ID: 321242
Cookbook: browseurl.jbs
Time: 17:05:41
Date: 20/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

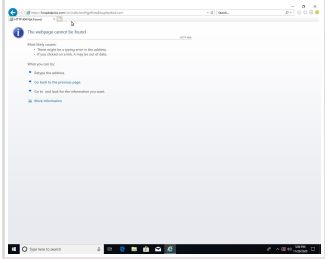
Analysis Report https://bakrisoil.com/wp-content/cd.ph…

Overview

General Information

Sample URL:	http://https://bakrisoil.com/wp-content/cd.php?e=gjeffries@hughesellard.com
Analysis ID:	321242

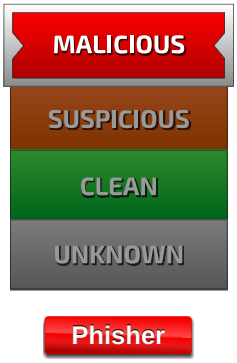
Most interesting Screenshot:



Errors

URL not reachable

Detection

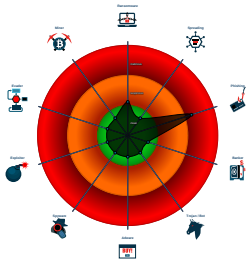


Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for doma…
- Yara detected Phisher
- URL contains potential PII (phishing…

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 6864 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6912 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6864 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

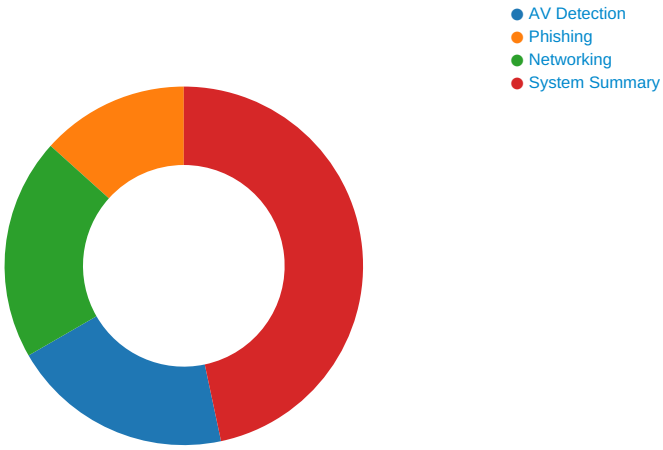
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\cd[1].htm	JoeSecurity_Phisher_1	Yara detected Phisher	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

Multi AV Scanner detection for domain / URL

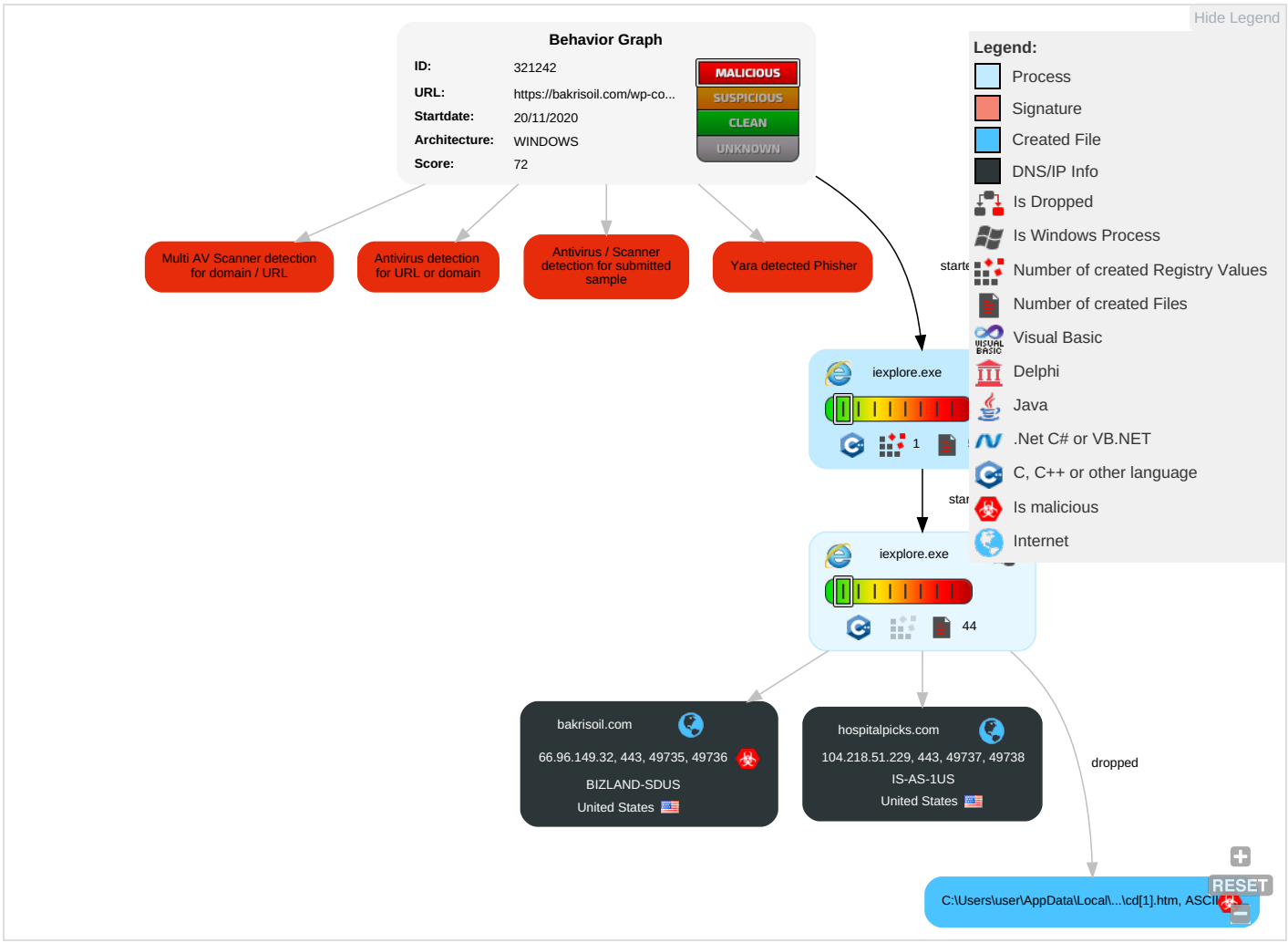
Phishing:

