`....)s.U..m.....y*..V.I..)O.....Z.....i..q.}0L...:.....wt...._....m9..CgIW...Q...k.....F.oV].1SJ.T...._...~..:.r.....s.a.....k..`.pMMr.r....-(.kq.i-.5s...S..D.6....`p<... s.A4`..I_.....Au....@.....lH..6..C.)...b..g..v^.r.6.-.....U.i.0V.O.\:0[.#a.k.....(.2.N...*&.e.S..-..%.....Yf$H.....Y.0.`<.w;..W...7....Oq<.v.8..... .....k.r.Q.(*5.....:.;9[.....k..H..WQ...`....C.va....c.y...|f.1.V...r.]..#.&....:Y.F..0jm4..d.Y...l....Y*.u.{..T...y^.E_..^Wx..F.oC.....Y...j....2.....%#&125ACD ..!"$364.....d..V.^]PW.X.....h..<..d<...s.:.....j...6^.....w....q>..\..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\analytics[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	49377
Entropy (8bit):	5.521008419138659
Encrypted:	false
SSDEEP:	768:/yR3fYFBCwsNDsP5XqY0TyPnHpl1TY3SoavyVv6PU+CgYUD0lgEw0stZK:/y9g1r5h0UHp/Y3SowCw0sy
MD5:	042B7183D8645F5CF9D0D6ACD5FF8358
SHA1:	447A98467EA31E253ECB63EE8564C8B5E1E77D58
SHA-256:	73D6A5EA11FB7BF6E6A6CCD44B1635D52C79B0A00623D0387C9DDDD4B7C68E89
SHA-512:	72AA2F221BB5EFEC3A9C0CBC2D01DEBD827361369F7E84AA613D4CA70838FF68EA2C3300167FB263A4F416A857BABF0354A1FF8B3EC669BF88452633981CA18F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google-analytics.com/analytics.js
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var n=this||self,p=function(a,b){a=a.split(".");var c=n;a[0]in c||"undefined"==typeof c.execScript||c.execScript("var "+a[0]);for(var d;a.length&&(d=a.shift());)a.length||void 0===b?c=c[d]&&c[d]!==Object.prototype[d]?c[d]:c[d]={}:c[d]=b};var q={},r=function(){q.TAGGING=q.TAGGING||[];q.TAGGING[1]=!0};var t=function(a,b){for(var c in b)b.hasOwnProperty(c)&&(a[c]=b[c])},v=function(a){for(var b in a)if(a.hasOwnProperty(b))return!0;return!1};var x=/^(?:(?:https?|mailto|ftp):|[^:/?#]*(?:[/?#]|$))/i;var y=window,z=document,A=function(a,b){z.addEventListener?z.addEventListener(a,b,!1):z.attachEvent&&z.attachEvent("on"+a,b)};var B=/:[0-9]+$/,C=function(a,b,c){a=a.split("&");for(var d=0;d<a.length;d++){var e=a[d].split("=");if(decodeURIComponent(e[0]).replace(/\+/g," ")===b)return b=e.slice(1).join("="),c?b:decodeURIComponent(b).replace(/\+/g," ")}},F=function(a,b){b&&(b=String(b).toLowerCase());if("p

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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):	84940
Entropy (8bit):	5.8909791585543125
Encrypted:	false
SSDEEP:	768:v/StjwtC8GN/TqNDCyZguPt5Yi04Kl65LmbzV/Sil7EC8GN/TqNDCyZguH+vtSoE:ajwtCDcZLt5Odl6hmH79ECDcZzcSUk
MD5:	3A80540DDC2D1A070C8F75019A4DCC9F
SHA1:	3397610A8B55EF14D18D9D458863AE0EE7B761C7
