ID: 356851
Cookbook: browseurl.jbs
Time: 17:49:33
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

Copyright null 2021

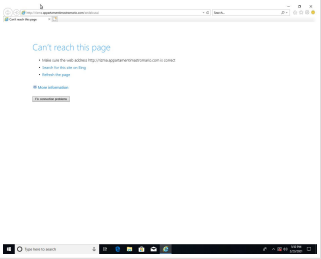
Analysis Report http://rizma.appartamentimastromario.c…

Overview

General Information

Sample URL:	http://rizma.appartamentimastromario.com/andaloussi
Analysis ID:	356851
Infos:	

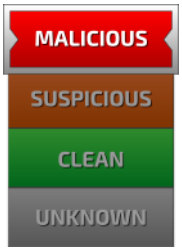
Most interesting Screenshot:



Errors

URL not reachable

Detection



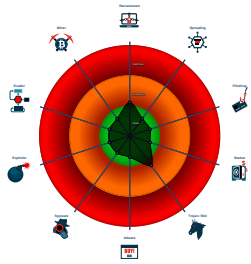
Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Antivirus / Scanner detection for sub…

Tries to resolve domain names, but …

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 5784 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5228 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5784 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

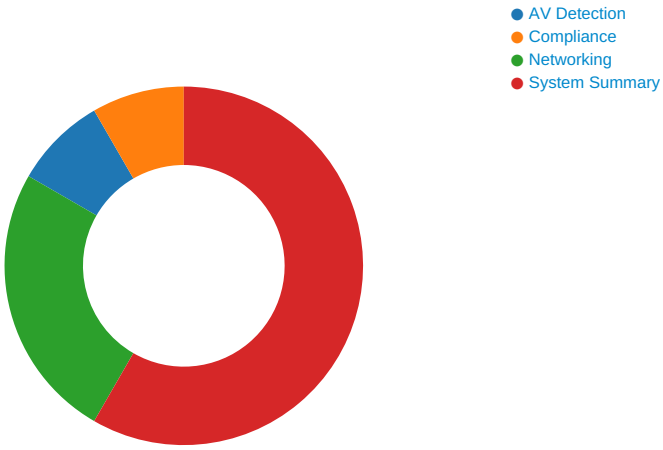
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