Yara detected Phisher

Mitre Att&ck Matrix

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

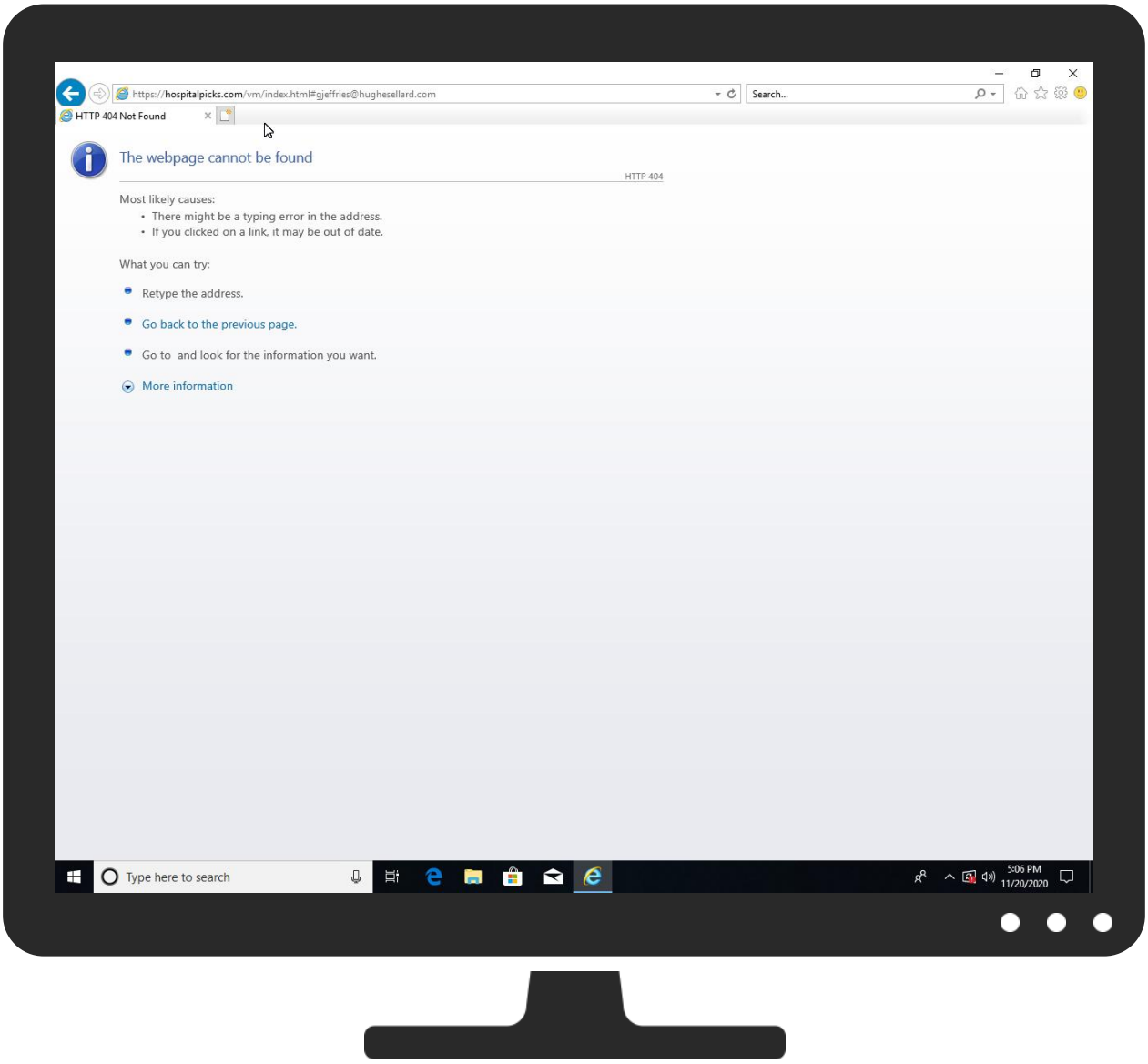
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://bakrisoil.com/wp-content/cd.php?e=gjeffries@hughesellard.com	100%	Avira URL Cloud	phishing	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
bakrisoil.com	6%	Virustotal		Browse
hospitalpicks.com	3%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://bakrisoil.com/	6%	Virustotal		Browse
http://https://bakrisoil.com/	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://hospitalpicks.com/vm/index.html#gjeffries	100%	Avira URL Cloud	phishing	
http://https://bakrisoilcom/vm/index.html#gjeffries	0%	Avira URL Cloud	safe	
http://https://bakrisoilwp-content/cd.php?e=gjeffries	0%	Avira URL Cloud	safe	
http://https://bakrisoil.com/wp-content/cd.php?e=gjeffries	100%	Avira URL Cloud	phishing	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
bakrisoil.com	66.96.149.32	true	true	• 6%, Virustotal, Browse	unknown
hospitalpicks.com	104.218.51.229	true	false	• 3%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://bakrisoil.com/	{5702468C-2B4A-11EB-90EB-ECF4BBEA1588}.dat.1.dr	true	• 6%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://hospitalpicks.com/vm/index.html#gjeffries	cd[1].htm.2.dr, ~DF240D9F52873C5C2B.TMP.1.dr	true	• Avira URL Cloud: phishing	unknown
http://https://bakrisoilcom/vm/index.html#gjeffries	{5702468C-2B4A-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	low
http://https://bakrisoilwp-content/cd.php?e=gjeffries	{5702468C-2B4A-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false	• Avira URL Cloud: safe	low
http://https://bakrisoil.com/wp-content/cd.php?e=gjeffries	{5702468C-2B4A-11EB-90EB-ECF4BBEA1588}.dat.1.dr	true	• Avira URL Cloud: phishing	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
66.96.149.32	unknown	United States		29873	BIZLAND-SDUS	true
104.218.51.229	unknown	United States		19318	IS-AS-1US	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321242
Start date:	20.11.2020
Start time:	17:05:41
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://bakrisoil.com/wp-content/cd.php?e=gjeffries@hughesellard.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:	7
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:	mal72.phis.win@3/15@2/2
Cookbook Comments:	• Adjust boot time • Enable AMSI • **URL browsing timeout or error**
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 13.88.21.125, 52.147.198.201, 104.108.39.131, 168.61.161.212, 51.104.146.109, 92.122.213.247, 92.122.213.194 • Excluded domains from analysis (whitelisted): skypedataprdcoleus16.cloudapp.net, e11290.dspg.akamaiedge.net, umwatsonrouting.trafficmanager.net, go.microsoft.com, arc.msn.com.nsatc.net, go.microsoft.com.edgekey.net, skypedataprdcolcus17.cloudapp.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, a1449.dscg2.akamai.net, skypedataprdcolwus15.cloudapp.net, arc.msn.com
Errors:	• URL not reachable

