ID: 385660
Cookbook: browseurl.jbs
Time: 19:40:41
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

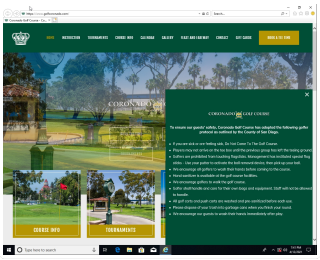
Analysis Report https://www.golfcoronado.com/

Overview

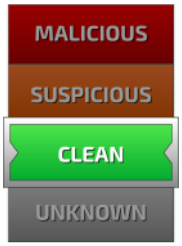
General Information

Sample URL:	http://https://www.golfcoronado.com/
Analysis ID:	385660
Infos:	

Most interesting Screenshot:



Detection

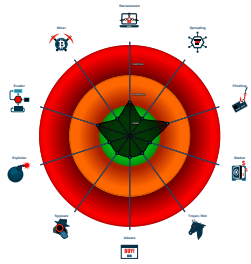


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Contains functionality to access load…
- HTML title does not match URL
- Submit button contains javascript call

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 5624 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6108 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5624 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - AcroRd32.exe (PID: 7108 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' /o /eo /l /b /ac /id 6108 MD5: B969CF0C7B2C443A99034881E8C8740A)
      - AcroRd32.exe (PID: 6172 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 /o /eo /l /b /ac /id 6108 MD5: B969CF0C7B2C443A99034881E8C8740A)
- **cleanup**

Malware Configuration

No configs have been found

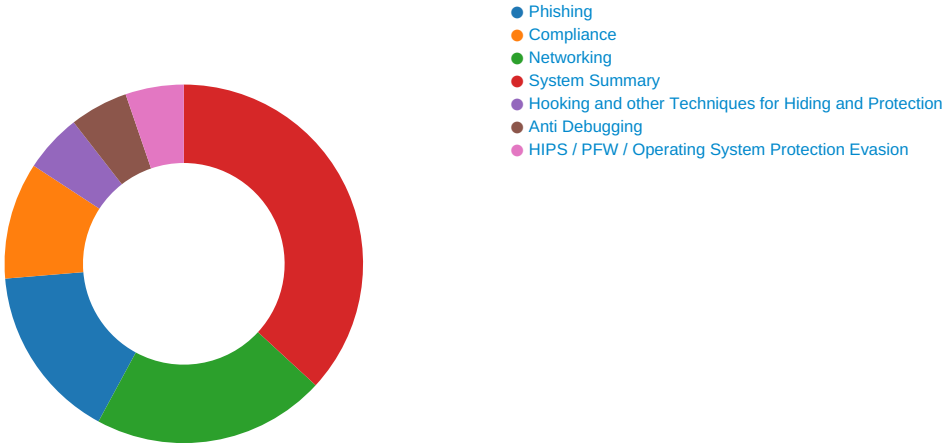
Yara Overview

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

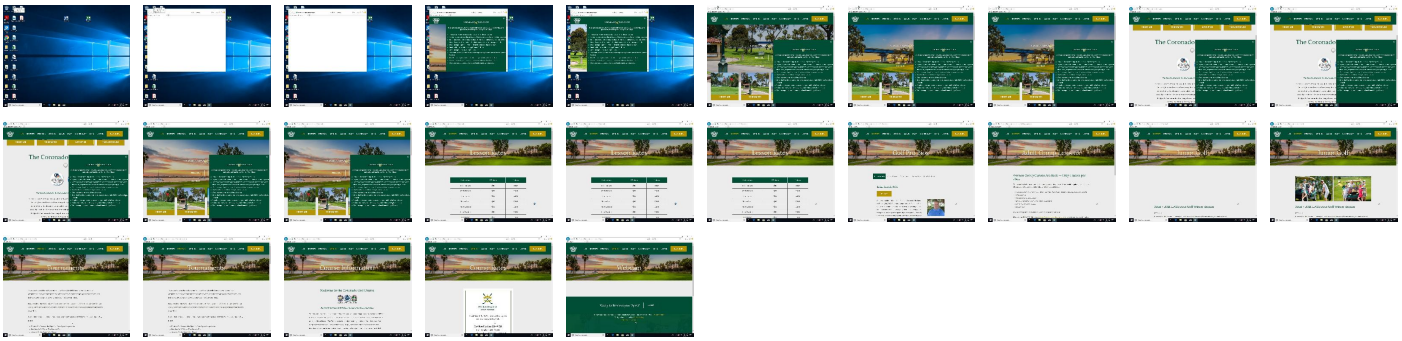
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Scripting 1	Path Interception	Process Injection 2	Masquerading 1	OS Credential Dumping	Process 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	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 2	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Scripting 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

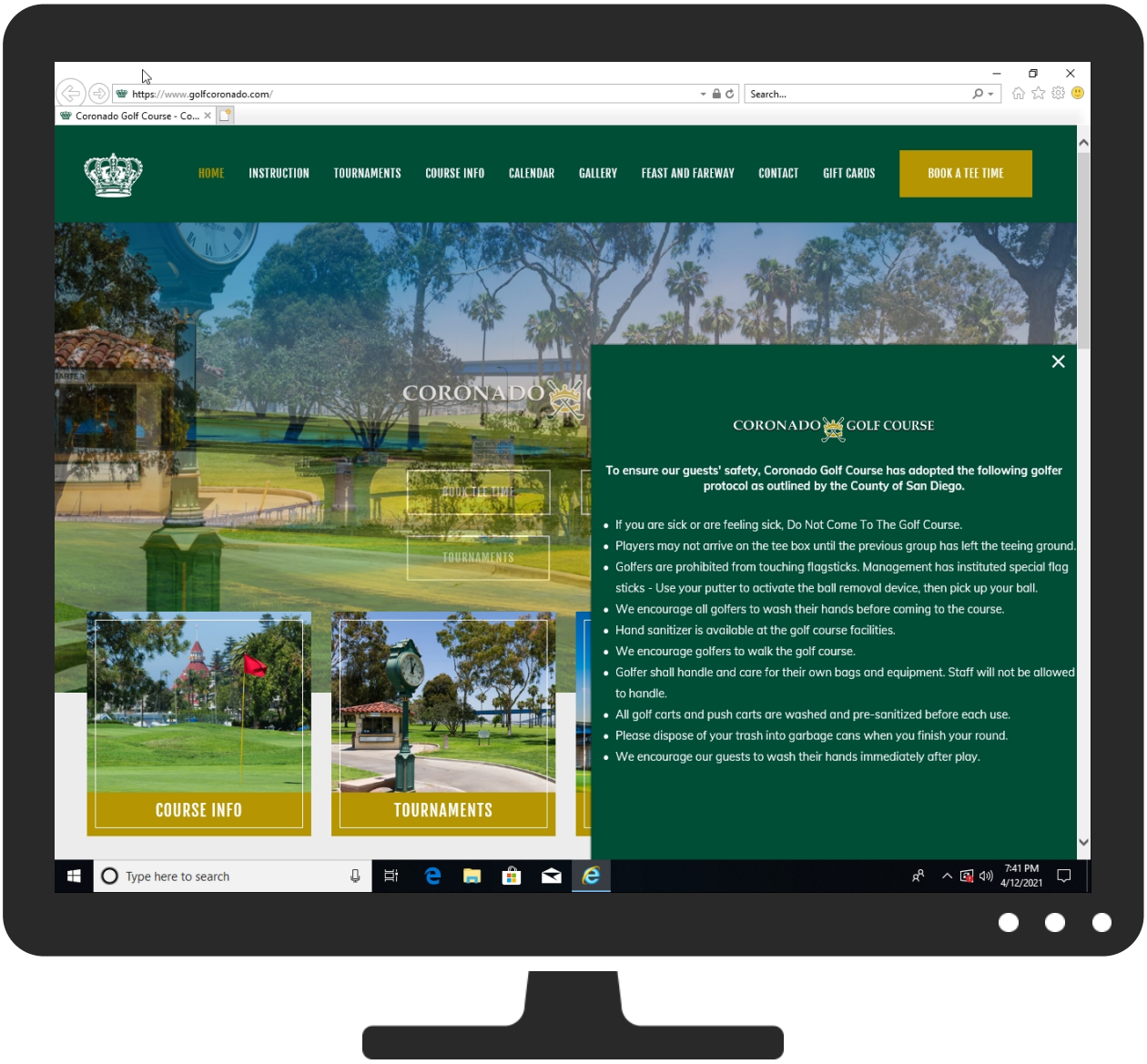
Behavior Graph

Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://www.golfcoronado.com/	1%	Virustotal		Browse
http://https://www.golfcoronado.com/	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
campaignpilot.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://www.smarterlessons.com/	0%	Virustotal		Browse
http://https://www.smarterlessons.com/	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://www.golfsandiego.com/welcome-coronado-golfers?utm_source=CoronadoGC_website&utm_medium=l	0%	Avira URL Cloud	safe	
http://https://www.golfcoronado.	0%	Avira URL Cloud	safe	
http://www.sdjuniorclub.com)	0%	Avira URL Cloud	safe	
http://https://campaignpilot.com/plugins/campaignpilot.js	0%	Avira URL Cloud	safe	
http://kevin.vanzonneveld.net	0%	Avira URL Cloud	safe	
http://https://feastandfarewaycoronado.com/	0%	Avira URL Cloud	safe	
http://www.girlsgolf.org	0%	Avira URL Cloud	safe	
http://https://www.golfsandiego.com/welcome-coronado-golfers?utm_source=CoronadoGC_website&utm_medium=link&	0%	Avira URL Cloud	safe	
http://https://www.golfcoronado.Root	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://kevin.vanzonneveld.net)	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
demo.1-2-1marketing.com	69.167.161.119	true	false		high
campaignpilot.com	13.32.25.34	true	false	• 0%, Virustotal, Browse	unknown
golfcoronado.com	69.167.161.101	true	false		high
www.golfcoronado.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.golfsandiego.com/welcome-coronado-golfers?utm_source=CoronadoGC_website&utm_medium=link&utm_campaign=CoronadoGC_referrals	false		unknown
http://https://www.golfcoronado.com/	false		high
http://https://www.golfcoronado.com/course-info/webcam	false		high
http://https://www.golfcoronado.com/instruction/lesson-rates	false		high
http://https://www.golfcoronado.com/course-info/rates	false		high
http://https://www.golfcoronado.com/instruction/junior-golf	false		high
http://https://www.golfcoronado.com/#tm-top-a	false		high
http://https://www.golfcoronado.com/instruction/golf-pro-bios	false		high
http://https://www.golfcoronado.com/course-info/course-information	false		high
http://https://www.golfcoronado.com/tournaments	false		high
http://https://www.golfcoronado.com/instruction/adult-group-lessons	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.golfcoronado.com/FCoronado	{BCC0B376-9C01-11EB-90E5-ECF4BB2D2496}.dat.2.dr	false		high
http://www.apache.org/licenses/LICENSE-2.0.txt	bootstrap.min[1].js.3.dr	false		high
http://www.golfchannel.com/media?guid=9VqDBlqa25FOw9wVpJgZYptJ_R_tRmh2	622COIJN.htm.3.dr	false		high
http://https://www.smarterlessons.com/	adult-group-lessons[1].htm.3.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://www.golfcoronado.com/instruction/adult-group-lessonsF	~DF9BE3C77B1405F18B.TMP.2.dr	false		high
http://https://www.golfcoronado.com/instruction/golf-pro-bios	~DF9BE3C77B1405F18B.TMP.2.dr, golf-pro-bios[1].htm.3.dr	false		high
http://https://www.golfcoronado.com/instruction/lesson-rates	~DF9BE3C77B1405F18B.TMP.2.dr, lesson-rates[1].htm.3.dr	false		high
http://https://www.golfcoronado.com/course-info/webcam	~DF9BE3C77B1405F18B.TMP.2.dr	false		high
http://https://www.golfsandiego.com/welcome-coronado-golfers?utm_source=CoronadoGC_website&utm_medium=l	course-information[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.golfcoronado.com/course-info/course-information$Course	~DF9BE3C77B1405F18B.TMP.2.dr	false		high
http://www.getuikit.com	uikit2-2143e9f4[1].js.3.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.golfcoronado.com/Root	{BCC0B376-9C01-11EB-90E5-ECF4BB2D2496}.dat.2.dr	false		high
http://https://www.golfcoronado.com/course-info/webcaminformation~	~DF9BE3C77B1405F18B.TMP.2.dr	false		high
http://https://www.golfcoronado.	{BCC0B376-9C01-11EB-90E5-ECF4BB2D2496}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.golfcoronado.com	webcam[1].htm.3.dr	false		high
http://https://www.golfcoronado.com/tournaments	~DF9BE3C77B1405F18B.TMP.2.dr	false		high
http://https://www.golfcoronado.com/instruction/junior-golfessons	~DF9BE3C77B1405F18B.TMP.2.dr	false		high
http://developer.yahoo.net/yui/license.txt	calendar[1].css.3.dr	false		high
http://https://www.golfcoronado.com/media/com_acymailing/css/module_default.css?v=1573072179	622COIJN.htm.3.dr	false		high
http://www.gnu.org/licenses/gpl-2.0.html	jcemediabox.min[1].js.3.dr	false		high
http://https://www.golfcoronado.com/course-info/webcaminformations	~DF9BE3C77B1405F18B.TMP.2.dr	false		high
http://https://www.golfcoronado.com/	~DF9BE3C77B1405F18B.TMP.2.dr, {BCC0B376-9C01-11EB-90E5-ECF4BB2D2496}.dat.2.dr	false		high
http://www.sdjuniorclub.com)	PGA-Profile-Coronado[1].pdf.3.dr	false	• Avira URL Cloud: safe	low
http://https://campaignpilot.com/plugins/campaignpilot.js	622COIJN.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://www.golfcoronado.com/25-uncategorized/17-welcome	622COIJN.htm.3.dr	false		high
http://https://www.golfcoronado.com/templates/yoo_avanti/favicon.ico~	imagestore.dat.3.dr	false		high
http://twitter.com/share	social[1].js.3.dr	false		high
http://www.yootheme.com/license)	bootstrap[1].css.3.dr	false		high
http://https://stats.g.doubleclick.net/j/collect	analytics[1].js.3.dr	false		high
http://https://www.golfcoronado.com/course-info/rates	~DF9BE3C77B1405F18B.TMP.2.dr	false		high
http://kevin.vanzonneveld.net	script[1].js0.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.golfcoronado.com/tm-top-a.com/#tm-top-a	~DF9BE3C77B1405F18B.TMP.2.dr	false		high
http://https://www.golfcoronado.com/tournamentsunior-golfessonsr	~DF9BE3C77B1405F18B.TMP.2.dr	false		high
http://www.1-2-1marketing.com	webcam[1].htm.3.dr	false		high
http://www.apache.org/licenses/LICENSE-2.0	KFOmCnqEu92Fr1Mu4mxP[1].ttf.3.dr, KFOlCnqEu92Fr1MmEU9fBBc9[1].ttf.3.dr, KFOlCnqEu92Fr1MmYUtfBBc9[1].ttf.3.dr	false		high
http://https://www.golfcoronado.com/instruction/adult-group-lessons&Adult	~DF9BE3C77B1405F18B.TMP.2.dr	false		high
http://https://feastandfarewaycoronado.com/	622COIJN.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://www.girlsgolf.org	junior-golf[1].htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.golfcoronado.com/course-info/ratesinformation	~DF9BE3C77B1405F18B.TMP.2.dr	false		high
http://https://www.golfcoronado.com/#tm-top-a	~DF9BE3C77B1405F18B.TMP.2.dr	false		high
http://https://www.golfsandiego.com/welcome-coronado-golfers?utm_source=CoronadoGC_website&utm_medium=link&	622COIJN.htm.3.dr, ~DF9BE3C77B1405F18B.TMP.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.dreamstime.com/stock-images-kids-golf-competition-children-playing-taking-part-course-sum	junior_golf[1].jpg.3.dr	false		high
http://https://www.golfcoronado.Root	{BCC0B376-9C01-11EB-90E5-ECF4BB2D2496}.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.joomlacontenteditor.net	jcemediabox.min[1].js.3.dr	false		high
http://https://www.golfcoronado.com/instruction/adult-group-lessons	~DF9BE3C77B1405F18B.TMP.2.dr	false		high
http://https://www.golfcoronado.com/course-info/webcaminformation	~DF9BE3C77B1405F18B.TMP.2.dr	false		high
http://https://www.golfcoronado.com/instruction/junior-golf	~DF9BE3C77B1405F18B.TMP.2.dr	false		high
http://https://www.golfcoronado.com/course-info/course-information	~DF9BE3C77B1405F18B.TMP.2.dr	false		high
http://www.gnu.org/licenses/gpl-3.0.html	acymailing_module[1].js.3.dr	false		high
http://https://www.golfcoronado.com/images/PGA-Profile-Coronado.pdf	~DF9BE3C77B1405F18B.TMP.2.dr	false		high
http://www.dreamstime.com/royalty-free-stock-photos-kids-golf-competition-children-posing-near-car-c	juniors[1].jpg.3.dr	false		high
http://https://www.google.%/ads/ga-audiences	analytics[1].js.3.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://kevin.vanzonneveld.net)	script[1].js0.3.dr	false	• Avira URL Cloud: safe	low
http://https://www.golfcoronado.com/tournamentsunior-golfessons	~DF9BE3C77B1405F18B.TMP.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.gnu.org/licenses/gpl.html	social[1].js.3.dr	false		high
http:// https://www.golfcoronado.com/media/com_acymailing/js/acymailing_module.js?v=51010	622COIJN.htm.3.dr	false		high
http://https://www.golfcoronado.com/tm-top-a	~DF9BE3C77B1405F18B.TMP.2.dr	false		high
http://https://ims-na1.adobelogin.com	AcroRd32.exe, 00000008.00000003.408522785.0000000009502000.00000004.00000001.sdmp	false		high
http://developer.yahoo.com/yui/license.html	calendar[1].js.3.dr	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
69.167.161.101	golfcoronado.com	United States		32244	LIQUIDWEBUS	false
13.32.25.34	campaignpilot.com	United States		7018	ATT-INTERNET4US	false
69.167.161.119	demo.1-2-1marketing.com	United States		32244	LIQUIDWEBUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385660
Start date:	12.04.2021
Start time:	19:40:41
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://www.golfcoronado.com/
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211

Number of analysed new started processes analysed:	15
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean1.win@7/126@4/3
EGA Information:	• Successful, ratio: 100%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://www.golfcoronado.com/#tm-top-a • Browsing link: https://www.golfcoronado.com/ • Browsing link: https://www.golfcoronado.com/instruction/lesson-rates • Browsing link: https://www.golfcoronado.com/instruction/golf-pro-bios • Browsing link: https://www.golfcoronado.com/instruction/adult-group-lessons • Browsing link: https://www.golfcoronado.com/instruction/junior-golf • Browsing link: https://www.golfcoronado.com/tournaments • Browsing link: https://www.golfcoronado.com/course-info/course-information • Browsing link: https://www.golfcoronado.com/course-info/rates • Browsing link: https://www.golfcoronado.com/course-info/webcam • Browsing link: https://www.golfsandiego.com/welcome-coronado-golfers?utm_source=CoronadoGC_website&utm_medium=link&utm_campaign=CoronadoGC_referrals

Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 52.147.198.201, 92.122.145.220, 168.61.161.212, 88.221.62.148, 13.64.90.137, 172.217.168.68, 216.58.215.227, 172.217.168.74, 172.217.168.3, 172.217.23.110, 2.23.155.241, 2.23.155.184, 104.43.139.144, 152.199.19.161, 20.82.210.154, 2.20.142.209, 2.20.142.210, 92.122.213.194, 92.122.213.247 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, 2-01-3cf7-0009.cdx.cedexis.net, store-images.s-microsoft.com-c.edgekey.net, a767.dspw65.akamai.net, wu-fg-shim.trafficmanager.net, a1449.dscg2.akamai.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, e12564.dspb.akamaiedge.net, go.microsoft.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, www.google.com, arc.trafficmanager.net, watson.telemetry.microsoft.com, www.gstatic.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, www.google-analytics.com, www.bing.com, skypedataprdcolwus17.cloudapp.net, fonts.googleapis.com, www-google-analytics.l.google.com, dual-a-0001.a-msedge.net, fonts.gstatic.com, ie9comview.vo.msecnd.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, download.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, download.windowsupdate.com.edgesuite.net, skypedataprdcoleus16.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, cs9.wpc.v0cdn.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found.

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\UM9GSJ8J\www.google[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	95
Entropy (8bit):	4.968664724768266
Encrypted:	false
SSDEEP:	3:D9yRtFwsW+pEeAq2XJgjR3SaRM9qSQcj/K9LKb:JUFy+pEeAq2583SeMlQsLb
MD5:	933C23F84AE4F512133135CD1679D1DF
SHA1:	9DE2BDEF1E749B3DC8A175B3DC9B848DFA8AC260
SHA-256:	18049AB849912D978067F5B4505D4CD8DD576560980A8C370D52EDEFD7EAD434
SHA-512:	96C03C89451F2C8A41F19389AFF38909E4B64D6E05C24AE839E1619F868C4B3ADB83A8E8EE6D9B17F32F963BAEAE387A507E14A5A4B6F876CDF82DFBDA80FF3 6
Malicious:	false
Reputation:	low
Preview:	<root><item name="rc::a" value="cDB2NzFreXpmbnE2" ltime="2195105632" htime="30879758" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{BCC0B374-9C01-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.849048074490619
Encrypted:	false
SSDEEP:	96:rlZKZA2tWdtcAfkiu1MImTagRx+fzizlX:rlZKZA2tWdtffkRMRbMfzcX
MD5:	E33C0857A68197BFD79BF9E3ED32842D
SHA1:	63B69F0B2BD2C776582515082F6EBD868B6B310B
SHA-256:	5D7AD39FBC606ECDDDD714345DD423E4E3E7F923383BC1E1E6AA1B30F2A62046
SHA-512:	EEA0E117FE8BFA1CBBC1D555ABA6CAC470876E46C5186FAAACA1F2E90FB3D98F46DC2330199783B3359662132BA8D553EC609DE02BC7485CF8D73A1BBC2E4 8D
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\{BCC0B376-9C01-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	202650
Entropy (8bit):	2.770464395214044
Encrypted:	false
SSDEEP:	768:YvuxGsvuxkGvzrARwgNC7vU0zfI+9wvUibdHdoUhyrNEnKiK:Yvu7vuXY5CrNEnVK
MD5:	CDF4D0079008A64690F1B114187401F6
SHA1:	41FEB78DEFEC6ACFC91CB3843922B4BBB0399CB8
SHA-256:	357A5FA774CD2F0881AE65596D6C1FF5794BEF4166300889B7487CF4E8C43858
SHA-512:	8182279B63F4EEA4521C58DFF9C874097969F8BBB905F86A3EFBB820CD1E7C527F9EED331D5F89FBA5D0A62C5818016363C89362FCD944ABCFADA13575B85BC 7
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{BCC0B376-9C01-11EB-90E5-ECF4BB2D2496}.dat	
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{C4144EC6-9C01-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5637994953145242
Encrypted:	false
SSDEEP:	48:Iw4GcprRGwpaCG4pQGGrapbS0TGQpKtG7HpRgITGIpG:rMZLQy6IBS0tAMTrA
MD5:	4877FCEFE6ACDC4ED97C9CFDC74E69E8
SHA1:	B2FCA047F4A460F3D408D8BB287C4B66542ACC2A
SHA-256:	C0E370AD9FCE3EFB497477FD808A8DBD432C0209163B5C59B766913E5659627C
SHA-512:	26AB35B2CDEC5C30A667A27F0C9F83CAFBDEEEA3859763A557AFD68F632F54727E40AC319BF33A7BAF7CD0BEF1B4CD7E53888BEFC9219E0CA7C1476543065 B1
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\wlm7n14\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	2.9387551882676055
Encrypted:	false
SSDEEP:	12:2Lg0lYp+xp7plOQHtg/ITCv8BFfmMPDL5ERBy6XQj+TImx0pQwKmz5TpD5v0:20TsxxO6ttCExB6gjsIAwP0
MD5:	A33AC91B4C2EF6B01F639F3EE6786BBC
SHA1:	5C68FF5B2EB9528E618755413F7E4355A0DBE41F
SHA-256:	744C0244DF12251B2B97455A5945A7B7FD30CC04F16C0F92FC959E0C8EB83327
SHA-512:	A760268CEEB9B2561ABAD69C9B77B50B57F7B5A02B21C15AEDD165CC385FB7C3215D10FE6ADDDFAACFAF840F1FE2841E839E71BEE203D803083D0B0440732F F5
Malicious:	false
Reputation:	low
Preview:	=.h.t.t.p.s.:././.w.w.w...g.o.l.f.c.o.r.o.n.a.d.o...c.o.m./.t.e.m.p.l.a.t.e.s./.y.o.o._.a.v.a.n.t.i./.f.a.v.i.c.o.n...i.c.o.~..... .h.....(..... ....6N.L6N..6N..6N..6N..6N..6N..6N..6N...,.....6N. P6N..6N.y6N..6N..6N..6N..6N.... .....6N..6N..6N.v6N.\6N.66N.V6N.r6N.j6N..6N.O.....6N.c6N..6N..6N.g6N..6N..6N..6N.w6N..6N.Z6N.3..... 6N.%6N..6N..6N.a6N..6N..6N.=6N..6N..6N..6N.\6N..6N.....6N..6N..6N..6N..6N..6N..6N..6N..6N..6N..6N..6N.....,6N.....6N..6N..6N..6N..6N..6N..6N.s6N ..6N..6N.36N.....6N.....6N.^6N.....36N..6N.x...D6N.'6N..6N.@...>6N.....6N.S6N..6N..6N..6N..6N.|6N..6N..6N..6N..6N.o6N..6N.'.....C...1...6...:6N..6N..... ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\7Aulp_0qiz-aVz7u3PJLcUMYOFnOkEk30e4[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20644, version 1.1
Category:	downloaded
Size (bytes):	20644
Entropy (8bit):	7.974584602073737
Encrypted:	false
SSDEEP:	384:K8Jjwpsv+ttgJpnjJmZ5tgpvVyrfJFkW7l0dcxBIcGYnB7zo5mqmK:Pwsv+tty5jJmZredydFdigejSm5ms
MD5:	91288B87B7BBE6D6FBFB131D5DBACBF1
SHA1:	E8D1EE39BBDF5DEA50861488704490C66CFC602A
SHA-256:	0A34DA75A521DA237A12876684AC11B2C21D9B8D47FB9E9DEEAA998FB98324E1
SHA-512:	767EF9CA0344FEAA444DCA0C48624AA85530F94199563D3CB7851823535CEE9FF1D540A9830D19F0398345E6E138F49075253CD325106143223C3C366109406E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/muli/v22/7Aulp_0qiz-aVz7u3PJLcUMYOFnOkEk30e4.woff