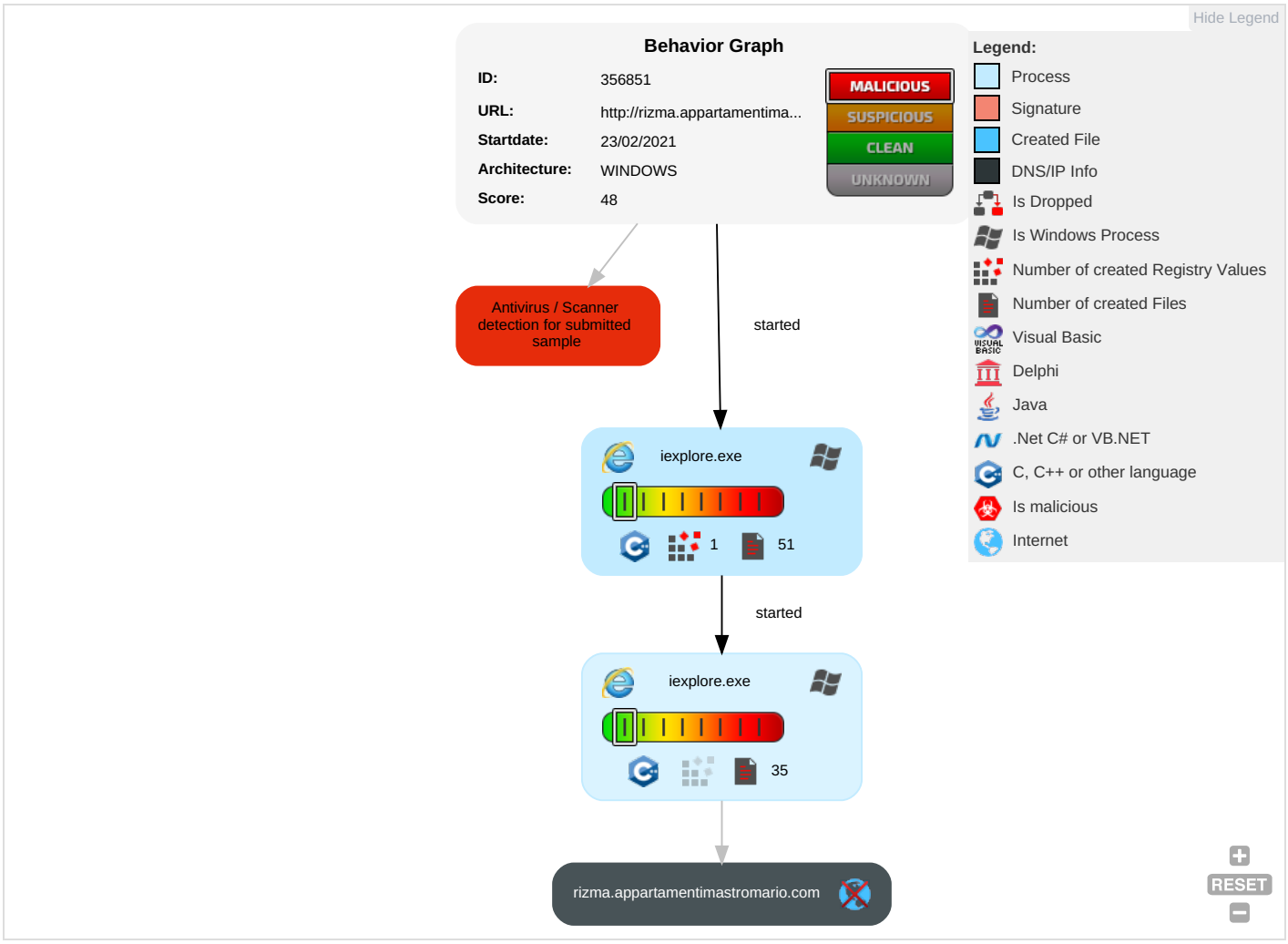
Compliance:

Uses new MSVCR Dlls

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	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 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

