ID: 412542
Cookbook: browseurl.jbs
Time: 19:04:51
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

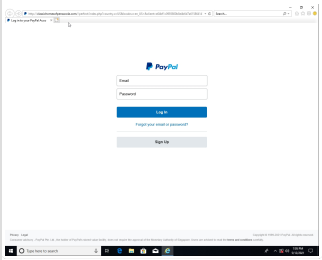
Analysis Report http://classichomesofpensacola.com//p…

Overview

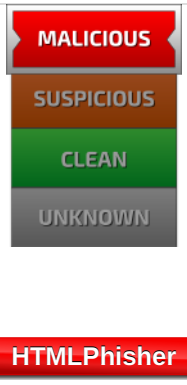
General Information

Sample URL:	http://classichomesofpensacola.com//perfect/index.php
Analysis ID:	412542
Infos:	

Most interesting Screenshot:



Detection



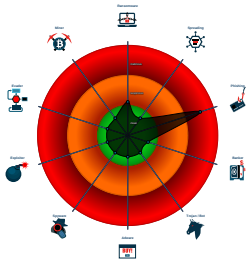
HTMLPhisher

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Phishing site detected (based on fav…
- Yara detected HtmlPhish10
- Phishing site detected (based on log…
- HTML body contains low number of …
- HTML title does not match URL
- Invalid 'forgot password' link found
- Invalid T&C link found
- None HTTPS page querying sensitiv…

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 6396 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6464 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6396 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

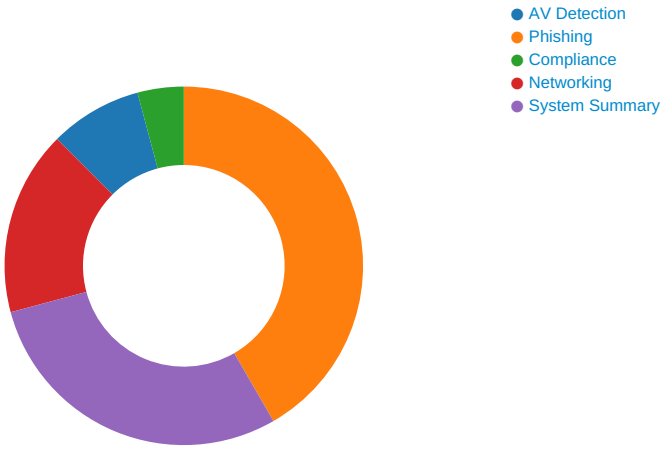
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\index[2].htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Phishing:

Phishing site detected (based on favicon image match)

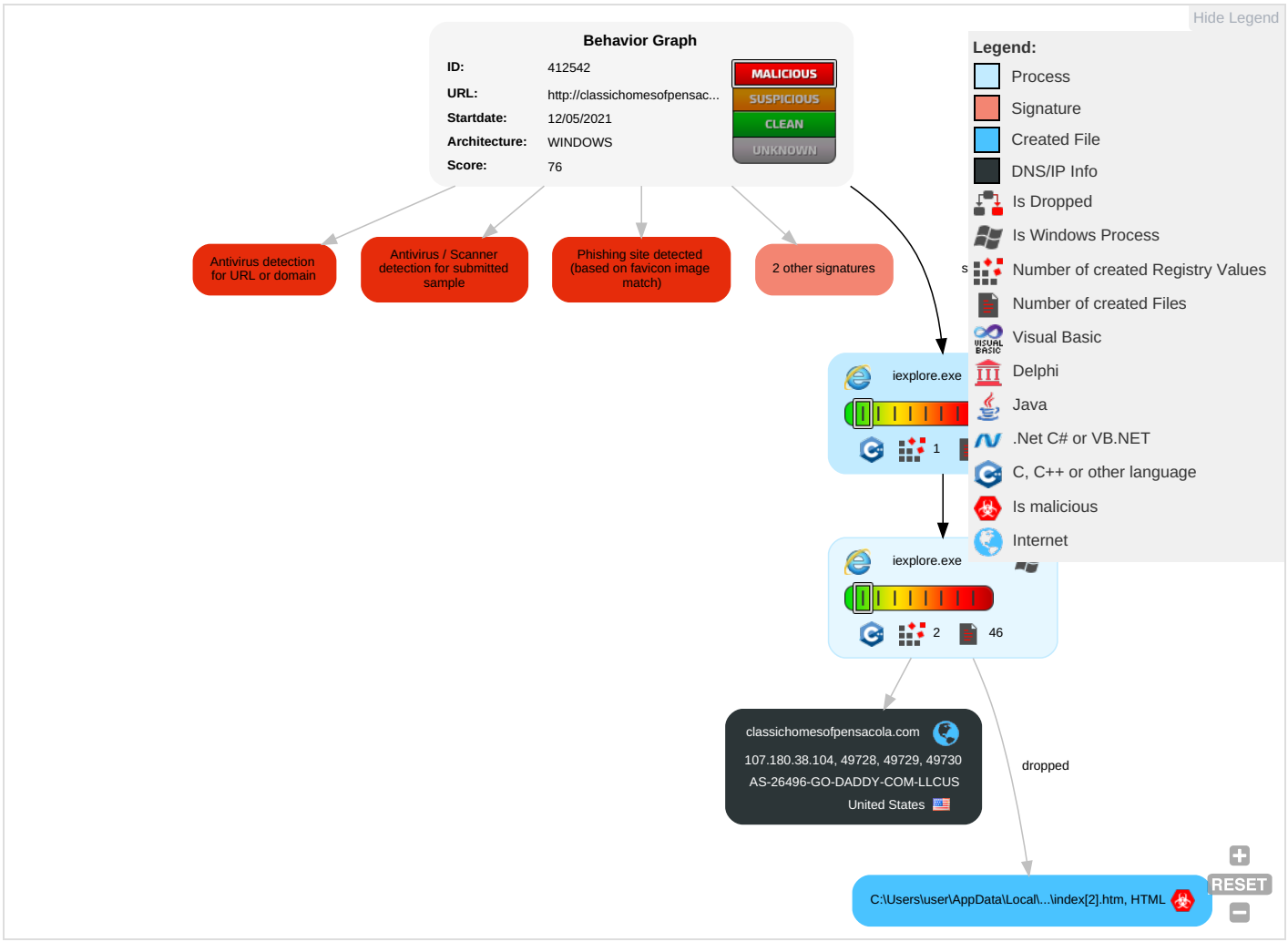
Yara detected HtmlPhish10

Phishing site detected (based on logo template match)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impac
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 3	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modif Syste Partiti
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 3	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lockc
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data

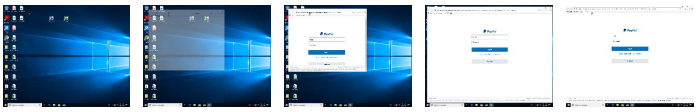
Behavior Graph

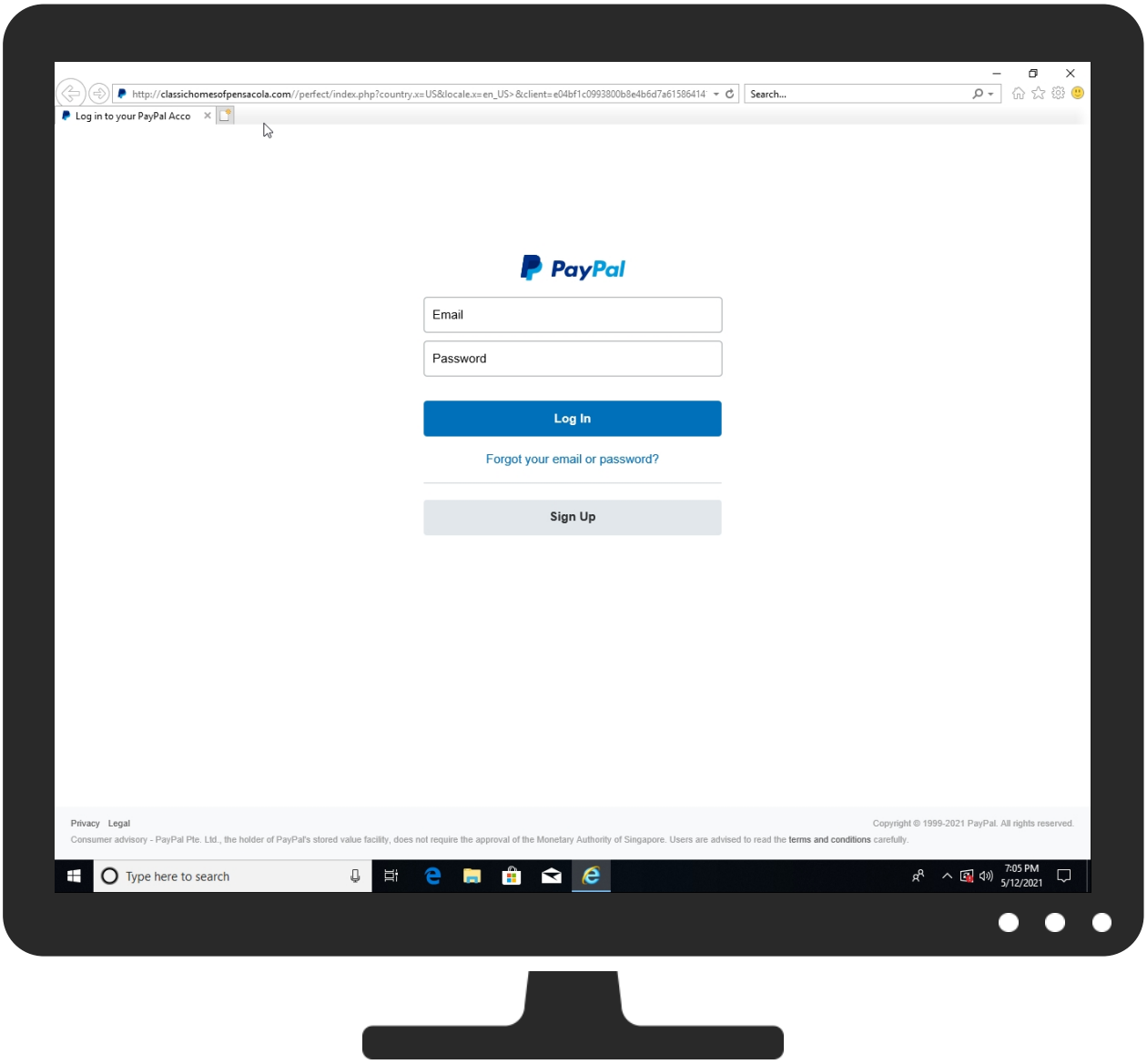


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://classichomesofpensacola.com//perfect/index.php	0%	Virustotal		Browse
http://classichomesofpensacola.com//perfect/index.php	0%	Avira URL Cloud	safe	
http://classichomesofpensacola.com//perfect/index.php	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://classichomesofpensacola.com//perfect/index.php?country.x=US&locale.x=en_US>&client=e04bf1c0993800b8e4b6d7a615864141	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://classichomesofpensacola.com//perfect/assets/js/b64.min.js	0%	Avira URL Cloud	safe	
http://classichomesofpensacola.com//perfect/assets/css/master.css	0%	Avira URL Cloud	safe	
http://classichomesofpensacola.com//perfect/index.phpRoot	0%	Avira URL Cloud	safe	
http://classichomesofpensacola.com//perfect/assets/img/logo.svg	0%	Avira URL Cloud	safe	
http://classichomesofpensacola.com//perfect/assets/js/master.js	0%	Avira URL Cloud	safe	
http://classichomesofpensacola.com//perfect/assets/img/favicon.ico	0%	Avira URL Cloud	safe	
http://classichomesofpensacola.com//perfect/assets/img/favicon.ico~	0%	Avira URL Cloud	safe	
http://classichomesofpensacola.com//perfect/assets/img/notif.png	0%	Avira URL Cloud	safe	
http://classichomesofpensacola.com//perfect/index.phpensacola.com//perfect/index.php?country.x=US&lo	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
classichomesofpensacola.com	107.180.38.104	true	false		unknown