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.{5702468A-2B4A-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8460232784674468
Encrypted:	false
SSDEEP:	192:rAZEZi2F9W3tqifOeMzMKkBtqDMsfeehjX:rw0BFUdzj36br
MD5:	A71188D61C2EEE9632C89C3C6E25BA97
SHA1:	59516B5FCE4AB54F8BEED061BDCFF8459EE11B92
SHA-256:	ABBB53CE87CA2241970B9023539049088B7634A6A5B05D46629307CC01D621A6
SHA-512:	6A396AA4DA42E3C3941B75E163EEBF4D136C048D34FA8951C530F6DF510A17BC60AE02DCE2CC8A11D3BECB7B8F0FA0A8AEBB073133898A79A84B7FC19BAD69C1
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\{5702468C-2B4A-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	34768
Entropy (8bit):	1.946453565593392
Encrypted:	false
SSDEEP:	192:raZIQY6GkmFjp2wkWvMmYDwo2R9eoWQMeg:rGxjHmh40kmGF2XrQZ
MD5:	F2E25C2B780C70D3AA9F4CA60AAD7663
SHA1:	93D2B0C82160E4A1F17C76C7827CD061BAFA77BD
SHA-256:	B76C2B4E499FFCF7FE2B1B8CBA48F902B5B34139E200E838890747868774CB38
SHA-512:	71AAEAEA297CEE0FAF994AB1A97D6154A3C5F30B37A8F73CF7350891B825430B69CB50F18C615516BB17B7D0163B2E91535E3E1BFA1990E610BACFE2F8A4F734
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\{5702468D-2B4A-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{5702468D-2B4A-11EB-90EB-ECF4BBEA1588}.dat	
Size (bytes):	16984
Entropy (8bit):	1.5638657029524614
Encrypted:	false
SSDEEP:	48:IwfGcpr1GwpacG4pQsGrapbSPrGQpKzG7HpR8/sTGIpG:r1ZfQ86qBSPFACT8/4A
MD5:	6D90230DC0CAF4C3352995DD82E6F9F7
SHA1:	4CE5B9DDC95D6D9563CE6A7446110F7E07D2FDAD
SHA-256:	AF3ADE2223F5B41C72F6F80854F6B698D541A24589EFA57D54BB91785C014E99
SHA-512:	E2A10690FEF555518435862F9CA6CAC366F9E206FD042F86A4834066C1CD3140F6BAF72DC06E054C5362456A32DB46F913B5DDE31A288780FD624B690D3CE026
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\cd[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	113
Entropy (8bit):	4.789317079178466
Encrypted:	false
SSDEEP:	3:nmNjJMzVJu+1zWNVYeWmiootTKADRCOLMMCNrL3n:GMRJVCNOeWmDoQADRCrMCJL3
MD5:	4AB0B10478383BD321BBBB9877ACACC9
SHA1:	55A0A2D167106E8F087580B052983887E301D86B
SHA-256:	11D88AC4B8E6CEF17BB533273B80F25EE1D5C5DFFA6F9F236AD64BB9A870C37F
SHA-512:	9E57115552FA569BF345E91363EC55939FC3231D406DEE938B752DA2C19260A220A9532105A420DAD845C80B9827E0C0AEB415EF0152F5C6EBD30904348BBEB0
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Phisher_1, Description: Yara detected Phisher, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\cd[1].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://bakrisoil.com/wp-content/cd.php?e=gjeffries@hughesellard.com
Preview:	<meta http-equiv="refresh" content="0; url=https://hospitalpicks.com/vm/index.html#gjeffries@hughesellard.com" />