SHA-256:	14CDEFC2CC6AEE7935E7158363276CA902DDA738A7B95143A86AEFA6E5F79C2C
SHA-512:	6797888D5457917D109A286CDD10237D6219BDDB8767719AEC9C9F0CE9527284CE84D15462D27DE45DA8C17F9512ACE088FD63837D8D0462322BE5EF1F40EB2
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="NgDQDuVq1L8/miuCtpAy8Q" type="text/javascript">window['__recaptcha_api'] = 'https://www.google.com/rec

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\anchor[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\anchor[2].htm	
Category:	dropped
Size (bytes):	43533
Entropy (8bit):	5.888608138830656
Encrypted:	false
SSDEEP:	768:v/SiG8CMC8GN/TqNDCyZgupx6Ae4tAHZUP2PXZH:BXCMCDcZD6Ae/mPw
MD5:	8D82A9ACE45157E480D9BA91E829EA7A
SHA1:	1C24A0886D3D2A206C223374081570105C647EE3
SHA-256:	6BDEF60E31C081A4DDD9CDBC09AC41344FC255401EA9F7D33619A34CA0339855
SHA-512:	09874C25951DAF015B6C46F55653F515C991BCFCEC7071CE0F4E29B47757457AB1BFC320D6B6EA69B37FA2C7E531AE34301240AC54E4B9F47328533BCD544253
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="Ow/t9Vf1Agh8iVd5+1iafA" type="text/javascript">window['__recaptcha_api'] = 'https://www.google.com/rec

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\bat[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):	30494
Entropy (8bit):	5.30355290011164
Encrypted:	false
SSDEEP:	384:otKVCwh9wC22fo5EB4b7AWhbwM05Jkr9qNHfs9nB/wDSliNqCET8zT7QAEqnyJYk:ZCwhBR/DOZwDhzT7QSnSYyebQ
MD5:	5562385CBAFDDC33276BA10BA59890F7
SHA1:	A030EE46C99511E12EBB6257138FBE3E75232540
SHA-256:	73E2E5173ED0D5A77B02914FA0EF1F67BB53143DA75F0348F558F95565220CA1
SHA-512:	3D12741A718FE0CC3756C8018E29C07B84D28702E8783F42677431213CC4F79A6852C3A26A8D29C6FC515A069D4543C6114A0C56FC19AC48F680EE9439D2ECE7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://bat.bing.com/bat.js
Preview:	function UET(o){this.stringExists=function(n){return n&&n.length>0};this.domain="bat.bing.com";this.URLLENGTHLIMIT=4096;this.pageLoadEvt="pageLoad";this.customEvt="custom";this.pageViewEvt="page_view";o.Ver=o.Ver!==undefined&&(o.Ver==="1"||o.Ver===1)?1:2;this.uetConfig={};this.uetConfig.consent={enabled:!1,adStorageAllowed:!0,adStorageUpdated:!1,hasWaited:!1,waitForUpdate:0};this.beaconParams={};this.supportsCORS=this.supportsXDR=!1;this.paramValidations={string_currency:{type:"regex",regex:/^[a-zA-Z]{3}$/,error:"{p} value must be ISO standard currency code"},number:{type:"num",digits:3,max:999999999999},integer:{type:"num",digits:0,max:999999999999},hct_los:{type:"num",digits:0,max:30},date:{type:"regex",regex:/^\d{4}-\d{2}-\d{2}$/,error:"{p} value must be in YYYY-MM-DD date format"},"enum":{type:"enum",error:"{p} value must be one of the allowed values"},array:{type:"array",error:"{p} must be an array with 1+ elements"}};this.knownParams={event_action:{beacon:"ea"},event_category:{be