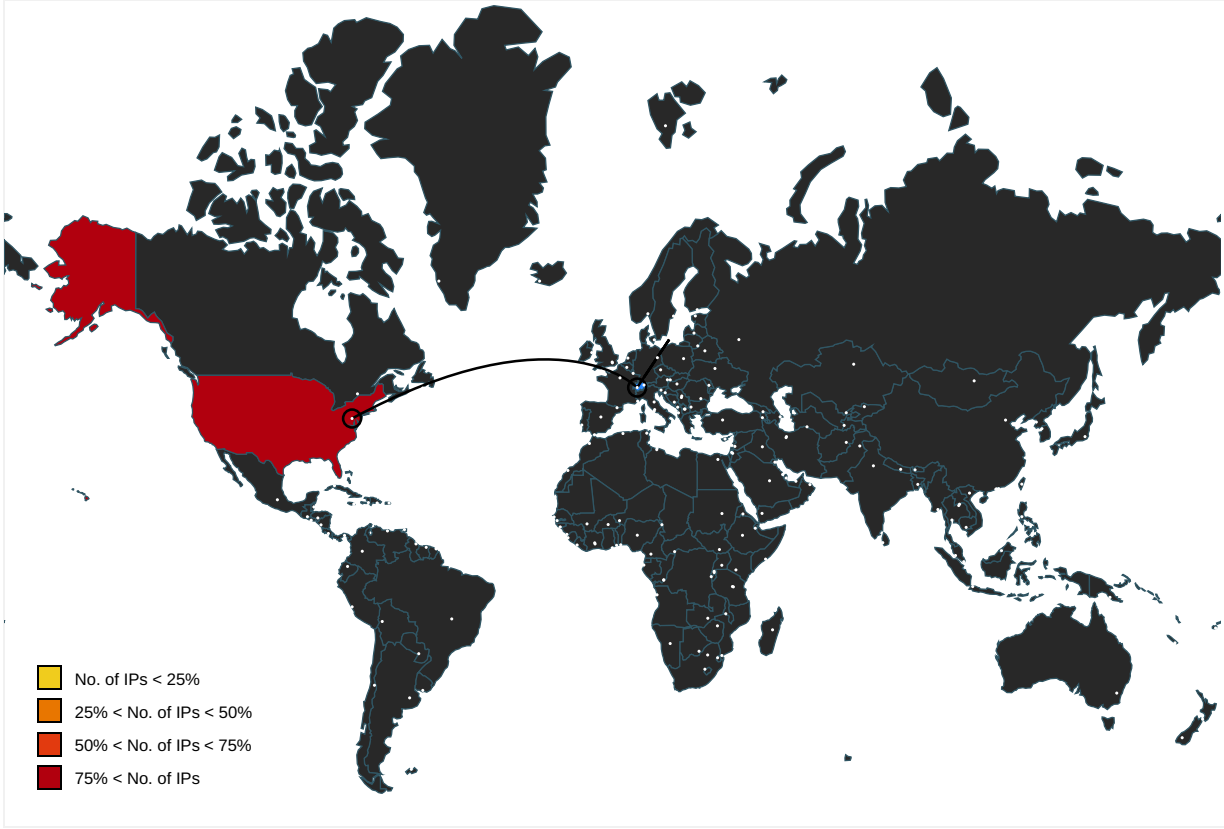
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://classichomesofpensacola.com//perfect/index.php	true		unknown
http://classichomesofpensacola.com//perfect/assets/js/b64.min.js	false	• Avira URL Cloud: safe	unknown
http://classichomesofpensacola.com//perfect/assets/css/master.css	false	• Avira URL Cloud: safe	unknown
http://classichomesofpensacola.com//perfect/assets/img/logo.svg	false	• Avira URL Cloud: safe	unknown
http://classichomesofpensacola.com//perfect/assets/js/master.js	false	• Avira URL Cloud: safe	unknown
http://classichomesofpensacola.com//perfect/assets/img/favicon.ico	false	• Avira URL Cloud: safe	unknown
http://classichomesofpensacola.com//perfect/assets/img/notif.png	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://classichomesofpensacola.com//perfect/index.phpRoot	{44CA2AF6-B344-11EB-90EB-ECF4BBEA1588}.dat.1.dr	true	• Avira URL Cloud: safe	unknown
http://classichomesofpensacola.com//perfect/assets/img/favicon.ico~	imagestore.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://classichomesofpensacola.com//perfect/index.phpensacola.com//perfect/index.php?country.x=US&lo	{44CA2AF6-B344-11EB-90EB-ECF4BBEA1588}.dat.1.dr	true	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
107.180.38.104	classichomesofpensacola.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412542
Start date:	12.05.2021
Start time:	19:04:51
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://classichomesofpensacola.com//perfect/index.php
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:	8
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:	MAL
Classification:	mal76.phis.win@3/17@1/1
Cookbook Comments:	• Adjust boot time • Enable AMSI

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\Recovery\High\Active\RecoveryStore.{44CA2AF4-B344-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8476222614429676
Encrypted:	false
SSDEEP:	192:rIZ/ZW2sWItSifG1LzM5DBBpDAsfG1CjX:rIBt7s73jv/T
MD5:	9E6C52C1FB6E4F6E9F3C7BBFDCFDFFE9
SHA1:	06E8D42C1D7443657A820EF02CE2DE5C58093EAE
SHA-256:	2B644DA1B568098888C13DD25502C72AAA56497C9B44CB6DB51830D10458ACDF
SHA-512:	E480DCF25A0B3ABD7218E7C630E9B18E26AC78B560AC90B6F1604EB74E3283D5E2B94AF0C58728334E840BCA7AAA2DBE71467C2C96D53A80463546731747FF5A
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\{44CA2AF6-B344-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	26980
Entropy (8bit):	1.6969748214562377

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{44CA2AF6-B344-11EB-90EB-ECF4BBEA1588}.dat	
Encrypted:	false
SSDEEP:	48:IwtGcprAGwpa4G4pQAGrapbSuGQpBqGHHpcnTGUp8GrGzYpmewQGopt0VG6Xpa0Z:rzZIQo6eBSmjx2xW2Majk8vnD2Lr
MD5:	07B0040BEB3CF1D0305AEAEF92DB9282
SHA1:	6BF077A8A61EEA3A23DF6AA75A2E9B9C8A720728
SHA-256:	B2B5BA48AF1E4C9CFE0AC19619A3517B67838996A6D9C3BFEB0233EB0C2D6248
SHA-512:	0ECB60DD10FAA2F92D3AB2F905E7E7BF0F51C260A9C15A5F1888A626D8B5F496F691AA6CF49D02C11A66ED3D9F4B429F2F193E9CE49B0390105E877183DB665A
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\{44CA2AF7-B344-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5647085335548412
Encrypted:	false
SSDEEP:	48:Iw9uGcprPVGwpaFuG4pQr8GrapbSotGQpKqxG7HpRZTGIpG:r4ZXQc62BSoXAqgTfA
MD5:	2D1CA6435A307DD761FF1D5B640682AA
SHA1:	AD6154EEE9A11C9498182B989F0E26544F457FB7
SHA-256:	A10CF633E1DF4A50FFD07F03D729FC149E64B2B63089DA810D33905DF4D0E862
SHA-512:	A34E8F7B28A7B23736854F82C526A01A6B5C8E454ED4CD76E0DF4C4EF00D56F84362D15E1301A61EFC3A1CC6C4E825167D8531FCF3AFC1F3836D34BFAE50B9C
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\gee00pr\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	5776
Entropy (8bit):	3.5576182707923585
Encrypted:	false
SSDEEP:	48:aF/s+/pSKnJ/3cCXndBlr9aPZ0M0V+2hDTGlpFR6vF/O4cPgCOfuw:aOASKJPcCXjgZ03Gr6vc1w
MD5:	D44BD2B69A31E1C45FFC5056B61E6230
SHA1:	DA1609C3288B2FC9E84B833C2AB511B8EA8F8B0D
SHA-256:	B8FF19396BA993E959667FEABCCBD370AEBB828DD273873D2E59B7AE97BF74CE
SHA-512:	45D7FAD85CD9530583B52327116E3C7142638EF37F1C47C432404CE58354EF0D8054EE5D7B66C24B89E33EBF18A6C8679F126FCFAC7211FDD46F31AF9859F1A(
Malicious:	false
Reputation:	low
Preview:	B.h.t.t.p.:.//.c.l.a.s.s.i.c.h.o.m.e.s.o.f.p.e.n.s.a.c.o.l.a...c.o.m././/.p.e.r.f.e.c.t./.a.s.s.e.t.s./.i.m.g./.f.a.v.i.c.o.n...i.c.o..... ....(... ...@..... .....0...0...0...0.....>.....X.....\.....$...<

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\index[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	126
Entropy (8bit):	4.970951059453435
Encrypted:	false
SSDEEP:	3:NjBI//wONTAafZauRLRtVodVvU/WB/ZNGXIL//n:4auL/eVv7d7
MD5:	8CE93C5F3E2C9E5BE682579F7A7858C1
SHA1:	DE7E7EBA0B1FDB52D8814B813B350D7EAEDEB3CC
SHA-256:	3B07047696BE8A6144F9573979398329790 1562BA32A2219D507269E818C498
SHA-512:	C420CE985D042CC2D8E81CDA773D3621908FEDD9CD13A0C173BB7F08DD0B05AAB7F18C07C2C9ED2F0AF76866394A6CB3275BFC84655A774085849AA65F3B9FA

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\index[1].htm	
Malicious:	false
Reputation:	low
Preview:	<script>. window.location = "?country.x=US&locale.x=en_US>&client=e04bf1c0993800b8e4b6d7a615864141";. </script>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\index[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	2414
Entropy (8bit):	5.02392341322843
Encrypted:	false
SSDEEP:	24:RYeY/MyBJl5eXQEAO8ZQyNccuOIQDFlM/Cv39noC4Y/NMdCBP9dwfQI:dQUyOTQplGCv39J4ENPI
MD5:	6031D1D58AB1CDEFFB79284DC38F1398
SHA1:	B18B4DC0C7026D8A44B753682507E2A70392809E
SHA-256:	2984F6ECB6BEECD264FFBD7A1712D5609E5B85DC37D52E0123CCDD3A530042F9
SHA-512:	F23597EEA8AE3F021870EBF8B6E51E0BC92FD63F3546EFC3532C14D4705FCAFE8913964AEB4A42C0B5D32C47F5E431734768AD186CD02F29BE1B42611D901AD E
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\index[2].htm, Author: Joe Security
Reputation:	low
Preview:	<!DOCTYPE html>.<html>. <head>. <meta charset="utf-8">. <title>Log in to your PayPal Account</title>. <link rel="stylesheet" href="assets/css/master.css" me dia="screen" title="no title" charset="utf-8">. <link rel="icon" type="image/png" href="assets/img/favicon.ico" />. <script src="assets/js/master.js" charset="utf-8"> </script>. <script src="assets/js/b64.min.js" charset="utf-8"></script>. <meta name="viewport" content="width=device-width, user-scalable=no">. </head>. <body>. . . . . <input id="input[email]" placeholder="Email" />. . Email address is required. . . <div id="pas sword_input">. <input id="input[password]" type="password" class="password" placeholder="Password" />.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\master[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	32602
Entropy (8bit):	4.8836529954149865
Encrypted:	false
SSDEEP:	768:q3NFwLFUeDLCFP3rFPFQFU36sXmZxeFJy:W+LiOCdNPqK7y
MD5:	16360AC112D6BFB9C3250436E1B3D9D9
SHA1:	A9766F4F27D7429E8F44711287F29EFFC077ECE3
SHA-256:	263012469D3314A4978F3DC9F9974BA0E5413A923D9E0FDAA3EB0B62879459D8
SHA-512:	3EA131622C0BED9E5CFBCA76024BCB7EB2B4023FB2FDA6DF745CC024394CD154AF659B15500306B24CD10374DB5CB489B858A6735E2054D129990D00833DBC 6
Malicious:	false
Reputation:	low
IE Cache URL:	http://classichomesofpensacola.com//perfect/assets/css/master.css
Preview:	@import url('https://fonts.googleapis.com/css?family=Open+Sans');.@import url('https://fonts.googleapis.com/css?family=Open+Sans+Condensed:300');.body {. margin : 0;. padding : 0;. font-family : HelveticaNeue,"Helvetica Neue",Helvetica,Arial,sans-serif;. overflow-x : hidden;.}.input::placeholder {. color : #6c7378;.}.select::-ms-expand {. display: none;.}.select::-moz-expand {. display: none;.}.select::-webkit-expand {. display: none;.}.select::-o-expand {. display: none;.}.select::expand {. display: none;.}./* Main Login form */..errorPlace::-webkit-input-placeholder {. color : #c72f38;.}..errorPlace::-moz-placeholder {. color : #c72f38;.}..errorPlace::-moz-placeholder {. color : #c72f38;.}..errorPlace::-ms-input-placeholder {. color : #c72f38;.}..main_login {. width : 460px;. margin-top : 130px;. margin-left : auto;. margin-right : a uto;.}..main_login .inner_login {. padding : 30px 10% 50px;. text-align : center;.}..main_login .inner_login .logo {.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\master[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	3292
Entropy (8bit):	4.767880678334397
Encrypted:	false
SSDEEP:	96:C9mOB6Kb2Io9NyNYxANVy3dNMxvJJqNVIvCTg5yaM:C9NeFGSJ3dGRJqMaIyaM
MD5:	7A98467882FCD103AE6A0D64DB939C23
SHA1:	D582FB56C3654F5092E35E984F55EAC1527B8294
SHA-256:	808BA9B9EC55E6440E0CD75ED57A7D34C6F9D4EBA35D2D3D6E884948CBEC73F2
SHA-512:	4A5AC7442B4D9764E6182A6E5D32C032D62C4FCFA204FBEECACABA54391EC702EF06299788D4C4AC95B72C49BFFC286D557DEF7D307B66EDCEB18EDE7979 C04
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\master[1].js	
IE Cache URL:	http://classichomesofpensacola.com//perfect/assets/js/master.js
Preview:	window.onload = function() {. function $(element) {. return document.getElementById(element);. }. var errors = {. email : false,. password : false. }. docum ent.getElementById("input[login]").addEventListener("click", function() {. if($("input[email]").value == "" || $("input[password]").value == "") {. if($("input[email]").value == "") {. $("input[email]").className = $("input[email]").className+" inputError errorPlace";. errors.email = true;. }. if($("input[password]").value == "") {. $("input[password]").className = $("input[password]").className+" inputError errorPlace";. errors.password = true;. }. } else if($("input[email]").value != "" && $("input[password]").value != "") {.. }. }). document.getElementById("input[email]").addEventListener("focus", function() {. if(errors.email) {. if($("input[email]").value == "") {. $("errorMail").className = "emailError";. $("input[email]").className