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\7Aulp_0qiz-aVz7u3PJLcUMYOFnOkEk30e4[1].woff	
Preview:	wOFF.....P.....GDEF.....>...R.W..GPOS.....u.GSUB.....c....~.J.OS/2.....O...`aR..STAT...8...8...D...cmap...p.....G.e.cvt ... ...O.....)..fpgm...p..... 6..gasp...4.....glyf...<..6...f|+...head..J@...6...6..Ymhhea..Jx... ...$....hmtx..J.....0..0<loca..L.....t.maxp..N.... ... .m..name..N....0...X8.Y.post..O..... ...2prep..O.....' Dn.x.....P.F..~R..*....i...[..u..t..L.!...q..../w\|..Z*.....x.V...G.}>_....[.3s.%Q.Q.r+(..Kb(...23.q....r8..k...f-..z...Z.7.\|.;....i.....Z.\s.-...._x.]h.!R...?..S..@83.b....t.....M.2...Wc 5.q'.....p.;9..ql....Y.:w.F....Kq].".@2O.....$.Q...4?..j..3...G.....oDg....)K.H.... "$eU..'.\..c5...Eh.. ....c...b1.g...a...y...~]Y..._n...I,.,.~Pf.....%.,..{Y..~....>@47...1.5.....y..cZV.....x.N R..8...E...~.,.+..X.....p.....?.....q.T....r...v.....iS/s, .V-b.'..f.i....b.31.....{..T.eQ.<.p...e.=.aYs.....V<..')Z.S.i..?.....b...0...Y....PC..Z.|17./._..|.v

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\PGA-Profile-Coronado[1].pdf	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PDF document, version 1.3
Category:	downloaded
Size (bytes):	26560
Entropy (8bit):	7.839810594327402
Encrypted:	false
SSDEEP:	768:nK5yL/SWcTT+auTNV1acmo1oTskgglM/Q:hcTT+zTnTm2oTsaIQ
MD5:	2F5657E68F2228140BD5CA6391EED062
SHA1:	8DD09B9DD53E8B5B726B7EBA6E981E4C02D45A60
SHA-256:	F43EF967D5C93C7F767FC14B487C00D563E26DB8A675971BED65562C138339A2
SHA-512:	378C2E44E8D59077FB33FDD0929CC8EE40114C104F42D847A6C4FCE72ECD7EEB026FC1071C067CBC30E1E8DE5A510DBBC5C2E7F2701AA59BA6AC6E159DC2 22C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.golfcoronado.com/images/PGA-Profile-Coronado.pdf
Preview:	%PDF-1.3.%.....4 0 obj.<< /Length 5 0 R /Filter /FlateDecode >>.stream.x.....x..*..S...?.7Jb.q.)d...B.%.H.-..[....,.....K^....;.ht.>.h`Fo.S....y3.....k.....6..v....0^.>.zx.9.. ...6.+.w..c.....~..f8....s.....pl.7.....=>.Dw..b.....A..'...q...~a7..?m..._`.j.5....._.l.....4....k..j.....nu.{..6.i.s...+...4..2LN|..`.+.v.%.....K.{fyf.GN....."N3....${..t8.n.moq.;.c.X@7..o..G ..R....]..h8[5..\|e.:$..>Z...Q.]....j:...mV../.g_.'..rt9j.E....i.#...6f.u .F_w....3pl."[..w9hG.@.@4_.!....x8ZL=l...]..h.Mn.Dz.KF.... (..WB.'..;..M.....L..D`=. .{.$..=.].wD.;..8&)m...8.tQ.... D%!]H.....Q..r.....N.....h.;.p.N.....qe...J.....`"`.1..`.....d.`.Q...)4g.+.qM.r.....0....w.K.2V.#...~.K.....}.G..%.....e../...a.q./../....ujM...:"e]*...J#...b....!...?..y.%..G0F.&lc..(..y.Ad. .E..GdH..Fq...e..9..%...Z.nA.6..Y...-w.~..4.aX.`'.....,..T.P#.h..0.....DX|....`.U....q..:)KP.t."p.1F{...H.y. Z.!.i,..e./....r1.B.F!t.r<"..6>2.g.v.~.gY/e..F...>..f

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\Yq6R-LCAWCX3-6Ky7FAFrOF6lA[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 19976, version 1.1
Category:	downloaded
Size (bytes):	19976
Entropy (8bit):	7.978781526932054
Encrypted:	false
SSDEEP:	384:zzHQzdoue/1WVfLUISyJdSE4QVJx9cP5bw7L2qZzKTaiqiD5:zzHQzdxe/cVDUAdSkLcBw7L9OH9
MD5:	7710E53EE1E24055DD9BA499766CBF2A
SHA1:	84B6D697B33EBFBDC7E7892D1B51FEC3CC3AF64B
SHA-256:	DA9B29CAD35666AD35DF54FC721FF8D0838660640456185A86521E6C506B81CD
SHA-512:	5376CDD97C2E42C56CA7034CF8ABB12685F3DE5242FAE16D10C87339BB2C896281426946 62C35F64E7118AE1BD06BE53EA7A03820DD4799030DCE8CA3F28B74
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/fjallaone/v8/Yq6R-LCAWCX3-6Ky7FAFrOF6lA.woff
Preview:	wOFF.....N.....w.....GSUB...X.....A.J.OS/2.....W...`\[..cmap...<.....L..8..cvt .....'.....fpgm.....b....gasp.....glyf.....=_.._.....head..F0...4...6....hhea.. Fd.....$.Z..hmtx..F....f....N)O.loca..H.....l.%maxp..J.... ... ....name..J.....+.Ecpost..K.....D.~\|prep..Mx.....".x.E....Q.E..}.....B...( ..(1B...P..A.Y...`<.^.....Sau..(..mK...?. ..>.2S'....%.[!...)i.#0../...&..W.)..S.....t.....W....`...\...x.c`f..8.....u..1...<.f.....X.....^.P.....$.....C...P..$...H)0.....x.e.3.]....yX.....m.m.m....m..z.F.....o.pn.....E(K.Z.d.n.~.w.? H...)..A.`}..?_....,~5.....<...'."....<...Nln,mlmlal.m..?.....k..j.....rJ.]M.T..^..w.A..VFY.T....Ee..7..A...A*..O~.QZ.|/Nf..B...PK=....%.K...I,.?.....c?..._r.U....P...P.I3. VA..m.P.U.s.uw.r.U.LU.)...S.E.w..w.u.yGu..*su0C.K.4.Z..6...I.D7]..Pw..5....5E!.....u4]...2.&..5.:.T..p#...0..3.x+M4I~..V....x.N`}....x.c@.....0....vi.D..3...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\banner_1[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], progressive, precision 8, 2000x835, frames 3
Category:	downloaded
Size (bytes):	450662
Entropy (8bit):	7.968710736617798
Encrypted:	false
SSDEEP:	12288:2xOhnV1L/B1BfQXBRmUxwxW1Q4moERB3fTbt2LFwb8:QS/zpSB1Va4mbXLB2Ls8
MD5:	F5428635C480B8C986D17DA23FB93731
SHA1:	A9736B525B850860F4A198CC8899E9866CBB5C08
SHA-256:	4A2B14DAEACA298DA356826D9B9ABD19DA688AA8A1E1BA7D440D36BE0BF67C2C
SHA-512:	2A93442C03F2AC67145F736F51B0A9A147C7568C90BF443E6FF7DBA099E3A94AB782249E9E62336F088B94002A64B028EB91EB00E45DAE8974E91AE80BAE6EDA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.golfcoronado.com/images/slideshows/banner_1.jpg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\banner_1[1].jpg	
Preview:	.....Exif..II*.....Ducky.....P.....)http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c138 79.159824, 2016/09/14-01:09:01 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:DocumentID="xmp.did:0DEFA00293D011E7B3CDEFC761278C6C" xmpMM:InstanceID="xmp.iid:0DEFA00193D011E7B3CDEFC761278C6C" xmp:CreatorTool="Adobe Photoshop CS6 Windows"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:CC1B460B35B211E789CD9895221ECF84" stRef:documentID="xmp.did:CC1B460C35B211E789CD9895221ECF84"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>...&Adobe.d.....@....d.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\banner_button_1[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], progressive, precision 8, 400x400, frames 3
Category:	downloaded
Size (bytes):	100965
Entropy (8bit):	7.986037188492894
Encrypted:	false
SSDEEP:	1536:N440IMz1b9C4K+CeQ405hi5JaEmEYFiyFvyHliNin3CB/AdlOodLlHumoHHCHlj1:NB0L7r04JajEQyHINGC8MoZlO3CFj0Ub
MD5:	DF09C2ED6A97CBB5BE84950C8A598F23
SHA1:	5B3E53538B9B86EDBAE761980A6BBAE241F52A57
SHA-256:	BABD55E9F56A5D5B11CCBDA8A0E6E1D11633CB1D03F14A8755B722BA6D8BE428
SHA-512:	4D4F0D8BAC12D07DBB666621C1AB9DABC90F6D47916B98B54DEBA775F78B93107DE062CA7F5C16B74993F6C65298422843441F0A11D3872A69A542729210A42
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.golfcoronado.com/images/buttons/banner_button_1.jpg
Preview:	.....Exif..II*.....Ducky.....P.....khttp://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c138 79.159824, 2016/09/14-01:09:01 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="4C2B94376B6C90EDA87F0BE99B6823CD" xmpMM:DocumentID="xmp.did:479F466893D011E79513F171DAEEA806" xmpMM:InstanceID="xmp.iid:479F466793D011E79513F171DAEEA806" xmp:CreatorTool="Adobe Photoshop CC 2015 (Windows)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:149D39EC35B311E783CEDC6F0F50EF9C" stRef:documentID="xmp.did:149D39ED35B311E783CEDC6F0F50EF9C"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>...&Adobe.d.....J.....c.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\banner_button_3[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], progressive, precision 8, 400x400, frames 3
Category:	downloaded
Size (bytes):	65433
Entropy (8bit):	7.985340928076223
Encrypted:	false
SSDEEP:	1536:g9WEf/WGZQktLXhtdH/tZUeXm5kbCsKlr:wWGZzPrZUeXm5UChr
MD5:	B18B2B4C4CB99A1E66CB184F827C0282
SHA1:	B932BD4C77EC6BD87A92251B2DFA60C5FEE64F40
SHA-256:	BC701B05296D823978958899F37FCDAD8BA7FDD087F6ECF2243CF8E033E2B94C
SHA-512:	4E424E9DE3187BEEC651CF00D724E8AE0EF09821649A18F3CD3CA1D4E950645F13A16D3FB5016827F6DB8997C728B1CD8823F2BD3366D6DC64C053A00643DBF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.golfcoronado.com/images/buttons/banner_button_3.jpg
Preview:	.....Exif..II*.....Ducky.....P.....khttp://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c138 79.159824, 2016/09/14-01:09:01 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="4C2B94376B6C90EDA87F0BE99B6823CD" xmpMM:DocumentID="xmp.did:76FA314993D011E7AA4596CB3AD4FF3E" xmpMM:InstanceID="xmp.iid:76FA314893D011E7AA4596CB3AD4FF3E" xmp:CreatorTool="Adobe Photoshop CC 2015 (Windows)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:149D39EC35B311E783CEDC6F0F50EF9C" stRef:documentID="xmp.did:149D39ED35B311E783CEDC6F0F50EF9C"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>...&Adobe.d.....:7..b1.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\banner_button_4[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], progressive, precision 8, 400x400, frames 3
Category:	downloaded
Size (bytes):	110229
Entropy (8bit):	7.98817560765378
Encrypted:	false
SSDEEP:	3072:h0DdISGzp75xzcDtP+Gw5nGy/JvLkWexX2a:4hy0XCtYWelL
MD5:	7D71D98EA0AF9D22228CE07BCAA1DCB1
SHA1:	1BC40949742441FFCF8684E0C2632E2F9E9F4222
SHA-256:	85F3206BC7BC8440F59819A9F2F36A991925CB48032E90FDB083E4478C7BF82C
SHA-512:	BB9B46A74A5A5E3072FEFC7B0EF1CADD3AF428FBE6728E64269316857A989EF23D73E6734444C8B6C9CADE90CDBCA6A6B19C4862361CCE6AB8707A6A27E8F8D8
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\banner_button_4[1].jpg	
Reputation:	low
IE Cache URL:	http://https://www.golfcoronado.com/images/buttons/banner_button_4.jpg
Preview:	.....Exif..II*.....Ducky.....P.....khttp://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c138 79.159824, 2016/09/14-01:09:01 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="4C2B94376B6C90EDA87F0BE99B6823CD" xmpMM:DocumentID="xmp.did:9601DFB293D011E799CAC457CBCD52FF" xmpMM:InstanceID="xmp.iid:9601DFB193D011E799CAC457CBCD52FF" xmp:CreatorTool="Adobe Photoshop CC 2015 (Windows)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:149D39EC35B311E783CEDC6F0F50EF9C" stRef:documentID="xmp.did:149D39ED35B311E783CEDC6F0F50EF9C"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>...&Adobe.d.....YH...I.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\calendar[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	108024
Entropy (8bit):	5.66356166242494
Encrypted:	false
SSDEEP:	1536:t4LoDrJeVT5QJ03JjZMI8F3pOLI14/yVV6MWKJTjlh5wOYHx5Cpi7hY5k5s5lW5b:tGMEyJ03JV8p1HWSiEfYI+Ryc
MD5:	9A324D28D9904FCCE62478C3DE19FFC3
SHA1:	8381F14112706B6C003D7F50F5D57FE9F6E13B55
SHA-256:	8F441F14EDC55A96007732EE8BA5246B656051428C96CF9D8D7D5F0A5499E238
SHA-512:	C320E0B2F4009D87FF0D47ED31D7A2CED37823DA4BB4624CAC24E1F0EE3D1BF1E93BD0A1517272865F17FF830A7F4888201331067C5FADA86EBA2CA6CBAFA108
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.golfcoronado.com/media/com_rsform/js/calendar/calendar.js
Preview:	/*..Copyright (c) 2010, Yahoo! Inc. All rights reserved...Code licensed under the BSD License:...http://developer.yahoo.com/yui/license.html..version: 2.8.1..*/../* yahoo */..if(typeof rsf_CALENDAR=="undefined"||!rsf_CALENDAR){var rsf_CALENDAR={};}rsf_CALENDAR.namespace=function(){var A=arguments,E=null,C,B,D;for(C=0;C<A.length;C=C+1){D=(""+A[C]).split(".");E=rsf_CALENDAR;for(B=(D[0]=="rsf_CALENDAR")?1:0;B<D.length;B=B+1){E[D[B]]=E[D[B]]||{};E=E[D[B]];}}return E;};rsf_CALENDAR.log=function(D,A,C){var B=rsf_CALENDAR.widget.Logger;if(B&&B.log){return B.log(D,A,C);}else{return false;}};rsf_CALENDAR.register=function(A,E,D){var I=rsf_CALENDAR.env.modules,B,H,G,F,C;if(!I[A]){I[A]={versions:[],builds:[]};}B=I[A];H=D.version;G=D.build;F=rsf_CALENDAR.env.listeners;B.name=A;B.version=H;B.build=G;B.versions.push(H);B.builds.push(G);B.mainClass=E;for(C=0;C<F.length;C=C+1){F[C](B);}if(E){E.VERSION=H;E.BUILD=G;}else{rsf_CALENDAR.log("mainClass is undefined for module "+A,"warn");}};rsf_CALENDAR.env=

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\city-of-coronado-logo[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 300 x 300, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	64638
Entropy (8bit):	**7.9919571539830585**
Encrypted:	**true**
SSDEEP:	1536:xntfLAGd9RBO+DTBhcbVXTEAu0Oqw1tUgbPuLP7X:xxcuDBO2MVfu0OqwdbUX
MD5:	AF6CB4E3136F416712D32B9079DF8984
SHA1:	AB9E3D6D6BCF39B373F6DB2638D53A7D4506484D
SHA-256:	BDCA68C79BA53EB1701DC54AC3B1487809E2D4D52757FDB9D7B6DAF5EFBEBE8B
SHA-512:	3AEB1914D4740F00A39C040BAFB380096BAD28B7F1240796E44AA7F77C2C5BC3E12FFE61236703762DE779992650B087D273E720DCAAD7888E1517B9B7B569DA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.golfcoronado.com/images/city-of-coronado-logo.png
Preview:	.PNG.....IHDR...,...,.....y}.u....tEXtSoftware.Adobe ImageReadyq.e<...qiTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c138 79.159824, 2016/09/14-01:09:01 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpRights="http://ns.adobe.com/xap/1.0/rights/" 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/" xmpRights:Marked="False" xmpMM:DocumentID="xmp.did:1CF87073F7D511E7BECA9A803D038AE8" xmpMM:InstanceID="xmp.iid:1CF87072F7D511E7BECA9A803D038AE8" xmp:CreatorTool="Adobe Photoshop CS3 Macintosh"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:D21ACABCA2C511E79337E2265B622999" stRef:documentID="xmp.did:D21ACABDA2C511E79337E2265B622999"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>Q.#.....IDATx..].xSe.>7.^P.e.2d....(..7.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\custom[1].js	
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):	261
Entropy (8bit):	3.130989878227667
Encrypted:	false
SSDEEP:	3:3FmOmDDxOcobLC9xBCyBKowU1YmDRHSOoXp1TF2ahen:stBobyBKoyyS3LA7
MD5:	5517E5BFB948962C6A5999446BAAF409
SHA1:	7B060B8B4212D8B78E8AFDD65661E1981AD1B368

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\custom[1].js	
SHA-256:	48D481003AE7740D61DE8ED0BE2A090D24F53C9F8A93FEC7411DE403C5BE9163
SHA-512:	072734648BB7E0FD4D0CC524BCA9D9970F06DF3705C66244752D11BFBB11A6BC57BA38543793FE07E76E5722AE6F0D415A2B8A7FD5B1AAC133E1A66DBF3466D5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.golfcoronado.com/templates/yoo_avanti/styles/121/js/custom.js
Preview:	./* Copyright (C) 121 Marketing - 121marketing.com */..../* ========== Custom JS.. ========== */....jQuery(function($) { ....});

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 1 icon, 16x16, 32 bits/pixel
Category:	downloaded
Size (bytes):	1150
Entropy (8bit):	2.6789588132909428
Encrypted:	false
SSDEEP:	12:5Htg/ITCv8BFfmMPDL5ERBy6XQj+TImx0pQwKmz5TpD5n:RttCExB6gjsIAwH
MD5:	6CEFF6449F8F37889351B717609E67D2
SHA1:	C179D1FA5B6111AE45A7E45EDD1E80A0A07892CE
SHA-256:	FDB554EB67AF926326715B9B4D5B1877DD49DFC86386F59966172BE929345247
SHA-512:	2CFECC151940F911544BC0784CE817C9FD2EBA40AA8EEE0097811E955241ECF9EE715FD15E78092CE5F58AEB703F98F425252D76772D2035B08961DD46ECF5A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.golfcoronado.com/templates/yoo_avanti/favicon.ico
Preview:	..... .h.....(..... ....6N.L6N..6N..6N..6N..6N..6N..6N..6N....,.....6N.P6N..6N.y6N..6N..6N..6N..6N.... .....6N..6N..6N.v6N.\6N.66N.V6N.r6N.j6N..6N.O..... ..6N.c6N..6N..6N.g6N..6N..6N..6N.w6N..6N.Z6N.3.....6N.%6N..6N..6N.a6N..6N..6N.=6N..6N..6N..6N.\6N..6N.....6N..6N..6N..6N..6N..6N..6N..6N ..6N..6N..6N..6N..6N.....,6N.....6N..6N..6N..6N..6N..6N..6N.s6N..6N..6N.36N.....6N.....6N.^6N.....36N..6N.x...D6N.'6N..6N.@...>6N.....6N.S6N..6N.. 6N..6N..6N.]6N..6N..6N..6N..6N.o6N..6N.'.....C...1...6...:6N..6N..... ...3.....@.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\fontawesome-webfont[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 89076, version 1.0
Category:	downloaded
Size (bytes):	89076
Entropy (8bit):	**7.995495828866506**
Encrypted:	**true**
SSDEEP:	1536:O6YV8SiMqvSnPBMNxB70dQVZJ8P7X/SsZrXQNcsXepenjLyyox7g31K:OFKSiMLB+/0qZJ8P7PVCvuuIRg31K
MD5:	273F0BB520E37453D185A6EC9E566351
SHA1:	CFD0792239E00B4EFB4FA2383F85CA3F1E3DCDAB
SHA-256:	2411947E1534AB21E31D4E1C6C46214AE93D1A2BA2C643FF620568C585D949B9
SHA-512:	DC4F794208E819329CCF986042C82552FDAA52B8B1C6D6A53B32AD240B4EEA93508D6AAFD091EC22D001C761C0D007ABEE3F996ACBFAB35D295ECBDB2E954C8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.golfcoronado.com/templates/yoo_avanti/warp/vendor/uikit/fonts/fontawesome-webfont.woff
Preview:	wOFF.....[.....M.....FFTM...D.....j..zGDEF...`..... ....OS/2.....>...`.6z#cmap.....~...../t.gasp...@.....glyf...H..>.....j0_.head..AT...3...6..".hhea..A.....$ ....hmtx..A.....t+...loca..D.....O.maxp..K$..... ....name..KD.....2...post..L.....L..<.webf..[.....W.....=.....P.....1l.x.c`d``..b...`b`d`dZ.$Y.<...n...x.c`f.a.....b..... .....b.....l...|6.F.0#....F...U..x...K.q....Z....*.@W.q.....Cc...9./...B.....8H.q.(."".....5..W.B.]:.....<...#.....y.....w..^3.K..n.%...j.B_h.....X<..g.4.QMhJ3.....5]..m..A..H ..r(...jX...8F.". ...,c9+X.*V..3r...Q?>P..*.hL....e.j].uS.. .|L#.4...2..c..hB.L,fIK[..V..U.~Gu{n.w...s3.....72!.2&..JF..a..A.K....b.m.....5_.%_.9..)..1X.....C>.....?~y=..B....t^.).....n..... .....x....T.0..}[.....^....iz)..nv....E.\@A..J!*..(!....e.,.K.8.M'..$.l~.IL2q...7.....UUW7.3.|.....s.=..s.....x...N.L....A.....2.E..."q.8.....S...3....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\golf-channel-logo[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 164 x 163, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	29451
Entropy (8bit):	7.984527096984377
Encrypted:	false
SSDEEP:	768:MRk7l0Gv1M1rWeXOL6P2WHieTVTKsezDf04f1:hlZHqVTOt
MD5:	22AEB7803BB6332490B77C283D721419
SHA1:	092EA1578E62070C4B8BE9684644429D3D927AFE
SHA-256:	707D1C4866A50D9F02DE666E733FB1C0C2D6D9D8A824BAF9E346310691F721A5
SHA-512:	8CE7A2070586A7AC17C365F086BCD7AB09875D29E266160E16C8626174C0DC1FC0376D9EF3B138EDBB1812A275FA0CE3B60A66A828B85955B620460EE55B016
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\golf-channel-logo[1].png	
Reputation:	low
IE Cache URL:	http://https://www.golfcoronado.com/images/golf-channel-logo.png
Preview:	.PNG.....IHDR..... .IDATx..w|.....c.l\...@L....BI.K.m..%..M.n.....6.B.$4..l..-W.-[...[.:.?.,...-.]>~]..)3.3..9g.#.....2...U@.0..+...B....q!D.0...R..''...m.>...U...h...!.....7... .G.RJ.....&J)..!.J)..q..;.....O....I..u@.. ..;.mr4....RJ.....I)..BL.....5...k..UB....\C.....RF..s....V..R"e.....$.R.....(*..E...Rv.!^.....B4..<.._KH)e.p...B...../.7.]...R...^.. ..... LB.NH.0.....u!....B.MG.....W..8.\.\).<O.Q.v.]...p.....*.....\\7O..H..h:.i.....C:..u\.M#.....!.v..... .....')....r.M_..&e;.].=...4A.HZ..P.m3M;.....6..4../HH!.4...r..b....s.lF...@ [W...$..S..Q..a....@/...;!.....RN.>.|.(y...C[O..4..&.HP^QAo{;.....].;...h"A...**.....M&.....}{....A:.gx.h..u..\r..W.....F...dTI.M9b....K..!.s.....R.c.....{:{z.....^.p...kikj...~... >.i..7.c..e...TTT.HD)I.L.]Q.....}..<.Mww7M.;Y...^z.9.::8..s..._c..l.....F..c....#.D[.....:...)...|.....%.....hjb..f....7.KS../~.S.<..I.9....<..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\golf-digest-logo[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 163 x 163, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	26542
Entropy (8bit):	7.985403620983243
Encrypted:	false
SSDEEP:	768:/kI78gDUPjabhS9AI+5ISQwq74Vp6+anAJm:/R8gnVS9AI+pqaXm
MD5:	D931237D95A3F7B78B8736240E631557
SHA1:	2FA8E29A56F430EC18482D71385C0A8B49CB451C
SHA-256:	CD75C8575A2AE04D63EB6B6D6BFDF81FABF35736236F6CC8051F9344D80F688A
SHA-512:	15161E7BA208D6E7199F74F14B6CEDF4843729F2B3F9683F46788BF8D460629F9A70A72F37748547CB9CE754E6AC8428E68BB899A74D3E1B65C6B3196B2721E5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.golfcoronado.com/images/golf-digest-logo.png
Preview:	.PNG.....IHDR.....l.... .IDATx..w..U...gfn..M..j.5B.*."..)?+*...Q...."....APi.....{..f...~....c...MB/..y.n.f.3g>.?....).t`H".T....S...rQ.]WU{P&]U".*.<.F.@.8....DZ.$."&t.j .t..t QS....\.i.....}..6..z....R...3....eMoB.r':J.SR.P.J.T..J...J!.H.....U.sJ.oR..M.....B.&.h.....0.....R\\.y...@.....R.d....lKu..z.LG..\.).P.BJ.....O)\.p<.+.....$..A.I.R>(..gU....@....Q.4.....F .c..FP.0 .....byiX[>}d..!D.....N..]V..X.:1.x.9..m...H....g{....X}.;...z>.O.~.R(.../..Q .....]#hh.. .k.. (....pA.HPk....H.`.....|.....J.....q.>...+..^....-..#.\....LGb...'.....mW.H......../..)s.. g.B..PhB..1.F.+....}?a!.k.....p....K..xj...V.Fv..9~?...J).5n....I..)..U)G".xB.H..xd....=2.K.....$.%q.....x...:...0Q....[.}YQ...H.=.!...04..Fh?...4B.N$....D.:.M#.$.H.h..).....2.z ....''}.....<..R...s.i.....J.....~..%my.L....O..H..Y.#.HL.....Di.3F.1yD).NC[.....3.1f`!..&Y.!m.X..!n....:(..u.=..3.c...F....0...H..d4.....wC'.A...G.....=|

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C038
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\3Y2ADQKS\jcemediabox.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	21470
Entropy (8bit):	4.872209355758903
Encrypted:	false
SSDEEP:	384:MKE684V5VYVtpUfBfBQRYQsx0whWgI+sPI:MKE6xVXsjUfBfBeYP0wc/w
MD5:	9D108330040BD2B7386AD9C4CF8105FC
SHA1:	53594F946AF4896BB98AC91A817990EAA74B75D1
SHA-256:	CC61348D07D4BB7C569FED635C4FCBC26D5EC226657E7C4340C63D10093AF2F5
SHA-512:	E7278696375F0EA8B1B25C9D2844140753BBD4BA5290AA9AA871AB22E693E49C694E767C45BDA893D4D24D6BDC53552EF4EEC4A20C4CF33947A80A5437F72EF B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\jcemediabox.min[1].css	
IE Cache URL:	http://https://www.golfcoronado.com/plugins/system/jcemediabox/css/jcemediabox.min.css?9d108330040bd2b7386ad9c4cf8105fc
Preview:	@font-face{font-family:mediabox;src:url(../fonts/mediabox.woff?swjl0l) format('woff'),url(../fonts/mediabox.svg?swjl0l#mediabox) format('svg');font-weight:400;font-style:normal}[class*=" wf-icon-"],[class*=" wf-icon-"]:before,[class^=wf-icon-],[class^=wf-icon-]:before{font-family:mediabox!important;speak:none;font-style:normal;font-weight:400;font-variant:normal;text-transform:none;line-height:1;-webkit-font-smoothing:antialiased;-moz-osx-font-smoothing:grayscale}.wf-icon-search:before,.wf-icon-zoom-image:before{content:"\f002"}.wf-icon-next-squeeze:after{content:"\f01d";font-size:1.5em}.wf-icon-prev-squeeze:after{content:"\f01e";font-size:1.5em}.wf-icon-close-squeeze:after{content:"\f05c";font-size:1.5em}.wf-icon-prev-shadow:before{content:"\f04a"}.wf-icon-next-shadow:before{content:"\f04e"}.wf-icon-close-standard:before{content:"\f057";font-size:1.5em}.wf-icon-link:before,.wf-icon-zoom-link:before{content:"\f08e"}.wf-icon-prev-standard:before{content:"\f0a8";font-size:1.5em}.wf-icon-