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\bullet[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	447
Entropy (8bit):	7.304718288205936
Encrypted:	false
SSDEEP:	12:6v/71Cyt/JNTWxGdr+kZDWO7+4dKlv0b1GKuxu+R:/yBJNTqsSk9BTwE05su+R
MD5:	26F971D87CA00E23BD2D064524AEF838
SHA1:	7440BEFF2F4F8FABC9315608A13BF26CABAD27D9
SHA-256:	1D8E5FD3C1FD384C0A7507E7283C7FE8F65015E521B84569132A7EABEDC9D41D
SHA-512:	C62EB51BE301BB96C80539D66A73CD17CA2021D5D816233853A37DB72E04050271E581CC99652F3D8469B390003CA6C62DAD2A9D57164C620B7777AE99AA1B1
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/bullet.png
Preview:	.PNG.....IHDR.....ex....PLTE...(EkFRp&@e&@e)Af)AgANjBNjDNjDNj2Vv-Xz-Y{3XyC\}E_.2j.3l.8p.7q.;j.;l.Zj.\l.5o.7q.<..aw.<..dz.E.....1..@.7..~.....9..:.....A ..B..E..9..:..a..c..b..g.#M.%O.#r.#s.%y.2..4..+..-..?..@..;..p..s...G..H..M.....z`....#tRNS...../,....mIDATx^..C..`.....S....y'...05...|..k.X.....*`.F.K....JQ..u.<.}.. .. [U..m....'r%.....yn.`.7F..).5..b..rX.T.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\http_404[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	6495
Entropy (8bit):	3.8998802417135856
Encrypted:	false
SSDEEP:	48:up4d0yV4VkBXvLutC5N9J/1a5TI7kZ3GUXn3GFa7K083GJehBu01kptk7KwyBwpM:uKp6yN9JaKktZX36a7x05hwW7RM
MD5:	F65C729DC2D457B7A1093813F1253192
SHA1:	5006C9B50108CF582BE308411B157574E5A893FC
SHA-256:	B82BFB6FA37FD5D56AC7C00536F150C0F244C81F1FC2D4FEFBBDC5E175C71B4F
SHA-512:	717AFF18F105F342103D36270D642CC17BD9921FF0DBC87E3E3C2D897F490F4ECFAB29CF998D6D99C4951C3EABB356FE759C3483A33704CE9FCC1F546EBCBB 7
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/http_404.htm
Preview:	.<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">....<html dir="ltr">.... <head>.. <link rel="st ylesheet" type="text/css" href="ErrorPageTemplate.css">.... <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.... <title>HTTP 404 Not Foun d</title>.... <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="ja vascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="javascript:initHomepage(); expandCollapse('infoBlockID', true); initGoBack(); initM oreInfo('infoBlockID');">.... <table width="730" cellpadding="0" cellspacing="0" border="0">.... Error title -->.. <tr>.. <td id="infoIconAlign" wi dth="60" align="left" valign="top" rowspan="2">.. <img src="info_48.png" id="infoIcon" alt="Info icon">..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\down[1]	
Reputation:	low
IE Cache URL:	res://ieframe.dll/down.png
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W..W..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\CS6IXJW6\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\OR0WKIO1\ErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2168
Entropy (8bit):	5.207912016937144
Encrypted:	false
SSDEEP:	24:5+j5xU5k5N0ndgvoyeP0yyiyQCDr3nowMVworDtX3orKxWxDnCMA0da+hieyuSQK:5Q5K5k5pvFehWrrarrZIrHd3FIQfOS6
MD5:	F4FE1CB77E758E1BA56B8A8EC20417C5
SHA1:	F4EDA06901EDB98633A686B11D02F4925F827BF0
SHA-256:	8D018639281B33DA8EB3CE0B21D11E1D414E59024C3689F92BE8904EB5779B5F
SHA-512:	62514AB345B6648C5442200A8E9530DFB88A0355E262069E0A694289C39A4A1C06C6143E5961074BFAC219949102A416C09733F24E8468984B96843DC222B436
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/ErrorPageTemplate.css
Preview:	.body..{...font-family: "Segoe UI", "verdana", "arial";...background-image: url(background_gradient.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...ma rgin-top: 20px;...margin-left: 20px;...color: #575757;..}....body.securityError..{...font-family: "Segoe UI", "verdana" , "Arial";...background-image: url(background_grad ient_red.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;..}....body.tabInfo..{...background-image: none;...back ground-color: #F4F4F4;..}.. ..a..{...color: rgb(19,112,171);.font-size: 1em;...font-weight: normal;...text-decoration: none;...margin-left: 0px;...vertical-align: top;..}....a:link, a:visited..{...color: rgb(19,112,171);...text-decoration: none;...vertical-align: top;..}....a:hover..{...color: rgb(7,74,229);...text-decoration: underline;..}....p..{...font-size: 0.9em;..}.....h1 /* used for Title */..{...color: #4465A2;...font-size: 1.1em;...font-weight: normal;...vertical-align