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	184
Entropy (8bit):	5.10694341188927
Encrypted:	false
SSDEEP:	3:0SYWFFWIIYCiF15RI5XwDKLRIHDfFRWdFTfqzrZqcdJ2dTv8EuRlG1LQUYARNin:0IFFm15+56ZRWHTizlpd0aFlcLFNin
MD5:	408681294E6694B3929BBC0B3EE38A9D
SHA1:	4E9885F43559CABE1A3EB66C2B08840ADE077C5E
SHA-256:	0D9374CF3695C6E0627D1A183B86C1F7C2A65EE4619B90EF04176D9CF69DD2A3
SHA-512:	48CC0ABDBF7604CFA6BA4CE93300AB7D2E4175C3177F7A7ABFA9C97223F542F6B3B7AD4E28AEB2073459AD1A206160335914FF6D95DD1341AF9F1A659EC8125 6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.googleapis.com/css?family=Open+Sans
Preview:	@font-face {. font-family: 'Open Sans';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/opensans/v18/mem8YaGs126MiZpBA-UFVZ0d.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\css[2].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	221
Entropy (8bit):	5.336545865636817
Encrypted:	false
SSDEEP:	6:0IFFmjjQ+56ZzhizlpdnKKTO7MeHSzNin:jFjO6ZN6prMpHSzY
MD5:	21AC5C64739366D0DF1DD5DE7BAA0FF5
SHA1:	BB96B385323AA126D9EC2BC05237BF7673718578
SHA-256:	F37BFA8CE03C5937B6FC3C3438C8E2EE47E6F2718B920511D2F1D3E1A56F25CF
SHA-512:	CDF7B554EB6CAC323CE8B55A3C69E7ECEFF1E7A851924D2DC95384670E0E906C82DCDC7FF42C98DF415250816222CF5946FE30BB4C2ABF504EB47A8E34A3F7 A5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.googleapis.com/css?family=Open+Sans+Condensed:300
Preview:	@font-face {. font-family: 'Open Sans Condensed';. font-style: normal;. font-weight: 300;. src: url(https://fonts.gstatic.com/s/opensanscondensed/v15/z7NFdQ DnbTkabZAIOl9il_O6KJj73e7Ff1GhDuXMQQ.woff) format('woff');.}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 2 icons, 32x32, 32 bits/pixel, 16x16, 32 bits/pixel
Category:	downloaded
Size (bytes):	5430
Entropy (8bit):	3.4364435707992746
Encrypted:	false
SSDEEP:	48:++/pSKnJ/3cCXndBlr9aPZ0M0V+2hDTGlpFRlcPgCOfU:+ASKJPcCXjgZ03Gre9
MD5:	E1528B5176081F0ED963EC8397BC8FD3
SHA1:	FF60AFD001E924511E9B6F12C57B6BF26821FC1E
SHA-256:	1690C4E20869C3763B7FC111E2F94035B0A7EE830311DD680AC91421DAAD3667
SHA-512:	ACF71864E2844907752901EEEAF5C5648D9F6ACF3B73A2FB91E580BEE67A04FFE83BC2C984A9464732123BC43A3594007691653271BA94F95F7E1179F4146212
Malicious:	false
Reputation:	low
IE Cache URL:	http://classichomesofpensacola.com//perfect/assets/img/favicon.ico
Preview:	....&..... .h.....(... ...@.... .....0...0.. .0...0.....>.....X.....\..... .....$...<...:.:.:...d.....q

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\notif[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 40 x 2000, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	4675
Entropy (8bit):	7.068922588814696
Encrypted:	false
SSDEEP:	96:KQvlQTt8oYG/K6H5OwFMrd7qmFhjDvWshlt78YH:KJTt8oYG/K6H5OMMrdXFdTWshlt78a
MD5:	502378EEC366D5D25C22D1F0B33A33DB
SHA1:	975A45A856EBF52FC80A0BB97D25D822128347C6
SHA-256:	54436312813C5BA0070898EC0AC998A94E0486D12417A8FA4602CC501A94029E
SHA-512:	886BE7C0BA0C9B82944CCA997545587B7B204F343E0D9858E31B9D6032BD18B39585AAC5C7A7692E8DCFCFBFC078E208E800237EA4C12D7C93A03F4784D12B7
Malicious:	false
Reputation:	low
IE Cache URL:	http://classichomesofpensacola.com//perfect/assets/img/notif.png
Preview:	.PNG.....IHDR...(.....tEXtSoftware.Adobe ImageReadyq.e<...hiTXtXML:com.adobe.xmp.....<?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/" xmpMM:OriginalDocumentID="xmp.did:EC09E1E3AB20681183D1FA404987CC05" xmpMM:DocumentID="xmp.did:2E159D65158611E488FEC58FCFDABE46" xmpMM:InstanceID="xmp.iid:2E159D64158611E488FEC58FCFDABE46" xmp:CreatorTool="Adobe Photoshop CS6 (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:45AC8677B020681183D1FA404987CC05" stRef:documentID="xmp.did:EC09E1E3AB20681183D1FA404987CC05"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>.Y.....qIDATx...n....pj.".t.. ..".K'...+..0.4.{.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\b64.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	1570
Entropy (8bit):	5.45030392854939
Encrypted:	false
SSDEEP:	24:YSeK+C6uSKJwynFyzpzOYS/zjDeJbFn9pbzRHqg4cGpxOrSJ6NGGfCtfKGfqzPGT:YT1CTtyy5/zjDerlHd4cYOrSo6lhnV
MD5:	8FE41B3B3F0B14FDBA60E8FAA9C41E28
SHA1:	2EF946051315F85F7DAB000E830488CEF8A2B155
SHA-256:	B9986FECCDB9B6C99CC338802FAD3D6335B3FD5ECDB12EE5B3ABED91E0073036
SHA-512:	D598C059318A43CBD8939DF5E3F5DE67101F51E542735A647F6E782A1AE2862776ABBC19A0EAC686CB836900F9DA26BC908AE9101FD5BE4851318C641D93006
Malicious:	false
Reputation:	low
IE Cache URL:	http://classichomesofpensacola.com//perfect/assets/js/b64.min.js
Preview:	var Base64={_keyStr:"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=",encode:function(e){var t="";var n,r,i,s,o,u,a;var f=0;e=Base64._utf8_encode(e);while(f<e.length){n=e.charCodeAt(f++);r=e.charCodeAt(f++);i=e.charCodeAt(f++);s=n>>2;o=(n&3)<<4|r>>4;u=(r&15)<<2|i>>6;a=i&63;if(isNaN(r)){u=a=64}else if(isNaN(i)){a=64}t=t+this._keyStr.charAt(s)+this._keyStr.charAt(o)+this._keyStr.charAt(u)+this._keyStr.charAt(a)}return t},decode:function(e){var t="";var n,r,i;var s,o,u,a;var f=0;e=e.replace(/[^A-Za-z0-9+/=]/g,"");while(f<e.length){s=this._keyStr.indexOf(e.charAt(f++));o=this._keyStr.indexOf(e.charAt(f++));u=this._keyStr.indexOf(e.charAt(f++));a=this._keyStr.indexOf(e.charAt(f++));n=s<<2|o>>4;r=(o&15)<<4|u>>2;i=(u&3)<<6|a;t=t+String.fromCharCode(n);if(u!=64){t=t+String.fromCharCode(r)}if(a!=64){t=t+String.fromCharCode(i)}}t=Base64._utf8_decode(t);return t},_utf8_encode:function(e){e=e.replace(/rn/g,"n");var t="";for(var n=0;n<e.length;n++){var r=e.charCodeAt(n);if(r<128){

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\logo[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	4887
Entropy (8bit):	4.565733209566604
Encrypted:	false
SSDEEP:	96:bOKf0jFoS7sneGFDDZd+mwtNmxECm6v24G6vWTlCkKvt:yo0jFuWCxslTS
MD5:	38E8C0D05CEAA689DD28B9FE14DE9223
SHA1:	58F4E51CE99310EF1B6ADB30A1FD56D39B2C59B9
SHA-256:	F09F6C5B8970779BE19412B98E8CE4DF8DB12777ADE87D28D20EF2B2FB92C757
SHA-512:	1B7C517CEB7C4C4A181437DF85CA60CC39D295D32C3F1B21325D98CD9F84C4EE2937D6BEF96DE336648A07D565E6466F14A422A90DA989D54D7ED3CEBBE44B
Malicious:	false
Reputation:	low
IE Cache URL:	http://classichomesofpensacola.com//perfect/assets/img/logo.svg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\logo[1].svg	
Preview:	<?xml version="1.0" encoding="UTF-8"?>. Generator: Adobe Illustrator 16.0.0, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->.<!DOCTYPE svg PUBLIC "-//W3C //DTD SVG 1.1//EN" "http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd">.<svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px" width="127.769px" height="31.5px" viewBox="0 0 127.769 31.5" enable-background="new 0 0 127.769 31.5" xml:space="preserve">.<g>..<g>...<g>....<path fill="#009CDE" d="M98.396,6.933H91.37c-0.479,0-0.89,0.35-0.964,0.824l-2.841,18.015c-0.056,0.355,0.219,0.676,0.579,0.676 h3.604c0.335,0,0.622-0.244,0.674-0.576l0.807-5.107c0.074-0.474,0.483-0.824,0.964-0.824h2.223c4.628,0,7.298-2.239,7.996-6.678 c0.314-1.941,0.014-3.467-0.896-4.535C102.518,7.553,100.746,6.933,98.396,6.933z M99.207,13.512 c-0.384,2.522-2.31,2.522-4.173,2.522h-1.061l0.744-4.708c0.045-0.285,0.29-0.495,0.578-0.495h0.485c1.269,0,2.467,0,3.084,0.723 C99.234,11.98

C:\Users\user\AppData\Local\Temp\~DF2E3BD50B36985F65.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	38965
Entropy (8bit):	0.41370497072465917
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+PxzaeIe/0q020j7nD2Gh:kBqoxKAuvScS+PxzaBKRt0nD22
MD5:	0C6B77466CB3624B4F2D7E19DEFAE1C4
SHA1:	B61261731D8DEA7A6941A476DE2A578A61116312
SHA-256:	4F861FDDC8BA885E841FA96A40D1478B3B5DCE39D6A7EE9F94420BB7D2ECED9C
SHA-512:	6A1744969F8B0756998A60C5293451C33BDA387CD469CCC2735AADA6C07306BD719EC9D06CC3B4797DC29B0C5F8C75E61870B2E0BDE872D2258DCF22D412D7 8
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF33D489DE5A268363.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.3405746096014492
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laAIL19K:kBqoxxJhHWSVSEabS
MD5:	509CFEC3EA2755B9C331BC279853BE11
SHA1:	46B0DEB55D543FE1068B1EAE5C89258DC1CCF1D4
SHA-256:	A738D3920980D5F1031EB66277265F07E16B91B62FF1FAF1EB59D0F6B420953F
SHA-512:	D044C984FD4F9A40CE1F87D3A089E3702BEE513867196B34878A533D82F32303907B2876D2D086091DEA892D7C78DF4E254A7EFC87270290621D9A819F3F65FB
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