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\jcemediabox.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	44662
Entropy (8bit):	5.3782669171729385
Encrypted:	false
SSDEEP:	768:4o2YtKOlhRu+5zusMDcE4J7Bq1J4bR7yqahjKXiOch2Q5eF2a9S1Qy0xZh:4o2bdusMDcj1Bq1J4hyqkjKwh2QQ2qxD
MD5:	1B6E86F0CF3DB9F07A84A04E29A794E0
SHA1:	B4F87734D77B5B455272EED66254F872458E7605
SHA-256:	484976F805712704558C5AFB0145FA21E607B554DC8EC94B0088E8D5BA5FEBEF
SHA-512:	DB8F0E756F28C0B994436F4E436334826B67E199BB64402B0273311E06DFC45998D43BF157204C997EF679A3F299780A936C460C7F7247DC5AFEB751540EB66B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.golfcoronado.com/plugins/system/jcemediabox/js/jcemediabox.min.js?1b6e86f0cf3db9f07a84a04e29a794e0
Preview:	/* jcemediabox - 2.0.13 | 2019-10-31 | https://www.joomlacontenteditor.net | Copyright (C) 2006 - 2019 Ryan Demmer. All rights reserved | GNU/GPL Version 2 or later - http://www.gnu.org/licenses/gpl-2.0.html */.if("undefined"===window.jQuery)throw new Error("JQuery is required to run Mediabox!");!function($){function scrollIntoView(el,pos){var supported="scrollBehavior"in document.documentElement.style;if(supported)try{return void $(el).get(0).scrollIntoView({block:"center"})}catch(e){}var boxCenter=$(el).offset().top+$(el).outerHeight(!0)/2,windowCenter=window.innerHeight/2;window.scrollTo(0,boxCenter-windowCenter)}var autoplayInterval,MediaBox={util:{},settings:{selector:".jcepopup, .wfpopup, [data-mediabox]",labels:{close:"Close",next:"Next",previous:"Previous"},autoplay:0},popups:[],items:[],activator:null,getSite:function(){var base=this.settings.base||"";if(base){var site=document.location.href,parts=site.split("://"),port=parts[0],url=parts[1];return url=url.indexOf(base)!==-1?u

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\jquery-migrate.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	10056
Entropy (8bit):	5.308628526814024
Encrypted:	false
SSDEEP:	192:kZrk/GNyd31svs7wkX8KzJcqSDdAcHX4YE5NLR:srhNyNO0kkMKzFSDdAcIYwLR
MD5:	7121994EEC5320FBE6586463BF9651C2
SHA1:	90532AFF6D4121954254CDF04994D834F7EC169B
SHA-256:	48EB8B500AE6A38617B5738D2B3FAEC481922A7782246E31D2755C034A45CD5D
SHA-512:	B74A2F03C64E883B9A34DE43690429327DFB4AA230A7A6AFCA8150A16E3D84E98461245FF264C26368D9904562CC34FE219F71F951D364FA5C68C039B76776CD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.golfcoronado.com/media/jui/js/jquery-migrate.min.js?43572ae32cf0948c0b4f80000130ae29
Preview:	/*! jQuery Migrate v1.4.1 | (c) jQuery Foundation and other contributors | jquery.org/license */."undefined"==typeof jQuery.migrateMute&&(jQuery.migrateMute=!0),function(a,b,c){function d(c){var d=b.console;f[c]||(f[c]=!0,a.migrateWarnings.push(c),d&&d.warn&&!a.migrateMute&&(d.warn("JQMIGRATE: "+c),a.migrateTrace&&d.trace&&d.trace()))}function e(b,c,e,f){if(Object.defineProperty)try{return void Object.defineProperty(b,c,{configurable:!0,enumerable:!0,get:function(){return d(f),e},set:function(a){d(f),e=a}})}catch(g){}a._definePropertyBroken=!0,b[c]=e}a.migrateVersion="1.4.1";var f={};a.migrateWarnings=[],b.console&&b.console.log&&b.console.log("JQMIGRATE: Migrate is installed"+(a.migrateMute?"":" with logging active")+", version "+a.migrateVersion),a.migrateTrace===c&&(a.migrateTrace=!0),a.migrateReset=function(){f={},a.migrateWarnings.length=0},"BackCompat"===document.compatMode&&d("jQuery is not compatible with Quirks Mode");var g=a("<input/>",{size:1}).attr("size")&&a.attrFn,h=a.att

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\logo[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 76 x 62, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	9471
Entropy (8bit):	7.933264277808268
Encrypted:	false
SSDEEP:	192:ue7mUxUoQRTOZ98pSC7uxFCvT+mGrX1IsE/tPEFEXS2D4SOPmPUm:ue6URQROWSC7uub+vr3VFEbD4SO+L
MD5:	6026A7030CE11733FC9DDCAE281349C9
SHA1:	B97FA3146211D8FD6D2FCAAA04C31B91C8A032FD
SHA-256:	3DAA289A34ED6B38EDFBBFB76050E5B99DDCCB9314D56E493E5348EF98ABEF0A
SHA-512:	A00F1E167AE4BBFFCDB909201B1528EA70B6DC2616F55011BC8A17E3029CA8D201638BC231C91EF6C55DD914598576AD36C5A08A7C39EF8B0D7D1BD34C123B0
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\logo[1].png	
Reputation:	low
IE Cache URL:	http://https://www.golfcoronado.com/images/default/logo.png
Preview:	

.PNG........IHDR...L...>......}......tEXtSoftware.Adobe ImageReadyq.e<..."iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpme ta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c138 79.159824, 2016/09/14-01:09:01 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http ://ns.adobe.com/xap/1.0/" xmpMM:DocumentID="xmp.did:DF1331DD93D011E7B22EC3EFEDEBB063" xmpMM:InstanceID="xmp.iid:DF1331DC93D011E7B2 2EC3EFEDEBB063" xmp:CreatorTool="Adobe Photoshop CS6 (Windows)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:D5F0791A35B311E7B3E4DD5B1DF82A B9" stRef:documentID="xmp.did:D5F0791B35B311E7B3E4DD5B1DF82AB9"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>.aH...!sIDATx...XUg... .....Q1..{......+FM...c.5..hb.....S,..B....+.Xb/X.QT@T.r.o.9.|4..;..~..9g....o....,......o6.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\main[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	assembler source, ASCII text
Category:	downloaded
Size (bytes):	14150
Entropy (8bit):	5.102075825662535
Encrypted:	false
SSDEEP:	192:/V0DcDJcPN6NQmoGrhgYw8g5Lf1va8Z1AhhLokI0oFFatmYVuE5ntnf:9uPN6NQmo2eA08jyFatmYVuE5ntnf
MD5:	C59599C6D682548DD634B19BB8C025DA
SHA1:	BF23FEBF7062E53BE8BE8A8720A88EC439BE26C1
SHA-256:	3A4EC77FD81E5B08D00E41CA880E81BE1263309C9D4930D176E70603D549B620
SHA-512:	1F69AE7FF754B8D20EB75207F199A7D7F6E123995F8A7A95961F14EE7E82CB3E7EBBC29A0508C18592104A6D0250CD2462CBA042A74DC06FCF428BC32E4948D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.golfcoronado.com/components/com_dtregister/assets/css/main.css
Preview:	

/* DT Register CSS - ver. 3.2.2 */...jgrid span.state {. display: inline-block;. height: 16px;. width: 16px;.}..jgrid span.unpublish {. background-image: url("../images /publish_x.png");.}..jgrid span.publish {. background-image: url("../images/tick.png");.}..jgrid span.text {. display: none;.}.h2,div,dt,dd {..white-space: normal;.}..dt {. clear: left;. float: left;. padding: 3px 0;.}..#dt_tabs dt {..clear: none;.}..dd {..float: left;..padding: 3px 0;.}..dt.dtlabel {..position: relative;. font-size: 12px;. width: 16em;..background:none;..border:none;..text-transform:none;..font-weight:normal;..font-size:12px;..text-align: left;.}..dd.dtfield {..position: relative;..min-width: 300px;..max-w idth: 500px;.}..dd.dtfield input[type="text"],.dd.dtfield input[type="email"] {..max-width: 80% !important;.}..dd.dtfield img {..vertical-align: middle !important;.}..dd.dttip {..p osition: relative;..width: 30px;.}...dt_member_box dt.memheading,..dt_member_box dd.memhea

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\march12021rates[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 2550x3300, frames 3
Category:	downloaded
Size (bytes):	327080
Entropy (8bit):	7.116453600184137
Encrypted:	false
SSDEEP:	3072:w65WB5/QH5AEWTtTSRHPYEKwwBdzqaqUuczuaqRUDi7yWiPYudgp5PEl:grK5AE0axKwBaqrR8i8wQiNA
MD5:	B1648A8EA39EA2F21C4D42B4EA51F1DD
SHA1:	2CEF2A815ACFA766CCB7CD492529B31C04F79CDF
SHA-256:	1F7E4BE9A6A673F7A2BD773581D8CF0CF7BE9E1075A4A70E760B9B42C5ED6323
SHA-512:	5601AD950E34E25400B805E780CA891403D507FCBEC400C8E6B6EB30F2A5E249E719AE1AAE43E06A21D5B316B3481D93CBDF28A5DE64F8AB14B69AE0C0E053 B7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.golfcoronado.com/images/march12021rates.jpg
Preview:	

......JFIF.....,.,.....C.................................. $.' ",#..(7),01444.'9=82<.342...C...........2!.!22222222222222222222222222222222222222222222222222...........".................... ....}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.. ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.. ....?...(..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\markgedds[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 840 x 1050, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	586115
Entropy (8bit):	**7.998119065408088**
Encrypted:	**true**
SSDEEP:	12288:HWPQWkTID5LCmFLQ/Hwao/2/7mf64TdP2q7QH3xlwO:HWwT6n1QvwdeTO6UdO2QXl
MD5:	DC25E3FDA116F5802F600E080CC49E66
SHA1:	BFE631B285FDD7B16BD221C94F692A62B4327527
SHA-256:	BFBE6DDD45012E10CFC2946381D8BCFD40C24AAD4FA190B727603327E6CC388D
SHA-512:	8FE86B86EF25422499E1D09EC0CD0DBEEDF618079ED47AF9495F4B920F89213B807ED157C3B7947EADF672FF95759E4AF57DC41EB335D1B947F909D5D8F9EC 1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\markgedds[1].png	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.golfcoronado.com/images/markgedds.png
Preview:	.PNG........IHDR...H..........d......sRGB.........IDATx^...s$i..a_...:.=..\.+.Yl....).?......f..Pf..p(S..SU.U..kDx...........w.QU.G.....{..aaPS...).;v..NL..X.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\rates[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, CR, LF line terminators
Category:	dropped
Size (bytes):	21621
Entropy (8bit):	4.98667888335302
Encrypted:	false
SSDEEP:	384:XAO95KE1iiioiWixiNi/iwiPiZvQairimOqLdAtFk+HU79199W99977j5QRv5:XAO95KE1iiioiWixiNi/iwiPiZvQairL
MD5:	FBB4B3F0D89C7C7AB42310CABBDAD392
SHA1:	E43FFCC8897CD910F497B275BE25EB7398C8D24E
SHA-256:	5C21225100EB3E02A52BCC1E8A901EFB5A62891E3A9A42CDF060CE110D2F0E1B
SHA-512:	BA641A7EC663014357C7E87C86FA34DB8ABDAE566D1F6886E6A517C444C740C3412E84E9A0006CC65D33AEC4CBA3C93BDBB9568C92168AA8748C37BEF66F4C A
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE HTML>.<html lang="en-gb" dir="ltr" data-config='{"twitter":0,"plusone":0,"facebook":0,"style":"121"}'>.. <head>. <meta charset="utf-8">.<meta http-equiv="X-UA-Compatible" content="IE=edge">.<meta name="viewport" content="width=device-width, initial-scale=1">.<base href="https://www.golfcoronado.com/course-info/rates" />..<meta name="author" content="Super User" />..<meta http-equiv="content-type" content="text/html; charset=utf-8" />..<title>Rates</title>..<link href="/templates/yoo_avanti/favicon.ico" rel="shortcut icon" type="image/vnd.microsoft.icon" />..<link href="/components/com_dtregister/assets/css/main.css" rel="stylesheet" type="text/css" />..<link href="/plugins/system/jcemediabox/css/jcemediabox.min.css?9d108330040bd2b7386ad9c4cf8105fc" rel="stylesheet" type="text/css" />..<script src="/media/jui/js/jquery.min.js?43572ae32cf0948c0b4f80000130ae29" type="text/javascript"></script>..<script src="/media/jui/js/jquery-noconflict.js?43572ae32cf0948c0b4f80000130ae

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\script[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	12239
Entropy (8bit):	5.308165426564904
Encrypted:	false
SSDEEP:	192:+Qt91nom3+YghJLv5cr+X4t7c27re8mEPlzn6yXkyaPzajFdXZ:+QX+XY+0c27re8mylznsuFn
MD5:	85A8540321B88D1D2761775A91CB54B6
SHA1:	83D6873124051C8281BDE893AF1C965C42F96A08
SHA-256:	087F73EF30CC698B872ED48316FFE7EF38371A7E7635AE170222ECE9B919E71B
SHA-512:	65F764E68887B4AB24F6FB9E580840D419B1EED591DBCC35E5D1F7CDDE430D3E627A247C06D03A369B809A159A1A5F771E6BD148297A23DE58C05FE5C16B7E 2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.golfcoronado.com/media/com_rsform/js/calendar/script.js
Preview:	/* rsform pro */..// For convenience.....Date.prototype.rsfp_format = function (mask) {...return RSFormPro.YUICalendar.dateFormat(this, mask);..}....// if the browser has not defined the Object.keys function ..if (!Object.keys) Object.keys = function(o) {.. if (o !== Object(o)).. throw new TypeError('Object.keys called on a non-object');.. var k=[],p;.. for (p in o) if (Object.prototype.hasOwnProperty.call(o,p)) k.push(p);.. return k;..}....if (typeof RSFormPro != 'object') {...var RSFormPro = {};..}....RSFormPro.YUICalendar = {...settings: {},...calendars: {},...calendarsData: {},...setCalendar: function(formId, idCalendar, config) {....if (typeof RSFormPro.YUICalendar.calendarsData[formId] == 'undefined') {.....RSFormPro.YUICalendar.calendarsData[formId] = {};....} ....if (typeof RSFormPro.YUICalendar.calendarsData[formId][idCalendar] == 'undefined') {.....RSFormPro.YUICalendar.calendarsData[formId][idCalendar] = {};....}.........RSFormPro.YUICalendar.calendarsData[formId][id

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\theme-icons[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), theme-icons family
Category:	downloaded
Size (bytes):	3700
Entropy (8bit):	5.527083541382865
Encrypted:	false
SSDEEP:	48:hkZMDU3/YNVYdE9dkHQuIbHiGGt+/l/jw79UtDam/DIUGdAzhdDDil:LUwNVFbhbMt+/l/jwB4GmLI+BDG
MD5:	A22FD017802D49CC17805655A2D5F6AC
SHA1:	847E886C66325D2C34CDDC2B8FDD3C29417FF260

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\theme-icons[1].eot	
SHA-256:	973D087D28C27445989D03B0404F075395CB4C2D3DBC65F5953706534C7F6982
SHA-512:	CF33456A6376281983C794DE54AB1B0992515F19A9CD9DBDBEA8D727D369D8F45E69D09AA8C55A2074C125794C68900F0F1C32D32C174749AA44847E726B6361
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.golfcoronado.com/templates/yoo_avanti/fonts/theme-icons.eot?wjfxwa
Preview:	t.....LP.....o..R.....t.h.e.m.e.-.i.c.o.n.s.....R.e.g.u.l.a.r.....V.e.r.s.i.o.n. .1...0.....t.h.e.m.e.-.i.c.o.n.s.....0OS/2.....`cmap...v.... ....gasp.....glyf|..5.....<head.....6hhea.....$...$hmtxJ..O...H...Tloca...N.....,maxp...g..... namem|.....post..... .....3.....@..... .@...@..... .....p..... .6.t.v..... ..... .6.t.v..... .....t.....79.....79.....79.....+.....*.K...2 .....#"/....#"'&'&'&547676763."..... 3276767654'&'&'&#..NGG34....(.....2==CNHG33....33GHN=78((....((87=<87((....((78<....34GGNC=>2.....(....34GG NNGG43..U..((77==77((....((77==77((.....-.Q.d...2.....#!'"&=.476767&'&=.476763."..... 3!276=.4'&'&'&'&'&#

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\velocity[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):	44443
Entropy (8bit):	5.4794572400237564
Encrypted:	false
SSDEEP:	768:AUxWQTiyKkIk6PkMS9NQF+KLWFVAdYnqqtQIChVHmjHk1/UBHGPhLTi:7wfk68MS9CF+KKAOqiQTVHmjHk1MBHGQ
MD5:	C226BC08EA47F737C97BD45051A50E35
SHA1:	134F94D957FF76D1427AB41B1D61BA07E6057578
SHA-256:	9A6C90D617D93F4D7DF6D22B2F1592A81F5EE35F03B0EE3FCE723DC8E7426236
SHA-512:	F57C8334D7C11F3E8D53E92E65DC9C20D8CB9C049127F03CA0A6E8104DEA165F54830AF3E54E6408951D07086C4FC3869C3259610BE18984EED7541650170E5A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.golfcoronado.com/media/com_rstbox/js/velocity.js?v=3.3.3
Preview:	!function(e){"use strict";function t(e){var t=e.length,a=r.type(e);return"function"!==a&&!r.isWindow(e)&&(!(1!==e.nodeType||!t)||("array"===a||0===t||"number"==typeof t&& t>0&&t-1 in e))}if(!e.jQuery){var r=function(e,t){return new r.fn.init(e,t)};r.isWindow=function(e){return e&&e===e.window},r.type=function(e){return e?"object"==typeof e ||"function"==typeof e?n[o.call(e)]||"object":typeof e:e+""},r.isArray=Array.isArray||function(e){return"array"===r.type(e)},r.isPlainObject=function(e){var t;if(!e||"object"!==r.t ype(e)||e.nodeType||r.isWindow(e))return!1;try{if(e.constructor&&!i.call(e,"constructor")&&!i.call(e.constructor.prototype,"isPrototypeOf"))return!1}catch(e){return!1}for(t in e);return void 0===t||i.call(e,t)},r.each=function(e,r,a){var n=0,i=e.length,o=t(e);if(a){if(o)for(;n<i&&!1!==r.apply(e[n],a);n++);else for(n in e)if(e.hasOwnProperty(n)&&!1= ==r.apply(e[n],a))break}else if(o)for(;n<i&&!1!==r.call(e[n],n,e[n]);n++);else for(n in e)if(e.hasOwnProperty(n)&&!1===r.call(e[n]

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\0QI6MX1D_JOuGQbT0gvTJPa787weuxJBkqs[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 23256, version 1.1
Category:	downloaded
Size (bytes):	23256
Entropy (8bit):	7.9785272859711895
Encrypted:	false
SSDEEP:	384:u4+aa6Vn20vpN8aQ/iECNemb2aad54bQzQrLrioFSp/GrOmwWARI+eDuvj0Bgo:7xzX1Q/iJN12DVQrLNE/GCmnzSSgo
MD5:	18E48BEDF6F3FDF2A03A7E44D2AAA2CE
SHA1:	0EAF056823EDAA7D9BC51E05772FA28DA310FF57
SHA-256:	5FD9A5BE62963B7E2C9948047F7F7C70E1EC7194AB1D059F49BCCF88513C8E7F
SHA-512:	EDB74714C01D82583D0B824FA21A6FA84480A166C9BD1004A2A2A19C56A805CDB5F955600E150224E3CC39F6671344F65F036CBC3FCBA58CF5CAB28F640B24A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/lora/v17/0QI6MX1D_JOuGQbT0gvTJPa787weuxJBkqs.woff
Preview:	wOFF.....Z.....`.....GDEF...l...v.....h.JGPOS.....*..?..C.fGSUB.....(9+bOS/2.....O...`dY.dSTAT.....8...D...cmap...H.....r%.C.gasp.. .....glyf..!...3...R". G..head..T....6...6....hhea..T.... ...$.b..hmtx..T....Z...4*.-.loca..WL.....$....maxp..Yh..... .!..name..Y....5...f;y[.post..Z..... ...2prep..Z.....h...x...FC.....0.....".@.... P.$z.=.~. ....8..p.hd=rb#g..bd;r.J.GnFn.....gy.*o#.#.#.....&..`+....J...A....x.T..p$Q.E..=1.v.....m.fqm.m....n..oH...A%(*T.....{t..S.^].G.....?.r..=.@.y.....d....o....@....]#..Y.U.).....!..... ...A.f.K...t...a.....O..Z...!.....i.i....Y.k..d]...>&5.....+...Z_....5....p...d7U2.1...\...h.N....b.e..h.X....,.....Z.[.....&Z.c....#.I..QI3R<i.HY.r.....l....u.m...|....V.....?..0..0...<..H,a....1 .+.8.....zl.Dle..;0....3q.Gy.:n`1n..x....._..?.j....( n....BHF%....x....6..0.....).a.....&."..3._.-.\o.I<.L...@..`..P....IJR..4.%...H&2...d..`..A

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\0QI6MX1D_JOuGQbT0gvTJPa787z5vBJBkqs[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 23324, version 1.1
Category:	downloaded
Size (bytes):	23324
Entropy (8bit):	7.977664141028951
Encrypted:	false
SSDEEP:	384:9wFHrq5kxFfRxJ4Ck5rkYDgRXBn69pGUh9WuWo+CBiBuPUVnwejQE+/a+l/Y0K:9cHrskxFfRXVe42++BiKUVnwecEpe/Y3
MD5:	9FB83404675A55EDB22A417C958FDFAD
SHA1:	E09B6A97D55A7040683576CBB9B25D3CAF69AB0B
SHA-256:	39B7A1F170CFEA07CA7485087FF49BAFAF86FACB0A81E36AFA7904ED0C887A74
SHA-512:	7F994B766062C970A42C128F1C96496E703535F233212C1A73B9AD69DACD552BA090549362F9F30CDF127120F76A10822C44AA12EE8F4F62FA3ECD78E7CCB3B8

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\0QI6MX1D_JOuGQbT0gvTJPa787z5vBJBkqs[1].woff	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/lora/v17/0QI6MX1D_JOuGQbT0gvTJPa787z5vBJBkqs.woff
Preview:	wOFF.....[.....p.....GDEF...I...v.....h.JGPOS.....*..?H.&..GSUB.....(9+bOS/2.. ....O...`e..DSTAT..!....8...D....cmap..!H.....r%.C.gasp..".....glyf..#...1...Q. .#<|head..T....6...6....hhea..U,... ...$.b..hmtx..UL...N...47.(,loca..W.....$....maxp..Y..... .!..name..Y....,...N8.X.post..[..... ...2prep..[.....h...x...FC.....0....."..@.... P.$z.=.~ .....8..p.hd=rb#g..bd;r.J.GnFn.....gy.*o#.#.#.....&..`+....J...A....x.L....Q....cl.n....L..;.m.m.m...Sg..v.!.PAF..H.dEX.tj.....6..q. ...IP4..9t.j.n.=@"~.....D..:HR._w.KGcKr)..l.r t..o.....4;.e.).f.tv66..<[5Ru].P.S...y.A.n.[.[.h...,...MyXs.XK.....c..[=...YR...s.....,...^...\|#.i...y.....=.....#.....@$.+87.85.*.M.;.%C(..._..$g..if..r..K.....q...>.).p ..:.6....!. ..*...W.CG.e.1.....Y?..,...6..0....k0...Hl.F..f.....>.....+l.....;..G6..$Q...9.f.....PW.BKq...M.._...HFO.....G...q.s.1...|..+.....V.....o.>..*B...))..)..)..-....#=..H&2..ld'.9.En..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\622COIJN.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, CR, LF line terminators
Category:	dropped
Size (bytes):	38955
Entropy (8bit):	4.976684026689978
Encrypted:	false
SSDEEP:	768:iAt90E95KE1iiioiWixiNi/iwiPiZvQairin7LrvwvPvmCdSG/379199W9997c3j:8SJjB2uuTMavQa4i7/o3mCdSG/791995
MD5:	583703132A4D70FC0F76E8EE6FBAF9DB
SHA1:	D1CC3AD2CF2F1ACAFD7BD81AB82D6FBAE7F4DB0C
SHA-256:	F3017867067DC63E3E3E1B0A9C007564E0315DF5A0BCA1846910478D27F4A80B
SHA-512:	1F5B39BD32E99258B0FDF4523F800B1909B6C64FF2848A408FBFF0E2FC600A1F11994593331C33BA7D2753D0F41F59C8F2BFD56ABC117C69EC2F3A019C41CD3
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE HTML>.<html lang="en-gb" dir="ltr" data-config='{"twitter":0,"plusone":0,"facebook":0,"style":"121"}'>.. <head>. <meta charset="utf-8">.<meta http-equiv= "X-UA-Compatible" content="IE=edge">.<meta name="viewport" content="width=device-width, initial-scale=1">.<base href="https://www.golfcoronado.com/" />..<meta h ttp-equiv="content-type" content="text/html; charset=utf-8" />..<title>Coronado Golf Course - Coronado, CA</title>..<link href="/?format=feed&type=rss" rel="alternate " type="application/rss+xml" title="RSS 2.0" />..<link href="/?format=feed&type=atom" rel="alternate" type="application/atom+xml" title="Atom 1.0" />..<link href="/te mplates/yoo_avanti/favicon.ico" rel="shortcut icon" type="image/vnd.microsoft.icon" />..<link href="/components/com_dtregister/assets/css/main.css" rel="stylesheet" type= "text/css" />..<link href="/plugins/system/jcemediabox/css/jcemediabox.min.css?9d108330040bd2b7386ad9c4cf8105fc" rel="stylesheet" type="text/css" />..<link href