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\bg[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, 174x1743, frames 3
Category:	downloaded
Size (bytes):	56456
Entropy (8bit):	7.939813513002655
Encrypted:	false
SSDEEP:	1536:7UuPgcnAgrQhodRFrbREKFjBq/sLKqyt6rlUym56:w+KodjbRE0oE2FclUy86
MD5:	892FBEDF0127642D0497D0E7091A8338
SHA1:	C54638F18180D3B8BF1457D8E5C61BEF8EF48DD5
SHA-256:	4EDA9C1991D16677CCDB3F3C695D75032DFE0947CE758986E5FE745CD1CAD72B
SHA-512:	BA6EBA33235B946FD573C2755A9269C6862C89265166745ABF04383A227AE48B7CDC5FC9A95DEDB123957F94B12E6EAB410FE62452CB8CE44A4533F41196016E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/img/bg.jpg
Preview:	......JFIF.....8...SQ`T...Ri.S3.I.[u..y..Y-...4.*.!.....@.H.!0...N....P.]c.....H..YW5..b.....Y.-...U9.f..6.n..I..T.4.4B.QqCT.8..*3r...iT...@...4.P0."..@...`..`.....@.1.)..C..+..d.....hi...`g`4.M.."...0....2.`. .4...4...4.$....b..L.....s@...6E1.....3;`!..&.#.....&.& .....T4.I...D.J...j.....LI.....4!.M4.0...4....Lbm1T...`.E.@HM..%...&.....@.NX..&.....K....BZ...0.....@.....4....I.@..X..3V h.g`...0.$lLL.....L.0CC@0.Fh"`i.`.D....Y.7..2..z..E.....4.`.Z..g....I.C1..1.).(V....t..M1T.....*m11..So:.`./...).U*C.,...t.).b...8t;K..9nz..JY....K.W.^..^E2. .Yn...g.....U.k.G:..r..Y..*...iu>M./.....Wx.D..v..7..-u.U.Q.YvNw...-.;.=u.GFZ.k.'W...\.qz1.z^....g.....'.k...}+..r.g|.Ues.[.o<*o,v.....K.%m....\.c....K...H}sY..[.....WG.z."-.gh..*..h.2.l.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\bigVideo[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, 416x265, frames 3
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\bigVideo[1].jpg	
Size (bytes):	23017
Entropy (8bit):	7.969499315222531
Encrypted:	false
SSDEEP:	384:++aCnxJ2SVSWnroKedOPMWtQg8caPSgwqUidWUZ+n17bHMFP6ZEtHhdFIdUiv:+pCH2SVSWn0KeGMYJ9fqTdWUsn1nH0Gj
MD5:	6CFBDC29B5532A70485912028C843BE4
SHA1:	36E5C5A38083360474DF78C583652BC04E39CCE6
SHA-256:	D638F8C03F356A24C205F175E5E1C1D49EFE5F10A8CDBE29B7AF5D4AEAB712C9
SHA-512:	58BE1DA0EC6588EB28407600881A33A76FA6CC1948CB4BB36D89CD35055440D425F9342E767AF3EF30177173E7C0B23AC6A44D02D90A5874FBA6F8782456F2B8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/themes/duplicolor2019/assets/img/bigVideo.jpg