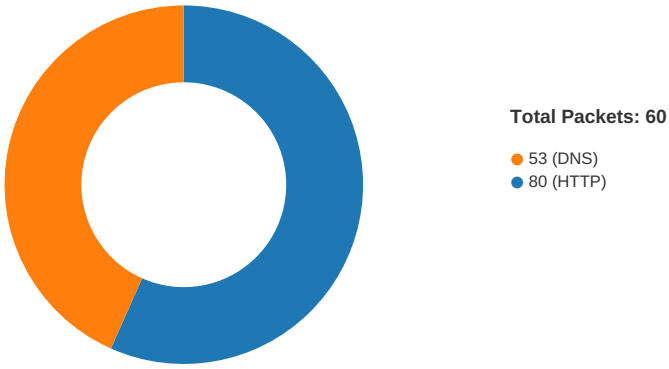
C:\Users\user\AppData\Local\Temp\~DF6E7407FC22AF9C37.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4718427408139265
Encrypted:	false
SSDEEP:	12:c9lCg5/9lCgeK9l26an9l26an9l8fR4oF9l8fR4Q9lTq4s43A0Z439G/v9tQZQB:c9lLh9lLh9lIn9lIn9loP9loP9lWU+0
MD5:	53EFBE0DB1E881BDB98FDB8142A121B7
SHA1:	08FCBD8D85F40142D6AB5CF3E0FAA7DF1CB8A369
SHA-256:	AE1911377B1C96BC2045E35F555AECF1432D0B8F331336067D41F63671A7EE16
SHA-512:	629D5B7B7FFA0D4688C3D086CAC021B62F53C924605C3BA60EFD4333873809D95B048DBED124D2E74B2FEE5309DB95C30BCE7E308D9AF9D691C476A90A5338 6
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 19:05:38.864056110 CEST	49728	80	192.168.2.4	107.180.38.104
May 12, 2021 19:05:38.865211010 CEST	49729	80	192.168.2.4	107.180.38.104
May 12, 2021 19:05:38.997952938 CEST	80	49728	107.180.38.104	192.168.2.4
May 12, 2021 19:05:38.998023987 CEST	80	49729	107.180.38.104	192.168.2.4
May 12, 2021 19:05:38.998048067 CEST	49728	80	192.168.2.4	107.180.38.104
May 12, 2021 19:05:38.998128891 CEST	49729	80	192.168.2.4	107.180.38.104
May 12, 2021 19:05:38.999253035 CEST	49728	80	192.168.2.4	107.180.38.104
May 12, 2021 19:05:39.131501913 CEST	80	49728	107.180.38.104	192.168.2.4
May 12, 2021 19:05:39.325696945 CEST	80	49728	107.180.38.104	192.168.2.4
May 12, 2021 19:05:39.325838089 CEST	49728	80	192.168.2.4	107.180.38.104
May 12, 2021 19:05:39.487900019 CEST	49728	80	192.168.2.4	107.180.38.104
May 12, 2021 19:05:39.625966072 CEST	80	49728	107.180.38.104	192.168.2.4
May 12, 2021 19:05:39.664980888 CEST	80	49728	107.180.38.104	192.168.2.4
May 12, 2021 19:05:39.665111065 CEST	49728	80	192.168.2.4	107.180.38.104
May 12, 2021 19:05:39.665407896 CEST	80	49728	107.180.38.104	192.168.2.4
May 12, 2021 19:05:39.665477991 CEST	49728	80	192.168.2.4	107.180.38.104
May 12, 2021 19:05:39.670811892 CEST	49728	80	192.168.2.4	107.180.38.104
May 12, 2021 19:05:39.671591997 CEST	49729	80	192.168.2.4	107.180.38.104
May 12, 2021 19:05:39.672554970 CEST	49730	80	192.168.2.4	107.180.38.104
May 12, 2021 19:05:39.803913116 CEST	80	49729	107.180.38.104	192.168.2.4
May 12, 2021 19:05:39.804802895 CEST	80	49730	107.180.38.104	192.168.2.4
May 12, 2021 19:05:39.804902077 CEST	49730	80	192.168.2.4	107.180.38.104
May 12, 2021 19:05:39.806071043 CEST	49730	80	192.168.2.4	107.180.38.104
May 12, 2021 19:05:39.809715986 CEST	80	49728	107.180.38.104	192.168.2.4
May 12, 2021 19:05:39.809739113 CEST	80	49729	107.180.38.104	192.168.2.4
May 12, 2021 19:05:39.809787035 CEST	49728	80	192.168.2.4	107.180.38.104
May 12, 2021 19:05:39.809822083 CEST	49729	80	192.168.2.4	107.180.38.104
May 12, 2021 19:05:39.811552048 CEST	80	49728	107.180.38.104	192.168.2.4
May 12, 2021 19:05:39.811619043 CEST	49728	80	192.168.2.4	107.180.38.104
May 12, 2021 19:05:39.814441919 CEST	80	49728	107.180.38.104	192.168.2.4
May 12, 2021 19:05:39.814513922 CEST	49728	80	192.168.2.4	107.180.38.104

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 19:05:39.818124056 CEST	80	49728	107.180.38.104	192.168.2.4
May 12, 2021 19:05:39.818201065 CEST	49728	80	192.168.2.4	107.180.38.104
May 12, 2021 19:05:39.938354969 CEST	80	49730	107.180.38.104	192.168.2.4
May 12, 2021 19:05:39.983629942 CEST	80	49730	107.180.38.104	192.168.2.4
May 12, 2021 19:05:39.983769894 CEST	49730	80	192.168.2.4	107.180.38.104
May 12, 2021 19:05:40.525440931 CEST	49730	80	192.168.2.4	107.180.38.104
May 12, 2021 19:05:40.559333086 CEST	49728	80	192.168.2.4	107.180.38.104
May 12, 2021 19:05:40.561331034 CEST	49729	80	192.168.2.4	107.180.38.104
May 12, 2021 19:05:40.673305988 CEST	80	49730	107.180.38.104	192.168.2.4
May 12, 2021 19:05:40.673480988 CEST	49730	80	192.168.2.4	107.180.38.104
May 12, 2021 19:05:40.674105883 CEST	80	49730	107.180.38.104	192.168.2.4
May 12, 2021 19:05:40.674639940 CEST	49730	80	192.168.2.4	107.180.38.104
May 12, 2021 19:05:40.698867083 CEST	80	49728	107.180.38.104	192.168.2.4
May 12, 2021 19:05:40.698973894 CEST	49728	80	192.168.2.4	107.180.38.104
May 12, 2021 19:05:40.699640036 CEST	80	49728	107.180.38.104	192.168.2.4
May 12, 2021 19:05:40.699716091 CEST	49728	80	192.168.2.4	107.180.38.104
May 12, 2021 19:05:40.735100985 CEST	80	49729	107.180.38.104	192.168.2.4
May 12, 2021 19:05:40.784804106 CEST	80	49729	107.180.38.104	192.168.2.4
May 12, 2021 19:05:40.785006046 CEST	49729	80	192.168.2.4	107.180.38.104
May 12, 2021 19:05:40.785126925 CEST	80	49729	107.180.38.104	192.168.2.4
May 12, 2021 19:05:40.785197973 CEST	49729	80	192.168.2.4	107.180.38.104
May 12, 2021 19:05:40.785481930 CEST	80	49729	107.180.38.104	192.168.2.4
May 12, 2021 19:05:40.785548925 CEST	49729	80	192.168.2.4	107.180.38.104
May 12, 2021 19:05:40.785701990 CEST	80	49729	107.180.38.104	192.168.2.4
May 12, 2021 19:05:40.785768032 CEST	49729	80	192.168.2.4	107.180.38.104
May 12, 2021 19:05:45.669260025 CEST	80	49730	107.180.38.104	192.168.2.4
May 12, 2021 19:05:45.670296907 CEST	49730	80	192.168.2.4	107.180.38.104
May 12, 2021 19:05:45.703239918 CEST	80	49728	107.180.38.104	192.168.2.4
May 12, 2021 19:05:45.703310966 CEST	49728	80	192.168.2.4	107.180.38.104
May 12, 2021 19:05:45.776909113 CEST	80	49729	107.180.38.104	192.168.2.4
May 12, 2021 19:05:45.782344103 CEST	49729	80	192.168.2.4	107.180.38.104