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\7Aulp_0qiz-aVz7u3PJLcUMYOFkQl0k30e4[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20708, version 1.1
Category:	downloaded
Size (bytes):	20708
Entropy (8bit):	7.9754280607630985
Encrypted:	false
SSDEEP:	384:XfQgjRnjJGvZRkL53S9pFwCIdkUG0ry0jQLe0gZ:XfQERjJSRkLxS9pKP6UG0z8C7Z
MD5:	992B9C11370518AECE1690BB6EC7BD3B
SHA1:	C474792143CF895DAA6341CAFF828B1BF4D385D0
SHA-256:	CDCFC6049038D4962A320D79831AD8D881BA92046684BA9C3C2675F7A0DE32EA
SHA-512:	9D0063ABBD4DCF6AD839E166A2DB386A6F3FD65E52A608B152FFAA66A1A5CE03D4F79959DD1925DD03096401636B427B94CF21B9BDB99EF4B33EEB0A01F65A DD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/muli/v22/7Aulp_0qiz-aVz7u3PJLcUMYOFkQl0k30e4.woff
Preview:	wOFF.....P.....GDEF.....>...R.W..GPOS.....|.....t.GSUB...P...c....~.J.OS/2.....M...`b...STAT.....8...D.t..cmap...<.....G.e.cvt .....P.....Nfpgm...<..... .6..gasp.....glyf.....6Q..fx...head..J\...6...6..Ymhhea..J.... ...$....hmtx..J.....0.../loca..L.....s.maxp..N.... ... .m..name..N....B....>adypost..P$..... ...2prep..P8.....' Dn.x.....P.F..~R..*....i...[..u..t..L.!...q..../w|..Z*.....x.V...g.....4g*Vc.....z-.@U..R..(h.U.P..@...!.9J.u..5.DW.\..k...=.uc.c..?..3..;.o.....p.@.....}..V.....X.k.@j..W_~s....ss..q...s .!..Bn.2..1.cR.....q...(...0.g..=..@<B."....13.|.!_...)./..a...z..C^..]Yl..x.5.Nr..\.;..Z7.]..78..?C.#..\.G...y...c..OQ.eZ.,.n).G..b..b.8r....G..!.0.S...&}...2q.l..]......A....P...~..y.....`...C. .:K.....Yv.|.#e&9.I.1N!N,..B.}.c.X.D.."...0.Dv.Ik.J..}.%....X....W.{F.=".....U....p2.....u.5..x8>D..._.sW.B#e`.....#.....\."..'.xb..H...gC.'.u..&....L....!.8.w....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\7Aulp_0qiz-aVz7u3PJLcUMYOFkpl0k30e4[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20756, version 1.1
Category:	downloaded
Size (bytes):	20756
Entropy (8bit):	7.975136650955638
Encrypted:	false
SSDEEP:	384:6oLABAsaWEtgqtnjJTvfrHtC0yEleATWHtw49sse:6oLmAsaXJVjJLfrNvyYeeWHvyH
MD5:	4103B329F719559FBA5FE266839C0431
SHA1:	32E4635A61F8D5340EA1FB0BD337A3C8C04C2069
SHA-256:	23D97C24A70B4BBDD28F76DBA3D50CCB71CD0B92288A4B16619EABF1BD38453A
SHA-512:	9E6ACCE2CB92B153BAC5F5E6C403212F1BEADF1693C72ED5C8D7A67EA14C08AD2A42B87E50940B63DAFF68B5DD88481715DAD11736B3FE0E7FC3563846127E A1
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\7Aulp_0qiz-aVz7u3PJLcUMYOFkpl0k30e4[1].woff	
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/muli/v22/7Aulp_0qiz-aVz7u3PJLcUMYOFkpl0k30e4.woff
Preview:	wOFF.....Q.....GDEF.....>...R.W..GPOS.....rt.GSUB.....c....~.J.OS/2.....O...`b~..STAT...@...9...D....cmap...|.....G.e.cvt ...,...P.....fpgm...|..... .6..gasp...@.....glyf...H..6S..f|^_.fhead..J....6...6..Ymhhea..J.... ...$....hmtx..J.....0.a'"loca..L.....sKmaxp..O.... ... .m..name..O$.....@5.W'post..PT..... ...2prep.. Ph.....'Dn.x.....P.F..~R..*....i...[..u..t..L.!...q..../w|..Z*.....x.V..\W...I2.Ow...tS..+.....R.j.P.....Z....@. Q..JL.....t".]...5.n.O...;.73.....7]4....{..{.}..9$".....;.} .O?...T.(..?...].c.Q..J..- U7...kn.....9mO.L.!u:..q....Q..}.&.]P..#..b.#.L.\..U.....[...1..l..j..o.K...+....eVB.\....:.....b..>.6...(.xKW\..8b.g.Y$.I.q.....H.c7.c.[..c..bL..a..."...r.r...<....n Ry.#.,!..7.....6c.....?.>V]..y M...*.%....h;....I..::^.#.ytP%.R9.0."[.e.VB.....>.*b.9O.hS.....k.~.'..6..]...$@IV..IY.4....b...Y.@.e3....H].Y...r !...9.^.N(fe.$0..>...../F.I...'4...I.....u..,g.a.e

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\Petra-Cole[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=5, orientation=upper-left, xresolution=74, yresolution=82, resolutionunit=2], baseline, precision 8, 231x228, frames 3
Category:	downloaded
Size (bytes):	14472
Entropy (8bit):	7.924460751199298
Encrypted:	false
SSDEEP:	384:MdB2SVMXT+uCYKlV4MznaOg+zIRBEuXCfUF1p:MdBtMXGYOV/zVYR1Cip
MD5:	201F7E0614C023AFEFA4B872CF78E3F9
SHA1:	399D33ABE4650B9FAB478DDCB123FB2E78F2C51C
SHA-256:	CDCB3BAE2888EAB28F3339F0E07C75367EB63CD5BBEDB89C95AF556483D1869C
SHA-512:	B9743ABD99C865981E9B31A5475D7967807F6E1E1650D3C016FC405CF22C98CB225546EAC755734C94461CD5211B97B57365765BC5FCB8DF70EF0FEC5F43B4E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.golfcoronado.com/images/Petra-Cole.jpeg
Preview:	.....JFIF.....H.H.....Exif..MM.*.....J.....R.(.....i.....Z.....H.....H.....8Photoshop 3.0.8BIM.....8BIM.%.....B~... .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....C.....C.....?.....q.7.....x..wikm.....<..09'..v.W;...5.....~..gl,..b .)g.B.qH.KZ.d..s...#..h>3..6.2j7....dV]&.*.$.|..n..b.@#.%.....+Y6..w..g...?yA.&._.....o.4.N.B..m..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\acymailing_module[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	14245
Entropy (8bit):	5.199485135755587
Encrypted:	false
SSDEEP:	384:8aRShYjfHYHdfH/1eSHSNJTS4+5SwOLj6HtpjX4/0cxI2lEYxIacM25BJ/iJbmJe:TRShYjfldfZyNJ+Qt6HBdBJ/iJbmJM48
MD5:	A7FCC00D95E6FD756371B579925166C0
SHA1:	BF3EF179917D611AC24F377479208D76418F6236
SHA-256:	A1B5DDC720119BF45D047BB0CF293D74CB5388199B775292C92E1215B04E6D5F
SHA-512:	07B4891FE41F4B1EC86CBDBB49D2C53AB8180BAE333894B318F9B6E542B164D153719C5859E1B4C7782B4B9D51CE1162156CEC8A0BA0B1310FDDEC5E8BA338 A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.golfcoronado.com/media/com_acymailing/js/acymailing_module.js?v=51010
Preview:	/**.. * @package AcyMailing for Joomla!.. * @version 5.10.10.. * @author acyba.com.. * @copyright (C) 2009-2019 ACYBA S.A.R.L. All rights reserved... * @licens e GNU/GPLv3 http://www.gnu.org/licenses/gpl-3.0.html.. */....var task, formName;....function submitacymailingform(newtask, newformName) {...task = newtask;.. .formName = newformName;.....var recaptchaid = 'acymailing-captcha';...if(newformName) recaptchaid = newformName+'-captcha';.....var invisibleRecaptcha = docume nt.querySelector('#'+recaptchaid+'[class="g-recaptcha"][data-size="invisible"]');...if(invisibleRecaptcha && typeof grecaptcha == "object"){.....var grcID = invisibleRec aptcha.getAttribute('grcID');.....if(!grcID) {.....grcID = grecaptcha.render(recaptchaid, {.....'sitekey': invisibleRecaptcha.getAttribute("data-sitekey"),.....'callback': 'acyS ubmitSubForm',.....'size': 'invisible',.....'expired-callback': 'resetRecaptcha'.....});.....invisibleRecaptcha.setAttribute('grcID', grcID);....}.....var

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\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):	14525
Entropy (8bit):	5.949398802803795
Encrypted:	false
SSDEEP:	384:L/SZxnOmmHLQbpspl/q63S+1Cl9ve8IHzgu0zFxm2deWWEN:L/SZBO1HLQapYd+mNWz1yFI2UEN
MD5:	416C70DF6057A105C3BAAAEC586FB0DC
SHA1:	EE899A9B2FC3A31C9C755588CC91C632B6A9619A
SHA-256:	52924E3AF1CD6DD1A542A70A478D3D1705A07E3173294CE05C42F6427BFA4A79
SHA-512:	5B372C76D2424275A5C7EC81C29D05D3C4B1335C68FCEB23BC3FC81F61B2F05CD2331AAE4911FB1EAB710682E15104225AAE05C05E4E1467781A55F90B86CE8 D
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\anchor[1].htm	
Reputation:	low
Preview:	<!DOCTYPE HTML><html dir="ltr" lang="en_gb"><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/539Evs44yecoSf-lkJBQzKKj/styles__ltr.css" nonce="k9aRrjccFeEkJpqSkspU1w">.<script nonce="k9aRrjccFeEkJpqSkspU1w" type="text/javascript">window['__recaptcha_a

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\api[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	918
Entropy (8bit):	5.518957732852477
Encrypted:	false
SSDEEP:	24:2jkm94/zKPccAjZJll+KVCetu1qINqKsLqo40RWUnYN:VKEciwKoeM1qINgLrwUnG
MD5:	890F7543EEF2F069670C8B933B9349AE
SHA1:	7FB4A333BFFE173DC8CE40D94BB568042CF3EBFB
SHA-256:	7E3525E11B949337962EAFF81221EA335BEEFC4F8D55F8ED4B7304BADAB6BB23
SHA-512:	5A2A4FCD4AB65635F26AF310EFEF01D5CA0B7E1DAF2B2F109E9A8C37425B3ECF9119FFB959DB30E1F881846F64533BDC8CB8D6D590FED7FDDA332CE3FDFC4CDC
Malicious:	false
Reputation:	low
Preview:	/* PLEASE DO NOT COPY AND PASTE THIS CODE. */(function(){var w=window,C='___grecaptcha_cfg',cfg=w[C]=w[C]||{},N='grecaptcha';var gr=w[N]=w[N]||{};gr.ready=gr.ready||function(f){(cfg['fns']=cfg['fns']||[]).push(f);};w['__recaptcha_api']='https://www.google.com/recaptcha/api2/';(cfg['render']=cfg['render']||[]).push('explicit');(cfg['onload']=cfg['onload']||[]).push('JoomlaInitReCaptcha2');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/539Evs44yecoSf-lkJBQzKKj/recaptcha__en_gb.js';po.crossOrigin='anonymous';po.integrity='sha384-G6ApfRuP9Hf6JcEk9h+EjYqPOGGj8YNdlip1vZcjGp8sJpKytgRA7zkvWexqmxDR';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\9QTQHWWN\api[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	918
Entropy (8bit):	5.518957732852477
Encrypted:	false
SSDEEP:	24:2jkm94/zKPccAjZJll+KVCetu1qINqKsLqo40RWUnYN:VKEciwKoeM1qINgLrwUnG
MD5:	890F7543EEF2F069670C8B933B9349AE
SHA1:	7FB4A333BFFE173DC8CE40D94BB568042CF3EBFB
SHA-256:	7E3525E11B949337962EAFF81221EA335BEEFC4F8D55F8ED4B7304BADAB6BB23
SHA-512:	5A2A4FCD4AB65635F26AF310EFEF01D5CA0B7E1DAF2B2F109E9A8C37425B3ECF9119FFB959DB30E1F881846F64533BDC8CB8D6D590FED7FDDA332CE3FDFC4CDC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google.com/recaptcha/api.js?onload=JoomlaInitReCaptcha2&render=explicit&hl=en-GB
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('explicit');(cfg['onload']=cfg['onload']||[]).push('JoomlaInitReCaptcha2');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/539Evs44yecoSf-lkJBQzKKj/recaptcha__en_gb.js';po.crossOrigin='anonymous';po.integrity='sha384-G6ApfRuP9Hf6JcEk9h+EjYqPOGGj8YNdlip1vZcjGp8sJpKytgRA7zkvWexqmxDR';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\9QTQHWWN\banner-new-2[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=1, copyright=Fitzgerald Visuals], baseline, precision 8, 1478x617, frames 3
Category:	downloaded
Size (bytes):	371924
Entropy (8bit):	7.986823096173208
Encrypted:	false
SSDEEP:	6144:N2Ml9pRZ8d2WOgViBqrLU6dIkEEizZ20XpoLRXIIjAhaAWiz6HxCsrH4Yk6d:N2M1RZ22WOgUEbNizAYiLKAhaAWdxCk7
MD5:	9DB0D38F2FC76BCD9E1975B1D780B845
SHA1:	1738D6F752C2B7954C7AC0C4DE88921C2A27BFCB
SHA-256:	945762E9F78133BE1322444DF04D9D893B21B28FDBBE4644F626036A141947B1
SHA-512:	3F30842F7F80AB08F08EF94D7608FD5D01D823F57B968C913370A9AE7D1239D84FEBC5EE223B82CE3CBAFC8348F103CCD7ACCBF84D69F57CF1B8E163249190
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\banner-new-2[1].jpg	
Reputation:	low
IE Cache URL:	http://https://www.golfcoronado.com/images/slideshows/banner-new-2.jpg
Preview:	.....8Exif..II*.....Fitzgerald Visuals.....Ducky.....P.....ahttp://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.3-c011 66.145661, 2012/02/06-14:56:27 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpRights="http://ns.adobe.com/xap/1.0/rights/" 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/" xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:Iptc4xmpCore="http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/" xmpRights:Marked="True" xmpRights:WebStatement="http://phil-fitzgerald.pixels.com" xmpMM:OriginalDocumentID="EB7B7C6BBE80449CF862E0E23E5C2E29" xmpMM:DocumentID="xmp.did:78CCA372A2C411E7BD4C8EFB409C18C5" xmpMM:InstanceID="xmp.iid:78CCA371A2C411E7BD4C8EFB409C18C5" xmp:CreatorTool="Adobe Photoshop Lightroom 6.8 (Macint

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\banner-new-3[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=1, copyright=@ 2013 Oscar G Medina 858.274.0665], baseline, precision 8, 1600x669, frames 3
Category:	downloaded
Size (bytes):	662739
Entropy (8bit):	7.983623957395648
Encrypted:	false
SSDEEP:	12288:ct1Gtt6C01ocyQj+q+ghWCo1Dl0X7fjlJAcBhN82iy1i3ssnut:Y1Gtt6C0KcbWudo1Dla7pJAohtniPut
MD5:	78514FB4C15B8612F01307B7861D6029
SHA1:	E63264FB6723A6C5EB6C40E01BA90F60A6F999D7
SHA-256:	8A3C6059848E41CDFCF23E2590478071C71F0D5D62E9759CB3DF20510B28C83F
SHA-512:	ABB7BFC859150001E124F206D61A612FFACD1C9DE27DB1A532208648B0622B414558673F258F953D02050890A093F2B0B91320E1447B33F4DDBFEA7A4D58144C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.golfcoronado.com/images/slideshows/banner-new-3.jpg
Preview:	.....JExif..II*.....%.....@ 2013 Oscar G Medina 858.274.0665.....Ducky.....P.....nhttp://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.3-c011 66.145661, 2012/02/06-14:56:27 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:dc="http://purl.org/dc/elements/1.1/" xmpMM:OriginalDocumentID="B033343A853DFAE8520F4F36D47F1668" xmpMM:DocumentID="xmp.did:AD09A1BFA2C411E78028DFEAE2572E8B" xmpMM:InstanceID="xmp.iid:AD09A1BEA2C411E78028DFEAE2572E8B" xmp:CreatorTool="Adobe Photoshop CS6 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:8472A68DD49511E6A365DFE50656B4A0" stRef:documentID="xmp.did:8472A68ED49511E6A365DFE50656B4A0"/> <dc:rights> <rdf:Alt> <rdf:li xml:lang="x-defa

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\banner_button_2[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], progressive, precision 8, 400x400, frames 3
Category:	downloaded
Size (bytes):	85926
Entropy (8bit):	7.980723898143576
Encrypted:	false
SSDEEP:	1536:GIXH4FuAt1bg3y1kl/mdQYUV/D0RPaWnAhGnkJDPy1Nu5saMjSUD/pp3oqf:GIXYrvEum/IRSWnAhPJDj5saxa/ppYO
MD5:	7881BE6A8EC7EC06B54CEF70BFCCBA0B
SHA1:	F96DA104EC069599EEF8B670A46CB78EFE60DAF1
SHA-256:	DD9A784A4826E55D67FB3D58D65DC7DEF4C2527EFD186AE00022AA9A14F9094B
SHA-512:	6B7F16E497F9E6D4418C69826503465B9F24BA8008E68D86E67499BE6D0D01B3E0D0E8F313B0E41BCA1CCACC64D56109D93D6BE5F991D9BEB9E921A53B2DDAC4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.golfcoronado.com/images/buttons/banner_button_2.jpg
Preview:	......Exif..II*.....Ducky.....P.....khttp://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c138 79.159824, 2016/09/14-01:09:01 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="4C2B94376B6C90EDA87F0BE99B6823CD" xmpMM:DocumentID="xmp.did:5F6B615E93D011E7A147A2BE0285871A" xmpMM:InstanceID="xmp.iid:5F6B615D93D011E7A147A2BE0285871A" xmp:CreatorTool="Adobe Photoshop CC 2015 (Windows)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:149D39EC35B311E783CEDC6F0F50EF9C" stRef:documentID="xmp.did:149D39ED35B311E783CEDC6F0F50EF9C"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>...&Adobe.d.....@...|....s..O.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\bframe[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	3118
Entropy (8bit):	5.593613599176476
Encrypted:	false
SSDEEP:	96:aA1OLKIXOgKNOMK53Q3VIA1OLKIXOgKNOMK5UpQQBFVE4:pAKIVKfKFQlDAKIVKfKmpQQBzE4
MD5:	D490665160AA5220EA94324E1088BF36
SHA1:	6E3640FA0AD74A42F4152E8A1B3143FCEC672F8E
SHA-256:	A10D6A1E237D59AB31DF58F1C20F7C49E8707D04CA846CA0FF63C60BC0E77E1D

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\bframe[1].htm	
SHA-512:	1D5912FAF53B798F6025C4C8BD1B7FB912309A247988792287970A04CA0CAC78384073E57A863246C7C039003086110052A084F552DB016A49EB9ED7C1FB8FEC
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE HTML><html dir="ltr" lang="en_gb"><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/539Evs44yecoSf-lkJBQzKKj/styles__ltr.css" nonce="hgqeqvRL5/raKA4eHqoY5g">.<script nonce="hgqeqvRL5/raKA4eHqoY5g" type="text/javascript">window['__recaptcha_

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\campaignpilot[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):	266616
Entropy (8bit):	5.017545588174341
Encrypted:	false
SSDEEP:	1536:NJL+ZMdM7HozxV3jcTU3dbkGi9ZdsQ6jXAbXJaqYNcJbFRbSmkZPBr57CfS:NJL+lO5
MD5:	6049B6F2CE95F622566657901F6966B2
SHA1:	BC26066A3221242828AE2517DACFC2B094077286
SHA-256:	53F8AEC2AA02D057DE5D49D3820D4C08627517B3E23961E08CC0F2110983C147
SHA-512:	C9A0199FDEF689C501AF319EF6A692C13101AEED3B91942548F4630D55F8B8B6D39BBA01F9FEADF4C927C987804CEB1E9DE2BC091D0230A97E9CC80C185542D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://campaignpilot.com/plugins/campaignpilot.js
Preview:	!function(i){var a={};function o(t){if(a[t])return a[t].exports;var n=a[t]={i:t,l:!1,exports:{}};return i[t].call(n.exports,n,n.exports,o),n.l=!0,n.exports}o.m=i,o.c=a,o.d=function(i,a,t){o.o(i,a)||Object.defineProperty(i,a,{enumerable:!0,get:t})},o.r=function(i){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(i,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(i,"__esModule",{value:!0})},o.t=function(i,a){if(1&a&&(i=o(i)),8&a)return i;if(4&a&&"object"==typeof i&&i&&i.__esModule)return i;var t=Object.create(null);if(o.r(t),Object.defineProperty(t,"default",{enumerable:!0,value:i}),2&a&&"string"!=typeof i)for(var n in i)o.d(t,n,function(a){return i[a]}.bind(null,n));return t},o.n=function(i){var a=i&&i.__esModule?function(){return i.default}:function(){return i};return o.d(a,"a",a),a},o.o=function(i,a){return Object.prototype.hasOwnProperty.call(i,a)},o.p="",o(o.s=11)}([function(i,a){var o;o=function(){return this}();try{o=o||new Function("return this")()}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\course-information[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, CR, LF line terminators
Category:	dropped
Size (bytes):	25797
Entropy (8bit):	4.8971616640046
Encrypted:	false
SSDEEP:	768:sAO95KE1iiioiWixiNi/iwiPiZvQairixuLyaK1uwGQ79199W9997X5ERx:CJjB2uuTMavQa4ig+aKgQ79199W9997w
MD5:	6E714B1DD108BBC3C645A0F0A9EAECDB
SHA1:	66C0E4B232E4189926BB20159CC09D652C19ED61
SHA-256:	2A8EFA3E0B91FF7FA34F56BD74B6EDEB6301A5D30B06743A05742FDE63CEDFA5
SHA-512:	01FF9AAFF66420976258C90410F645EE35CBC8DAA48118F79A077527255120AE8C6DB6A10E0010880CB21BF405F822AB84355B8609AE2E35FC9759D90E0E3CEB
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE HTML>.<html lang="en-gb" dir="ltr" data-config='{"twitter":0,"plusone":0,"facebook":0,"style":"121"}'>.. <head>. <meta charset="utf-8">.<meta http-equiv="X-UA-Compatible" content="IE=edge">.<meta name="viewport" content="width=device-width, initial-scale=1">.<base href="https://www.golfcoronado.com/course-info/course-information" />..<meta name="author" content="Super User" />..<meta http-equiv="content-type" content="text/html; charset=utf-8" />..<title>Course Information</title>..<link href="/templates/yoo_avanti/favicon.ico" rel="shortcut icon" type="image/vnd.microsoft.icon" />..<link href="/components/com_dtregister/assets/css/main.css" rel="stylesheet" type="text/css" />..<link href="/plugins/system/jcemediabox/css/jcemediabox.min.css?9d108330040bd2b7386ad9c4cf8105fc" rel="stylesheet" type="text/css" />..<script src="/media/jui/js/jquery.min.js?43572ae32cf0948c0b4f80000130ae29" type="text/javascript"></script>..<script src="/media/jui/js/jquery-noconflict.js?4357

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	376
Entropy (8bit):	5.096039971389907
Encrypted:	false
SSDEEP:	6:0IFF8FXAQYTLQ6ZRWHTizlpdkR5BylA3VuNijFF8FXAQ+56ZRWHTizlpdkR5D7eu:jFmhY3Q6ZRoT6pWR5HuqFmhO6ZRoT6ps
MD5:	36D808AFD866423BAEBCED2A3738F224
SHA1:	859CE6B4933055C377CF49EEA278A25EEAE230EC
SHA-256:	F4B1829668E9570372C8600D16829CFE4830CDBAF4DDF1B58D24E0FD85C79E85

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\css[1].css	
SHA-512:	96E1DC6756E2FE7AC9D91C1504105F0A0C20B27470C14F8F9D8DC60A3D4EB66CA7AC705539FD703BFAEE849C3B853D3926C24DDC96AAE00E9E4A25FF81E641 A1
Malicious:	false
Reputation:	low
Preview:	@font-face {. font-family: 'Noto Serif';. font-style: italic;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/notoserif/v9/ga6Kaw1J5X9T9RW6j9bNfFImajC9.woff) format('woff');.}.@font-face {. font-family: 'Noto Serif';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/notoserif/v9/ga6Iaw1J5X9T9RW 6j9bNfFcWbg.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\css[2].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	189
Entropy (8bit):	5.155585185455369
Encrypted:	false
SSDEEP:	3:0SYWFFWlIYCUwyXY0RI5XwDKLRIHDfFRWdFTfqzrZqcdKEzJKv2EwdMaWnfSDMUg:0IFFrEY0+56ZRWHTizlpdKES2EwLWnam
MD5:	0646418C7AEE21185C202EE136F7AA24
SHA1:	8D5C652ACD0993148978709AC0AA91954EA9F7E9
SHA-256:	1CED2BEE5AB9F13FFACC51B4F4232EF4779576ED39A96FFC57A778AA094A890D
SHA-512:	42A6124C08CA6F16AED032C32EED46F8A0378837C68848A8C527A852060BFC29E45AADE6746DCF0C7D18FA6CD992A467663C7E7A90E4F1E6B9E954250C68BD 4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.googleapis.com/css?family=Montserrat
Preview:	@font-face {. font-family: 'Montserrat';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/montserrat/v15/JTUSjIg1_i6t8kCHKm459WlhzQ.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\errorPageStrings[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):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/errorPageStrings.js
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts ";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet conn ection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";..../used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\extensions[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	assembler source, ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	35137
Entropy (8bit):	5.181642342706989
Encrypted:	false
SSDEEP:	768:7rPm/Vr/vxJoiUdO88fdySHz22D6AYpvMn/Kc:3PmFzpSeYpvMCc
MD5:	B918063EE0B5EBCEE8B632A5F438924C
SHA1:	A49B20C1AA588BDE53E66A756674D6388FD7B1AA
SHA-256:	0C05A7B918840F28CE7AAD8ACB1D35E0043514641D39D6B8EDBE9C63FBACF9F6
SHA-512:	2FFE9BE7D6875C58F29220098D0C6E9A735636732D280CCDDCC740805D1CAA2064E432F1A1CD3B5E30B544B6D794FB7F9BB57A8EA00A2B2B38693F3495A2D5 2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://demo.1-2-1marketing.com/resources/121/css/extensions.css