Preview:	......JFIF.....##########.....##########..... .....Sq.H...D..:*..y.V.!..vo..2...M..2.9...T&A-.sDHq.u. ..{.R.....;.%&.....XN`.{0sd.Dg.,.^.j{.TI.!.y\.].....6.j...}..k...Qybx..*W....rq.6...q.....a.)....*.:.Y...Le..H&k...y....\..*iz..5..b.b....C`. K.B..[..[.O3.e*..Hi2c.;2]7h.U.]...B....+1.....4*..!.X:.nD'd.`...V]s.m.....P.....k.f-.-..P.I.s K...|.l.2..T....<.....f.8.1H+...)\@...wY#*.zA.....8..|....P.[.u.N\+.\.K..&y..=..6{.a.>WK.L0 .g...qN...-...g.G.?b..dY2{..@r...C.*..N[.x..C..m..!.;..Q\.:..L.Z.qkx...#fw.(l=.K....R.n u.9..#.gfSnt.l.e..RA)....Sus9....P?g..\p.....|..{...0.mq4.6.!.".D.l.Kx..WH.E..w.UE.jg..Td..{..... ....#W..f.B...!Z.;.z..$....>+.j.0.{..q..tP.f.P."..c.!.,....2...IL.....t<?%O....."..&.x/..j,.N..n.8w.Ud.zJ..Kn;.i_G{....(..8..M.5..(.;...I....3..*...HL!.Zy.i_G{1..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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
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\9026IKNJ\bullet[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	447
Entropy (8bit):	7.304718288205936
Encrypted:	false
SSDEEP:	12:6v/71Cyt/JNTWxGdr+kZDWO7+4dKIv0b1GKuxu+R:/yBJNTqsSk9BTwE05su+R
MD5:	26F971D87CA00E23BD2D064524AEF838
SHA1:	7440BEFF2F4F8FABC9315608A13BF26CABAD27D9
SHA-256:	1D8E5FD3C1FD384C0A7507E7283C7FE8F65015E521B84569132A7EABEDC9D41D
SHA-512:	C62EB51BE301BB96C80539D66A73CD17CA2021D5D816233853A37DB72E04050271E581CC99652F3D8469B390003CA6C62DAD2A9D57164C620B7777AE99AA1B1
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/bullet.png
Preview:	.PNG.....IHDR.....ex....PLTE...(EkFRp&@e&@e)Af)AgANjBNjDNjDNj2Vv-Xz-Y{3XyC\}E_.2j.3l.8p.7q.;j.;l.Zj.\l.5o.7q.<..aw.<..dz.E.....1..@.7..~.....9..:.....A ..B..E..9..:...a..c..b..g.#M.%O.#r.#s.%y.2..4..+..-..?..@..;..p..s...G..H..M.....z`....#tRNS...../,....mIDATx^..C..`.....S....y'...05...|..k.X.....*`.F.K....JQ..u.<.}.. .. [U..m....'r%.....yn.`.7F..).5..b..rX.T.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\cat_engine-1[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):	47803
Entropy (8bit):	7.980836467594972
Encrypted:	false
SSDEEP:	768:zu+1J1++oOioJTyrAUDdiiH3kLQIy8vmm7+k17FhOfq9uNc9gRSW:y+1VMAUBi0Iy/W+05uNrh
MD5:	EA068B1675729AB9BB1F15B63E73BDC8
SHA1:	6E6F2F806B29C12393394874179FD80FA1586225
SHA-256:	3014029D45D3AEE97710B8B6D1A8EEACF5DBDF4982515A69835E7570F712EFD7

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\cat_engine-1[1].jpg	
SHA-512:	7082FB343BE0D5948D5453CF6C0B4A1ED30B34D95FAA64D40D3AC57A15332EF79389F7C4480EE7AA936BA9AF8C437300DA2D9F1321BF41FA0F716C9D1FAC94E0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.duplicolor.com/wp-content/uploads/2019/01/cat_engine-1.jpg