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 19:05:30.052668095 CEST	64646	53	192.168.2.4	8.8.8.8
May 12, 2021 19:05:30.121035099 CEST	53	64646	8.8.8.8	192.168.2.4
May 12, 2021 19:05:30.233241081 CEST	65298	53	192.168.2.4	8.8.8.8
May 12, 2021 19:05:30.291071892 CEST	53	65298	8.8.8.8	192.168.2.4
May 12, 2021 19:05:31.051233053 CEST	59123	53	192.168.2.4	8.8.8.8
May 12, 2021 19:05:31.102936983 CEST	53	59123	8.8.8.8	192.168.2.4
May 12, 2021 19:05:32.061033010 CEST	54531	53	192.168.2.4	8.8.8.8
May 12, 2021 19:05:32.109885931 CEST	53	54531	8.8.8.8	192.168.2.4
May 12, 2021 19:05:33.538014889 CEST	49714	53	192.168.2.4	8.8.8.8
May 12, 2021 19:05:33.589356899 CEST	53	49714	8.8.8.8	192.168.2.4
May 12, 2021 19:05:33.774245024 CEST	58028	53	192.168.2.4	8.8.8.8
May 12, 2021 19:05:33.834352970 CEST	53	58028	8.8.8.8	192.168.2.4
May 12, 2021 19:05:34.712474108 CEST	53097	53	192.168.2.4	8.8.8.8
May 12, 2021 19:05:34.761321068 CEST	53	53097	8.8.8.8	192.168.2.4
May 12, 2021 19:05:37.369528055 CEST	49257	53	192.168.2.4	8.8.8.8
May 12, 2021 19:05:37.423398018 CEST	53	49257	8.8.8.8	192.168.2.4
May 12, 2021 19:05:37.704683065 CEST	62389	53	192.168.2.4	8.8.8.8
May 12, 2021 19:05:37.765980005 CEST	53	62389	8.8.8.8	192.168.2.4
May 12, 2021 19:05:38.779921055 CEST	49910	53	192.168.2.4	8.8.8.8
May 12, 2021 19:05:38.844640970 CEST	53	49910	8.8.8.8	192.168.2.4
May 12, 2021 19:05:39.831617117 CEST	55854	53	192.168.2.4	8.8.8.8
May 12, 2021 19:05:39.904166937 CEST	53	55854	8.8.8.8	192.168.2.4
May 12, 2021 19:05:41.286748886 CEST	64549	53	192.168.2.4	8.8.8.8
May 12, 2021 19:05:41.338649988 CEST	53	64549	8.8.8.8	192.168.2.4
May 12, 2021 19:05:42.626038074 CEST	63153	53	192.168.2.4	8.8.8.8
May 12, 2021 19:05:42.676764965 CEST	53	63153	8.8.8.8	192.168.2.4
May 12, 2021 19:05:43.421603918 CEST	52991	53	192.168.2.4	8.8.8.8
May 12, 2021 19:05:43.470455885 CEST	53	52991	8.8.8.8	192.168.2.4
May 12, 2021 19:05:44.237828016 CEST	53700	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 19:05:44.286623955 CEST	53	53700	8.8.8.8	192.168.2.4
May 12, 2021 19:05:45.333461046 CEST	51726	53	192.168.2.4	8.8.8.8
May 12, 2021 19:05:45.382297993 CEST	53	51726	8.8.8.8	192.168.2.4
May 12, 2021 19:05:47.367012024 CEST	56794	53	192.168.2.4	8.8.8.8
May 12, 2021 19:05:47.416155100 CEST	53	56794	8.8.8.8	192.168.2.4
May 12, 2021 19:05:48.440351009 CEST	56534	53	192.168.2.4	8.8.8.8
May 12, 2021 19:05:48.492067099 CEST	53	56534	8.8.8.8	192.168.2.4
May 12, 2021 19:05:49.215802908 CEST	56627	53	192.168.2.4	8.8.8.8
May 12, 2021 19:05:49.266083002 CEST	53	56627	8.8.8.8	192.168.2.4
May 12, 2021 19:05:49.992485046 CEST	56621	53	192.168.2.4	8.8.8.8
May 12, 2021 19:05:50.041348934 CEST	53	56621	8.8.8.8	192.168.2.4
May 12, 2021 19:05:51.023152113 CEST	63116	53	192.168.2.4	8.8.8.8
May 12, 2021 19:05:51.076323032 CEST	53	63116	8.8.8.8	192.168.2.4
May 12, 2021 19:05:57.519047022 CEST	64078	53	192.168.2.4	8.8.8.8
May 12, 2021 19:05:57.570036888 CEST	53	64078	8.8.8.8	192.168.2.4
May 12, 2021 19:05:58.524960995 CEST	64801	53	192.168.2.4	8.8.8.8
May 12, 2021 19:05:58.573765039 CEST	53	64801	8.8.8.8	192.168.2.4
May 12, 2021 19:05:59.346257925 CEST	61721	53	192.168.2.4	8.8.8.8
May 12, 2021 19:05:59.395066977 CEST	53	61721	8.8.8.8	192.168.2.4
May 12, 2021 19:06:00.152112007 CEST	51255	53	192.168.2.4	8.8.8.8
May 12, 2021 19:06:00.201400042 CEST	53	51255	8.8.8.8	192.168.2.4
May 12, 2021 19:06:03.282721043 CEST	61522	53	192.168.2.4	8.8.8.8
May 12, 2021 19:06:03.363210917 CEST	53	61522	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 19:05:38.779921055 CEST	192.168.2.4	8.8.8.8	0x2c9b	Standard query (0)	classichomesofpensacola.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 19:05:38.844640970 CEST	8.8.8.8	192.168.2.4	0x2c9b	No error (0)	classichomesofpensacola.com		107.180.38.104	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- classichomesofpensacola.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49728	107.180.38.104	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 19:05:38.999253035 CEST	688	OUT	GET //perfect/index.php HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: classichomesofpensacola.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 19:05:39.325696945 CEST	814	IN	HTTP/1.1 200 OK Date: Wed, 12 May 2021 17:05:39 GMT Server: Apache X-Powered-By: PHP/7.2.34 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache Set-Cookie: PHPSESSID=246684c564be415c52dea90bfde17d98; path=/ Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Vary: Accept-Encoding,User-Agent Content-Encoding: gzip Cache-Control: private, must-revalidate Content-Length: 128 Keep-Alive: timeout=5 Content-Type: text/html; charset=UTF-8 Data Raw: 1f 8b 08 00 00 00 00 00 00 03 53 50 50 50 b0 29 4e 2e ca 2c 28 b1 e3 02 b2 15 ca 33 f3 52 f2 cb f5 72 f2 93 13 4b 32 f3 f3 14 6c 15 94 ec 93 f3 4b f3 4a 8a 2a f5 2a 6c 43 83 d5 40 32 39 a9 40 76 6a 5e 7c 68 b0 9d 5a 72 4e 66 6a 5e 89 6d aa 81 49 52 9a 61 b2 81 a5 a5 b1 85 81 41 92 45 aa 49 92 59 8a 79 a2 99 a1 a9 85 99 89 a1 89 a1 92 35 d8 78 1b 7d 64 cb 00 bc 38 e6 f4 7e 00 00 00 Data Ascii: SPPP)N.,(3RrK2lKJ**lC@29@vj^|hZrNfj^mIRaAElYy5x}d8~
May 12, 2021 19:05:39.487900019 CEST	826	OUT	GET //perfect/index.php?country.x=US&locale.x=en_US>&client=e04bf1c0993800b8e4b6d7a615864141 HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: http://classichomesofpensacola.com//perfect/index.php Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: classichomesofpensacola.com Connection: Keep-Alive Cookie: PHPSESSID=246684c564be415c52dea90bfde17d98
May 12, 2021 19:05:39.664980888 CEST	827	IN	HTTP/1.1 200 OK Date: Wed, 12 May 2021 17:05:39 GMT Server: Apache X-Powered-By: PHP/7.2.34 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache Vary: Accept-Encoding,User-Agent Content-Encoding: gzip Cache-Control: private, must-revalidate Content-Length: 1033 Keep-Alive: timeout=5 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 1f 8b 08 00 00 00 00 00 00 03 95 56 dd 72 ea 36 10 be ef 53 a8 ee c5 49 66 1a 1c 48 d3 29 53 a0 73 4c 82 71 26 49 21 39 01 4c 27 93 91 25 c5 56 90 25 1f 49 36 71 ae fa 34 9d e9 6b f4 51 fa 24 95 6d 20 fc b6 e9 05 20 af be dd ef db d5 6a 0d 00 00 b4 be bd f8 b5 fb c5 1f 5c 82 48 c7 ac f3 4d ab fa 31 1b 11 81 b8 58 98 65 4c 34 04 28 82 52 11 dd b6 52 fd 7c f2 93 b5 d8 d2 54 33 d2 b9 16 21 a0 1c 68 01 72 91 4a 30 80 f9 00 32 f0 19 21 91 72 dd b2 2b 50 e5 c0 28 9f 01 49 58 db 52 3a 67 44 45 84 68 0b 44 92 3c b7 2d a8 0c 81 b2 91 52 76 0c 95 26 b2 66 96 16 88 09 a6 d0 e0 91 24 84 5b a0 8c d6 b6 b8 a8 56 d6 01 65 ef 44 14 89 c2 2d 4f 8c 17 8d 61 48 ec 84 87 5b 9c 34 0e ed 67 98 15 d0 9a f9 b2 80 bd 08 63 58 69 a2 81 92 68 85 7d 59 c9 7b 51 bb ec 2d bb 72 f9 57 ff e0 c7 1f 6a 31 e5 1f 09 50 16 9f c3 d8 88 cf 28 99 27 42 9a 7a 19 99 9a 70 e3 33 a7 58 47 6d 4c 8c 72 72 52 3e 7c 0f 52 45 e4 89 42 90 c1 c0 14 8a 8b b2 22 2d 7b 79 a0 ad 40 e0 7c 11 1c d3 0c 20 66 74 b5 ad 18 52 fe c4 44 48 f9 a2 82 9b db 94 73 22 b7 f6 37 11 66 4f 14 ea 8d 69 3f 80 48 29 24 88 28 c6 a4 88 f1 8e d9 e3 42 b1 c1 1b 49 ec 89 f2 24 d5 6b 94 06 50 9a 4a 48 b9 fa ad 04 3e 5a 20 61 10 91 48 30 4c 64 db ba 2c 8c ab 73 dc 55 b3 d0 51 31 15 ca 6e 0a fc 3a 1a 80 32 06 80 18 4b a2 14 a0 ca f4 d3 d7 94 4a 82 6b 6b 31 b7 d4 1f 48 26 31 a4 73 21 f1 47 f2 59 62 1f 97 5d bb 34 58 4b f1 ef 86 8d 9c 07 2b f3 c7 d3 5e f9 6c a6 be 34 ff af ac df 9f 83 54 6b c1 d7 72 2a 3b e7 71 95 00 44 9a 66 e6 ee 0a 8e 18 45 b3 b2 7b 28 27 47 c7 56 39 4c 3c de b2 ab 10 6b 1c 70 71 65 bf b3 3a 3d 21 43 a1 ab 69 53 9e 3e 30 9d b5 2c ca 2f 2d 1b ee ef 40 95 30 aa cd c5 dd 6d d3 1d bd 92 84 b4 b8 e3 ef 92 29 5f 88 ee dc d3 90 83 87 64 8f c4 35 ae 67 21 4a a6 03 e7 30 97 30 49 b6 f6 37 73 1c 48 9a 41 94 6f 24 b3 8d b9 26 21 64 bb 88 a8 de e9 8a 24 97 34 8c 34 f8 eb 4f 50 6f 36 9b 27 8b 51 d4 c1 02 a5 b1 19 1e b5 b9 a4 9a 1c 71 32 07 17 d0 2c 8e 6b 21 d1 bd 94 31 9f 40 79 74 7c fc f3 6a 10 81 03 ae 0e 54 c4 0c 32 4c 90 c0 e4 e8 d3 83 db 3b 37 1f f5 69 dd b7 06 3e 33 06 4a 25 45 23 99 d1 94 99 46 32 d3 a8 be ad b9 d1 f9 10 8d 35 6c 34 53 74 36 d2 d3 89 17 fa e3 bb 06 9c dc 66 88 cf c2 eb 7b 67 e8 4f d8 d0 1f cf c3 87 fe 1d bb a6 ce 0d 76 87 e9 75 d7 39 85 ee 43 08 dd a6 9a ba a3 dc 73 9b b1 d7 73 22 32 72 a2 a0 8b df bc fe ed 69 70 76 c5 a6 5d a7 e1 8f 5f eb d3 7b 27 f6 c7 b7 49 e0 b2 53 72 3f 0f a7 6e 93 a1 dc 49 83 b3 61 88 e2 d1 2b 1e b3 dc 60 ca 98 fe c4 99 a3 b8 d9 28 38 83 86 1f 62 37 62 de 65 3d 0b e2 d1 a9 3f b9 3a f7 2e 7b 75 63 cb 50 5c c4 72 b2 29 75 be c0 f1 39 37 7e c6 f6 90 7a bd d1 db 74 72 f5 e6 b9 bd 22 66 34 ed 4f 13 d4 18 cd bc fe 5d e6 f5 af 98 3f 1e 56 31 2f 5e 23 cf 8d f2 e9 d8 6f 5e e5 37 7c c0 ef 18 8a eb 85 5f 6a 74 bf 04 8d f3 19 9c dc 25 e6 f7 6d d0 6d 46 03 ea Data Ascii: Vr6SIfH)SsLq&I!9L'%V%I6q4kQ$m j\HM1XeL4(RR\|T3!hrJ02!r+P(IXR:gDEhD<-Rv&f$[VeD-OaH[4gcXih}Y{Q-rWj1P('Bzp3XGmLrrR>|REB"-{y@| ftRDHs"7fOi?H)$(BI$kPJH>Z aH0Ld,sUQ1n:2KJkk1H&1s!GYb]4XK+^l4Tkr*;qDfE{('GV9L<kpqe:=!CiS>0,/-@0m)_d5g!J00l7sHAo$&!d$44OPo6'Qq2,k!1@ytljT2L;7i>3J%E#F25l4St6f{gOvu9Css"2ripv]_{'ISr?nIa+`(8b7be=?:.{ucP\r)u97~ztr"f4O]?V1/^#o^7|_jt%mmF
May 12, 2021 19:05:39.670811892 CEST	828	OUT	GET //perfect/assets/css/master.css HTTP/1.1 Accept: text/css, */* Referer: http://classichomesofpensacola.com//perfect/index.php?country.x=US&locale.x=en_US%3E&client=e04bf1c0993800b8e4b6d7a615864141 Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: classichomesofpensacola.com Connection: Keep-Alive Cookie: PHPSESSID=246684c564be415c52dea90bfde17d98