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\extensions[1].css	
Preview:	/* Copyright (C) 121 Marketing - 121marketing.com */..../* ========== 1-2-1 Modifications - Extensions.. ========== */.. .... .. /* Skip Link */.. ..#skiptocontent a {left:-999px; position:absolute; top:auto; width:1px; height:1px; overflow:hidden; z-index:-999;}..#skiptocontent a:focus, #skiptocontent a:active {color: #fff;background-color: #b30000;left: 0;top: 0;width: auto;height: auto;overflow:auto;margin: 0;padding: 10px 20px;border-radius: 0 0 15px 0;text-align:center;font-size: 1.1em;z-index:999;}...../* Events Calendar */...ev_table {max-width: 800px; width: 100% !important}..div.ev_navigation {margin-bottom: 15px;}..a.ev_link_row {font-weight: 600;}...ev_table td.ev_td_left { vertical-align: middle;padding: 5px; text-align: center;}...ev_table td.ev_td_right {padding: 0;}..ul.ev_ul {margin: 0 !important;}..#cal_title, div#jevents_header { display:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\jquery-noconflict[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	21
Entropy (8bit):	4.20184123230257
Encrypted:	false
SSDEEP:	3:RAK+mK1RNH:1+91RNH
MD5:	E2060C4E5E5955C824723B13A212D3EC
SHA1:	18420CE484978F8BA3D7371FEBF1638828BB7A67
SHA-256:	5B6CF4E6EDA02F7C90B60B3C32413C0851915F8F80A268A913B92929085132A6
SHA-512:	DCC2117E42859D51017047B468A99F65D74D45AC2E86AE1CC5605E39041FF2164E562756D93A89FA1F71CBD331F958B351C5AFE952A47A560120E080D63BD623
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.golfcoronado.com/media/jui/js/jquery-noconflict.js?43572ae32cf0948c0b4f80000130ae29
Preview:	jQuery.noConflict();.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\lesson-rates[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, CR, LF line terminators
Category:	dropped
Size (bytes):	18957
Entropy (8bit):	4.954504553960309
Encrypted:	false
SSDEEP:	384:oAO95KE1iiioiWixiNi/iwiPiZvQairim97LdAt8H5IE79199W9997Dj2vRv5:oAO95KE1iiioiWixiNi/iwiPiZvQair7
MD5:	3B3F334BDA23FDC69D371E5E731619DE
SHA1:	FB72A898A013C1F4CB3D9CACD3BAD553B402C917
SHA-256:	1E6A5F20CE40C864DA8BCE04AFDFB6F9B960969955A155A84292512D852AA3CE
SHA-512:	A3F5947DE8507DC5E64A4CEEFD7F617644F4E2480A646CB0B2971A98390035E53C694CC5A9FBF5C478F3820ADD6301C002C8F61F6EC45745A0B58DB9D589ED6
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE HTML>.<html lang="en-gb" dir="ltr" data-config='{"twitter":0,"plusone":0,"facebook":0,"style":"121"}'>.. <head>. <meta charset="utf-8">.<meta http-equiv="X-UA-Compatible" content="IE=edge">.<meta name="viewport" content="width=device-width, initial-scale=1">.<base href="https://www.golfcoronado.com/instruction/lesson-rates" />..<meta name="author" content="Super User" />..<meta http-equiv="content-type" content="text/html; charset=utf-8" />..<title>Lesson Rates</title>..<link href="/templates/yoo_avanti/favicon.ico" rel="shortcut icon" type="image/vnd.microsoft.icon" />..<link href="/components/com_dtregister/assets/css/main.css" rel="stylesheet" type="text/css" />..<link href="/plugins/system/jcemediabox/css/jcemediabox.min.css?9d108330040bd2b7386ad9c4cf8105fc" rel="stylesheet" type="text/css" />..<script src="/media/jui/js/jquery.min.js?43572ae32cf0948c0b4f80000130ae29" type="text/javascript"></script>..<script src="/media/jui/js/jquery-noconflict.js?43572ae32cf0948c

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\logo_slideshow[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 593 x 73, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	38350
Entropy (8bit):	7.983366384752861
Encrypted:	false
SSDEEP:	768:I5h190TCqCpJoCxoG9TC9tZc3I/4G8yVCcSS853k+D745vkf6Nu:I5h1qTxQoCxhkdgGIS81k+D7aru
MD5:	195D241513685302C4F120A2F8291BC5
SHA1:	F2DF6BE11FC2877BC1DDE60710DA105AA166D081
SHA-256:	6DA961504EBC0C1C587288800C8C6BB2DCE39161600B2EBD7F37FE3D1AC0DEE7
SHA-512:	1686DAFE56AD09A0CF6ED2EAAC9F62E6E6690A27B1A65473D5384D8A49BAAA86C34E319034B4F341E933AD7B0AE64CA1051BEA21C6F5FFAED253EB40AA02D364
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.golfcoronado.com/images/default/logo_slideshow.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\logo_slideshow[1].png	
Preview:	.PNG.....IHDR...Q...I.....fs.....tEXtSoftware.Adobe ImageReadyq.e<..."iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c138 79.159824, 2016/09/14-01:09:01 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:DocumentID="xmp.did:F8FF032793D011E7961DA38488EFB44B" xmpMM:InstanceID="xmp.iid:F8FF032693D011E7961DA38488EFB44B" xmp:CreatorTool="Adobe Photoshop CS6 (Windows)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:D5F0791A35B311E7B3E4DD5B1DF82AB9" stRef:documentID="xmp.did:D5F0791B35B311E7B3E4DD5B1DF82AB9"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>JJ.....BIDATx...xU....NKB.-..HG...RE,....AE.....*.El....D..... @Bz=.....O(....._.;7.sv....Y...|.S'aIII...+J.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\module_default[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2264
Entropy (8bit):	5.13300016250957
Encrypted:	false
SSDEEP:	48:3dHWbBT7nEWXpLeMcRDWKZ55vsIPV0DlNJYS1Xw5J5Hw1hXvTwYvTe:3dHWbB3dXpLe1FjWIPbS1Xw5J5Hw1Fvc
MD5:	39A533A38EA6F34D73C209208351155E
SHA1:	0CAF31F5800E3D01DDF70D67FA62E0BB316C7194
SHA-256:	3C6D689F7C27EF95F57FEEBC3A6DDF1711BC2D1E6225498D558D7DA996AC0076
SHA-512:	69D7664C3D0DCA09B27EA0CA2BD731B7A33CF76D85673C65CE68855713360D40033361F26FA930AB15BA1422080E6583915E182C6202EABD2270D4DE2E48983E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.golfcoronado.com/media/com_acymailing/css/module_default.css?v=1573072179
Preview:	/**.. * @package AcyMailing for Joomla!.. * @version 5.10.10.. * @author acyba.com.. * @copyright (C) 2009-2019 ACYBA S.A.R.L. All rights reserved... * @license GNU/GPLv3 http://www.gnu.org/licenses/gpl-3.0.html.. */.....acymailing_form .grecaptcha-badge{...display: none;..}....div.acymailing_module, .acymailing_module div{...padding: 0 !important;...margin: 0 !important;...border-style:none !important;..}....table.acymailing_form{...margin:auto;...border:0px !important;..}....a.acymailing_togglemodule{...display : block;...font-size:16px;..}.....acymailing_mootoolsbutton p{...text-align:center;..}.....acysubbuttons{...text-align:center;..}....img.captchaimagemodule{...border:1px solid #dddddd;...float: left;..}.....captchakeymodule .captchafield{...margin-top:3px;...margin-left:2px;..}.....acymailing_fulldiv tr, .acymailing_fulldiv td{...border:0px;..}.....acymailing_module_form td {...padding-bottom: 5px;...vertical-align:top;..}....div.acymailing_module_error {...color

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\pga-symbols[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 200 x 89, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	40915
Entropy (8bit):	7.989875312861293
Encrypted:	false
SSDEEP:	768:nOtMhKPE5ht+kSWldDYvsOiJwDEnY/IfNIesql6x/5rd2zsjykZ6s1VnJfK4Z:nOtBPEXt7VlFYv7iJsEnlSegjy7E3Z
MD5:	EA2D20821810A2EDA0408C307519133C
SHA1:	16B7191E231752338BFBC35C11D6E925BCA06E91
SHA-256:	8AC0135A702E36BA253944C78275CD794031AF4647C9162D25133CF6134C3EF2
SHA-512:	566DF5F10E8543674AFA8F9CC1E73AB836E1589D940AAEFD4B5C5A0FBB490FB8F2A25E110D6CBB6525F77B12294A94BCDB84E31F45199B23635D0AC7D040684D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.golfcoronado.com/images/pga-symbols.png
Preview:	.PNG.....IHDR.....Y.....{bkx....tEXtSoftware.Adobe ImageReadyq.e<...fiTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.0-c060 61.134777, 2010/02/12-17:32:00 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="xmp.did:01801174072068119109DFBA8FAD4B6A" xmpMM:DocumentID="xmp.did:0DAE5C7BDB0C11E2A0EAFB44AC454D04" xmpMM:InstanceID="xmp.iid:0DAE5C7ADB0C11E2A0EAFB44AC454D04" xmp:CreatorTool="Adobe Photoshop CS5 Macintosh"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:01801174072068119109DFBA8FAD4B6A" stRef:documentID="xmp.did:01801174072068119109DFBA8FAD4B6A"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>W4.....IDATx..w|.U.5...Lz... ..B.....)....ET.RDA.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\recaptcha__en_gb[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):	340667
Entropy (8bit):	5.688901255172372
Encrypted:	false
SSDEEP:	6144:FAil/eCeI6koTOppAu7jDUHP5rEvcYEGBkms/HZqlG36vAd:mSkrAu7MBrEEGBraHMAd
MD5:	D2A824A6770005938DDC5ABBBC85542D
SHA1:	2E3EAF9360305988AFCFEDB3A0C0B3C17EE2496A
SHA-256:	C7A2E2F328B3BE757106DAA4497F0CDFD45C222FC722739946CF7A3E62D56619
SHA-512:	61C6A389B715E512CAF961932B8C6250E8A60750756C8AC8B81F6E0F996BC1BC24BE454D142DDD0D2025B4924155B909805ADA9F483FBD3D98702F0C66C6786E
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\recaptcha__en_gb[1].js	
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/recaptcha/releases/539Evs44yecoSf-lkJBQzKKj/recaptcha__en_gb.js
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var K=function(){return[function(E,J,u,M,C,p,x){return(E-6)%(((((E^635)%(x=[24,-1,2],14)||(C.W=!1,C.G&&(C.A=J,C.G.abort(),C.A=!1),C.I=M,C.P=u,F[35](30,!0,"error",C),K[x[0]](x[2],null,C)),E>>1&15)==x[2]&&(this.W=function(){return!0}),E)+x[2]&15)==x[2]&&(this.W=new ub),4)||(this.A=x[1]),p},function(E,J,u,M,C,p,x,m,v,t,Q,X,c,O,H,y){if(H=[12,"",1],3==(E+3&7))a:if(X=["[",1,"number"],null==M)C.push("null");else{if("object"==typeof M){if(Array.isArray(M)){for(O=(c=(C.push((v=(t=M,t).length,X[0])),J),0);O<.v;O++)C.push(c),K[H[2]](24,H[1],u,t[O],C),c=",";C.push("]"),y=void 0;break a}if(M instanceof String||M instanceof Number||M instanceof Boolean)M=M.valueOf();else{for(Q in p=(C.push((m=M,"{")),J),m)Object.prototype.hasOwnProperty.call(m,Q)&&(x=m[Q],"function"!=typeof x&&(C.push(p),N[42](10,"\\u",X[H[2]],C,Q),C.push(":"),K[H[2]](16,H[1],u,x,C),p=","));y=(C.push("}"),void 0);break a}}switch(typeof M)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\script[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	downloaded
Size (bytes):	42577
Entropy (8bit):	5.21583748325005
Encrypted:	false
SSDEEP:	768:7bVt8AX2B1oxJ6PjIN9DnspkgspdEIP1xMElgB4YLglxP6yNR/M0LXwQhWazNAtj:7bVt8AX2B2xJ6PjI9jspkgspdEIP1xMJ
MD5:	94CB6C19794ACB22C4FC199FBC6338D8
SHA1:	A71A2395EFD0AF2994DBC71A24E1E6CCE5549538
SHA-256:	9C18AE9B31E16AF8358DBA57A85EAD002B1CD0769EDF325373EFC2E69CB1C802
SHA-512:	EA5CC806B19089FC51BA768D93DE1826D978AA0715AACA70326A7C6D0CC85E9976CC695D40F369EE789BED369B333332E8ABAD67ADB6F635948270B9E30629 4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.golfcoronado.com/media/com_rsform/js/script.js
Preview:	var RSFormProCalendars = {};..var RSFormProPrices = {};..var ajaxExtraValidationScript = {};..var RSClickedSubmitElement = false;....if (typeof RSFormPro != 'object') {...var RSFormPro = {};..}....RSFormPro.Forms = {};..RSFormPro.Editors = {};..RSFormPro.scrollToError = false;..../* Handle HTML5 form fields validation for the forms without AjaxValidation enabled */..RSFormPro.setHTML5Validation = function (formId, isDisabledSubmit, layoutErrorClass) {...var submitElement = RSFormPro.getElementByType(formId, 'submit');...for (i = 0; i < submitElement.length; i++) {....if (RSFormProUtils.hasClass(submitElement[i],'rsform-submit-button')) {.....RSFormProUtils.addEvent(submitElement[i], 'click', (function (event) {......errorElements = RSFormPro.HTML5.validation(formId);.....if (errorElements.length) {.....for (j = 0; j < errorElements.length; j++) {.....errorElements[j].field.className = errorElements[j].field.className.replace(' rsform-error', '') + ' rsform-error';.....if (docu

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\sub_banner_1[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], progressive, precision 8, 2000x500, frames 3
Category:	downloaded
Size (bytes):	367671
Entropy (8bit):	7.975545700579442
Encrypted:	false
SSDEEP:	6144:fLHf7Lli1iWeRTQUQAuDEdOwXI4bBB4jtO5d7XHa+ohUxCERJjcwIKrj9oH:fLHTLlwiWeRTQUQAdXVTcOnD6+oibFrA
MD5:	1AAAC083C8076AFDA75F084F74000113
SHA1:	505A22342196E41A82AB433C9C86689721FBC189
SHA-256:	66A45840CCDEB364AB652877DC6C680CFAF0529F8B6D3E55C59EA89E254FA672
SHA-512:	AFF71448D021B6A99026A82029195837EC1B596F96F17075B2A7866926ACF1A1B8F3FAFD7D32932D5B72DAE8A6389155B21341391AD99763985BBF45711FC5BD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.golfcoronado.com/images/slideshows/sub_banner_1.jpg
Preview:	......Exif..II*.................Ducky.....P.....)http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c138 79.159824, 2016/09/14-01:09:01 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:DocumentID="xmp.did:25A0FFB493D011E7A054833303133F8B" xmpMM:InstanceID="xmp.iid:25A0FFB393D011E7A054833303133F8B" xmp:CreatorTool="Adobe Photoshop CS6 Windows"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:EA1FB01335B211E79E57E4EA31DEB17A" stRef:documentID="xmp.did:EA1FB01435B211E79E57E4EA31DEB17A"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>...&Adobe.d.....@...0.....5..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\tim[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 250x271, frames 3
Category:	downloaded
Size (bytes):	26935
Entropy (8bit):	7.968326953487846
Encrypted:	false
SSDEEP:	768:AU8F5xr8R1kcb+wFQeZtLiUUXgrV2G9nEZ:Arbl8XkFQBUGZy
MD5:	91448350848B84E523A98C221344C569
SHA1:	09942010853DA36B004A5A01F486FEC5F1CD85E8
SHA-256:	FE9E6938A05A450466D380B446488C48B08BF0A12EACC5BBD7B65385DF62DD21

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\tim[1].jpg	
SHA-512:	37A0D8797DCEEF736B4187B880BE5E715470218D548ECF44E544A2DAA8486A7D8EC5ADDCED8FCBFE32622B59B5CB480B34938CEB3DA97031C12E8EB382FA7(E4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.golfcoronado.com/images/tim.jpg
Preview:	.....Exif..II*.....Ducky.....<.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x: xmptk="Adobe XMP Core 5.6-c138 79.159824, 2016/09/14-01:09:01 "> <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:DocumentID="xmp.did:1EC1E687379111E7B87DE3E3B50409BD" xmpMM:InstanceID="xmp.iid:1EC1E686379111E7B87DE3E3B50409BD" xmp:CreatorToo l="Picasa"> <xmpMM:DerivedFrom stRef:instanceID="00EADC41A1EA1B718F845FC2CD343C82" stRef:documentID="00EADC41A1EA1B718F845FC2CD343C82"/> </r df:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>....Adobe.d.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\velocity.ui[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):	13532
Entropy (8bit):	5.2187976373075005
Encrypted:	false
SSDEEP:	192:jiQyqkgd8kIentWUUUlZKddp4TXA2jB+Ty0nynDU2np58Dv9:jiukgmddWTXkyLTWV
MD5:	6773BC8C6AB7F71DD7AF54364B3C9E8F
SHA1:	11A380044D24E427A0C6D7DA7D114D46413C49D6
SHA-256:	6D07C90B8431C31152A84722BBA0B488B88311C3F66D6D62D7231D968DF6FF31
SHA-512:	F1E10CD96CD338415E3744B6A2D16D1B5ABA13728E8AA42F9C51EDBDCEE63570FABF334C986F796AD5720D0C8C48FAD2E7E2C315CFCCEB530117D8BE93B67 07
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.golfcoronado.com/media/com_rstbox/js/velocity.ui.js?v=3.3.3
Preview:	!function(t){"use strict";"function"==typeof require&&"object"==typeof exports?module.exports=t():"function"==typeof define&&define.amd?define(["velocity"],t):t()}(function() {"use strict";return function(t,a,e,r){var n=t.Velocity;if(n&&n.Utilities){var i=n.Utilities;if(function(t,a){var e=[];return!(!t||!a)&&(i.each([t,a],function(t,a){var r=[];i.each(a,func tion(t,a){for(;a.toString().length<5;)a="0"+a;r.push(a)}),e.push(r.join(""))}),parseFloat(e[0])>parseFloat(e[1]))){{major:1,minor:1,patch:0},n.version)){var s="Velocity UI Pack: You need to update Velocity (velocity.js) to a newer version. Visit http://github.com/julianshapiro/velocity.";throw alert(s),new Error(s)}n.RegisterEffect=n.RegisterUI=fun ction(t,a){function e(t,a,e,r){var s,o=0;i.each(t.nodeType?[t]:t,function(t,a){r&&(e+=t*r),s=a.parentNode;var l=["height","paddingTop","paddingBottom","marginTop","margin Bottom"];"border-box"===n.CSS.getPropertyValue(a,"boxSizing").toString().toLowerCase()&&(l=["height"]),i.each(l,function

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\webworker[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	105
Entropy (8bit):	4.942139566434552
Encrypted:	false
SSDEEP:	3:JSbMqSL1cdXWKQKLbgasj/u8WWHSCf:PLKdXNQK5sjm8Nf
MD5:	38C3525E8D73FD8314A2C33D7CA1AAE9
SHA1:	19E620E7F25113902265184776AE1862FB0E8D0F
SHA-256:	4FA982263F2FD4FCA6A3FCDCAB5196E77464E3ECC158BCCD9AEEC9B7732B117B
SHA-512:	A96E5FF268721823B5FC5BA3349D100CA06A17543EB9A8F9297F05A911EC0244DFD94785C9C0F5DC2969AE4B890D8EDFA61E7C49638E68B3D0006201104C48C
Malicious:	false
Reputation:	low
Preview:	importScripts('https://www.gstatic.com/recaptcha/releases/539Evs44yecoSf-lkJBQzKKj/recaptcha__en_gb.js');

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\webworker[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	105
Entropy (8bit):	4.942139566434552
Encrypted:	false
SSDEEP:	3:JSbMqSL1cdXWKQKLbgasj/u8WWHSCf:PLKdXNQK5sjm8Nf
MD5:	38C3525E8D73FD8314A2C33D7CA1AAE9
SHA1:	19E620E7F25113902265184776AE1862FB0E8D0F
SHA-256:	4FA982263F2FD4FCA6A3FCDCAB5196E77464E3ECC158BCCD9AEEC9B7732B117B
SHA-512:	A96E5FF268721823B5FC5BA3349D100CA06A17543EB9A8F9297F05A911EC0244DFD94785C9C0F5DC2969AE4B890D8EDFA61E7C49638E68B3D0006201104C48C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\webworker[2].js	
IE Cache URL:	http://https://www.google.com/recaptcha/api2/webworker.js?hl=en-GB&v=539Evs44yecoSf-lkJBQzKKj
Preview:	importScripts('https://www.gstatic.com/recaptcha/releases/539Evs44yecoSf-lkJBQzKKj/recaptcha__en_gb.js');

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\7Aulp_0qiz-aVz7u3PJLcUMYOFmQkEk30e4[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20616, version 1.1
Category:	downloaded
Size (bytes):	20616
Entropy (8bit):	7.975466659735134
Encrypted:	false
SSDEEP:	384:wJokRB8gQmIFnjJuWgh8owj/WFUzek0vrXfNVWgxw8FgWs7SMkcUqM:wWkccUjJdg2owjUbWr8mWnM1U3
MD5:	76FA45D4455A086B9132FEEA5F587330
SHA1:	B7258076BD6781D78300E83BB6E8BB37CA7CA329
SHA-256:	45BD0FCC14529DDE76DB9204A56040DDBDC1BCC0C4C3299DADBF97D69A751EED
SHA-512:	92B54C54E080377F59D94672869929FC0187F10A4219506851F50C14C63BD4EF169AA553591C96CFE72B50E93A6C1E90FBAD1D2CBA2F942D4919BA96AD5D7269
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/muli/v22/7Aulp_0qiz-aVz7u3PJLcUMYOFmQkEk30e4.woff
Preview:	wOFF.....P.....GDEF.....>...R.W..GPOS.....S.....8u.GSUB...(...c....~.J.OS/2.....O...``...STAT.....8...D.H..cmap.....G.e.cvt .....O.....fpgm..... .6..gasp.....glyf.....64..f..7s.head..J....6...6..Ymhhea..JL... ...$....hmtx..Jl.....0..4mloca..LX.....v,maxp..Nh... ... .m..name..N....=...n<.a.post..O..... ...2prep..O..... 'Dn.x.....P.F..~R..*....i...[..u..t..L.!...q..../w|..Z*.....x..Ah$.....7.t.L...=..$.*. .d.;. .k..+..._.p.;..rfa...,ZH6%8.tp.:.LFS...T.R./..T.1....:..9..s.._B.....:O<....._.<..$.'/.....8G.U.V..9X{ ..Gx...U..E....Gk..4.. .]U...\...T..&....9.$.....X..c...@5.D.#.....d.uQ3g<.....b..#A...+....J?.....6z.k..jL.3....$.(.;.%`-T.F.....t.{r...#...Cp..*U.VW]A..\.....B....=wAcR.<...vIIU+. .@..+.+.U-zV...Q..P.+;h.(.OSUd:l.%%.U...W.9....%.N0.K.k...UJB.T%...c....5&Y..{y...f..-#e.l..a.....C..1%..4.d...J.4W...k....^h.C3s.;..c.4Q...*...L7A{.....cey.wfj..>&eK..#

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\JTUSjIg1_i6t8kCHKm459WlhzQ[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 23480, version 1.1
Category:	downloaded
Size (bytes):	23480
Entropy (8bit):	7.981253427621622
Encrypted:	false
SSDEEP:	384:lEfDbJfERirQIhTVId2GTJO8Z84zUE8EW3md2T0LuYXDbMdK3OLmvTHc5qawV:lEf3JPrQI8d2F8WDE9w0FLTbMdK+Cvj3
MD5:	8102C4838F9E3D08DAD644290A9CB701
SHA1:	5AF1938D1327395F47C84E57B6BA7756234D2262
SHA-256:	60CEBEA4C9183F51FBD323F14DD729E18768BE4F6395467013216AE36526CF9C
SHA-512:	E8A0D6B72163E407DE82170E4560044CAE90116D1DD3CFA20F140E4379C8AABDC5BEAC6DD965D0E925CA673E41C42A858975C47F1F8152637958569D239E91F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/montserrat/v15/JTUSjIg1_i6t8kCHKm459WlhzQ.woff
Preview:	wOFF.....[.....8.....GDEF.....G...X.g.^GPOS.....2.....GSUB.....,.OS/2...\...N...`S..Ucmap.....h.cvt ...p...\..../R.Hfpgm.....F...mM$.\|gasp..... ...glyf.....3X..],..$head..Rt...6...6.F.nhhea..R.... ...$....hmtx..R....%...>.x..loca..T.....(..*0maxp..W.... ... .h.Yname..W4.....-5H.post..X$.....D.z.prep..Z.....K..x.%.... P.....@:D...$..]!....h.....2/.$.....D.^.F..ua.].N....%>./...x..ut.I.....e+..o...g.^..13333333333.-.e/.cgYAs....R.{.G..^.L.....j.....R.z..D..o...~.....$.`.BY.21.W.....9...f.C..(..M.!..D....1rT ...w6cG.J....U.....]..>.....q..jhT\l..;,M.zYK..x:.n.R...(.....g)..~...Xl#`.....-.#..T...]..Tw.....k.7....I.....@..$..r....X.\..L....._.H.2".V... .1...".._d.#R..4c"...2> ..A..D;..e>".|Tt.1. .....8...._.K..+.....Y~'r.A.....D.../..W..ob.....[.8K.8Gtq..0...|....D.KE+..".-V.....\vr.._-.Se..=..A.1$...<.E.CL..%QB.8.9.....,.Jv.=,...%.i..:U*V..U.b..]N.D..O..'...1.$.....<

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\KFOlCnqEu92Fr1MmEU9fBBc9[1].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...../.....+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\G62TDH9B\KFOlCnqEu92Fr1MmYUtfBBc9[1].ttf	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	TrueType Font data, 18 tables, 1st "GDEF", 8 names, Microsoft, language 0x409, Copyright 2011 Google Inc. All Rights Reserved.Roboto BlackRegularVersion 2.137; 2017Roboto-Bla
Category:	downloaded
Size (bytes):	35208
Entropy (8bit):	6.392518822467014
Encrypted:	false
SSDEEP:	768:53Dmu13ucOmpIN22bN8o6Ze0XlGV+uM49pSeCu7XniviDffw6mo/quUR:lD13DjSNz0XlG0uL9YeCu7Xn4iTo9o/4
MD5:	4D99B85FA964307056C1410F78F51439
SHA1:	F8E30A1A61011F1EE42435D7E18BA7E21D4EE894
SHA-256:	01027695832F4A3850663C9E798EB03EADFD1462D0B76E7C5AC6465D2D77DBD0
SHA-512:	13D93544B16453FE9AC9FC025C3D4320C1C83A2ECA4CD01132CE5C68B12E150BC7D96341F10CBAA2777526CF72B2CA0CD64458B3DF1875A184BBB907C5E3D71
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmYUtfBBc9.ttf
Preview:	..... GDEF.....z\...dGPOS.....z.....GSUB7b.....OS/2ve#...p....`cmap.....r....Lcvt ...=..xX...Zfpgm..#...ud....gasp.....zP....glyf.....,..i~hdmx.....q ....head...R..l....6hh ea.]....p....$hmtx..<...l.....locaK./...j.....maxp.....j.... name..9...x....|post.m.d..z0... prep...C..w ...8...d...(.....P...EX../....>Y..EX../....>Y.....9.....9.....9.....9.....9.....0 1!!.!.....!.5.!.(.<..6.....}.w...x.^.^..^....g.....<.....9.....EX../....>Y..EX../....>Y....+X!...Y..../01.!.!.462..."&....+.g..k.kk.k.....J__.__.....^.....&.....9...../.....9../. .....01..#.3..#.3.+..._+...v.S.8..S.8.....z..... !..9.....EX../....>Y..EX../....>Y..EX../....>Y..EX../....>Y.....9../.....+X!...Y...../.....+X!...Y.....01.#.#.#5 3.#53.3.3.3.3.!.3.!.#.3.#.d.C.C.,..E.D.E.E...,...C.@.,....f....../...`...`.....f.Q.....S.&.Q...-.r.+./..9...EX../....>Y..EX.!/..!.>Y..!...9.....!..9.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\KFOmCnqEu92Fr1Mu4mxP[1].ttf	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	TrueType Font data, 18 tables, 1st "GDEF", 8 names, Microsoft, language 0x409, Copyright 2011 Google Inc. All Rights Reserved.RobotoRegularVersion 2.137; 2017Roboto-Regularht
Category:	downloaded
Size (bytes):	35408
Entropy (8bit):	6.412277939913633
Encrypted:	false
SSDEEP:	768:PX4i+tezjtQYgu30G0xL9nQbuEL7LQo9SBxQbptqKmomjJlvh:PJ2z3G0xpUusLEBKptqNomjV
MD5:	372D0CC3288FE8E97DF49742BAEFCE90
SHA1:	754D9EAA4A009C42E8D6D40C632A1DAD6D44EC21
SHA-256:	466989FD178CA6ED13641893B7003E5D6EC36E42C2A816DEE71F87B775EA097F
SHA-512:	8447BC59795B16877974CD77C52729F6FF08A1E741F68FF445C087ECC09C8C4822B83E8907D156A00BE81CB2C0259081926E758C12B3AEA023AC574E4A6C9885
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4mxP.ttf
Preview:	..... GDEF.....{`...dGPOS...h..{.....GSUB7b.....OS/2tq#...q....`cmap.....s....Lcvt +.....yl...Tfpgmw.`...vd....gasp.....{T....glyf.....,..j.hdmx.....r ....head.j.z..m....6hh ea.....q....$hmtx..Vl..m.....loca?.#...k.....maxp.....k.... name.U9...y....tpost.m.d..{4... prep.f....x ...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\G62TDH9B\accordion-parent[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	259
Entropy (8bit):	4.793726348810922
Encrypted:	false
SSDEEP:	3:RAMTFxHCGzEJdUKZkuQlw2/WO8ZWIAFv//BVkb6LqEJbGbcQDrAF5e6LqEJbG0t9:zCGzkjQ0ZRgHI2983D8F5p9qKRVQLJe
MD5:	4D8303E315C9A58D34FEC81202E893B4
SHA1:	9D39FE103CC0CA082AE39FDA2A41A048FD6DB6E0
SHA-256:	86719B89CF556A8E8C2028D899E4A6B335F6B4EB4FA93369BD81CF830B4BC66B
SHA-512:	745B7C8C2D7EF4BCB13CC84CDB80276D5076ACD3E5131E885D02DC3C15E8A5A2C1B474DE6AB75978B713AA777E06E7E1098F567C1565464604AB411CBB02435
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://demo.1-2-1marketing.com/resources/121/js/accordion-parent.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\accordion-parent[1].js	
Preview:	jQuery(function($) { .. // "Neutralize" the URL in parent menu items for an accordion style offcanvas menu . $(".uk-offcanvas-bar .uk-nav > .uk-parent > a").attr("href", "#"); ...$(".uk-offcanvas-bar .uk-nav > .uk-parent").removeClass("uk-open");..});