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\info_48[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 47 x 48, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	4113
Entropy (8bit):	7.9370830126943375
Encrypted:	false
SSDEEP:	96:WNTJL8szf79M8FUjE39KJoUUuJPnvmKacs6Uq7qDMj1XPL:WNrzFoQSJPnvzs6rL
MD5:	5565250FCC163AA3A79F0B746416CE69
SHA1:	B97CC66471FCDEE07D0EE36C7FB03F342C231F8F
SHA-256:	51129C6C98A82EA491F89857C31146ECEC14C4AF184517450A7A20C699C84859
SHA-512:	E60EA153B0FECE4D311769391D3B763B14B9A140105A36A13DAD23C2906735EAAB9092236DEB8C68EF078E8864D6E288BEF7EF1731C1E9F1AD9B0170B95AC13 4
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\info_48[1]	
Reputation:	low
IE Cache URL:	res://ieframe.dll/info_48.png
Preview:	.PNG.....IHDR.../...0.....#.....IDATx^...pUU..{....KB.....!....F.....jp.Q.....Vg.F..m.Q....{...,m.@.56D...&$d!.<..}....s..K9.....{.....[./<..T..I.I..JR)).9.k.N.%.E.W^}....Po.....X..;.=.P...../...+...9./..s....9..\|.....*.7v.`..V.....-^.$S[[[.....K..z.....3..3....5 ...0..''/n/.c...&.{.ht..?....A..I{.n...|...t.....N}..%.v...:.E..i...`....a.k.mg.LX..fcFU.fO-..YEfd.}...~.''.. ....}l$....^.re..'^X..*}.?.^U.G..... .30...X.....f[.l0.P`..KC...[..[..6....~..i..Q.|;x..T .....s.5...n+.0..;...H#.2..#.M..m[^3x&E.Ya..\K..{[..M..g...yf0..~....M.]7..ZZZ:..a.O.G64]....9..l[..a... .N,,.h.....5...f*.y...}...BX{.G^...?.c.....s^..P.(..G...t.0.:.X.DCs.....]vf...py).....x..>-..Be.a...G...Y!...z...g.{....d.s.o.....%.x.....R.W.....Z.b,....!..6Ub....U.qY(/v..m.a...4.`Qr\.E.G..a)..t..e.j.W.....C<.1.....c..l1w....]3%....tR;,..3..-.NW.5...t..H..h..D..b.....M....)B..2J...)..o..m..M.t....wn./....+Wv....xkg..*..

C:\Users\user\AppData\Local\Temp\~DF1BC5B961A0D11AC7.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4732522445853055
Encrypted:	false
SSDEEP:	12:c9lCg5/9lCgeK9l26an9l26an9l8fRyF9l8fRO9lTqA3Feh:c9lLh9lLh9lIn9lIn9loe9loO9lWx
MD5:	902046EA1EB9EBBB43B3D5F447675486
SHA1:	289D971ED12FFA782CE816E0D1D7F6CD51BD3E9F
SHA-256:	302F5282AC57014775EA3556C0D5578199AA6F91A56348F07A149CE2C9D00612
SHA-512:	35EFC69D4F7C2B6CBB8300D551F647C0D3D3436A6F86545B20281069F428F38EB23A0E87051CF5BFD0776667874AB32F40E8A0FC2E03C116861609A091E11D1B
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF240D9F52873C5C2B.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	43817
Entropy (8bit):	0.7089060333324206
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+yUZYZpZyZZTAswsxsxisKs4shsHlTDsIT:kBqoxKAuqR+yU+Xkb2y/
MD5:	942034A5675F1939FC7FAC1482E8BCAC
SHA1:	E1F154124487853518EECC4019DF8A708CF3F685
SHA-256:	8048FA3855BA1B695F480857A5638DA66A677040A30CDC023B68F88597C2C950
SHA-512:	E12518DD090DDE04115F450889992D44A7D5BDE919D6D7F29279DC0B9EF5A75006DC5879C8A729254CF615F38FFB15DAE229DAFC9073498B2E6ED9C7BBCA8D E
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