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 19:05:39.809715986 CEST	832	IN	HTTP/1.1 200 OK Date: Wed, 12 May 2021 17:05:39 GMT Server: Apache Last-Modified: Wed, 22 Mar 2017 13:39:40 GMT Accept-Ranges: bytes Cache-Control: max-age=2592000, public Expires: Fri, 11 Jun 2021 17:05:39 GMT Vary: Accept-Encoding,User-Agent Content-Encoding: gzip Content-Length: 4864 Keep-Alive: timeout=5 Connection: Keep-Alive Content-Type: text/css Data Raw: 1f 8b 08 00 00 00 00 00 03 ed 1d 59 6f db 46 fa 79 f3 2b b8 09 82 c4 a9 49 f3 10 45 49 c1 62 9b 16 36 f6 61 2f 6c 5f 17 08 28 6a 64 b3 a1 48 82 a4 6c a7 41 ff fb ce 49 ce 49 8e 0e e7 e8 a6 69 1c 9b 1a ce 7c f3 dd d7 8c 7f cc 77 75 d5 74 ce be 29 5e bf ba eb ba ba 5d 5d 5d 6d ab b2 6b bd db aa ba 2d 40 5a e7 ad 97 55 bb ab ac 6d ff ba 4d 77 79 f1 f1 2f ff aa 41 f9 c3 2f 69 d9 be ba 78 fb ec c7 93 66 f8 e1 e7 aa dc 80 b2 05 9b 55 e4 fb 68 be 75 b5 f9 e8 7c 7a e6 38 bb b4 b9 cd 4b 67 e5 f8 6f e1 4f 75 ba d9 e4 e5 2d fb 11 2d e0 92 c9 e0 a3 bf 81 e2 1e 74 79 96 fe 13 ec c1 e5 f3 fe 47 07 fd fc fc b2 ff f9 f2 5d 93 a7 c5 65 0b 17 76 5b d0 e4 5b 34 55 75 0f 9a 6d 51 3d b8 8f 70 a6 bb 7c 03 c1 79 fb ec f7 67 79 59 ef bb d5 aa 2e d2 0c dc 55 c5 06 34 18 aa ac 2a aa 06 0e 7c 31 cf 92 28 59 a0 91 2d 28 40 06 87 ba bb d6 05 8f 75 5a 6e f0 48 c7 d9 e4 2d 7c fd e3 ca 29 ab 12 88 23 ab df 6c 87 3e 80 f5 87 bc b3 1d 5d 59 0e 1c 1f 75 f5 c6 f9 47 0a 71 ff f7 0a 51 60 5 b 35 3b e7 cd d5 33 0f 34 4d d5 fc 1b 21 64 80 0b a3 c9 95 b1 c4 e1 29 4b c2 6d 84 f1 24 be 8f 50 a0 bc f6 54 6f b5 26 38 75 af ee e0 d6 df 17 78 eb 68 cc 43 be e9 ee e0 90 d9 dc af 1f df f6 8c e9 76 55 0d 9f 06 91 f8 b4 00 db 0e 3e 4e f7 5d c5 3d 6d f2 db bb e1 b1 b8 86 97 97 25 68 b8 05 07 56 47 73 3b 81 ff d2 89 e9 22 1d 78 ec dc b4 c8 6f 91 5c 64 a0 ec 40 33 3a 9d 07 ff a9 f0 a4 eb 34 fb 70 db 54 fb 72 e3 e6 bb f4 16 c0 f7 b1 c4 7a de 55 be bb bd 42 e3 bc f6 fe 16 49 e0 b0 e5 20 5c 92 75 ef 00 dd 40 14 92 07 dc 74 6d fe 1b 60 63 fb cf cf 83 0d 4c 34 81 08 cb 99 17 be 14 20 9a d1 15 39 05 01 51 46 a1 ac 1a 44 69 08 1c 04 ad ad 8a 7c e3 bc 58 6e d2 28 9d f7 c8 64 d2 0f 07 81 a2 c8 eb 36 6f 87 37 dd 26 dd e4 fb 16 ad 42 26 c4 6a 87 6e d8 f7 96 31 d8 8d 28 23 ad b6 c1 63 1f 7a e0 7d 5f e1 a8 90 02 df b3 a6 4f 06 d5 55 9b 77 79 85 28 df 80 22 ed f2 7b 80 1e ff 06 59 7b 03 90 ee 9a 8d e2 f2 05 80 9f 14 ef 07 94 6a e7 1b e3 25 3c c1 35 92 2b 81 24 81 ef 8b 14 09 16 94 22 c3 02 e9 1a 62 7f df 01 75 b3 11 19 db d3 37 f1 62 71 36 26 5f 03 c7 f1 e2 ca a1 e9 e6 e6 06 53 15 cf eb d2 79 07 ec 44 8a fc 20 e6 e4 38 87 31 2b 62 1e e7 cf c4 aa a5 a5 30 82 8a 7c 3c c6 0c 69 09 e5 8b 6e 7b d3 c0 17 7c 2f 6a 91 0e 7d 48 9b 4d eb 80 b4 05 6e b5 ef 78 cb 23 d8 1d 33 fe 31 e9 06 fc 13 16 5d 71 ac 3d 20 a5 6b 20 d3 61 e4 bb 9b 7d c3 c0 f1 5b 49 74 75 9a a0 ad 9b bc 03 5e 5d 52 5d c0 0d 6f 40 0d 52 84 a2 b2 a2 df eb 55 41 18 2b 4a 82 e3 05 84 44 77 e6 23 6d 41 14 01 91 56 bb 9d af ee 10 d2 46 f7 2f d1 ce 80 0a 2f 6e ad d7 dc 56 19 54 02 4f bf e6 8b 3a 6d db 07 b8 c4 29 52 ca e6 38 b3 a0 06 9f 4d 50 83 2f 24 a8 67 94 54 46 03 ce 8f 65 20 a9 30 0f 3b 0f 47 67 5d ef bb ae 2a c7 29 3a 9b 29 c6 50 b0 83 c4 c1 fb 2a 4c 5f 42 ac 9a d6 a3 91 90 16 c9 16 31 fc 39 bc 0e 6f 24 15 d3 7f 7a 1d 5c 27 d7 3f a1 4f a9 63 0b 1f ae 8b 2a fb 80 e7 d8 37 2d 1e 56 57 39 5b ec 48 71 1d 84 f4 94 09 14 ed 22 ba 2b be 9f f8 eb f4 14 45 96 66 48 Data Ascii: YoFy+IEIb6a/l_(jdHlAIIi|wut)^]]]mk-@ZUmMwy/A/ixfUhu|z8KgoOu--tyG]ev[[4UumQ=p|ygyY.U4*|1(Y-(@uZnH-|)#!>]YuGqQ`[5;34M!d)Km$PTo&8uxhCvU>N]=m%hVGs;"xo\d@3:4pTrzUBl \u@tm`cL4 9QFDi\|Xn(d6o7&B&jn1(#cz}_OUwy("{Y{j%<5+$"bu7bq6&_SyD 81+b0|<in{|/j}HMnx#31]q= k a}[ltu^]R]o@RUA+JDw#mAVF//nVTO:m)R8MP/$gTFe 0;Gg]*):)P*L_B19o$z\'?Oc*7-VW9[Hq"+EfH
May 12, 2021 19:05:40.559333086 CEST	853	OUT	GET //perfect/assets/img/logo.svg HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: http://classichomesofpensacola.com//perfect/index.php?country.x=US&locale.x=en_US%3E&client=e04bf1c0993800b8e4b6d7a615864141 Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: classichomesofpensacola.com Connection: Keep-Alive Cookie: PHPSESSID=246684c564be415c52dea90bfde17d98

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 19:05:40.698867083 CEST	856	IN	HTTP/1.1 200 OK Date: Wed, 12 May 2021 17:05:40 GMT Server: Apache Last-Modified: Thu, 16 Mar 2017 21:33:48 GMT Accept-Ranges: bytes Cache-Control: max-age=2592000 Expires: Fri, 11 Jun 2021 17:05:40 GMT Vary: Accept-Encoding,User-Agent Content-Encoding: gzip Content-Length: 1921 Keep-Alive: timeout=5 Connection: Keep-Alive Content-Type: image/svg+xml Data Raw: 1f 8b 08 00 00 00 00 00 03 d5 97 4b 6f 1b 47 12 c7 cf c9 a7 98 4c 4e 01 66 9a 5d d5 6f c1 72 10 d3 8e 63 40 4e 0c ac 93 c5 9e 16 32 c5 15 89 4c 28 81 a2 25 c7 9f 3e ff aa 1e 4a a3 15 1d f9 90 60 b1 3a 8c aa 87 fd a8 c7 af ab 6a 9e 7c fb e1 b7 a1 b9 5e 6e af d6 17 9b e3 96 8c 6d 9b e5 66 71 71 b6 de 9c 1f b7 3f bf fd be cf ed b7 4f bf 7c f2 55 df 37 2f 97 9b e5 f6 74 77 b1 3d 6a be 3b bb 78 b7 6c 5e 0d c3 fb ab 9d be 6a 28 1a 6b 6c d7 fc e3 97 97 cd 8b 0f 97 17 db 5d f3 66 78 7f de bf da 34 46 5f fe 52 cf 38 6a 30 d1 36 cf de af 87 b3 c6 7e d3 34 7d 2f db 3f ff 69 fe f6 5f 6f 5e 34 57 d7 e7 cd 9b 9f 9f 9d bc 9a 37 6d 3f 9b fd d3 cd 67 b3 e7 6f 9f eb 0e 64 68 36 7b f1 63 db b4 ab dd ee f2 68 36 bb b9 b9 31 37 ce 5c 6c cf 67 2f b7 a7 97 ab f5 e2 6a 86 89 33 99 88 45 33 6c 46 64 ce 76 67 2d 8e 90 9d 27 76 52 db ac cf 8e db 93 d3 df 97 db 7f 63 00 37 6c ae 8e 0f ec cc d6 5a d9 69 9c 72 f4 61 58 6f 7e 3d 34 91 4a 29 33 fd 15 53 8f 5b 7b f9 a1 6d 7e 1f ff df a c cf 76 2b 1c cb c9 a4 58 e4 cd 6a b9 3e 5f ed 8e 5b 47 26 c8 f8 7a bd bc 79 76 21 eb 1a db 8c f3 1a f9 51 e2 71 fa 6e 58 f6 ef 4e 17 bf 9e 6f 2f de 6f a0 f6 66 79 d3 3c 9c 08 05 8f ae 2e 4f 17 cb e3 f6 72 bb bc 5a 6e af 97 62 f9 f9 d3 2f bf d0 c7 f8 fc e2 c9 e5 e9 6e d5 fc 67 3d 0c c7 ed d7 d6 96 f9 f3 17 6d 83 5d 5f 97 6c 5c 89 5d 34 c5 b9 1f 0a 19 97 16 bd 35 3e 95 ce e2 7f c6 3f e3 02 a4 12 3d c4 cc 7e e8 d9 64 4f 1d 65 63 29 c8 64 1b a2 ce 0a 78 32 c9 8a 98 e4 4d 48 a3 dc c8 df ca 99 68 fd 02 13 1d 26 ca 0f cc 58 cc de eb 24 df cb 82 38 e0 0c 9b fa 60 c8 26 cc b5 fa de 27 99 e3 b3 eb 55 83 4e b5 a9 f2 8a 0d b3 5b 78 ec 96 b1 6b 32 5c 32 14 64 57 20 97 12 fb 88 bd b3 2a 20 47 93 ef c9 14 68 8f ad 21 3b e3 63 52 33 63 ef 4d 70 61 4e 96 4d a0 8c c5 21 b8 8e ac 35 c9 8f de e9 a6 ae fa d8 bc 2e c5 b0 4d 1d 39 2c e0 7a 02 b6 72 d9 77 d8 02 b6 31 8e 1b 45 6f 28 b9 2a af a0 80 8d 34 c8 c6 1e 3f 24 9b c5 4e 2f 3e e6 ac 2e 2c 62 72 09 ea c1 5c e5 95 98 1f 16 64 38 c2 a7 d8 09 7a e3 bf 33 36 8b 3b 12 3b 55 60 2e 3a 39 df e1 0a 94 1c 3b 8c 9c 87 86 0c ef e8 e8 4e df 8f ed ec 10 17 ce e6 54 b9 f0 19 ea e4 6a ec aa 4f c6 b2 c6 da 67 7a 00 46 38 04 c6 ad 43 1e a5 03 60 b8 20 60 f8 ac 5c e4 2c 0e 70 be 4c e2 ec c4 5f 08 95 37 39 2a 16 61 82 85 7f 88 45 25 ee 8e 8d 74 80 8d 54 d9 78 80 05 1f c0 22 c0 e3 b6 8c 54 04 a8 ed 46 d7 74 53 3f 7d d4 63 9b d7 be 18 5b ca e8 e9 cf 87 42 99 70 9f 60 82 26 50 94 09 14 f5 72 29 19 79 24 23 8e 64 b8 4a c6 1c ea 10 e2 3f 42 e1 05 91 bc 87 e2 9e aa 8f 42 11 b1 16 5b 60 b6 77 50 1a 81 8b 6e a1 4a d6 74 11 9c 44 81 6d e9 f7 f1 f5 05 5c 58 43 c0 10 e1 51 99 5d d4 f8 d2 2d 22 89 b3 38 20 48 74 5c 60 c8 9e b0 79 49 4e c5 05 e4 44 b0 0a 01 cb 45 dc 97 29 02 c9 80 88 44 60 11 d5 c5 cc 1d 0c 4c 12 43 42 86 71 26 07 5c 04 c3 81 3b 64 13 24 cc d1 4f 56 5c 01 1d b3 f8 aa c8 22 ac f1 d0 2a a9 b8 60 a0 21 09 0a d8 84 24 58 80 ac 89 ac d6 48 18 8a 3b 90 fc b2 22 9d ea d5 ad 32 f0 b6 6e 9f 80 0e 22 Data Ascii: KoGLNf]orc@N2L(%>J`:j|^nmfqq?O|U7/tw=j;xl^j(kl]fx4F_R8j06~4}/?i_o^4W7m?godh6{ch617\lg/j3E3lFdvg-'v Rc7lZiraXo~=4J)3S[{m~v+Xj>_[G&zyv!QqnXNo/ofy<.OrZnb/ng=m]_l\]45>?=~dOec)dx2MHh&X$8`&'UN[xk2\2dW * Gh !;cR3cMpaNM!5.M9,zrw1Eo(*4?$N/>.,br\d8z36;;U`.:9;NTjOgzF8C` `\,pL_79*aE%tTx"TFtS?}c[Bp`&Pr)y$#dJ?BB[`wPnJtDm\XCQ]-"8 Ht\`yINDE)D`LCBq&\;d$OV\"*`!$XH;"2n"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49729	107.180.38.104	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 19:05:39.671591997 CEST	829	OUT	GET //perfect/assets/js/master.js HTTP/1.1 Accept: application/javascript, */*;q=0.8 Referer: http://classichomesofpensacola.com//perfect/index.php?country.x=US&locale.x=en_US%3E&client=e04bf1c0993800b8e4b6d7a615864141 Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: classichomesofpensacola.com Connection: Keep-Alive Cookie: PHPSESSID=246684c564be415c52dea90bfde17d98