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\adult-group-lessons[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, CR, LF line terminators
Category:	dropped
Size (bytes):	19750
Entropy (8bit):	4.9978840274421605
Encrypted:	false
SSDEEP:	384:HAO95KE1iiioiWixiNi/iwiPiZvQairimTlLdAt5r4FYk7z79199W9997ajoVRv5:HAO95KE1iiioiWixiNi/iwiPiZvQair2
MD5:	9349593412D58837662DEA103AA2D2A7
SHA1:	9883D994582797A331B4596BCB5C69056B6E9130
SHA-256:	6210D56C95E1E529A901B60DF1ABD397A10BFCE6A33EDFD8014BF79AD5ED42D5
SHA-512:	7E247353A1BD61441F07CA2DBC6A9A73D9A38F7D9C8D360FC3431DFE2B67A1B033621ABA217169FFB54C8436F24B64E401F92CEDEB11C95B36FAB8FE93EB42C
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE HTML>.<html lang="en-gb" dir="ltr" data-config='{"twitter":0,"plusone":0,"facebook":0,"style":"121"}'>.. <head>. <meta charset="utf-8">.<meta http-equiv="X-UA-Compatible" content="IE=edge">.<meta name="viewport" content="width=device-width, initial-scale=1">.<base href="https://www.golfcoronado.com/instruction/adult-group-lessons" />..<meta name="author" content="Super User" />..<meta http-equiv="content-type" content="text/html; charset=utf-8" />..<title>Adult Group Lessons</title>..<link href="/templates/yoo_avanti/favicon.ico" rel="shortcut icon" type="image/vnd.microsoft.icon" />..<link href="/components/com_dtregister/assets/css/main.css" rel="stylesheet" type="text/css" />..<link href="/plugins/system/jcemediabox/css/jcemediabox.min.css?9d108330040bd2b7386ad9c4cf8105fc" rel="stylesheet" type="text/css" />..<script src="/media/jui/js/jquery.min.js?43572ae32cf0948c0b4f80000130ae29" type="text/javascript"></script>..<script src="/media/jui/js/jquery-noconflict.js?43

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\analytics[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	48759
Entropy (8bit):	5.5215063523389265
Encrypted:	false
SSDEEP:	768:/yR3fYFBLbfsce5XqY1TyPnHpX/KWY3SoavPVRhwmCgYUD0lgEw0stZc:/y9gZfA5h1UHpXxY3Soiuw0sU
MD5:	0A4E309B5F2D7439B4F8876B19F37FC7
SHA1:	7AC30F933A2B889EDBE5D3449F4EC90049B0E2A9
SHA-256:	F79723478F4C48501CD49AC52B81D6244A6562B9D3F08CE8AB208A8B8878D4C4
SHA-512:	891337D9CD308331BD0166BAA7C99C2B856D47F0ADE8AF596F71AFFC962546BBE0952554C51CC9A10E28BB4CEE3648AEC819D83A8935E69E95F53F5CBF141C4
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\G62TDH9B\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):	14591
Entropy (8bit):	5.951233123677449
Encrypted:	false
SSDEEP:	384:L/SZ4Bzc3G3sRklYKN7dJTSu9MfB5A8lET:L/SZ4oisRkCKNf9M7vET
MD5:	62709BE7851FB416E5AD7C7488982C51
SHA1:	AC6B236C2F1DD2907A3889866EAA5F9BB406B93C
SHA-256:	979BF4B1CA1779E34A0B86CEEFEFD2AAB0F96C80AAB26416101041B45B4E666B
SHA-512:	B20E022D76C387C5BD80151E7ED49BA2B299A1894842FFFFCDDBC2C19C36710143A45B85F6B19B5A521639548DC3540D9A690315C75370167C36042A5CCE13B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\anchor[1].htm	
Preview:	<!DOCTYPE HTML><html dir="ltr" lang="en_gb"><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/539Evs44yecoSf-lkJBQzKKj/styles__ltr.css" nonce="xE5n4h+gJHwH/P+uSQhEug">.<script nonce="xE5n4h+gJHwH/P+uSQhEug" type="text/javascript">window['__recaptcha_a

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\bootstrap[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	188766
Entropy (8bit):	5.14156663997269
Encrypted:	false
SSDEEP:	3072:h5vYrcLiT0dQgoopSR55Al4+8UIEAKOLpQW+9Cb3IzlJ6GNpRqaLjnQKwGyc+U3h:h5wrcLiT0dQZopSR55Al4+8UIEAKOLpQ
MD5:	119E02F23B1BC8FBC54F475A2E598A79
SHA1:	F2B32B7F971365AC1A98E19097E7BC23B3E132CB
SHA-256:	3DDA9689ADCB6BD7C8F5857E1EE695864AAF366909994B0061ED3FAD2B5F7FEB
SHA-512:	9D7DBF412DF02987C2F22CF158F07A99165ED0C56642A3868AAB231FF9A3C37628CB253F7346B69CCA43DE9F704004FB26F8B8AE6D9A200F05B1490A429D245E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.golfcoronado.com/templates/yoo_avanti/css/bootstrap.css
Preview:	/* Copyright (C) YOOtheme GmbH, YOOtheme Proprietary Use License (http://www.yootheme.com/license) */..@import 'https://fonts.googleapis.com/css?family=Noto+Serif:400,400italic';.@import 'https://fonts.googleapis.com/css?family=Montserrat';.article,.aside,.details,.figcaption,.figure,.footer,.header,.hgroup,.nav,.section {. display: block;.}.audio,.canvas,.video {. display: inline-block;. *display: inline;. *zoom: 1;.}.audio:not([controls]) {. display: none;.}.html {. font-size: 100%;. -webkit-text-size-adjust: 100%;. -ms-text-size-adjust: 100%;.}.a:focus {. outline: thin dotted #333;. outline: 5px auto -webkit-focus-ring-color;. outline-offset: -2px;.}.a:hover,.a:active {. outline: 0;.}.sub,.sup {. position: relative;. font-size: 75%;. line-height: 0;. vertical-align: baseline;.}.sup {. top: -0.5em;.}.sub {. bottom: -0.25em;.}.img {. /* Responsive images (ensure images don't scale beyond their parents) */. max-width: 100%;. /* Part 1: Set a maxium relative to the

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\brian[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 250x238, frames 3
Category:	downloaded
Size (bytes):	23963
Entropy (8bit):	7.967294235530662
Encrypted:	false
SSDEEP:	384:ycREjZhP72HISnwK7hAjMbyPnFnflQrNvl7FaASr+GPtMy6xIYXusvZ2GKsBAW1X:ycREFl72oSnwoyguPnplmJZFSiZZ6eNr
MD5:	43DD35A924C0DF13CF223F9E7941656D
SHA1:	B22438CE96E32032305262C54710EA1142A56314
SHA-256:	E7B6D36355DCDD635090486B67CBFE7407A8005F5F617D1D9F9D7D85BE945544
SHA-512:	BE9662FE230488D9B20DA50C4F4FC792EAD33E40C400B3280B813228E7D25E28349AEA71BA14B6FD4AF739DAD992645AFEA4039F4D3D717BCC90AF4A0861A6E3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.golfcoronado.com/images/brian.jpg
Preview:	.....Exif..II*.....Ducky.....<.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c138 79.159824, 2016/09/14-01:09:01 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:DocumentID="xmp.did:1EC1E683379111E7B87DE3E3B50409BD" xmpMM:InstanceID="xmp.iid:1EC1E682379111E7B87DE3E3B50409BD" xmp:CreatorTool="Picasa"> <xmpMM:DerivedFrom stRef:instanceID="C56009A605DB68C370CCBD1B07D2AB8A" stRef:documentID="C56009A605DB68C370CCBD1B07D2AB8A"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>....Adobe.d.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\callt[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 9 x 12
Category:	downloaded
Size (bytes):	93
Entropy (8bit):	5.040234882752285
Encrypted:	false
SSDEEP:	3:CT/wiRalll/DylOrPP2hjLHaybQn:kLRultFr325jbQn
MD5:	0718C393FBD4095B219803CB6B7BCBF8
SHA1:	88A51E34BC8C5D616B76743A52AD1FE0CAE8232E
SHA-256:	FA25AB37F9AB93F593B571405719BC288EB285210C5C0450E4D7D0EE7ECECB38
SHA-512:	D8846866CA053C69307B6507C590851AABB2E82B9D3CA0947C9B6443DFABB2B9B906784A462516C28D64ECBC5B5C96A0C5FA1F84214884A3FE2914965BAC840
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\callt[1].gif	
Reputation:	low
IE Cache URL:	http://https://www.golfcoronado.com/media/com_rsform/css/calendar/callt.gif
Preview:	GIF89a.....3f.....3ff.....!.....,.....''X.....!..{1.A.....v^.....A.UN..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	1303
Entropy (8bit):	5.3619822684805
Encrypted:	false
SSDEEP:	24:5+0OYskJOYsGVU2JOYN7GVTdV0OYN4B+V0OYsD+V0OYUTfV0OYN78:E0OL4OLGVU2OCGVTMOW4rOLNOxTSOC8
MD5:	5C3A2BFCF7CCC53DD57FB41069074FA4
SHA1:	D0E7028E5F1A7972D05DE298B8F10D93A24931D1
SHA-256:	54DCC0DD0A721BBF8A600A5CCB7AA62F2E25944C6519A52495194FD483A41A48
SHA-512:	2FC6A6C62111270B6E94CA722A93E4ABDAA11002B0924C29718A70AD67B4B02D466D3CF02FD8CDEF3420DE1C9B19C6AA7B130A0A5A5448CA9318ABDE4AE5F27
Malicious:	false
Reputation:	low
Preview:	@font-face {. font-family: 'Fjalla One';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/fjallaone/v8/Yq6R-LCAWCX3-6Ky7FAFrOF6lA.woff) format('woff');.}.@font-face {. font-family: 'Lora';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/lora/v17/0QI6MX1D_JOuGQbT0gvTJPa787weuxJBkqs.woff) format('woff');.}.@font-face {. font-family: 'Lora';. font-style: normal;. font-weight: 700;. src: url(https://fonts.gstatic.com/s/lora/v17/0QI6MX1D_JOuGQbT0gvTJPa787z5vBJBkqs.woff) format('woff');.}.@font-face {. font-family: 'Muli';. font-style: normal;. font-weight: 300;. src: url(https://fonts.gstatic.com/s/muli/v22/7Aulp_0qiz-aVz7u3PJLcUMYOFmQkEk30e4.woff) format('woff');.}.@font-face {. font-family: 'Muli';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/muli/v22/7Aulp_0qiz-aVz7u3PJLcUMYOFnOkEk30e4.woff) format('woff');.}.@font-face {. font-family: 'Muli';. font-style: normal;. font-weig

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vIlJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/dnserror.htm?ErrorStatus=0x800C0005&DNSError=1460
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMoreInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/down.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\down[1]	
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~..... ....b.....$..s...7tRNS.a.o(,.s....e.....q*..... .....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV ...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\engagebox[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):	13652
Entropy (8bit):	5.259006093033364
Encrypted:	false
SSDEEP:	384:2hQ9//fVi7bwamWbnLawN5Orc3zRav4dH7XaG:2hKXVi9mCLawNgGzRtH7X9
MD5:	3FB262C100089B5C2746B85EEEFC5379
SHA1:	F29F9BA1C2C8B7A45043A8B09B6777A18D630C5B
SHA-256:	9B2C4C124A927D28ED07FCA1DD848E9FC2EF4BE5F181799ECB5B02C765CFA920
SHA-512:	7D87DCF94D8374673F4639C363D455433877D3CB188A75FB305DA52290980EDC625EE9DEC0443EDB16262824458B198637A65B58F6FEFD2B685A5E7913374A99
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.golfcoronado.com/media/com_rstbox/js/engagebox.js?v=3.3.3
Preview:	if(jQuery(function(e){function t(){return[-(o("padding-top")+o("margin-top")+o("border-top-width")),-(o("padding-right")+o("margin-right")+o("border-right-width")),0,-(o("padding-left")+o("margin-left")+o("border-left-width"))].join("px ")+"px"}function o(t){return body=parseInt(e("body").css(t)||0),html=parseInt(e("html").css(t)||0),body+html}e(document).on("ebox:OnAfterInit",function(){$mats=e(".rstboxes .welcomemat"),$mats.length&&($mats.each(function(t,o){$mat=e(o),$mat.css({height:$mat.css("height")}),$mat.bind("beforeOpen",function(){window.scrollTo(0,0)}),$mat.bind("afterOpen",function(){e("html").addClass("eboxWelcomeMat")}).bind("afterClose",function(){e("html").removeClass("eboxWelcomeMat")})}),e(" ").addClass("rstboxes eboxWelcomeMats").prependTo("body").css({margin:t()}),$mats.appendTo(e("body .eboxWelcomeMats")))})}),void 0===rstbox)var rstbox={};void 0===rstbox.jQuery&&(rstbox.jQuery=jQuery.noConflict()),function(e){e(document).ready(function(){function t(e){e&&u&&(co

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\extensions[1].js	
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):	23278
Entropy (8bit):	5.221713990573416
Encrypted:	false
SSDEEP:	192:R0dMOZ9k6rVYqz5O8dQLXGSmqq5KOueJeLjz8fGO2LSqVMtkR9P07ue6PKHO+dic:WdjuqE/LjKdWSqVZ67mKuSitMT
MD5:	14EA1230601E3A436C3467FD442E6287
SHA1:	CCF6A8176FA75C15AF510DAF5154A4D325136C5B
SHA-256:	5F3933028E1C14007641C529D4D30E265CBAE4E642DFB6534B9988F1A1C3ADFF
SHA-512:	2BCD847F7F9559BE83CC16210B0031520807420C17A179641E62619BCF4772AB980700C0F388477485D1291D98853AF49FD818734A08595AB4EAD1D366B77D29
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://demo.1-2-1marketing.com/resources/121/js/extensions.js
Preview:	.jQuery(function($) { ..../// Uk Touch.....$('html.uk-touch').addClass('touch-121');...$(document).ready(function() {.....touchCheckSize();.....$(window).resize(function () {.....touchCheckSize();.....});...});.....function touchCheckSize(){.....touchWidth = $(window).width();.....if ((touchWidth > 1219) && ($('html.touch-121').hasClass('uk-touch'))){.....$('html.touch-121').addClass('uk-notouch').removeClass('uk-touch');.....}.....else if ((touchWidth <= 1219) && ($('html.touch-121').hasClass('uk-notouch'))){.....$('html.touch-121').addClass('uk-touch').removeClass('uk-notouch');.....}...}...../// RS Forms...$('fieldset.uk-form').find('input, textarea, select').each(function() {....var $this = $(this);....var $label = $this.parent().parent().find('label');.....if($(this).index('select') !== -1) {.....$(this).prepend('<option disabled selected value>' + $label.text() + '</option>');.....} else {.....$this.attr("placeholder", $label.text());....}.....$this.on("inpu

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\ga6law1J5X9T9RW6j9bNfFcWbg[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 27712, version 1.1
Category:	downloaded
Size (bytes):	27712
Entropy (8bit):	7.977092137796619
Encrypted:	false
SSDEEP:	768:3bu1OjSDcLmopzKXKdZ5+hMK+mqxggoh9OV7:3pSDcLvmXK/5deg37
MD5:	0976453A63382A978530EB81326C3FDB
SHA1:	BC9426351CA65609C3801F62D86D489798FCE252
SHA-256:	D399584AA6FD33B0A36FA34D0EE39C22D5080D30C8ACEB2B5C4051C707A33873
SHA-512:	C2D7F6CCDB02D57C109EA7A8409AF8DBAE78FDA6453E8E6423F1CD69DD8E4BB3EC02EE8CF4DB9E9662C7DCA571DD22A9FE63EE01D0B1E4506F2F038C42C700A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/notoserif/v9/ga6law1J5X9T9RW6j9bNfFcWbg.woff

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\ga6law1J5X9T9RW6j9bNfFcWbg[1].woff	
Preview:	wOFF.....l@.....P.....GDEF.....GPOS.....~..{.GSUB.....l.t.OS/2.....`...`~O0acmap...$.....>D6^cvt .....+...8tGg.fpgm.....1...1....gasp...@.....glyf...L..X5.....q/head..d....6...6..g.hhea..d.....$....hmtx..d.....J.loca..f.....J.mNmaxp..h.... ... .name..h.....<.post..i..... .i.fprep..i....{...S~.J.....x.L...Ua.@..T.i.m.msf.m...1/7.y....{...R..''...fN& ....@d...#..u.A.v.]#.#..5#S..Sk...X...x4.6^S.....;s..y....9..A..._.k06...M}...+..Sj..%w.....#.....P2]8].(.I..,B....1.P..T!lu...%..M;.K..Gg.O7zP.^V.~.....YHq...r..J.e#....jp..4....h....}..G.$%....3.....<...-.S.#._J.p...y...P^.USu...{..Z;n..j.....Y.x..k.6j..h..i.vx.!..uDGuL.uV.t^.tQ.uEWuM.u..n..w..;...~o..A.....>.V.6.W.B.ck....D....8t..75..}.....".p).7.!.k.....E..ss.....;..0.ul....1...0.]d.e.....yc..>.s.x...a\...d.b..../.L..VY.....)Q.B..6.b..v.c...9.S:C..')........u.....N..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\ga6Kaw1J5X9T9RW6j9bNfFImajC9[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 26232, version 1.1
Category:	downloaded
Size (bytes):	26232
Entropy (8bit):	7.981160135332649
Encrypted:	false
SSDEEP:	768:CgSt4m/4FfAOGxUUlnij4rOkKEJyZ7Di8JB1:Ct4F4OGxHlniUazvXJj
MD5:	A9B2BA1FE8CE0F484DF31E6D730174C8
SHA1:	F0D9464873D6B872A7ABEA83146073D6AEFD37E7
SHA-256:	D70C8A917EF93366A8ABBDB8F8956855C25CDF44040EA6239188AB7AC18D25FC
SHA-512:	9EE4CB8C052B01066DADC7BBF41EEB4087B87DB1B91C40C937F21B50E8A8916005ACCD4509765974E121CDB0BB494612AD4D01F91B488FE5C04B310305E6B3B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/notoserif/v9/ga6Kaw1J5X9T9RW6j9bNfFImajC9.woff
Preview:	wOFF.....fx.....t.....GDEF.....GPOS.....xU...GSUB.....l.t.OS/2.....^...`~O0.cmap.....>D6^cvt .....&...:j.j.fpgm.....&....s.#.gasp...(.....glyf...4..R...zJ.h.head..^....6...6....hhea.._....''...$.d..hmtx.._P...+.....9)loca..a|.....R.maxp..cD... ... .u.;name..cd.....%.B.post..dP..... .].fprep..dh.....,.....x.L..\Q.@.3.7..m.m.1k...6...6v^O.|..O...B#b...ZB@. .....Wx...[.S.q.....H..-...wd..k.>.Y.x.#.J...R-2.i.oJ.g..../.... t.~.....$...l.O.....'g..'..$...d.e....)..b.X.Z.&A]....dhA'...7e.o..h..b..H*2.0..Te.Ug.....S.=.}.rb.Gi.....w.C....2..6....l....u..i.6h.6E!.I....-.F..:.G...Z..w.\.....:.....Q.....=dR..>..u@.uH..S..T."g.w=..:...K..+..k.....Q.....#=u..}R....MKTQ....%.8..>....e...-D..''..E.E.....P.8.~m./..;...m...P..w.''h.x.....=.{.....b.....3..s...q.E.....S.8.IH.?.f'.$....`~.%r,...e.X3_.D..Uj...&[l...{.s.!G.p?.Dq.&.*..^.q.|..%q.....1Q.zT

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\golf-pro-bios[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, CR, LF line terminators
Category:	dropped
Size (bytes):	30851
Entropy (8bit):	5.073924635086475
Encrypted:	false
SSDEEP:	768:zbAO95KE1iiioiWixiNi/iwiPiZvQairie7LANS6nlPYV6RrJfU2iC/P79199W9z:TJjB2uuTMavQa4icGNn9QSdsdE79199C
MD5:	01322DA6261B5C2A90FAF52821898CFD
SHA1:	9B4E81E6D9B9919C3AA96D96AEEFF24586583832
SHA-256:	614F705BE7A41C3848E5D1903DB422AD1C174655451102B7C2AF7416CC841BED
SHA-512:	CFFFBD00293B94C9DE73A3D5CFFD74F1DFC0947A85C2250BC0B4A6F6BC9907DDD1BE7D66F07875E90186B049DB21CC02432F8664FDB2A4B8D155F789F7B6119
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE HTML>.<html lang="en-gb" dir="ltr" data-config='{"twitter":0,"plusone":0,"facebook":0,"style":"121"}'>.. <head>. <meta charset="utf-8">.<meta http-equiv="X-UA-Compatible" content="IE=edge">.<meta name="viewport" content="width=device-width, initial-scale=1">.<base href="https://www.golfcoronado.com/instruction/golf-pro-bios" />..<meta name="author" content="Super User" />..<meta http-equiv="content-type" content="text/html; charset=utf-8" />..<title>Golf Pro Bios</title>..<link href="/templates/yoo_avanti/favicon.ico" rel="shortcut icon" type="image/vnd.microsoft.icon" />..<link href="/components/com_dtregister/assets/css/main.css" rel="stylesheet" type="text/css" />..<link href="/plugins/system/jcemediabox/css/jcemediabox.min.css?9d108330040bd2b7386ad9c4cf8105fc" rel="stylesheet" type="text/css" />..<script src="/media/jui/js/jquery.min.js?43572ae32cf0948c0b4f80000130ae29" type="text/javascript"></script>..<script src="/media/jui/js/jquery-noconflict.js?43572ae32cf094

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\junior-golf[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, CR, LF line terminators
Category:	dropped
Size (bytes):	22274
Entropy (8bit):	4.9582839147163025
Encrypted:	false
SSDEEP:	384:6AO95KE1iiioiWixiNi/iwiPiZvQairimTJLdAtXQ83XAvire79199W9997Fjoxv:6AO95KE1iiioiWixiNi/iwiPiZvQairV
MD5:	F2E5E6B6CC39E67DBB55C3ED5C41F30A
SHA1:	BC41F5DE746C14B00338F15C1469E8714FBBBD49
SHA-256:	4DE0FC94A85111CB0E0E1778472FD2D19087E32E98F71015F03DA71172C995A1
SHA-512:	DB85C2EC8DD7B71580FD9AA08ED3076B364111F39ACFBF8A04BE50874A510E000732B7DEB457424A9FFA6CAB7C8C422974BFDB621676CD414F1F25F3A631CA4
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\junior-golf[1].htm	
Preview:	<!DOCTYPE HTML>.<html lang="en-gb" dir="ltr" data-config='{"twitter":0,"plusone":0,"facebook":0,"style":"121"}'>.. <head>. <meta charset="utf-8">.<meta http-equiv="X-UA-Compatible" content="IE=edge">.<meta name="viewport" content="width=device-width, initial-scale=1">.<base href="https://www.golfcoronado.com/instruction/junior-golf" />..<meta name="author" content="Super User" />..<meta http-equiv="content-type" content="text/html; charset=utf-8" />..<title>Junior Golf</title>..<link href="/templates/yoo_avanti/favicon.ico" rel="shortcut icon" type="image/vnd.microsoft.icon" />..<link href="/components/com_dtregister/assets/css/main.css" rel="stylesheet" type="text/css" />..<link href="/plugins/system/jcemediabox/css/jcemediabox.min.css?9d108330040bd2b7386ad9c4cf8105fc" rel="stylesheet" type="text/css" />..<script src="/media/jui/js/jquery.min.js?43572ae32cf0948c0b4f80000130ae29" type="text/javascript"></script>..<script src="/media/jui/js/jquery-noconflict.js?43572ae32cf0948c0b

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\junior_golf[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=6, xresolution=86, yresolution=94, resolutionunit=2, copyright=(c) Iuriisokolov | Dreamstime.com], baseline, precision 8, 800x533, frames 3
Category:	downloaded
Size (bytes):	514882
Entropy (8bit):	7.963785931116415
Encrypted:	false
SSDEEP:	12288:+K0iBcrXguCayrKnqUJ+uvKOpHjk/oDZXpoH7xX1wO88H9V8Wwe:pG7gu9KM50LckwDZC7xn9SWwe
MD5:	33E7FC74AAEFB4F8F1A6205B546B16B4
SHA1:	9CF7F1E4B59F611BE959D1FBC87C724BE2F3B553
SHA-256:	32277454C7E1030BF82A019CCFDB49AC61245AA3B0DB6292C6B7DEDE4D9DB031
SHA-512:	B8A0B226056A925486C2C5F30924C6F58F49E31F3985855F086CD15CB889716E7D3261085F233802C5E48B942095A05211748AF99C1EB7CC6138F6C2AEC92E86
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.golfcoronado.com/images/junior_golf.jpg
Preview:	.....Exif..MM.*.....V.....^.(.....)...f.....,.....,....(c) Iuriisokolov | Dreamstime.com.h.t.t.p.:././.w.w.w...d.r.e.a.m.s.t.i.m.e...c.o.m./.s.t.o.c.k.-.i.m.a.g.e.s.-.k.i.d.s.-.g.o.l.f.-.c.o.m.p.e.t.i.t.i.o.n.-.c.h.i.l.d.r.e.n.-.p.l.a.y.i.n.g.-.t.a.k.i.n.g.-.p.a.r.t.-.c.o.u.r.s.e.-.s.u.m.m.e.r.-.d.a.y.-.i.m.a.g.e.5.8.2.2.6.2.9.4.....JPhotoshop 3.0.8BIM.....-..t.!(c) Iuriisokolov | Dreamstime.com.....C.....C..... ....Q.....!...1.."AQ.a.2q.#B....R...$3...br..%C.S...&4Dcs.5.du.....R.....!..1.A.."Qa2q....#B..R....$3b....CrS..%4.c...DTs.&5d...EU.....?...u..ej.....9...Pr@,s.r.\|....H..l.bF2c..A.....B.S$.. bDw..&...{..0*.F..fm..3w=L{{d...^Rfm.q....=..2N..cO..&..B.. D.fs....e.bJ