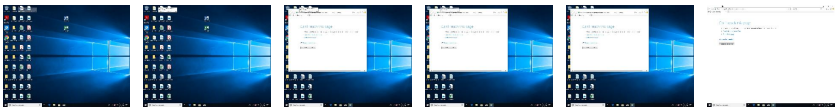
Behavior Graph

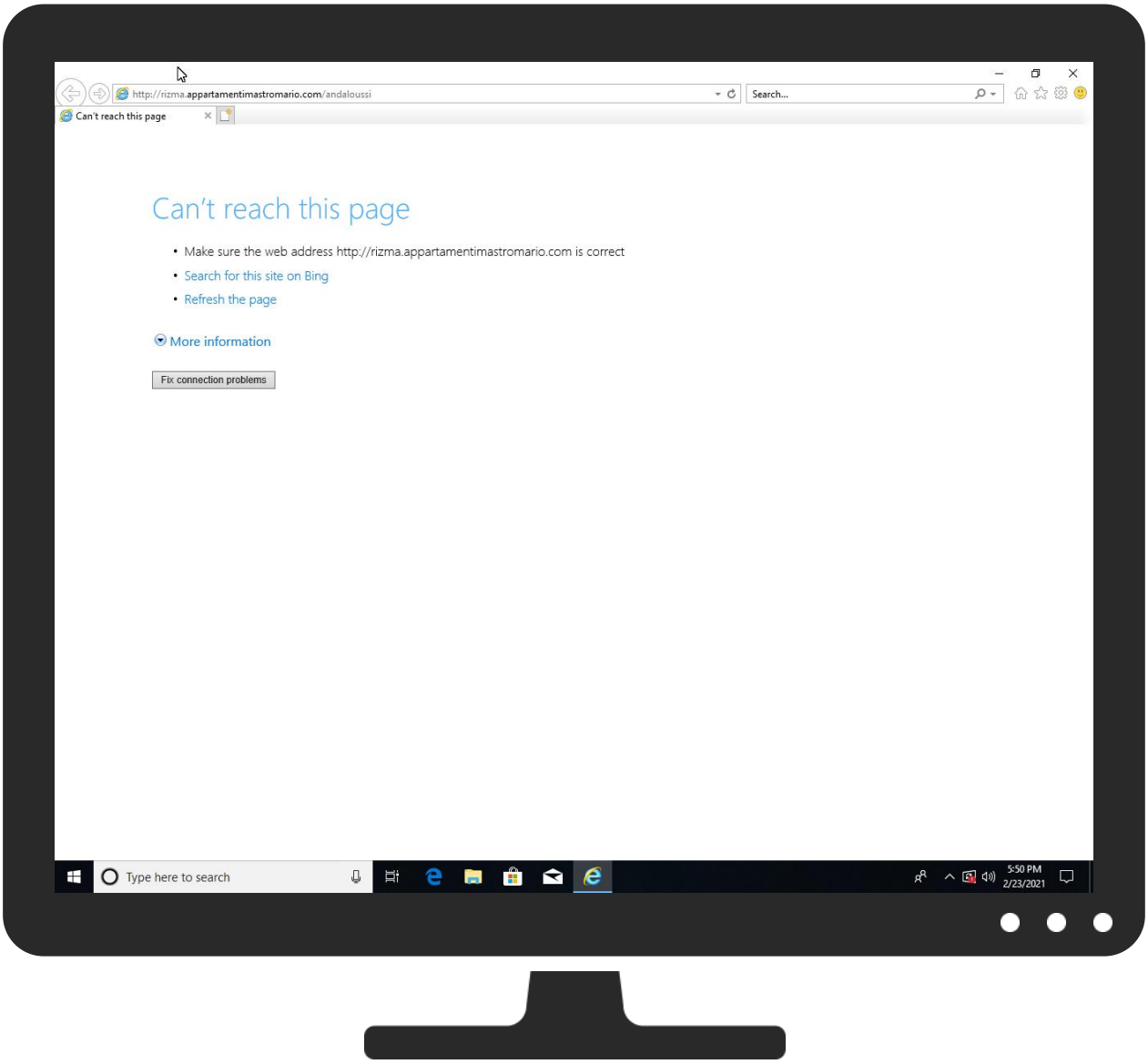


Screenshots

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://rizma.appartamentimastromario.com/andaloussi	2%	Virustotal		Browse
http://rizma.appartamentimastromario.com/andaloussi	100%	Avira URL Cloud	phishing	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://rizma.appartamentimastromario.com/andaloussiRoot	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
rizma.appartamentimastromario.com	unknown	unknown	false		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://rizma.appartamentimastromario.com/andaloussiRoot	{A6DFA4D6-7642-11EB-90E6-ECF4BB82F7E0}.dat.1.dr	true	• Avira URL Cloud: safe	unknown
http://rizma.appartamentimastromario.com/andaloussi	~DF9C8CC8F981501DD5.TMP.1.dr	true		unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356851
Start date:	23.02.2021
Start time:	17:49:33
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://rizma.appartamentimastromario.com/andaloussi
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:	mal48.win@3/11@3/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • **URL browsing timeout or error**