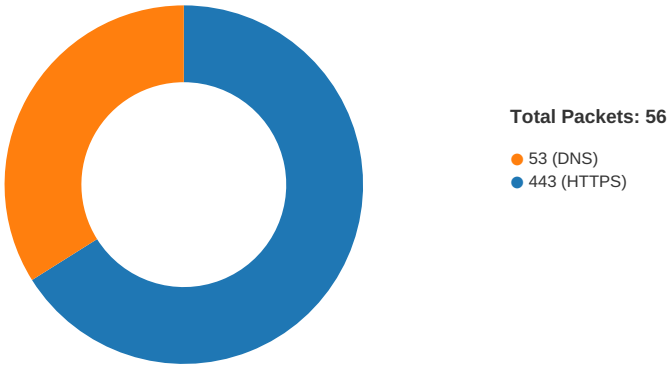
C:\Users\user\AppData\Local\Temp\~DFB0837B9923C992D7.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.3965906005726941
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laAggiS/aWtsx:kBqoxxJhHWSVSEabpiWti5
MD5:	4B5EB521F39B42A4B3FC13CC6A46D20C
SHA1:	82AA1DFE0AC1C3CBC5A63256EBC9B00D92054028
SHA-256:	43A044F08329F57FE7146E3ED89B46D6051C717634F46F5F7FFD214C12CCC8EC
SHA-512:	912BADC2F26ABCECFBA30C34DDD6ED6BBAD2016F3CD0FD3C313CD63ABF5892BE663F7A9C918C9E8E0EA5A93CD7DB2AD4135F2EA94FF8F9350B092DFE0A0 62A1
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
Nov 20, 2020 17:06:29.013952017 CET	49735	443	192.168.2.4	66.96.149.32
Nov 20, 2020 17:06:29.014013052 CET	49736	443	192.168.2.4	66.96.149.32
Nov 20, 2020 17:06:29.112319946 CET	443	49735	66.96.149.32	192.168.2.4
Nov 20, 2020 17:06:29.112339973 CET	443	49736	66.96.149.32	192.168.2.4
Nov 20, 2020 17:06:29.112504005 CET	49735	443	192.168.2.4	66.96.149.32
Nov 20, 2020 17:06:29.112540007 CET	49736	443	192.168.2.4	66.96.149.32
Nov 20, 2020 17:06:29.117741108 CET	49735	443	192.168.2.4	66.96.149.32
Nov 20, 2020 17:06:29.117899895 CET	49736	443	192.168.2.4	66.96.149.32
Nov 20, 2020 17:06:29.215852022 CET	443	49735	66.96.149.32	192.168.2.4
Nov 20, 2020 17:06:29.215938091 CET	443	49736	66.96.149.32	192.168.2.4
Nov 20, 2020 17:06:29.241905928 CET	443	49735	66.96.149.32	192.168.2.4
Nov 20, 2020 17:06:29.241930008 CET	443	49735	66.96.149.32	192.168.2.4
Nov 20, 2020 17:06:29.242018938 CET	49735	443	192.168.2.4	66.96.149.32
Nov 20, 2020 17:06:29.242063046 CET	49735	443	192.168.2.4	66.96.149.32
Nov 20, 2020 17:06:29.272898912 CET	49735	443	192.168.2.4	66.96.149.32
Nov 20, 2020 17:06:29.278409958 CET	49735	443	192.168.2.4	66.96.149.32
Nov 20, 2020 17:06:29.285166025 CET	443	49736	66.96.149.32	192.168.2.4
Nov 20, 2020 17:06:29.285187960 CET	443	49736	66.96.149.32	192.168.2.4
Nov 20, 2020 17:06:29.285309076 CET	49736	443	192.168.2.4	66.96.149.32
Nov 20, 2020 17:06:29.285348892 CET	49736	443	192.168.2.4	66.96.149.32
Nov 20, 2020 17:06:29.289577961 CET	49736	443	192.168.2.4	66.96.149.32
Nov 20, 2020 17:06:29.371015072 CET	443	49735	66.96.149.32	192.168.2.4
Nov 20, 2020 17:06:29.371237993 CET	443	49735	66.96.149.32	192.168.2.4
Nov 20, 2020 17:06:29.371382952 CET	49735	443	192.168.2.4	66.96.149.32
Nov 20, 2020 17:06:29.376456976 CET	443	49735	66.96.149.32	192.168.2.4
Nov 20, 2020 17:06:29.387639046 CET	443	49736	66.96.149.32	192.168.2.4
Nov 20, 2020 17:06:29.387837887 CET	443	49736	66.96.149.32	192.168.2.4
Nov 20, 2020 17:06:29.388032913 CET	49736	443	192.168.2.4	66.96.149.32
Nov 20, 2020 17:06:29.452203035 CET	443	49735	66.96.149.32	192.168.2.4
Nov 20, 2020 17:06:29.452295065 CET	49735	443	192.168.2.4	66.96.149.32