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\juniors[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, big-endian, direntries=6, xresolution=86, yresolution=94, resolutionunit=2, copyright=(c) Alexsokolov | Dreamstime.com], baseline, precision 8, 800x533, frames 3
Category:	downloaded
Size (bytes):	513758
Entropy (8bit):	7.961710422641516
Encrypted:	false
SSDEEP:	12288:z/JOX66zqiljECyMmRhjAJTZb3qDkOaCmxIB52QrFzThrR8Oa4S2J:zIq62M5yvRhjyqDkOa3YHVRb5J
MD5:	D160E2F93CAF1D5056598C9F39257E8A
SHA1:	3F9748C5BDAEC7BFA626A674B211136CEE38C950
SHA-256:	67045855CA7D50CD0C24B95FA7617201478EE90293BAD83FD9088E44D5A73699
SHA-512:	4E9C9FF8B62B9B430507ADBAECEA0BE7B56729DC86181EA242A3141F37B582B84D78C028FEB748018775CA08424E32C91BA1FDC1E4D2BD9D63DED8633F01F7D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.golfcoronado.com/images/juniors.jpg
Preview:	.....Exif..MM.*.....V.....^.(.....)...f.....,.....,....(c) Alexsokolov | Dreamstime.com..h.t.t.p.:././.w.w.w...d.r.e.a.m.s.t.i.m.e...c.o.m./.r.o.y.a.l.t.y.-.f.r.e.e.-.s.t.o.c.k.-.p.h.o.t.o.s.-.k.i.d.s.-.g.o.l.f.-.c.o.m.p.e.t.i.t.i.o.n.-.c.h.i.l.d.r.e.n.-.p.o.s.i.n.g.-.n.e.a.r.-.c.a.r.-.c.o.u.r.s.e.-.s.u.m.m.e.r.-.d.a.y.-.i.m.a.g.e.5.9.1.1.9.3.1.8...HPhotoshop 3.0.8BIM.....,.t. (c) Alexsokolov | Dreamstime.com.....C.....C..... ....X.....!...1."AQ.aq..#2..B....R...$3...%Cb.4Sr.D.&Ts.56Ec...'det.....\.....!...1AQa.."q...2...#....BR...3$Cb.Sr..%4c..Ds.....&5Tdt..F...'.....?..X7...D.....@.s.....dgn.v..$.....q..~q...%..V.:f.y..9o{....G.-.KN.E#8'# aG...lm.2.l.....7.gy

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\master[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	20415
Entropy (8bit):	5.245607082405494
Encrypted:	false
SSDEEP:	384:B3UTkpCIXAa+wnjzOp/bcswces75TpF/QmZopkx4Fb7E0HXw7HU8/I:B6632/bhesw
MD5:	3530B649417DA9D546FCC9AC12A26D6C
SHA1:	26340C3ADEA92D927479061520EEDD27B71C32D2
SHA-256:	BB5025507F418466DD68E3AD5ACC37465CAEADD33EFA5E2007B4B17B15401EE2
SHA-512:	BB57357AEC6302B2FD6944281C0AAC8FC376D422033D8B998655DD7D06246565FCB14C39251228E92E91AA8BEF994C616F90CE321BE79A5AA5EC0B5167D43F1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://demo.1-2-1marketing.com/resources/avanti/greens/css/master.css

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\master[1].css	
Preview:	./* Copyright (C) 121 Marketing - 121marketing.com */..../* ========== 1-2-1 Modifications - Master.. ========== */..../* ========== Fonts ========== */..h1, h2, h3, h4, h5, h6, .uk-h1, .uk-h2, .uk-h3, .uk-h4, .uk-h5, .uk-h6, .uk-subnav > * > * {line-height: 1.2;}....h3, .uk-h3, .uk-panel-title {margin-top: 0;}....a:hover, .uk-link:hover, a:focus {...text-decoration: none;..}../* ========== Backgrounds ========== */ ...homepage #tm-main, form#contact-form .form-actions, .uk-offcanvas-bar:after, .uk-offcanvas-bar-flip:after, .uk-contrast .uk-button, .uk-nav-offcanvas > li > a, .uk-panel-box .uk-nav-side > li > a, .uk-nav-side > li > a {...background: none;..}...uk-button-link, html .uk-nav.uk-nav-offcanvas > li.uk-active > a, .uk-nav-offcanvas > .uk-open > a, html:not(.uk-touch)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\master[1].js	
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):	1421
Entropy (8bit):	4.8458812129831825
Encrypted:	false
SSDEEP:	24:PyBKnkkAyRenRvhHRXiHeM6BB0nJpAmZSMviwJhvGB9Gt:D0qHepwcBM7XGrg
MD5:	996DD100988B7B224D72CBDA6FCD9077
SHA1:	255A0EF34D039320F0CA0457B6E9FA458CE0E0C0
SHA-256:	7E7AE39EB0179ACE0AE15EE4F618C195BC16A5D702149AEF3549CE0C3BA2A5CB
SHA-512:	ECC63A47EA2EDA6D9052FECA2CF26D3685780C54397882F0D980DF851D7DF2E7A1A1F0234540FCC1D3CD06D98BC3951582C4249A36EA825B6708DF269BD5C33
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://demo.1-2-1marketing.com/resources/avanti/greens/js/master.js
Preview:	./* Copyright (C) 121 Marketing - 121marketing.com */..../* ========== 1-2-1 Modifications - Master.. ========== */....jQuery(function($) { ...../// Virtuemart...$(".vm-col .addtocart-button input, .checkout-button-top .vm-button-correct").addClass(" uk-button uk-button-large");...$(".vm-col input.uk-button").removeClass(" addtocart-button");...$(".checkout-button-top .uk-button").removeClass(" vm-button-correct ");..../// ## Score Components ## //..../Scorecard and Hole by Hole.. $('#holebyhole .uk-button').addClass(' uk-button-large ');...../* ========== Greens Specific ADA fixes.. ========== */... .. // Toolbar Icon...$('.tm-toolbar .uk-icon-map-marker, .toolbar-assets .uk-icon-map-marker').html('<span class="uk-h

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\recaptcha.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	302
Entropy (8bit):	4.875379617517705
Encrypted:	false
SSDEEP:	6:32yXjg9pbDRW6AHCCjn/GDk6++gLeCwhaDf761whREoU52A1whXogVeRFg:32Q65DRW7+IferOnmoU52H4gs8
MD5:	3B5EC6E98154E4EC7E71025DCBADAE01
SHA1:	21DDBBB12E63DA831C2C260532BD03EF4176FDA2
SHA-256:	5046D067E2A7078DC5E279DF9577B611DAF40CB37B1877A727086C7D66955F5C
SHA-512:	1E2DA89404108861C5ED85B859AC33C1407B48EC15A8C31A1282D9C15E4CA7E01B5C2EB54F72EC7CCCEE3846F2207BF3F44D726C2AECD429C2B084606E148ED
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.golfcoronado.com/media/plg_captcha_recaptcha/js/recaptcha.min.js?43572ae32cf0948c0b4f80000130ae29
Preview:	window.JoomlaInitReCaptcha2=function(){"use strict";var e=document.getElementsByClassName("g-recaptcha"),t,n;for(var r=0,i=e.length;r<i;r++)t=e[r],n=t.dataset?t.dataset:{sitekey:t.getAttribute("data-sitekey"),theme:t.getAttribute("data-theme"),size:t.getAttribute("data-size")},grecaptcha.render(t,n)};

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\styles__ltr[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	51290
Entropy (8bit):	5.966981029136845
Encrypted:	false
SSDEEP:	768:+LUmmAWTe2uXYp8Mi+yKSrKebyBwpDl+xedtY5PoiDH1fkQJVEwY:4UcW6v+2rKwpDliP7dnY
MD5:	2CC638EE58191086E0661BE1D50F58FE
SHA1:	F744D6C9BD84D98DCBCFE94A2A7EB986B58302F3
SHA-256:	9FCB26C87712320932EA7FB2434BA2737AF71B6E96DD238DBCB312E454992837
SHA-512:	7A836350AF3FBB293A50889CC676D5A3ABBBE40C24E12D77F6BC94A6AA8A383E3ABB91DA533D68C7CB333E7A004902638A65A1E662431F897D7095866A6EE891
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/recaptcha/releases/539Evs44yecoSf-lkJBQzKKj/styles__ltr.css

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\styles__ltr[1].css	
Preview:	.goog-inline-block{position:relative;display:-moz-inline-box;display:inline-block}* html .goog-inline-block{display:inline}*:first-child+html .goog-inline-block{display:inline}.recaptcha-checkbox{border:none;font-size:1px;height:28px;margin:4px;width:28px;overflow:visible;outline:0;vertical-align:text-bottom}.recaptcha-checkbox-border{-webkit-border-radius:2px;-moz-border-radius:2px;border-radius:2px;background-color:#fff;border:2px solid #c1c1c1;font-size:1px;height:24px;position:absolute;width:24px;z-index:1}.recaptcha-checkbox-borderAnimation{background-image:url(
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\theme[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	272406
Entropy (8bit):	5.063606401697672
Encrypted:	false
SSDEEP:	6144:1SU+5oPJwa+hQfYvacEitQfQuaYKUbd+Sfc5XAPxVc+l5pRqA:rea+hQfYvacEitQfQuaYKUbd+acis+lX
MD5:	1C02BFA7CD88DF72F14F0BB0E282CAA7
SHA1:	7C9A503DFCD7C298CB4B413345F89D363E7C682D
SHA-256:	832CB7432A395CE2787132007B9E57070C582F214CD6F8921874C8B5CA071AE4
SHA-512:	EECFACB0DE9CBAFA8875B76B5DE42377B8EEEA4A4D6FF410EAD7763D1EC9BEFF473094B893F423EC79BE1BA29EF11D827247620D5077EFA7EF723E1FBD2024C7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.golfcoronado.com/templates/yoo_avanti/css/theme.css
Preview:	/* Copyright (C) YOOtheme GmbH, YOOtheme Proprietary Use License (http://www.yootheme.com/license) */..@import 'https://fonts.googleapis.com/css?family=Noto+Serif:400,400italic';.@import 'https://fonts.googleapis.com/css?family=Montserrat';./* ==. Component: Base. == */./*. * 1. Normalize default `font-family` and set `font-size` to support `rem` units. * 2. Prevents iOS text size adjust after orientation change, without disabling user zoom. * 3. Style. */.html {. /* 1 */. font: normal 15px / 26px 'Noto Serif', Times New Roman, serif;. /* 2 */. -webkit-text-size-adjust: 100%;. -ms-text-size-adjust: 100%;. /* 3 */. background: #ffffff;. color: #666666;.}./*. * Removes default margin.. */.body {. margin: 0;.}./* Links. == */./*. * Remove the gray background color fro

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\uikit2-2143e9f4[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	193886
Entropy (8bit):	5.1704399567375265
Encrypted:	false
SSDEEP:	3072:h0ErpuMioN0fY8nZPMf9p9w0ORGN3RJduaiCFeDOHk:9cMioqQ8nZT8ByaiC02k
MD5:	B57AFDD1303BA16D8D18B80CBD7F750A
SHA1:	68A207AA6A8657A8AE43213D72B317D0F99C36B6
SHA-256:	76239E32B2020ACC0AFA076C1FAE77521E565B210B80BDE9F531C6FFBF6721F4
SHA-512:	3FE115BEB2DA3DBAB4966C227E22EF770F032CAB37D9CD6A0B88C577F198177202B8CA1F87314FC15D162ED1A34F273CA6607C91C6A8D6C25736947E919D6F8C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.golfcoronado.com/media/widgetkit/uikit2-2143e9f4.js
Preview:	/*! UIkit 2.27.4 | http://www.getuikit.com | (c) 2014 YOOtheme | MIT License */.!function(t){var i;if(!window.jQuery)throw new Error("UIkit 2.x requires jQuery");i=t(window.jQuery),"function"==typeof define&&define.amd&&define("uikit",function(){return i.load=function(t,e,n,o){var s,a=t.split(","),r=[],l=(o.config&&o.config.uikit&&o.config.uikit.base?o.config.uikit.base:"").replace(/\/+$/g,"");if(!l)throw new Error("Please define base path to UIkit in the requirejs config.");for(s=0;s<a.length;s+=1){var c=a[s].replace(/\./g,"/");r.push(l+"/components/"+c)}e(r,function(){n(i)})},i})}(function(t){"use strict";if(window.UIkit2)return window.UIkit2;var i={},e=window.UIkit\|\|void 0;if(i.version="2.27.4",i.noConflict=function(){return e&&(window.UIkit=e,t.UIkit=e,t.fn.uk=e.fn),i},window.UIkit2=i,e\|\|(window.UIkit=i),i.$=t,i.$doc=i.$(document),i.$win=i.$(window),i.$html=i.$("html"),i.support={},i.support.transition=function(){var t=function(){var t,i=document.body||document.documentElement,e={W

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\webcam[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, CR, LF line terminators
Category:	dropped
Size (bytes):	18641
Entropy (8bit):	4.905364667453658
Encrypted:	false
SSDEEP:	384:JAO95KE1iiioiWixiNi/iwiPiZvQairimOyLdAtGKC79199W99979j5oRv5:JAO95KE1iiioiWixiNi/iwiPiZvQair3
MD5:	688CFC6C72B8BF6D8C840F2211C64B16
SHA1:	83810AB6D441E77AD58751CD75C2F2282498597A
SHA-256:	8BBEED62954B1045D41F3F4772E9626B35EB88D7B321DACAE092D564E8B4D3A4
SHA-512:	CBA3E0DD66180FFA3DCA0AC1DE8091C853A40F11C5A04229B8DEBF53AE95EB788EF2A7343463FB4080982506907B6B8541D8E2474AEC0C3ACD1651616DCBDE66

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\webcam[1].htm	
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE HTML>.<html lang="en-gb" dir="ltr" data-config='{"twitter":0,"plusone":0,"facebook":0,"style":"121"}'>.. <head>. <meta charset="utf-8">.<meta http-equiv="X-UA-Compatible" content="IE=edge">.<meta name="viewport" content="width=device-width, initial-scale=1">.<base href="https://www.golfcoronado.com/course-info/webcam" />..<meta name="author" content="Super User" />..<meta http-equiv="content-type" content="text/html; charset=utf-8" />..<title>Webcam</title>..<link href="/templates/yoo_avanti/favicon.ico" rel="shortcut icon" type="image/vnd.microsoft.icon" />..<link href="/components/com_dtregister/assets/css/main.css" rel="stylesheet" type="text/css" />..<link href="/plugins/system/jcemediabox/css/jcemediabox.min.css?9d108330040bd2b7386ad9c4cf8105fc" rel="stylesheet" type="text/css" />..<script src="/media/jui/js/jquery.min.js?43572ae32cf0948c0b4f80000130ae29" type="text/javascript"></script>..<script src="/media/jui/js/jquery-noconflict.js?43572ae32cf0948c0b4f80000130

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\BhXhPg3d42Qn3k48YRS7u-t2FTc2Jg9-RS73ZPaiDMM[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):	21001
Entropy (8bit):	5.606075882010642
Encrypted:	false
SSDEEP:	384:m/6NH31LwWF/X/FR6q07Yfw4p4mWB8GrLzmf3wnh50EmE4c:m4FMy/76cJ4m9qC3whx4c
MD5:	CF699004DC20C10E4569F72C10814C70
SHA1:	AB072CC03FE1418B4E7D2489F8BCB129D5C6E8CE
SHA-256:	0615E13E0DDDE36427DE4E3C6114BBBBEB76153736260F7E452EF764F6A20CC3
SHA-512:	7DCC01A60583529037BB7836557D171A8A562F4054B01C1C1FDAE0EA1F4A136A1AB8EA3DA63A6676DD4075D051997952B1D18BA56EA8B29A1B1FF5994670038E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google.com/js/bg/BhXhPg3d42Qn3k48YRS7u-t2FTc2Jg9-RS73ZPaiDMM.js
Preview:	/* Anti-spam. Want to say hello? Contact (base64) Ym90Z3VhcmQtY29udGFjdEBnb29nbGUuY29t */ (function(){var U=this||self,A=function(g){return g},J=function(g,L){if((g=(L=null,U).trustedTypes,!g)||!g.createPolicy)return L;try{L=g.createPolicy("bg",{createHTML:A,createScript:A,createScriptURL:A})}catch(Y){U.console&&U.console.error(Y.message)}return L};(0,eval)(function(g,L){return(L=J())&&1===g.eval(L.createScript("1"))?function(Y){return L.createScript(Y)}:function(Y){return""+Y}}(U)(Array(7824*Math.random()|0).join("\n")+'(function(){var g2=function(g,L){return g(function(Y){Y(L)}),[function(){return L}]},Y8=function(g,L,Y,A,X){return{invoke:(X=(A=(Y=void 0,function(){}),LV(g,function(U){A&&(L&&e(L),Y=U,A(),A=void 0)},!!L)[0]),function(U,J,b,z,N){if(!J)return J=X(b),U&&U(J),J;N=function(){Y(function(h){e(function(){U(h)})},b)},Y?N():(z=A,A=function(){z(),e(N)}))}}},C=this||self,U2=function(g,L,Y){for(Y in g)if(L.call(void 0,g[Y],Y,g))return true;return false},A8=function(){},J8=function

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284FD
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/NewErrorPageTemplate.css
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt;..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\TRY2H1XU.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, CR, LF line terminators
Category:	dropped
Size (bytes):	38955
Entropy (8bit):	4.977574591595892
Encrypted:	false
SSDEEP:	768:iAt9PL95KE1iiioiWixiNi/iwiPiZvQairin7LrvwvPviidVG9r79199W9997Q3j:nFJjB2uuTMavQa4i7/o3iidVGx79199R
MD5:	0D91ECC87DBF0A44C5A8EE2CD431A16D
SHA1:	E5392E803210FA4A3E63216960FE0C1F59DB8DD9
SHA-256:	49F7556E64E18E1E12C7FFC274F13A1A4C5306870DFCFCCF4ACE1DE90986098F
SHA-512:	91CFC01E279F05C9EF5258B34681B5428CF49AB3BEE140D25246254AD34097E527A708D3409A8B1D11C09EAD33F20178F098598A552C17B3EA8AE1653732DE86

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\TRY2H1XU.htm	
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE HTML>.<html lang="en-gb" dir="ltr" data-config='{"twitter":0,"plusone":0,"facebook":0,"style":"121"}'>.. <head>. <meta charset="utf-8">.<meta http-equiv="X-UA-Compatible" content="IE=edge">.<meta name="viewport" content="width=device-width, initial-scale=1">.<base href="https://www.golfcoronado.com/" />..<meta http-equiv="content-type" content="text/html; charset=utf-8" />..<title>Coronado Golf Course - Coronado, CA</title>..<link href="/?format=feed&type=rss" rel="alternate" type="application/rss+xml" title="RSS 2.0" />..<link href="/?format=feed&type=atom" rel="alternate" type="application/atom+xml" title="Atom 1.0" />..<link href="/templates/yoo_avanti/favicon.ico" rel="shortcut icon" type="image/vnd.microsoft.icon" />..<link href="/components/com_dtregister/assets/css/main.css" rel="stylesheet" type="text/css" />..<link href="/plugins/system/jcemediabox/css/jcemediabox.min.css?9d108330040bd2b7386ad9c4cf8105fc" rel="stylesheet" type="text/css" />..<link href

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\animated-text[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	978
Entropy (8bit):	5.096898570311842
Encrypted:	false
SSDEEP:	24:UQi7p2JexAFINFAMMRAC1QxAGxAA3RMMRAfPIzJAlgqwRzeHoLLul:UD7p5xIUFpMRCxrxrqMRYmmYwhUyul
MD5:	8FC75FEFFEA6880B80178E73BAD81B1C
SHA1:	6E4D43444560924A898B48E81D91008B247A6DE0
SHA-256:	A85E3DF8721E8C89664B7EE01EDC3FA76B7BB179D535F44CBBC6191A4ECAB945
SHA-512:	1638F6058981FDB719057EDE76A624B548FDD097722CB175020196E30B2F16D7A26BD74D5FEB8FD487BF457CB7B903D2BD142BED2709BE3A0463649687AEB2B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.golfcoronado.com/templates/yoo_avanti/js/animated-text.js
Preview:	/* Copyright (C) YOOtheme GmbH, YOOtheme Proprietary Use License (http://www.yootheme.com/license) */..!function(t){"use strict";function n(t){for(var n=t.length-1;n>0;n--){var i=Math.floor(Math.random()*(n+1)),a=t[n];t[n]=t[i],t[i]=a}return t}t.component("animatedText",{defaults:{animation:"uk-animation-fade",duration:40},boot:function(){t.ready(function(n){t.$("[data-uk-animatedtext]",n).each(function(){var n,i=t.$(this);i.data("animatedText")||(n=t.animatedText(i,t.Utils.options(i.attr("data-uk-animatedtext"))))})})},init:function(){this.on("display.uk.check",function(t){this.element.is(":visible")&&this.process()}.bind(this)),this.process()},process:function(){for(var t=this,i=this.element.text().split(""),a=[],e=0;e<i.length;e++)a.push(e);a=n(a),i=i.map(function(n,i,e){return e=a[i]*t.options.duration,'<span class="'+t.options.animation+'" style="-webkit-animation-delay:'+e+"ms;animation-delay:"+e+'ms">'+n+""}).join(""),this.element.html(i)})}(UIkit);

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\autocomplete[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):	4169
Entropy (8bit):	5.020734768631628
Encrypted:	false
SSDEEP:	96:+jUO6EGeJZlNjjaPSIDKx+/EmbzpLmJe3trlOL:n52lNjjMSIDXzpKc3trsL
MD5:	957DE82B7F4A7B34A9685ED4E7544DB6
SHA1:	80FB0F4D128D9A83D6DFE84B80DC79FEA4B42515
SHA-256:	B1D0F07DC31826330885C166EEFEF01B79CD635E73B84EFE279B0B12304461D5
SHA-512:	1044959C515FD8B398319BCC1A06F1A9581DB6269753015F54BBA0AB6A4292F72BF313EA749DD2BAD264EA2D92DE68F3BE1E1E7E8426FC8106A5E26DCB3C212 9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.golfcoronado.com/templates/yoo_avanti/warp/vendor/uikit/js/components/autocomplete.js
Preview:	!function(t){var e;window.UIkit&&(e=t(UIkit)),"function"==typeof define&&define.amd&&define("uikit-autocomplete",["uikit"],function(){return e||t(UIkit)})}(function(t){"use strict";var e;return t.component("autocomplete",{defaults:{minLength:3,param:"search",method:"post",delay:300,loadingClass:"uk-loading",flipDropdown:!1,skipClass:"uk-skip",hoverClass:"uk-active",source:null,renderer:null,template:'<ul class="uk-nav uk-nav-autocomplete uk-autocomplete-results">{{~items}}<li data-value="{{$item.value}}"><a>{{$item.value}} {{/items}} ',visible:!1,value:null,selected:null,boot:function(){t.$html.on("focus.autocomplete.uikit","[data-uk-autocomplete]",function(e){var i=t.$(this);i.data("autocomplete")||t.autocomplete(i,t.Utils.options(i.attr("data-uk-autocomplete")))}),t.$html.on("click.autocomplete.uikit",function(t){e&&t.target!=e.input[0]&&e.hide()})},init:function(){var e=this,i=!1,s=t.Utils.debounce(function(t){return i?i=!1:void e.handle()},this.options.delay);this.drop

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\bootstrap.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	29156
Entropy (8bit):	5.003748738791064
Encrypted:	false
SSDEEP:	768:s7S57QFwktDm0INVIPWr8gJBQcqYn0SUs8q:p0OfNs+0WT
MD5:	94935933A620FEF61D4B0C15C664F8B3
SHA1:	E879415D9CDDA4AE99767995F49560440025AD74
SHA-256:	6EBE64DE8E1C2F92400A03A97250C8B2F7443025D53FA42DF90CB0589350C233
SHA-512:	CC5ABF82A7160881FA8EFA8C31AF480AB65FA72D5826DE66946D1CC9B28845C1146C19F0549459FC8BE67ACDE4DFA6A94F173F26BBB654E2721FD7F619D1103 5

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\bootstrap.min[1].js	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.golfcoronado.com/media/jui/js/bootstrap.min.js?43572ae32cf0948c0b4f80000130ae29
Preview:	/*!. * Bootstrap.js by @fat & @mdo. * Copyright 2012 Twitter, Inc.. * http://www.apache.org/licenses/LICENSE-2.0.txt. *. * Custom version for Joomla!. */.!function(e){"use strict";e(function(){e.support.transition=function(){var e=function(){var e=document.createElement("bootstrap"),t={WebkitTransition:"webkitTransitionEnd",MozTransition:"transitionend",OTransition:"oTransitionEnd otransitionend",transition:"transitionend"},n;for(n in t)if(e.style[n]!==undefined)return t[n]}();return e&&{end:e}}()})}(window.jQuery),!function(e){"use strict";var t='[data-dismiss="alert"]',n=function(n){e(n).on("click",t,this.close)};n.prototype.close=function(t){function s(){i.trigger("closed").remove()}var n=e(this),r=n.attr("data-target"),i;r||(r=n.attr("href"),r=r&&r.replace(/.*(?=#[^\s]*$)/,"")),i=e(r),t&&t.preventDefault(),i.length||(i=n.hasClass("alert")?n:n.parent()),i.trigger(t=e.Event("close"));if(t.isDefaultPrevented())return;i.removeClass("in"),e.support.transition&&i.hasClass("fade")?i.on(e.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\calendar[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	5713
Entropy (8bit):	5.135104793466268
Encrypted:	false
SSDEEP:	96:7NP3qhaRMBNuMJJ/FGH2kt+f7Bvgf7BC3A25xDxmBBt0rniMTj5TB42FYolO3DQX:7IgCBNuWLGH2DBvkBC3A25xDgBBWrnie
MD5:	6275668E173B6EEB5CBAF890DF53D8B8
SHA1:	A3CAB022052042FDFBCC565B44BEDDA538C943A4
SHA-256:	4AEA1DB7C94B2ABDF65D50863EDF69FFFB39CD3EB032117A854C27979B171624
SHA-512:	09C6B25A17A0CEC9D00E697CDBE65D0815AC4A55CDC6835F7429DCC0C4E6B44051EF96ECA685B04844F700D3BFB1598910FDC9D81FCB315EFE1D0A35CE527FE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.golfcoronado.com/media/com_rsform/css/calendar/calendar.css
Preview:	/*..Copyright (c) 2007, Yahoo! Inc. All rights reserved...Code licensed under the BSD License:..http://developer.yahoo.net/yui/license.txt..version: 2.2.2..*/.....txtCal{...width:210px;..}...btnCal{...padding-left:5px;...padding-right: 5px;..}...yui-calcontainer {...position:relative;...padding:5px;...background-color:#F7F9FB;...border:1px solid #7B9EBD;...float:left;...overflow:hidden;..}.....yui-calcontainer iframe {...position:absolute;...border:none;...margin:0;padding:0;...left:-1px;...top:-1px;...z-index:0;...width:50em;...height:50em;..}.....yui-calcontainer.multi {...padding:0;..}.....yui-calcontainer.multi .groupcal {...padding:5px;...background-color:transparent;...z-index:1;...float:left;...position:relative;...border:none;..}.....yui-calcontainer .title {...font:100% sans-serif;...color:#000;...font-weight:bold;...margin-bottom:5px;...height:25px;...position:absolute;...top:3px;left:5px;...z-index:1;..}.....yui-calcontainer .close-icon {...position:absolute;...right:3px;..