Preview:	......JFIF.....","..".....m.....{uz...4 .dv..$f.fT.i Af..Ek....tY#.$.*I.k..B.mu.P.....M.J..._..N....g...f.....da!.....v.Qf.:*..s@.H...m.X{ZJ.. T..a..V.....I!.iK...F.....l.....s)y!..]..K.H.&.3d.B,.%..Q.!$6..JP5.....3.hH..Lf..u..].)~...7..>.O.....c*...r..3....7 @.f.w.E....5.Ey".n...G{%iUgb....46h)....e.M2..)...?V$.F.W..y....u.4XcB...pa....5.Yk.zkED...3B....].$c}.A`.V.V.ZB....ESoB.*.....f..}.k.n.=.9}]om.-ja.(J9.N>l9UM...+K....F...]%..n.i.. .....l....,.=. R..2..&q.....z/?o.4[..n..w..a . ..]Ts..2..d....M.%.....T...-....f.A*.....^uh.k..``.#..e..Q..Zt-...i....Q..E...WNNw7..UX.WN[.@..j..}Y.eG(.c.....{....Hl.JV....U....\.gG.....e.e..... ...p<.$.....r... .....b.R.t..DQ..Z.+.f.E..*.-...K;.$.F.a_....Gc....b..x.....e{>.....rr...w?-.....5`.W<.@.$5.&...].-1..hU..u....7.}..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	1732
Entropy (8bit):	5.147472644053231
Encrypted:	false
SSDEEP:	48:vY3QEa7Y3QxMawY3QpayY3QwhafJOEajOxMa1OpaDOwha1:vYgEa7YgxMawYgpayYgwhahOEajOxMaS
MD5:	9B3A23A845FC0134034855EE19C68379
SHA1:	1DAEDD6EB0FA93C2B94D2085791919FD44C52853
SHA-256:	F7D939D6280DF8829500AD4F4BCB9CE9ED596581ABA73B16A40E597C671B607C
SHA-512:	ACA47B1A897A3F99ACB19F895BD150CD092B3CFE2C11D9560C9AD483152AD736D8F336584A65EE5B91C21E424572D750F9239ABEB0A5794C4D164EDFC9D284E
Malicious:	false
Reputation:	low
Preview:	@font-face {. font-family: 'Nunito Sans';. font-style: italic;. font-weight: 400;. font-display: swap;. src: url(https://fonts.gstatic.com/s/nunitosans/v6/pe0oMImSLYBIv1o4X1M8cce4E9lKcA.woff) format('woff');.}.@font-face {. font-family: 'Nunito Sans';. font-style: italic;. font-weight: 600;. font-display: swap;. src: url(https://fonts.gstatic.com/s/nunitosans/v6/pe01MImSLYBIv1o4X1M8cce4GwZuY1MIVA.woff) format('woff');.}.@font-face {. font-family: 'Nunito Sans';. font-style: italic;. font-weight: 700;. font-display: swap;. src: url(https://fonts.gstatic.com/s/nunitosans/v6/pe01MImSLYBIv1o4X1M8cce4G2JvY1MIVA.woff) format('woff');.}.@font-face {. font-family: 'Nunito Sans';. font-style: italic;. font-weight: 800;. font-display: swap;. src: url(https://fonts.gstatic.com/s/nunitosans/v6/pe01MImSLYBIv1o4X1M8cce4G35sY1MIVA.woff) format('woff');.}.@font-face {. font-family: 'Nunito Sans';. font-style: normal;. font-weight: 400;. font-display: swap;. src: url(https://fo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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=....~I..=!.M.. ..O...^..u.&.D..D.RG...U.....f.oO.[6.f...D. . .2.RK[K..%.....J..$ ...(...2.(Ij....F.....Q.E.4.I#!.@.............J9.....IEND.B`.