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 19:05:39.809739113 CEST	833	IN	HTTP/1.1 200 OK Date: Wed, 12 May 2021 17:05:39 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Last-Modified: Mon, 20 Mar 2017 19:22:14 GMT Accept-Ranges: bytes Cache-Control: max-age=2592000, private Expires: Fri, 11 Jun 2021 17:05:39 GMT Vary: Accept-Encoding,User-Agent Content-Encoding: gzip Content-Length: 736 Keep-Alive: timeout=5 Content-Type: application/javascript Data Raw: 1f 8b 08 00 00 00 00 00 00 03 c5 57 6d 6b db 30 10 fe 9e 5f 71 15 a5 38 6d 70 b3 b1 4f 0d de 60 2c 6c 83 be 8c 36 83 c1 18 43 b3 2f 89 a9 23 79 92 dc 24 b4 fe ef 93 e5 c8 71 1d 3b f1 9a 85 7d 08 c4 a7 e7 4e 77 cf 3d 96 ce f3 90 05 7c ee 72 16 71 1a 80 07 e3 84 f9 2a e4 cc e9 c2 63 07 8a 47 38 76 30 c2 19 32 95 db 01 04 aa 44 30 08 b8 9f 64 66 77 82 6a 98 23 de 2f 3f 07 05 7a a0 c1 a9 fe 3d 50 01 28 04 17 52 6f 92 47 c0 19 0d 23 b8 80 31 8d 24 f6 8c 29 a6 52 ce b9 08 ac 75 e5 dc b4 09 09 59 9c a8 ef 11 9f 84 ec 07 e9 ba 34 08 86 0f 7a f1 32 94 0a 19 0a 87 f8 51 e8 df 93 5e b5 2c 80 70 ec 1c 5b 7f 93 48 e6 ff 40 a3 04 c1 f3 80 10 78 7a 82 02 60 d3 aa 60 6c ac dd d1 d6 48 80 4d a0 1f e9 f8 d7 74 a6 c1 db 56 cf 08 98 a5 61 46 63 4e e6 97 88 fa 48 06 45 ec 9c 61 37 67 d6 03 25 12 b4 8b 69 4d aa 3b eb 82 7a 0e 6a 13 ae 05 b4 cf b9 68 7d 5d da 29 a0 56 c3 36 9a 8f 4c d3 4e 4e b6 35 ed c8 16 d7 b1 91 d3 ee 6e 75 15 1b 6d aa 6b ac 3d 65 83 ba ca ad 78 b1 50 4c 90 2b 0d ab 90 4e 8c af 21 b5 c4 e4 76 65 91 75 23 48 85 dd 96 4c 94 19 7d 11 19 36 40 3d 1f ed d4 98 6b 68 05 ad 96 68 43 34 32 d3 a4 e2 c2 13 f6 66 69 97 5e 78 a2 fe 8b 64 a6 61 10 20 7b 89 5c ea de db 7f ae 9c 9d b4 1c 5c 3c cd 04 fd 8d 6a 76 92 b5 97 82 ee 71 a9 af 6b b6 b7 80 d6 67 e1 21 a4 73 10 95 b4 2a bd b5 48 9a 09 38 80 3c ea f9 48 3b c5 74 65 26 18 5c d5 a3 c4 72 95 56 36 34 ad ae f2 96 92 e9 15 d9 95 ee d3 f6 b4 0f 2c 9d 59 b8 ea cd 6a 71 d5 db 34 df af 71 13 19 87 4c 37 b0 ca 4d 36 6f fe 94 be c0 12 a7 59 bd 0b bd c8 70 0e df ae 2e 3f 29 15 df e2 ef 04 a5 b2 88 85 cb 63 64 0e f9 38 1c 69 21 10 6a e8 93 e7 86 3f 37 9e c6 ef 0c 11 1e 39 5b 17 70 46 4e 6c e6 da fe bc 08 bd 26 93 5f b3 30 3b 7a b2 a9 a3 bb de 47 22 0b 9c d2 33 67 02 69 b0 94 8a 2a f4 a7 94 4d 70 73 5a 2e 14 a7 dd 35 2e 91 d9 21 f4 ba df cf d8 5b b8 c6 ff 2e f3 cf cc 6f ca 2e 2b 27 81 32 d6 e5 e0 08 17 ca d5 83 39 2e 6e c6 0e b9 1d de 7d bd 1c 5d 7c b8 b9 1e 0e 34 e1 6f 3d e8 3f f7 05 90 a8 46 e1 0c f5 19 ea d4 a6 b4 77 8b 60 43 fd 46 c8 3d 78 d5 ef f7 bb cf ad f3 fc 93 22 e2 3e 35 e2 f6 aa 96 32 3c ed 54 ff 95 de 11 d0 78 7f ea a0 2d c5 d7 e4 f0 08 75 a0 89 63 7b 75 7e 0a f9 b9 ab 7b 12 44 21 9b c0 e9 b9 f9 6c 48 3b 7f 00 99 6d d5 98 dc 0c 00 00 Data Ascii: Wmk0_q8mpO`,l6C/#y$q;}Nw=\|rq*cG8v02D0dfwj#/?z=P(RoG#1$)RuY4z2Q^,p[H@xz``lHMtVaFcNHEa7g%iM;zjh}])V6LNN5numk=exPL+N!veu#HL}6@=khhC42fi^xda {\\<jvqkg!s*H8<H;te&\rV64,Yjq4qL7M6oYp.?)cd8i!j?79[pFNl&_0;zG"3gi*MpsZ.5.![.o.+'29.n}]|4o=?Fw`CF=x">52<Tx-uc{u~{D!lH;m
May 12, 2021 19:05:40.561331034 CEST	853	OUT	GET //perfect/assets/img/notif.png HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: http://classichomesofpensacola.com//perfect/index.php?country.x=US&locale.x=en_US%3E&client=e04bf1c0993800b8e4b6d7a615864141 Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: classichomesofpensacola.com Connection: Keep-Alive Cookie: PHPSESSID=246684c564be415c52dea90bfde17d98

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 19:05:40.784804106 CEST	859	IN	HTTP/1.1 200 OK Date: Wed, 12 May 2021 17:05:40 GMT Server: Apache Last-Modified: Fri, 17 Mar 2017 19:52:54 GMT Accept-Ranges: bytes Content-Length: 4675 Cache-Control: max-age=31536000, public Expires: Thu, 12 May 2022 17:05:40 GMT Keep-Alive: timeout=5 Connection: Keep-Alive Content-Type: image/png Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 28 00 00 07 d0 08 06 00 00 00 b0 98 1d 97 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 20 49 6d 61 67 65 52 65 61 64 79 71 c9 65 3c 00 00 03 68 69 54 58 74 58 4d 4c 3a 63 6f 6d 2e 61 64 6f 62 65 2e 78 6d 70 00 00 00 00 00 00 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b 63 39 64 22 3f 3e 20 3c 78 3a 78 6d 70 6d 65 74 61 20 78 6d 6c 6e 73 3a 78 3d 22 61 64 6f 62 65 3a 6e 73 3a 6d 65 74 61 2f 22 20 78 3a 78 6d 70 74 6b 3d 22 41 64 6f 62 65 20 58 4d 50 20 43 6f 72 65 20 35 2e 33 2d 63 30 31 31 20 36 36 2e 31 34 35 36 36 31 2c 20 32 30 31 32 2f 30 32 2f 30 36 2d 31 34 3a 35 36 3a 32 37 20 20 20 20 20 20 20 20 22 3e 20 3c 72 64 66 3a 52 44 46 20 78 6d 6c 6e 73 3a 72 64 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 30 32 2f 32 32 2d 72 64 66 2d 73 79 6e 74 61 78 2d 6e 73 23 22 3e 20 3c 72 64 66 3a 44 65 73 63 72 69 70 74 69 6f 6e 20 72 64 66 3a 61 62 6f 75 74 3d 22 22 20 78 6d 6c 6e 73 3a 78 6d 70 4d 4d 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 6d 6d 2f 22 20 78 6d 6c 6e 73 3a 73 74 52 65 66 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 73 54 79 70 65 2f 52 65 73 6f 75 72 63 65 52 65 66 23 22 20 78 6d 6c 6e 73 3a 78 6d 70 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 22 20 78 6d 70 4d 4d 3a 4f 72 69 67 69 6e 61 6c 44 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 45 43 30 39 45 31 45 33 41 42 32 30 36 38 31 31 38 33 44 31 46 41 34 30 34 39 38 37 43 43 30 35 22 20 78 6d 70 4d 4d 3a 44 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 32 45 31 35 39 44 36 35 31 35 38 36 31 31 45 34 38 38 46 45 43 35 38 46 43 46 44 41 42 45 34 36 22 20 78 6d 70 4d 4d 3a 49 6e 73 74 61 6e 63 65 49 44 3d 22 78 6d 70 2e 69 69 64 3a 32 45 31 35 39 44 36 34 31 35 38 36 31 31 45 34 38 38 46 45 43 35 38 46 43 46 44 41 42 45 34 36 22 20 73 74 52 65 66 3a 64 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 45 43 30 39 45 31 45 33 41 42 32 30 36 38 31 31 38 33 44 31 46 41 34 30 34 39 38 37 43 43 30 35 22 2f 3e 20 3c 2f 72 64 66 3a 44 65 73 63 72 69 70 74 69 6f 6e 3e 20 3c 2f 72 64 66 3a 52 44 46 3e 20 3c 2f 78 3a 78 6d 70 6d 65 74 61 3e 20 3c 3f 78 70 61 63 6b 65 74 20 65 6e 64 3d 22 72 22 3f 3e c9 59 c1 1f 00 00 0e 71 49 44 41 54 78 da ec d9 bf 6e 1b c9 19 00 70 6a a1 22 9d 74 f5 1d 20 f9 05 22 a6 4b 27 fa 09 cc 2b 03 04 30 9d 34 e9 a4 7b 82 a3 9e 20 74 97 22 39 d1 40 80 94 a6 9f c0 54 95 94 e4 0b c4 32 70 7d Data Ascii: PNGIHDR(tEXtSoftwareAdobe ImageReadyqe<hiTXtXML:com.adobe.xmp<?xpacket begin="" id="W5M0 MpCehiHzreSzNTczkc9d"?> <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/Resourc eRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="xmp.did:EC09E1E3AB20681183 D1FA404987CC05" xmpMM:DocumentID="xmp.did:2E159D65158611E488FEC58FCFDABE46" xmpMM:Instance ID="xmp.iid:2E159D64158611E488FEC58FCFDABE46" xmp:CreatorTool="Adobe Photoshop CS6 (Macintosh)"> <xm pMM:DerivedFrom stRef:instanceID="xmp.iid:45AC8677B020681183D1FA404987CC05" stRef:documentID="xmp.di d:EC09E1E3AB20681183D1FA404987CC05"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?> YqIDATxnpj"t "K'+04{ t"9@T2p}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49730	107.180.38.104	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

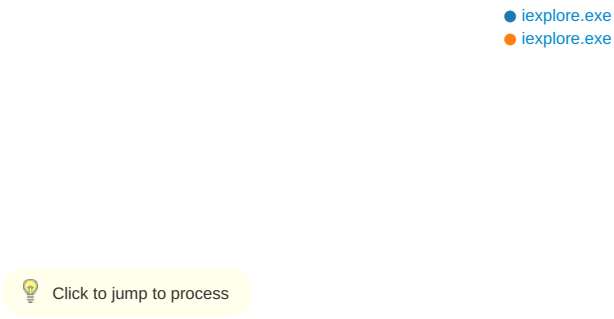
Timestamp	kBytes transferred	Direction	Data
May 12, 2021 19:05:39.806071043 CEST	831	OUT	GET //perfect/assets/js/b64.min.js HTTP/1.1 Accept: application/javascript, */*;q=0.8 Referer: http://classichomesofpensacola.com//perfect/index.php?country.x=US&locale.x=en_US%3E&client=e04bf1c09 93800b8e4b6d7a615864141 Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: classichomesofpensacola.com Connection: Keep-Alive Cookie: PHPSESSID=246684c564be415c52dea90bfde17d98