Static File Info

No static file info

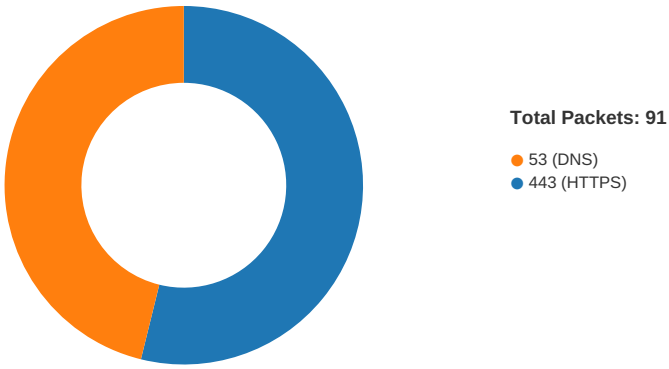
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/12/21-19:41:31.589455	ICMP	384	ICMP PING			192.168.2.6	2.23.155.241
04/12/21-19:41:31.624460	ICMP	449	ICMP Time-To-Live Exceeded in Transit			84.17.52.126	192.168.2.6
04/12/21-19:41:31.626212	ICMP	384	ICMP PING			192.168.2.6	2.23.155.241
04/12/21-19:41:31.662029	ICMP	449	ICMP Time-To-Live Exceeded in Transit			149.11.89.129	192.168.2.6
04/12/21-19:41:31.685363	ICMP	384	ICMP PING			192.168.2.6	2.23.155.241
04/12/21-19:41:31.720930	ICMP	449	ICMP Time-To-Live Exceeded in Transit			130.117.49.165	192.168.2.6
04/12/21-19:41:31.738860	ICMP	384	ICMP PING			192.168.2.6	2.23.155.241
04/12/21-19:41:31.780285	ICMP	449	ICMP Time-To-Live Exceeded in Transit			130.117.0.18	192.168.2.6
04/12/21-19:41:31.780614	ICMP	384	ICMP PING			192.168.2.6	2.23.155.241
04/12/21-19:41:31.828039	ICMP	449	ICMP Time-To-Live Exceeded in Transit			154.54.36.53	192.168.2.6

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/12/21-19:41:31.845384	ICMP	384	ICMP PING			192.168.2.6	2.23.155.241
04/12/21-19:41:31.892481	ICMP	449	ICMP Time-To-Live Exceeded in Transit			130.117.15.66	192.168.2.6
04/12/21-19:41:31.892887	ICMP	384	ICMP PING			192.168.2.6	2.23.155.241
04/12/21-19:41:31.961485	ICMP	449	ICMP Time-To-Live Exceeded in Transit			195.22.208.79	192.168.2.6
04/12/21-19:41:31.961932	ICMP	384	ICMP PING			192.168.2.6	2.23.155.241
04/12/21-19:41:32.020393	ICMP	449	ICMP Time-To-Live Exceeded in Transit			93.186.128.39	192.168.2.6
04/12/21-19:41:32.021268	ICMP	384	ICMP PING			192.168.2.6	2.23.155.241
04/12/21-19:41:32.076572	ICMP	408	ICMP Echo Reply			2.23.155.241	192.168.2.6

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 19:41:27.969753027 CEST	49716	443	192.168.2.6	69.167.161.101
Apr 12, 2021 19:41:27.971249104 CEST	49717	443	192.168.2.6	69.167.161.101
Apr 12, 2021 19:41:28.122648954 CEST	443	49716	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:28.122795105 CEST	49716	443	192.168.2.6	69.167.161.101
Apr 12, 2021 19:41:28.125633955 CEST	443	49717	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:28.126192093 CEST	49717	443	192.168.2.6	69.167.161.101
Apr 12, 2021 19:41:28.128853083 CEST	49716	443	192.168.2.6	69.167.161.101
Apr 12, 2021 19:41:28.129731894 CEST	49717	443	192.168.2.6	69.167.161.101
Apr 12, 2021 19:41:28.281583071 CEST	443	49716	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:28.282655001 CEST	443	49716	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:28.282674074 CEST	443	49716	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:28.282691002 CEST	443	49716	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:28.282702923 CEST	443	49716	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:28.282772064 CEST	49716	443	192.168.2.6	69.167.161.101
Apr 12, 2021 19:41:28.282804966 CEST	49716	443	192.168.2.6	69.167.161.101
Apr 12, 2021 19:41:28.284631014 CEST	443	49716	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:28.284744978 CEST	49716	443	192.168.2.6	69.167.161.101
Apr 12, 2021 19:41:28.288084030 CEST	443	49717	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:28.288439035 CEST	443	49717	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:28.288492918 CEST	443	49717	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:28.288516045 CEST	49717	443	192.168.2.6	69.167.161.101
Apr 12, 2021 19:41:28.288558006 CEST	443	49717	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:28.288573027 CEST	443	49717	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:28.288594961 CEST	49717	443	192.168.2.6	69.167.161.101
Apr 12, 2021 19:41:28.288614035 CEST	49717	443	192.168.2.6	69.167.161.101
Apr 12, 2021 19:41:28.291347027 CEST	443	49717	69.167.161.101	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 19:41:28.291477919 CEST	49717	443	192.168.2.6	69.167.161.101
Apr 12, 2021 19:41:28.347115040 CEST	49716	443	192.168.2.6	69.167.161.101
Apr 12, 2021 19:41:28.353142977 CEST	49716	443	192.168.2.6	69.167.161.101
Apr 12, 2021 19:41:28.353368998 CEST	49716	443	192.168.2.6	69.167.161.101
Apr 12, 2021 19:41:28.353773117 CEST	49717	443	192.168.2.6	69.167.161.101
Apr 12, 2021 19:41:28.354123116 CEST	49717	443	192.168.2.6	69.167.161.101
Apr 12, 2021 19:41:28.501638889 CEST	443	49716	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:28.501667976 CEST	443	49716	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:28.501774073 CEST	49716	443	192.168.2.6	69.167.161.101
Apr 12, 2021 19:41:28.502363920 CEST	49716	443	192.168.2.6	69.167.161.101
Apr 12, 2021 19:41:28.505548000 CEST	443	49716	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:28.505655050 CEST	49716	443	192.168.2.6	69.167.161.101
Apr 12, 2021 19:41:28.508121014 CEST	443	49717	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:28.508533955 CEST	443	49717	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:28.508649111 CEST	443	49717	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:28.508651018 CEST	49717	443	192.168.2.6	69.167.161.101
Apr 12, 2021 19:41:28.508708954 CEST	49717	443	192.168.2.6	69.167.161.101
Apr 12, 2021 19:41:28.509315014 CEST	49717	443	192.168.2.6	69.167.161.101
Apr 12, 2021 19:41:28.547211885 CEST	443	49716	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:28.654380083 CEST	443	49716	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:28.703006029 CEST	443	49717	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:29.221106052 CEST	443	49716	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:29.221132040 CEST	443	49716	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:29.221152067 CEST	443	49716	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:29.221174002 CEST	49716	443	192.168.2.6	69.167.161.101
Apr 12, 2021 19:41:29.221175909 CEST	443	49716	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:29.221195936 CEST	443	49716	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:29.221204042 CEST	49716	443	192.168.2.6	69.167.161.101
Apr 12, 2021 19:41:29.221214056 CEST	443	49716	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:29.221231937 CEST	443	49716	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:29.221245050 CEST	49716	443	192.168.2.6	69.167.161.101
Apr 12, 2021 19:41:29.221245050 CEST	443	49716	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:29.221278906 CEST	49716	443	192.168.2.6	69.167.161.101
Apr 12, 2021 19:41:29.221295118 CEST	49716	443	192.168.2.6	69.167.161.101
Apr 12, 2021 19:41:29.287358046 CEST	49716	443	192.168.2.6	69.167.161.101
Apr 12, 2021 19:41:29.287543058 CEST	49716	443	192.168.2.6	69.167.161.101
Apr 12, 2021 19:41:29.287733078 CEST	49716	443	192.168.2.6	69.167.161.101
Apr 12, 2021 19:41:29.287905931 CEST	49716	443	192.168.2.6	69.167.161.101
Apr 12, 2021 19:41:29.288059950 CEST	49716	443	192.168.2.6	69.167.161.101
Apr 12, 2021 19:41:29.288208008 CEST	49716	443	192.168.2.6	69.167.161.101
Apr 12, 2021 19:41:29.288356066 CEST	49716	443	192.168.2.6	69.167.161.101
Apr 12, 2021 19:41:29.288517952 CEST	49716	443	192.168.2.6	69.167.161.101
Apr 12, 2021 19:41:29.288665056 CEST	49716	443	192.168.2.6	69.167.161.101
Apr 12, 2021 19:41:29.288810015 CEST	49716	443	192.168.2.6	69.167.161.101
Apr 12, 2021 19:41:29.289037943 CEST	49716	443	192.168.2.6	69.167.161.101
Apr 12, 2021 19:41:29.289113045 CEST	49716	443	192.168.2.6	69.167.161.101
Apr 12, 2021 19:41:29.289263010 CEST	49716	443	192.168.2.6	69.167.161.101
Apr 12, 2021 19:41:29.323251009 CEST	49716	443	192.168.2.6	69.167.161.101
Apr 12, 2021 19:41:29.323456049 CEST	49716	443	192.168.2.6	69.167.161.101
Apr 12, 2021 19:41:29.439984083 CEST	443	49716	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:29.440016985 CEST	443	49716	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:29.440043926 CEST	443	49716	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:29.440071106 CEST	443	49716	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:29.440143108 CEST	443	49716	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:29.440181017 CEST	443	49716	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:29.440295935 CEST	443	49716	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:29.440484047 CEST	443	49716	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:29.440704107 CEST	443	49716	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:29.441071987 CEST	443	49716	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:29.441098928 CEST	443	49716	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:29.441314936 CEST	443	49716	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:29.441344023 CEST	443	49716	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:29.443842888 CEST	443	49716	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:29.443948984 CEST	49716	443	192.168.2.6	69.167.161.101

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 19:41:29.443994045 CEST	443	49716	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:29.444055080 CEST	49716	443	192.168.2.6	69.167.161.101
Apr 12, 2021 19:41:29.444201946 CEST	443	49716	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:29.444230080 CEST	443	49716	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:29.444277048 CEST	49716	443	192.168.2.6	69.167.161.101
Apr 12, 2021 19:41:29.444854021 CEST	443	49716	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:29.444899082 CEST	443	49716	69.167.161.101	192.168.2.6
Apr 12, 2021 19:41:29.444901943 CEST	49716	443	192.168.2.6	69.167.161.101
Apr 12, 2021 19:41:29.444933891 CEST	49716	443	192.168.2.6	69.167.161.101
Apr 12, 2021 19:41:29.444941044 CEST	443	49716	69.167.161.101	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 19:41:18.654860020 CEST	53	63791	8.8.8.8	192.168.2.6
Apr 12, 2021 19:41:19.473150969 CEST	64267	53	192.168.2.6	8.8.8.8
Apr 12, 2021 19:41:19.521774054 CEST	53	64267	8.8.8.8	192.168.2.6
Apr 12, 2021 19:41:20.177308083 CEST	49448	53	192.168.2.6	8.8.8.8
Apr 12, 2021 19:41:20.233375072 CEST	60342	53	192.168.2.6	8.8.8.8
Apr 12, 2021 19:41:20.236103058 CEST	53	49448	8.8.8.8	192.168.2.6
Apr 12, 2021 19:41:20.284862995 CEST	53	60342	8.8.8.8	192.168.2.6
Apr 12, 2021 19:41:21.056250095 CEST	61346	53	192.168.2.6	8.8.8.8
Apr 12, 2021 19:41:21.104938030 CEST	53	61346	8.8.8.8	192.168.2.6
Apr 12, 2021 19:41:22.022418976 CEST	51774	53	192.168.2.6	8.8.8.8
Apr 12, 2021 19:41:22.071305037 CEST	53	51774	8.8.8.8	192.168.2.6
Apr 12, 2021 19:41:23.408385038 CEST	56023	53	192.168.2.6	8.8.8.8
Apr 12, 2021 19:41:23.457179070 CEST	53	56023	8.8.8.8	192.168.2.6
Apr 12, 2021 19:41:24.237732887 CEST	58384	53	192.168.2.6	8.8.8.8
Apr 12, 2021 19:41:24.290332079 CEST	53	58384	8.8.8.8	192.168.2.6
Apr 12, 2021 19:41:25.696738958 CEST	60261	53	192.168.2.6	8.8.8.8
Apr 12, 2021 19:41:25.748178005 CEST	53	60261	8.8.8.8	192.168.2.6
Apr 12, 2021 19:41:26.386184931 CEST	56061	53	192.168.2.6	8.8.8.8
Apr 12, 2021 19:41:26.444936037 CEST	53	56061	8.8.8.8	192.168.2.6
Apr 12, 2021 19:41:26.653811932 CEST	58336	53	192.168.2.6	8.8.8.8
Apr 12, 2021 19:41:26.711493015 CEST	53	58336	8.8.8.8	192.168.2.6
Apr 12, 2021 19:41:27.755703926 CEST	53781	53	192.168.2.6	8.8.8.8
Apr 12, 2021 19:41:27.902072906 CEST	54064	53	192.168.2.6	8.8.8.8
Apr 12, 2021 19:41:27.950795889 CEST	53	54064	8.8.8.8	192.168.2.6
Apr 12, 2021 19:41:27.959790945 CEST	53	53781	8.8.8.8	192.168.2.6
Apr 12, 2021 19:41:28.781441927 CEST	52811	53	192.168.2.6	8.8.8.8
Apr 12, 2021 19:41:28.842128992 CEST	53	52811	8.8.8.8	192.168.2.6
Apr 12, 2021 19:41:29.329461098 CEST	55299	53	192.168.2.6	8.8.8.8
Apr 12, 2021 19:41:29.381570101 CEST	53	55299	8.8.8.8	192.168.2.6
Apr 12, 2021 19:41:30.057918072 CEST	63745	53	192.168.2.6	8.8.8.8
Apr 12, 2021 19:41:30.197550058 CEST	53	63745	8.8.8.8	192.168.2.6
Apr 12, 2021 19:41:30.834588051 CEST	50055	53	192.168.2.6	8.8.8.8
Apr 12, 2021 19:41:30.891879082 CEST	53	50055	8.8.8.8	192.168.2.6
Apr 12, 2021 19:41:30.907356024 CEST	61374	53	192.168.2.6	8.8.8.8
Apr 12, 2021 19:41:30.966670990 CEST	53	61374	8.8.8.8	192.168.2.6
Apr 12, 2021 19:41:31.290991068 CEST	50339	53	192.168.2.6	8.8.8.8
Apr 12, 2021 19:41:31.351208925 CEST	53	50339	8.8.8.8	192.168.2.6
Apr 12, 2021 19:41:31.372312069 CEST	63307	53	192.168.2.6	8.8.8.8
Apr 12, 2021 19:41:31.424021006 CEST	53	63307	8.8.8.8	192.168.2.6
Apr 12, 2021 19:41:31.497988939 CEST	49694	53	192.168.2.6	8.8.8.8
Apr 12, 2021 19:41:31.525559902 CEST	54982	53	192.168.2.6	8.8.8.8
Apr 12, 2021 19:41:31.557307959 CEST	53	49694	8.8.8.8	192.168.2.6
Apr 12, 2021 19:41:31.584059000 CEST	53	54982	8.8.8.8	192.168.2.6
Apr 12, 2021 19:41:31.904372931 CEST	50010	53	192.168.2.6	8.8.8.8
Apr 12, 2021 19:41:31.956139088 CEST	53	50010	8.8.8.8	192.168.2.6
Apr 12, 2021 19:41:33.081820011 CEST	63718	53	192.168.2.6	8.8.8.8
Apr 12, 2021 19:41:33.130558014 CEST	53	63718	8.8.8.8	192.168.2.6
Apr 12, 2021 19:41:35.687598944 CEST	62116	53	192.168.2.6	8.8.8.8
Apr 12, 2021 19:41:35.739403963 CEST	53	62116	8.8.8.8	192.168.2.6
Apr 12, 2021 19:41:37.319397926 CEST	63816	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 19:41:37.369425058 CEST	53	63816	8.8.8.8	192.168.2.6
Apr 12, 2021 19:41:38.234019041 CEST	55014	53	192.168.2.6	8.8.8.8
Apr 12, 2021 19:41:38.282757044 CEST	53	55014	8.8.8.8	192.168.2.6
Apr 12, 2021 19:41:45.375291109 CEST	62208	53	192.168.2.6	8.8.8.8
Apr 12, 2021 19:41:45.582114935 CEST	53	62208	8.8.8.8	192.168.2.6
Apr 12, 2021 19:41:45.811227083 CEST	57574	53	192.168.2.6	8.8.8.8
Apr 12, 2021 19:41:45.860404968 CEST	53	57574	8.8.8.8	192.168.2.6
Apr 12, 2021 19:41:46.733302116 CEST	51818	53	192.168.2.6	8.8.8.8
Apr 12, 2021 19:41:46.781938076 CEST	53	51818	8.8.8.8	192.168.2.6
Apr 12, 2021 19:41:56.483119011 CEST	56628	53	192.168.2.6	8.8.8.8
Apr 12, 2021 19:41:56.543015003 CEST	53	56628	8.8.8.8	192.168.2.6
Apr 12, 2021 19:41:57.168584108 CEST	60778	53	192.168.2.6	8.8.8.8
Apr 12, 2021 19:41:57.217379093 CEST	53	60778	8.8.8.8	192.168.2.6
Apr 12, 2021 19:41:57.481468916 CEST	56628	53	192.168.2.6	8.8.8.8
Apr 12, 2021 19:41:57.541801929 CEST	53	56628	8.8.8.8	192.168.2.6
Apr 12, 2021 19:41:58.171003103 CEST	60778	53	192.168.2.6	8.8.8.8
Apr 12, 2021 19:41:58.232306957 CEST	53	60778	8.8.8.8	192.168.2.6
Apr 12, 2021 19:41:58.484296083 CEST	56628	53	192.168.2.6	8.8.8.8
Apr 12, 2021 19:41:58.535701990 CEST	53	56628	8.8.8.8	192.168.2.6
Apr 12, 2021 19:41:58.794879913 CEST	53799	53	192.168.2.6	8.8.8.8
Apr 12, 2021 19:41:58.846373081 CEST	53	53799	8.8.8.8	192.168.2.6
Apr 12, 2021 19:41:59.185420036 CEST	60778	53	192.168.2.6	8.8.8.8
Apr 12, 2021 19:41:59.234309912 CEST	53	60778	8.8.8.8	192.168.2.6
Apr 12, 2021 19:42:00.485229969 CEST	56628	53	192.168.2.6	8.8.8.8
Apr 12, 2021 19:42:00.545273066 CEST	53	56628	8.8.8.8	192.168.2.6
Apr 12, 2021 19:42:01.205414057 CEST	60778	53	192.168.2.6	8.8.8.8
Apr 12, 2021 19:42:01.262758970 CEST	53	60778	8.8.8.8	192.168.2.6
Apr 12, 2021 19:42:04.495893955 CEST	56628	53	192.168.2.6	8.8.8.8
Apr 12, 2021 19:42:04.547333002 CEST	53	56628	8.8.8.8	192.168.2.6
Apr 12, 2021 19:42:05.203380108 CEST	60778	53	192.168.2.6	8.8.8.8
Apr 12, 2021 19:42:05.252435923 CEST	53	60778	8.8.8.8	192.168.2.6
Apr 12, 2021 19:42:13.826317072 CEST	54683	53	192.168.2.6	8.8.8.8
Apr 12, 2021 19:42:13.888705015 CEST	53	54683	8.8.8.8	192.168.2.6
Apr 12, 2021 19:42:22.738866091 CEST	59329	53	192.168.2.6	8.8.8.8
Apr 12, 2021 19:42:22.798091888 CEST	53	59329	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 19:41:27.755703926 CEST	192.168.2.6	8.8.8.8	0x5c1e	Standard query (0)	www.golfco ronado.com	A (IP address)	IN (0x0001)
Apr 12, 2021 19:41:30.057918072 CEST	192.168.2.6	8.8.8.8	0x4aa6	Standard query (0)	demo.1-2-1 marketing.com	A (IP address)	IN (0x0001)
Apr 12, 2021 19:41:31.497988939 CEST	192.168.2.6	8.8.8.8	0x8ab2	Standard query (0)	campaignpi lot.com	A (IP address)	IN (0x0001)
Apr 12, 2021 19:41:45.375291109 CEST	192.168.2.6	8.8.8.8	0xa371	Standard query (0)	www.golfco ronado.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 19:41:27.959790945 CEST	8.8.8.8	192.168.2.6	0x5c1e	No error (0)	www.golfco ronado.com	golfcoronado.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 19:41:27.959790945 CEST	8.8.8.8	192.168.2.6	0x5c1e	No error (0)	golfcorona do.com		69.167.161.101	A (IP address)	IN (0x0001)
Apr 12, 2021 19:41:30.197550058 CEST	8.8.8.8	192.168.2.6	0x4aa6	No error (0)	demo.1-2-1 marketing.com		69.167.161.119	A (IP address)	IN (0x0001)
Apr 12, 2021 19:41:31.557307959 CEST	8.8.8.8	192.168.2.6	0x8ab2	No error (0)	campaignpi lot.com		13.32.25.34	A (IP address)	IN (0x0001)
Apr 12, 2021 19:41:31.557307959 CEST	8.8.8.8	192.168.2.6	0x8ab2	No error (0)	campaignpi lot.com		13.32.25.14	A (IP address)	IN (0x0001)
Apr 12, 2021 19:41:31.557307959 CEST	8.8.8.8	192.168.2.6	0x8ab2	No error (0)	campaignpi lot.com		13.32.25.60	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 19:41:31.557307959 CEST	8.8.8.8	192.168.2.6	0x8ab2	No error (0)	campaignpilot.com		13.32.25.82	A (IP address)	IN (0x0001)
Apr 12, 2021 19:41:45.582114935 CEST	8.8.8.8	192.168.2.6	0xa371	No error (0)	www.golfcoronado.com	golfcoronado.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 19:41:45.582114935 CEST	8.8.8.8	192.168.2.6	0xa371	No error (0)	golfcoronado.com		69.167.161.101	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 12, 2021 19:41:28.284631014 CEST	69.167.161.101	443	192.168.2.6	49716	CN=golfcoronado.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sat Mar 20 01:00:00 CET 2021	Sat Jun 19 01:59:59 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Apr 12, 2021 19:41:28.291347027 CEST	69.167.161.101	443	192.168.2.6	49717	CN=golfcoronado.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sat Mar 20 01:00:00 CET 2021	Sat Jun 19 01:59:59 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 12, 2021 19:41:30.540388107 CEST	69.167.161.119	443	192.168.2.6	49721	CN=demo.1-2-1marketing.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sat Mar 20 01:00:00 CET 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Sat Jun 19 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Apr 12, 2021 19:41:30.545665979 CEST	69.167.161.119	443	192.168.2.6	49722	CN=demo.1-2-1marketing.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sat Mar 20 01:00:00 CET 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Sat Jun 19 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Apr 12, 2021 19:41:30.568258047 CEST	69.167.161.119	443	192.168.2.6	49723	CN=demo.1-2-1marketing.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sat Mar 20 01:00:00 CET 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Sat Jun 19 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Apr 12, 2021 19:41:30.572824001 CEST	69.167.161.119	443	192.168.2.6	49724	CN=demo.1-2-1marketing.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sat Mar 20 01:00:00 CET 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Sat Jun 19 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Apr 12, 2021 19:41:30.659321070 CEST	69.167.161.119	443	192.168.2.6	49725	CN=demo.1-2-1marketing.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sat Mar 20 01:00:00 CET 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Sat Jun 19 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

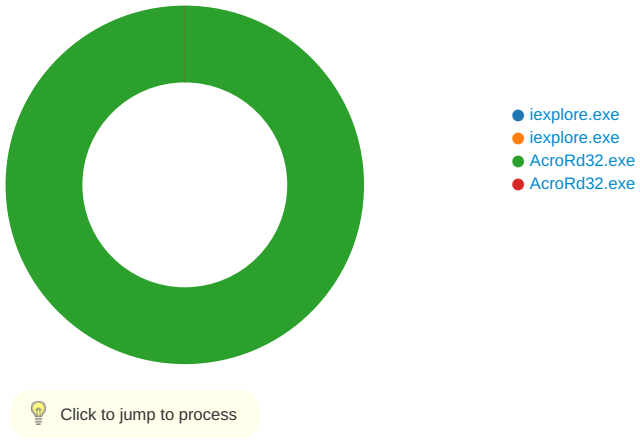
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 12, 2021 19:41:31.650134087 CEST	13.32.25.34	443	192.168.2.6	49739	CN=*.campaignpilot.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Thu Nov 05 01:00:00 CET 2020	Tue Dec 07 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Apr 12, 2021 19:41:31.650393963 CEST	13.32.25.34	443	192.168.2.6	49738	CN=*.campaignpilot.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Thu Nov 05 01:00:00 CET 2020	Tue Dec 07 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 12, 2021 19:41:45.896352053 CEST	69.167.161.101	443	192.168.2.6	49745	CN=golfcoronado.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sat Mar 20 01:00:00 CET 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Sat Jun 19 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: iexplore.exe PID: 5624 Parent PID: 792

General

Start time:	19:41:24
Start date:	12/04/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff721e20000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 6108 Parent PID: 5624

General

Start time:	19:41:25
Start date:	12/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5624 CREDAT:17410 /prefetch:2
Imagebase:	0xd30000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: AcroRd32.exe PID: 7108 Parent PID: 6108

General

Start time:	19:42:02
Start date:	12/04/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' /o /eo /l /b /ac /id 6108
Imagebase:	0x9b0000
File size:	2571312 bytes
MD5 hash:	B969CF0C7B2C443A99034881E8C8740A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\acrord32_sbx	read data or list directory | read attributes | write attributes | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	9E65C3	CreateDirectoryExW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
\Device\NamedPipe\AIPC_SRV\AcroSBL_6108_7108	unknown	1040	success or wait	2	A15549	ReadFile
\Device\NamedPipe\AIPC_SRV\AcroSBL_6108_7108	unknown	1040	success or wait	1	A15505	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\System\Acrobatbrokerserverdispatchercpp789	success or wait	1	9FCF19	RegCreateKeyW

Analysis Process: AcroRd32.exe PID: 6172 Parent PID: 7108

General

Start time:	19:42:03
Start date:	12/04/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 /o /eo /l /b /ac /id 6108
Imagebase:	0x9b0000

File size:	2571312 bytes
MD5 hash:	B969CF0C7B2C443A99034881E8C8740A
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Disassembly

Code Analysis