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 18:18:26.300440073 CEST	192.168.2.4	8.8.8.8	0xabb6	Standard query (0)	duplicolor.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:26.809500933 CEST	192.168.2.4	8.8.8.8	0xb267	Standard query (0)	www.duplicolor.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:27.238946915 CEST	192.168.2.4	8.8.8.8	0x9e1	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:27.252785921 CEST	192.168.2.4	8.8.8.8	0x1d60	Standard query (0)	nexus.ensighten.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:27.258131981 CEST	192.168.2.4	8.8.8.8	0x5067	Standard query (0)	code.jquery-ul.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:27.272564888 CEST	192.168.2.4	8.8.8.8	0xccfe	Standard query (0)	ws.sharethis.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:27.299823046 CEST	192.168.2.4	8.8.8.8	0x5e37	Standard query (0)	platform-api.sharethis.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:27.910402060 CEST	192.168.2.4	8.8.8.8	0xc0d5	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:28.364072084 CEST	192.168.2.4	8.8.8.8	0xa124	Standard query (0)	platform.twitter.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:29.032071114 CEST	192.168.2.4	8.8.8.8	0x3ab1	Standard query (0)	s7.addthis.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:29.682421923 CEST	192.168.2.4	8.8.8.8	0xc583	Standard query (0)	buttons-config.sharethis.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:30.671941042 CEST	192.168.2.4	8.8.8.8	0xc541	Standard query (0)	c.sharethis.mgr.consensu.org	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:31.143378019 CEST	192.168.2.4	8.8.8.8	0x69b5	Standard query (0)	z.moatads.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:31.382663012 CEST	192.168.2.4	8.8.8.8	0xf608	Standard query (0)	scontent-ort2-2.cdninstagram.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:31.392880917 CEST	192.168.2.4	8.8.8.8	0xb06f	Standard query (0)	v1.addthisedge.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:31.430948019 CEST	192.168.2.4	8.8.8.8	0xd4d7	Standard query (0)	m.addthis.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:31.951167107 CEST	192.168.2.4	8.8.8.8	0x9f3e	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:32.063416004 CEST	192.168.2.4	8.8.8.8	0x1be7	Standard query (0)	seg.sharethis.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:32.483222961 CEST	192.168.2.4	8.8.8.8	0x71dd	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:33.071595907 CEST	192.168.2.4	8.8.8.8	0x984e	Standard query (0)	l.sharethis.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:43.765734911 CEST	192.168.2.4	8.8.8.8	0x5a15	Standard query (0)	www.duplicolor.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:19:03.830856085 CEST	192.168.2.4	8.8.8.8	0x6da	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 18:18:26.365480900 CEST	8.8.8.8	192.168.2.4	0xabb6	No error (0)	duplicolor.com		151.101.66.159	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:26.874293089 CEST	8.8.8.8	192.168.2.4	0xb267	No error (0)	www.duplicolor.com		151.101.66.159	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:27.297714949 CEST	8.8.8.8	192.168.2.4	0x9e1	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:27.297714949 CEST	8.8.8.8	192.168.2.4	0x9e1	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:27.317866087 CEST	8.8.8.8	192.168.2.4	0x1d60	No error (0)	nexus.ensighten.com		18.195.42.228	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 22, 2021 18:18:27.323178053 CEST	8.8.8.8	192.168.2.4	0x5067	No error (0)	code.jquery-ui.com		172.67.192.205	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:27.323178053 CEST	8.8.8.8	192.168.2.4	0x5067	No error (0)	code.jquery-ui.com		104.21.44.14	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:27.334867001 CEST	8.8.8.8	192.168.2.4	0xccfe	No error (0)	ws.sharethis.com	d3mdrpbbs8qfxa.