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 19:05:39.983629942 CEST	839	IN	HTTP/1.1 200 OK Date: Wed, 12 May 2021 17:05:39 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Last-Modified: Wed, 22 Mar 2017 13:50:42 GMT Accept-Ranges: bytes Cache-Control: max-age=2592000, private Expires: Fri, 11 Jun 2021 17:05:39 GMT Vary: Accept-Encoding,User-Agent Content-Encoding: gzip Content-Length: 614 Keep-Alive: timeout=5 Content-Type: application/javascript Data Raw: 1f 8b 08 00 00 00 00 00 00 03 9d 94 5b 73 da 30 10 85 df fb 2b 28 0f 8c 34 98 8b 65 87 40 8c 3c 43 d2 fb 85 b4 4d af e9 b4 8c 6a 64 50 43 e4 54 96 c9 c5 f6 7f ef da 0e 0c 50 43 98 be 99 f5 fa ac f6 7c 47 cc 99 aa 1c b3 90 77 6c 1a 8f 2e f8 ed 99 56 47 d5 c1 f1 c9 93 a7 cf 9e bf 78 f9 ea f5 9b b7 c3 d3 77 ef 3f 9c 7d fc f4 f9 cb d7 6f e7 ec 97 37 e6 fe 64 2a 7e 5f cc 2e 65 70 f5 47 85 3a 9a 5f df dc de b5 4d 62 d9 07 9d c3 6e af de a2 55 83 4b 2f 18 f3 23 3f 92 9e 16 81 44 1c c7 73 18 a5 69 b5 ea 64 0f d2 50 86 30 42 23 30 22 83 e5 15 9f b6 1d 4e 8b b3 34 47 91 f6 bb a3 42 04 be 75 ae a7 62 c6 91 df e7 cd 19 97 13 3d c5 b1 a4 bc e9 4d 99 3a 81 8e 81 46 7e bd 8e 1d 55 52 13 25 b5 90 4a d7 25 4e 40 91 ac 59 b8 df b7 13 e5 ba b6 13 51 a4 6a e6 01 14 48 22 5c b7 e3 30 2a 6a 1d cb 11 3e 12 e1 90 0d 91 c2 38 8e 28 a3 1d 3b e5 b3 90 57 96 2f 04 bc c8 cb 9a ea ba 9e 8a b0 79 ef 65 3e 1a c6 86 b8 b4 1c 94 97 a3 f2 32 c3 a9 e2 3a 52 b2 a2 53 63 cc f7 30 38 7f fa d7 64 de 54 fc 6a c6 3c 8e 5a df 7f 0e 1a e7 ac 71 d7 6e 64 dc 7e b4 26 46 b5 5a 66 77 48 d7 4e 24 e4 98 df 9c fa 88 2f ce 96 f9 8a c1 d1 7d ba a2 bd ba d8 5e 5d 92 86 19 ae 20 e3 a7 28 0a 0a 7e 76 12 65 80 05 45 51 0e b8 93 30 27 43 03 42 42 4e 9a be 0a 2e 4f ee 33 81 24 ce 00 47 8f 01 1f 8e b7 35 29 9c 42 13 db dd 24 70 0a 01 58 4b 70 41 09 69 c8 e6 92 dc 6a b6 d7 f8 ad 81 51 32 63 21 01 c6 12 ab 1f 28 94 a3 05 88 72 c9 c6 91 60 44 ce 7e 23 fe c5 62 aa 6f 92 2e 9c b9 4e b7 ec b5 48 b2 72 4d 72 58 ab a9 3e 69 db 3b 3e 80 7b 91 98 3d 82 9d 6d 0d 70 63 92 6c 64 2e bc 43 c6 24 09 21 f6 76 1d 18 b4 90 7a 78 56 ba 69 ef 83 d7 03 3c 2c 3c f3 4c ea 11 f8 55 64 5e ae 64 fe bf fc cc 70 ac 7a da 33 73 4f 61 d3 18 c6 ac 0b d6 cd ad ab c1 6e 96 99 27 d7 23 b0 65 26 4b 49 61 69 a9 8c 67 6d 16 b7 23 5a fc cb 01 01 54 a8 e7 73 ac c5 1c 6b c5 ce f4 d1 5f 84 0c 25 9b 22 06 00 00 Data Ascii: [s0+(4e@<CMjdPCTPC|Gwl.VGxw?}o7d*~_.epG:_MbnUK/#?DsidP0B#0"N4GBub=M:F~UR%J%N@Y QjH"\0*j>8(;W/ye>2:RSc08dTj<Zqnd~&FZfwHN$/}^] (~veEQ0'CBBN.O3$G5)B$pXKpAijQ2c!(r`D~#bo.NHrMrX>i;>{=m pcld.C$!vzxVi<,<LUd^dpz3sOan'#e&KIaigm#ZTsk_%"
May 12, 2021 19:05:40.525440931 CEST	852	OUT	GET //perfect/assets/img/favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: classichomesofpensacola.com Connection: Keep-Alive Cookie: PHPSESSID=246684c564be415c52dea90bfde17d98
May 12, 2021 19:05:40.673305988 CEST	854	IN	HTTP/1.1 200 OK Date: Wed, 12 May 2021 17:05:40 GMT Server: Apache Last-Modified: Fri, 17 Mar 2017 18:30:52 GMT Accept-Ranges: bytes Cache-Control: max-age=31536000, public Expires: Thu, 12 May 2022 17:05:40 GMT Vary: Accept-Encoding,User-Agent Content-Encoding: gzip Content-Length: 1405 Keep-Alive: timeout=5 Connection: Keep-Alive Content-Type: image/x-icon Data Raw: 1f 8b 08 00 00 00 00 00 00 03 ed 98 7b 50 54 55 18 c0 cf bd 6c c2 f0 47 32 8d 4d 56 c6 92 91 0f f0 b1 62 d1 e4 28 3a 66 8e e3 1f 54 36 4d 46 5a 23 82 90 1a 33 36 1a 1a ef 87 0b 0b ac 23 69 40 2e 0f dd 35 40 12 91 09 89 50 7c f0 4a 10 c1 4a 12 53 96 c5 e5 b9 06 fa 87 bc 56 ce 9e be b3 77 af fb e0 b9 2b 39 d3 e4 ce fc 66 9f df fe be 7b ce f9 ce e3 22 c4 20 16 b9 b8 20 78 76 41 b9 4e 08 cd 41 08 39 39 71 ef 03 05 08 d5 c3 eb 79 f0 19 fc 04 ad 42 dc e7 fa 87 13 1a f1 20 84 3c e5 3f 02 1e 1e 9a a5 7b d8 27 c2 06 f4 af 31 76 7c 52 fe ea 0c af 4b 1d c7 10 51 a6 73 74 29 10 a9 54 6c cc 79 52 fe 4b 8a 4d 8a 6e 70 2a 65 1c ea 2c 44 7e 4f 77 56 0d 0d 0d 4e 9b 6a 57 5b ab ca b5 b6 aa 7c 79 dd af 95 cb 28 57 80 12 99 9f ac fb 07 e3 f5 ab 32 10 69 c9 72 18 68 6f 53 39 4f b5 ff d4 ae f7 1b c4 f3 11 49 10 71 ec 77 43 e4 f8 47 2c 56 cb 8d 7e 4a f7 71 68 83 ba 8b 5e 53 ed 3f 1d be f5 97 58 f0 c7 2d e6 88 71 47 24 6d 2d 8b 5b 32 28 46 7f 4f 36 8c 81 92 23 7e 53 ed 2f 4e 15 1f 10 c3 35 8b 17 73 c4 2e 44 44 fa 36 8b 9b be 63 b1 2a d3 e8 d7 40 7f 94 9f d8 79 68 aa fd 15 3f e5 f9 99 fa c5 8b 00 11 8b eb 13 04 da d6 a3 e6 63 e0 56 96 53 6f 55 fe ee c4 aa c2 e8 d0 0b 85 07 83 1a 2e 17 af bb ab e9 7a fe 71 fc d7 af d6 7a ed 37 b4 3f 9f 43 34 e4 53 1e 22 d0 5a 8e 01 9a 83 06 c6 c1 5d 68 8b bf b3 b9 67 a5 7c 86 a6 f2 44 60 aa a6 bb 63 a6 2d fe ee ae ce 59 d1 0b 1d 06 e2 45 46 7f d4 3c 44 8a 77 08 b4 6d 0a 73 ff 68 b4 42 1f f5 e4 20 72 53 31 bb 59 a5 6c 9a 63 ad 5f 3b 34 34 4d bc 6a 76 b3 c4 c4 1f 3d 9f d6 80 40 db 05 ff db 01 d7 db 6e 02 cd a9 35 0b ea 31 c3 3c 8f 2e f8 ee 0f b9 a8 61 60 a0 df de da 1c a4 3e 6b ce 26 9a f8 29 31 40 da 06 3b 2c df 6c 87 8f 7d 6a 87 15 9f 3d a3 fd 71 1b 8b 4b 83 59 7c 4d 0a f5 09 f3 a3 65 ff d0 1a a9 fa 39 cd df 5a ff 91 7d 3b 0f 49 3d 8c 6e 7d 1d 42 1d f8 bf c4 90 2d 33 19 e2 6b 82 1f 7c f6 a5 2b 43 12 d7 d8 e1 8a 28 16 b7 2b 8c 6d d1 06 e3 b5 26 73 79 b9 b5 fe 82 8c 94 80 03 1e e6 d7 4f 09 7a 8d 21 81 2e 0c f9 c2 82 00 67 c8 e5 45 86 6c 7b 85 21 b9 7e 2c 6e 93 73 39 b4 40 0e b7 d2 9f bd 8f 87 b5 56 d5 44 f5 f9 73 ab a5 16 7e 3a 1e bf 7a 1d fc c2 91 7e b3 3c a0 4d 0a 76 70 ed 40 db 80 e6 40 d7 4b 6b fc ad 2d 4a a1 e4 8d 69 83 71 22 73 7f f0 5c 70 8c e3 a7 d0 36 08 82 3c 7f 3b c0 8d 4b 95 de ff c0 c3 1a ff 40 7f bf 7d d2 5a 17 a5 c4 c2 1f 0a f3 c0 44 7e ca 96 17 18 22 df cc e2 4e a8 81 db 99 4e bd 78 f8 e1 73 d6 8e 81 e4 4d ab 2e 98 d6 00 6d 8b c8 05 68 42 37 c5 ff 65 86 84 79 32 e4 5e 2e 8c ff 82 f0 28 5b e6 a1 f4 6f 02 53 2d 6b 20 16 e6 e2 ed af 72 7d 30 2e 30 0e f6 cc 67 c8 f9 ec bd 71 18 0f 33 b6 f8 4f c9 0e 06 59 d6 00 cd 81 f6 41 f0 dc b1 d9 07 73 65 38 ac 99 f1 f0 db a6 c6 eb 6e b6 b8 f5 35 50 56 b2 d6 b2 06 f8 7e 88 9f 04 49 4b 10 69 a8 bd fc a6 ad 7e e5 ed bf 5c 25 4b 05 da b8 c5 23 73 98 08 3a 6e 13 57 cc d0 dc bb d7 3b dd 56 7f 5f df 03 c7 a4 77 66 a9 25 22 eb dc 34 df 6f 97 22 92 9f 92 b0 db 56 37 8f c4 db b3 26 0e d6 Data Ascii: {PTUlG2MVb(:fT6MFZ#36#i@.5@P|JJSVw+9f{" xvANA99qyB <?{'1v|RKQst)TlyRKMnp*e,D~OwVNjW[|y(W2irhoS9OIqwCG,V~Jqh^S?X-qG$m-[2(FO6#~S/N5s.DD6c*@yh?cVSoU.zqz7?C4S"Z]hg|D`c-YEF<DwmshB rS 1Ylc_;44Mjv=@n51<.a`>k&)1@;,l}j=qKY|Me9Z};I=n}B-3k|+C(+m&syOz!.gEl{!~,ns9@VDs~:z~<Mvp@@Kk-Jiq"s\p6<; K@}ZD~"NNxsM.mhB7ey2^.([oS-k r}0.0gq3OYAse8n5PV~IKi~\%K#s:nW;V_wf%"4o"V7&

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 6396 Parent PID: 800

General

Start time:	19:05:36
Start date:	12/05/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff61b340000
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	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: 6464 Parent PID: 6396

General

Start time:	19:05:37
Start date:	12/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6396 CREDAT:17410 /prefetch:2
Imagebase:	0xb10000
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

Disassembly