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 17:06:29.864577055 CET	49735	443	192.168.2.4	66.96.149.32
Nov 20, 2020 17:06:29.962717056 CET	443	49735	66.96.149.32	192.168.2.4
Nov 20, 2020 17:06:29.968394041 CET	443	49735	66.96.149.32	192.168.2.4
Nov 20, 2020 17:06:29.968535900 CET	49735	443	192.168.2.4	66.96.149.32
Nov 20, 2020 17:06:30.026709080 CET	49737	443	192.168.2.4	104.218.51.229
Nov 20, 2020 17:06:30.028069019 CET	49738	443	192.168.2.4	104.218.51.229
Nov 20, 2020 17:06:30.129014015 CET	443	49737	104.218.51.229	192.168.2.4
Nov 20, 2020 17:06:30.129216909 CET	49737	443	192.168.2.4	104.218.51.229
Nov 20, 2020 17:06:30.131639004 CET	443	49738	104.218.51.229	192.168.2.4
Nov 20, 2020 17:06:30.131747961 CET	49738	443	192.168.2.4	104.218.51.229
Nov 20, 2020 17:06:30.132482052 CET	49738	443	192.168.2.4	104.218.51.229
Nov 20, 2020 17:06:30.132905960 CET	49737	443	192.168.2.4	104.218.51.229
Nov 20, 2020 17:06:30.235176086 CET	443	49737	104.218.51.229	192.168.2.4
Nov 20, 2020 17:06:30.235780954 CET	443	49737	104.218.51.229	192.168.2.4
Nov 20, 2020 17:06:30.235800982 CET	443	49737	104.218.51.229	192.168.2.4
Nov 20, 2020 17:06:30.235814095 CET	443	49737	104.218.51.229	192.168.2.4
Nov 20, 2020 17:06:30.235826015 CET	443	49737	104.218.51.229	192.168.2.4
Nov 20, 2020 17:06:30.235835075 CET	443	49738	104.218.51.229	192.168.2.4
Nov 20, 2020 17:06:30.235877991 CET	49737	443	192.168.2.4	104.218.51.229
Nov 20, 2020 17:06:30.235925913 CET	49737	443	192.168.2.4	104.218.51.229
Nov 20, 2020 17:06:30.236193895 CET	443	49738	104.218.51.229	192.168.2.4
Nov 20, 2020 17:06:30.236215115 CET	443	49738	104.218.51.229	192.168.2.4
Nov 20, 2020 17:06:30.236228943 CET	443	49738	104.218.51.229	192.168.2.4
Nov 20, 2020 17:06:30.236263037 CET	443	49738	104.218.51.229	192.168.2.4
Nov 20, 2020 17:06:30.236721039 CET	49738	443	192.168.2.4	104.218.51.229
Nov 20, 2020 17:06:30.237750053 CET	443	49737	104.218.51.229	192.168.2.4
Nov 20, 2020 17:06:30.237823963 CET	49737	443	192.168.2.4	104.218.51.229
Nov 20, 2020 17:06:30.238189936 CET	443	49738	104.218.51.229	192.168.2.4
Nov 20, 2020 17:06:30.238254070 CET	49738	443	192.168.2.4	104.218.51.229
Nov 20, 2020 17:06:30.321095943 CET	49738	443	192.168.2.4	104.218.51.229
Nov 20, 2020 17:06:30.321197987 CET	49737	443	192.168.2.4	104.218.51.229
Nov 20, 2020 17:06:30.321646929 CET	49738	443	192.168.2.4	104.218.51.229
Nov 20, 2020 17:06:30.424331903 CET	443	49737	104.218.51.229	192.168.2.4
Nov 20, 2020 17:06:30.424509048 CET	49737	443	192.168.2.4	104.218.51.229
Nov 20, 2020 17:06:30.425342083 CET	443	49738	104.218.51.229	192.168.2.4
Nov 20, 2020 17:06:30.425467968 CET	49738	443	192.168.2.4	104.218.51.229
Nov 20, 2020 17:06:30.443715096 CET	443	49738	104.218.51.229	192.168.2.4
Nov 20, 2020 17:06:30.443890095 CET	49738	443	192.168.2.4	104.218.51.229
Nov 20, 2020 17:06:35.449960947 CET	443	49738	104.218.51.229	192.168.2.4
Nov 20, 2020 17:06:35.450047016 CET	443	49738	104.218.51.229	192.168.2.4
Nov 20, 2020 17:06:35.450119019 CET	49738	443	192.168.2.4	104.218.51.229
Nov 20, 2020 17:06:35.450151920 CET	49738	443	192.168.2.4	104.218.51.229