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:18:27.334867001 CEST	8.8.8.8	192.168.2.4	0xccfe	No error (0)	d3mdrpbbs8qfxa.cloudfront.net		13.224.193.69	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:27.334867001 CEST	8.8.8.8	192.168.2.4	0xccfe	No error (0)	d3mdrpbbs8qfxa.cloudfront.net		13.224.193.5	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:27.334867001 CEST	8.8.8.8	192.168.2.4	0xccfe	No error (0)	d3mdrpbbs8qfxa.cloudfront.net		13.224.193.89	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:27.334867001 CEST	8.8.8.8	192.168.2.4	0xccfe	No error (0)	d3mdrpbbs8qfxa.cloudfront.net		13.224.193.25	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:27.371336937 CEST	8.8.8.8	192.168.2.4	0x5e37	No error (0)	platform-api.sharethis.com	d1r0ldx4ccoewq.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:18:27.371336937 CEST	8.8.8.8	192.168.2.4	0x5e37	No error (0)	d1r0ldx4ccoewq.cloudfront.net		13.224.193.66	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:27.371336937 CEST	8.8.8.8	192.168.2.4	0x5e37	No error (0)	d1r0ldx4ccoewq.cloudfront.net		13.224.193.17	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:27.371336937 CEST	8.8.8.8	192.168.2.4	0x5e37	No error (0)	d1r0ldx4ccoewq.cloudfront.net		13.224.193.52	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:27.371336937 CEST	8.8.8.8	192.168.2.4	0x5e37	No error (0)	d1r0ldx4ccoewq.cloudfront.net		13.224.193.25	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:27.970446110 CEST	8.8.8.8	192.168.2.4	0xc0d5	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:18:27.970446110 CEST	8.8.8.8	192.168.2.4	0xc0d5	No error (0)	scontent.xx.fbcdn.net		157.240.17.15	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:28.431525946 CEST	8.8.8.8	192.168.2.4	0xa124	No error (0)	platform.twitter.com	cs472.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:18:28.431525946 CEST	8.8.8.8	192.168.2.4	0xa124	No error (0)	cs472.wac.edgecastcdn.net	cs1-apr-8315.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:18:28.431525946 CEST	8.8.8.8	192.168.2.4	0xa124	No error (0)	cs1-apr-8315.wac.edgecastcdn.net	wac.apr-8315.edgecastdns.net		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:18:28.431525946 CEST	8.8.8.8	192.168.2.4	0xa124	No error (0)	cs1-lb-eu.8315.ecdns.net	cs41.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:18:28.431525946 CEST	8.8.8.8	192.168.2.4	0xa124	No error (0)	cs41.wac.edgecastcdn.net		93.184.220.66	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:29.093365908 CEST	8.8.8.8	192.168.2.4	0x3ab1	No error (0)	s7.addthis.com	s8.addthis.com		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:18:29.093365908 CEST	8.8.8.8	192.168.2.4	0x3ab1	No error (0)	s8.addthis.com	ds-s7.addthis.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:18:29.755918026 CEST	8.8.8.8	192.168.2.4	0xc583	No error (0)	buttons-config.sharethis.com	d2znr2yi078d75.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:18:29.755918026 CEST	8.8.8.8	192.168.2.4	0xc583	No error (0)	d2znr2yi078d75.cloudfront.net		13.224.193.6	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:29.755918026 CEST	8.8.8.8	192.168.2.4	0xc583	No error (0)	d2znr2yi078d75.cloudfront.net		13.224.193.81	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:29.755918026 CEST	8.8.8.8	192.168.2.4	0xc583	No error (0)	d2znr2yi078d75.cloudfront.net		13.224.193.72	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:29.755918026 CEST	8.8.8.8	192.168.2.4	0xc583	No error (0)	d2znr2yi078d75.cloudfront.net		13.224.193.13	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 22, 2021 18:18:30.739943981 CEST	8.8.8.8	192.168.2.4	0xc541	No error (0)	c.sharethis.mgr.consensu.org	dlaj66hdiarg7.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:18:30.739943981 CEST	8.8.8.8	192.168.2.4	0xc541	No error (0)	dlaj66hdiarg7.cloudfront.net		13.224.193.34	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:30.739943981 CEST	8.8.8.8	192.168.2.4	0xc541	No error (0)	dlaj66hdiarg7.cloudfront.net		13.224.193.31	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:30.739943981 CEST	8.8.8.8	192.168.2.4	0xc541	No error (0)	dlaj66hdiarg7.cloudfront.net		13.224.193.36	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:30.739943981 CEST	8.8.8.8	192.168.2.4	0xc541	No error (0)	dlaj66hdiarg7.cloudfront.net		13.224.193.15	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:31.208677053 CEST	8.8.8.8	192.168.2.4	0x69b5	No error (0)	z.moatads.com	wildcard.moatads.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:18:31.448472977 CEST	8.8.8.8	192.168.2.4	0xf608	No error (0)	scontent-ort2-2.cdninstagram.com		157.240.18.63	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:31.457752943 CEST	8.8.8.8	192.168.2.4	0xb06f	No error (0)	v1.addthisedge.com	v1.addthisedge.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:18:31.493499994 CEST	8.8.8.8	192.168.2.4	0xd4d7	No error (0)	m.addthis.com	m.addthisedge.com		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:18:31.493499994 CEST	8.8.8.8	192.168.2.4	0xd4d7	No error (0)	m.addthisedge.com	ds-m.addthisedge.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:18:32.011054039 CEST	8.8.8.8	192.168.2.4	0x9f3e	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:18:32.011054039 CEST	8.8.8.8	192.168.2.4	0x9f3e	No error (0)	star-mini.c10r.facebook.com		157.240.17.35	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:32.125859022 CEST	8.8.8.8	192.168.2.4	0x1be7	No error (0)	seg.sharethis.com	http-segserver-lb.global.unified-prod.sharethis.net		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:18:32.125859022 CEST	8.8.8.8	192.168.2.4	0x1be7	No error (0)	http-segserver-lb.global.unified-prod.sharethis.net		54.80.205.194	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:32.125859022 CEST	8.8.8.8	192.168.2.4	0x1be7	No error (0)	http-segserver-lb.global.unified-prod.sharethis.net		52.204.22.107	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:32.125859022 CEST	8.8.8.8	192.168.2.4	0x1be7	No error (0)	http-segserver-lb.global.unified-prod.sharethis.net		3.226.11.123	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:32.542643070 CEST	8.8.8.8	192.168.2.4	0x71dd	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:18:32.542643070 CEST	8.8.8.8	192.168.2.4	0x71dd	No error (0)	stats.l.doubleclick.net		74.125.140.157	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:32.542643070 CEST	8.8.8.8	192.168.2.4	0x71dd	No error (0)	stats.l.doubleclick.net		74.125.140.154	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:32.542643070 CEST	8.8.8.8	192.168.2.4	0x71dd	No error (0)	stats.l.doubleclick.net		74.125.140.156	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:32.542643070 CEST	8.8.8.8	192.168.2.4	0x71dd	No error (0)	stats.l.doubleclick.net		74.125.140.155	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:33.137324095 CEST	8.8.8.8	192.168.2.4	0x984e	No error (0)	l.sharethis.com	httplogserver-lb.global.unified-prod.sharethis.net		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:18:33.137324095 CEST	8.8.8.8	192.168.2.4	0x984e	No error (0)	httplogserver-lb.global.unified-prod.sharethis.net		52.29.0.64	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:33.137324095 CEST	8.8.8.8	192.168.2.4	0x984e	No error (0)	httplogserver-lb.global.unified-prod.sharethis.net		52.58.221.124	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 22, 2021 18:18:33.137324095 CEST	8.8.8.8	192.168.2.4	0x984e	No error (0)	httplogserver-lb.global.unified-prod.sharethis.net		18.198.109.212	A (IP address)	IN (0x0001)
Jun 22, 2021 18:18:43.825768948 CEST	8.8.8.8	192.168.2.4	0x5a15	No error (0)	www.duplicolor.com		151.101.66.159	A (IP address)	IN (0x0001)
Jun 22, 2021 18:19:03.892319918 CEST	8.8.8.8	192.168.2.4	0x6da	No error (0)	l.sharethis.mgr.consensu.org		3.124.55.148	A (IP address)	IN (0x0001)
Jun 22, 2021 18:19:03.892319918 CEST	8.8.8.8	192.168.2.4	0x6da	No error (0)	l.sharethis.mgr.consensu.org		3.122.221.110	A (IP address)	IN (0x0001)
Jun 22, 2021 18:19:03.892319918 CEST	8.8.8.8	192.168.2.4	0x6da	No error (0)	l.sharethis.mgr.consensu.org		18.194.206.135	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- duplicolor.com

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 6700 Parent PID: 800

General

Start time:	18:18:24
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:	0x7ff74ccb0000
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: 6796 Parent PID: 6700

General

Start time:	18:18:25
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:6700 CREDAT:17410 /prefetch:2
Imagebase:	0xd80000
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