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 17:06:21.860467911 CET	55854	53	192.168.2.4	8.8.8.8
Nov 20, 2020 17:06:21.887654066 CET	53	55854	8.8.8.8	192.168.2.4
Nov 20, 2020 17:06:23.127907038 CET	64549	53	192.168.2.4	8.8.8.8
Nov 20, 2020 17:06:23.154988050 CET	53	64549	8.8.8.8	192.168.2.4
Nov 20, 2020 17:06:27.154825926 CET	63153	53	192.168.2.4	8.8.8.8
Nov 20, 2020 17:06:27.192316055 CET	53	63153	8.8.8.8	192.168.2.4
Nov 20, 2020 17:06:28.869189978 CET	52991	53	192.168.2.4	8.8.8.8
Nov 20, 2020 17:06:29.001404047 CET	53	52991	8.8.8.8	192.168.2.4
Nov 20, 2020 17:06:29.900074959 CET	53700	53	192.168.2.4	8.8.8.8
Nov 20, 2020 17:06:30.023190975 CET	53	53700	8.8.8.8	192.168.2.4
Nov 20, 2020 17:06:31.007906914 CET	51726	53	192.168.2.4	8.8.8.8
Nov 20, 2020 17:06:31.035084963 CET	53	51726	8.8.8.8	192.168.2.4
Nov 20, 2020 17:06:31.654715061 CET	56794	53	192.168.2.4	8.8.8.8
Nov 20, 2020 17:06:31.682049036 CET	53	56794	8.8.8.8	192.168.2.4
Nov 20, 2020 17:06:32.288691998 CET	56534	53	192.168.2.4	8.8.8.8
Nov 20, 2020 17:06:32.315948963 CET	53	56534	8.8.8.8	192.168.2.4
Nov 20, 2020 17:06:32.924720049 CET	56627	53	192.168.2.4	8.8.8.8
Nov 20, 2020 17:06:32.951797962 CET	53	56627	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 17:06:33.701423883 CET	56621	53	192.168.2.4	8.8.8.8
Nov 20, 2020 17:06:33.728655100 CET	53	56621	8.8.8.8	192.168.2.4
Nov 20, 2020 17:06:34.374346972 CET	63116	53	192.168.2.4	8.8.8.8
Nov 20, 2020 17:06:34.401640892 CET	53	63116	8.8.8.8	192.168.2.4
Nov 20, 2020 17:06:35.149964094 CET	64078	53	192.168.2.4	8.8.8.8
Nov 20, 2020 17:06:35.177289009 CET	53	64078	8.8.8.8	192.168.2.4
Nov 20, 2020 17:06:36.028829098 CET	64801	53	192.168.2.4	8.8.8.8
Nov 20, 2020 17:06:36.064416885 CET	53	64801	8.8.8.8	192.168.2.4
Nov 20, 2020 17:06:36.718154907 CET	61721	53	192.168.2.4	8.8.8.8
Nov 20, 2020 17:06:36.745179892 CET	53	61721	8.8.8.8	192.168.2.4
Nov 20, 2020 17:06:43.882342100 CET	51255	53	192.168.2.4	8.8.8.8
Nov 20, 2020 17:06:43.909463882 CET	53	51255	8.8.8.8	192.168.2.4
Nov 20, 2020 17:06:44.756942034 CET	61522	53	192.168.2.4	8.8.8.8
Nov 20, 2020 17:06:44.784082890 CET	53	61522	8.8.8.8	192.168.2.4
Nov 20, 2020 17:06:45.711170912 CET	52337	53	192.168.2.4	8.8.8.8
Nov 20, 2020 17:06:45.738363028 CET	53	52337	8.8.8.8	192.168.2.4
Nov 20, 2020 17:06:46.940884113 CET	55046	53	192.168.2.4	8.8.8.8
Nov 20, 2020 17:06:46.968059063 CET	53	55046	8.8.8.8	192.168.2.4
Nov 20, 2020 17:06:50.367753983 CET	49612	53	192.168.2.4	8.8.8.8
Nov 20, 2020 17:06:50.409100056 CET	53	49612	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 20, 2020 17:06:28.869189978 CET	192.168.2.4	8.8.8.8	0x4bb8	Standard query (0)	bakrisoil.com	A (IP address)	IN (0x0001)
Nov 20, 2020 17:06:29.900074959 CET	192.168.2.4	8.8.8.8	0x50c7	Standard query (0)	hospitalpicks.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 17:06:29.001404047 CET	8.8.8.8	192.168.2.4	0x4bb8	No error (0)	bakrisoil.com		66.96.149.32	A (IP address)	IN (0x0001)
Nov 20, 2020 17:06:30.023190975 CET	8.8.8.8	192.168.2.4	0x50c7	No error (0)	hospitalpicks.com		104.218.51.229	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
Nov 20, 2020 17:06:29.241930008 CET	66.96.149.32	443	192.168.2.4	49735	CN=*.bakrisoil.com CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Fri Oct 23 22:23:06 CEST 2020	Thu Jan 21 21:23:06 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=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		
Nov 20, 2020 17:06:29.285187960 CET	66.96.149.32	443	192.168.2.4	49736	CN=*.bakrisoil.com CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Fri Oct 23 22:23:06 CEST 2020	Thu Jan 21 21:23:06 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=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 20, 2020 17:06:30.237750053 CET	104.218.51.229	443	192.168.2.4	49737	CN=hospitalpicks.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	Wed Oct 28 01:00:00 CET 2020 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Wed Jan 27 00:59:59 CET 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		
Nov 20, 2020 17:06:30.238189936 CET	104.218.51.229	443	192.168.2.4	49738	CN=hospitalpicks.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	Wed Oct 28 01:00:00 CET 2020 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Wed Jan 27 00:59:59 CET 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		

Code Manipulations

Statistics

Behavior

● iexplore.exe
● iexplore.exe

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 6864 Parent PID: 800

General

Start time:	17:06:25
Start date:	20/11/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff6e8310000
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: 6912 Parent PID: 6864

General

Start time:	17:06:26

Start date:	20/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6864 CREDAT:17410 /prefetch:2
Imagebase:	0xbf0000
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

Disassembly