Copyright null 2021

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, ielowutil.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 52.147.198.201, 23.211.6.115, 104.43.193.48, 88.221.62.148, 13.64.90.137, 184.30.20.56, 51.104.144.132 • Excluded domains from analysis (whitelisted): skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, e1723.g.akamaiedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, e11290.dspg.akamaiedge.net, e12564.dspb.akamaiedge.net, go.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net
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.{A6DFA4D4-7642-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{A6DFA4D4-7642-11EB-90E6-ECF4BB82F7E0}.dat	
Entropy (8bit):	1.8551043849463402
Encrypted:	false
SSDEEP:	192:rjZwZ+2XWct8ifwmUzM4MBRyDzsfPmJjX:rlg1moRlp++o
MD5:	0A86C15EA62FAC0CC957F0F723A69444
SHA1:	4A470D791ED4158F1ED97DE031C63203A40F1A84
SHA-256:	357690BC7B144D83B5B88F5339AF71238F1D07E8F1AB0CFE46C0A0862AD0C58F
SHA-512:	961D38AA26E7020F84038E10B3B70BB09B079B4FD1472666CFDC631C7EDD714F51E566A4A4BA6217F5597AFDDC41FF037620B4275DCB9F2E8696E89C5DE6771
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\{A6DFA4D6-7642-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24212
Entropy (8bit):	1.6381305581703651
Encrypted:	false
SSDEEP:	48:Iwu7Gcpr/Gwpa8oG4pQuaGrapbS2GQpBCGHHpcGmTGUp8GAGzYpmGNnGophUN9yo:rOZJQ846uMBSOjZ2hWTMIHhg
MD5:	E2D81969879F567E8F736909A6C7C82D
SHA1:	E363B9345BC33CBC7B2932CE2669C2C2287FF2A1
SHA-256:	FF6A192A87E0FCCC1A3BD325782AE9804E041B4F36BFE152063B2CFA171EE88D
SHA-512:	0A00AB145061FF61F1AE41D15557956A3CEBC1F999953BC159F163B44A7E9B398D4311076F61AB63A7CE0ABF47F61FA19075A48F968620DCF3B76A6A73A9059E
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\{A6DFA4D7-7642-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.565240234642426
Encrypted:	false
SSDEEP:	48:IwPGcpr2GwpaXG4pQvGrapbS1GQpK7G7HpRXTGIpG:rFZuQZ6zBS/A6TlA
MD5:	ECDC3691F448CF4ABD14C2AADDAD3468
SHA1:	1875988168FC546D84ADB4B721564ED30B391177
SHA-256:	35329799BEE3D32FD433BDEFA98FE11C5FBAF2478A1100E4F0607F53335B1377
SHA-512:	63C5C27AD979E461556638ADEB509DB53C3A70706A146FD96F540CFB594A416CA1F44D9C38C63A399B39B66360151B168256C3D066F07D508E90EDD9EE3C4AA
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284F D

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\NewErrorPageTemplate[1]	
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/NewErrorPageTemplate.css
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #00 0000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt; ..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\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\6M6D1PMD\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vIlJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493 AC6D
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/dnserror.htm?ErrorStatus=0x800C0005&DNSError=9002
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMo reInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\down[1]	
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
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.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\VAHFWDJC\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	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\Temp\~DF3D68923ED66E6C8A.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	modified
Size (bytes):	25441
Entropy (8bit):	0.3575883526974927
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laAa/St6N5sp3:kBqoxxJhHWSVSEab9I4lP1
MD5:	DB4C4E0DD1F3989FC1600FF1BE59F363
SHA1:	37F45034CCD62B8FEA7B2C0C103AFD1CB32AB1EC
SHA-256:	BA9486687862D102CA4EEF8AC7BDDDE4531CD18AFD7990B9E33565E87085FBBC
SHA-512:	5438CA8B513314F4D92A0DB36E4FF1FE4CB1B3D5E2CC31B4030D6ADB18F9E0ADAB89F473C50EA672759C86A801204C11622E297326168A2BF84DBBC2EEF6781
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF56FE44C79C55CB47.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.47885839464219737
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loWX9loWX9lWWdSrmW:kBqoItrz
MD5:	4F55BEF8A40C0D7634E3D46BE301BA09
SHA1:	DABBDFE8DBC0A03B27B0E6DC33194207586D915F
SHA-256:	085DA37FF8A55AA0776041E0E23750553142DECA60FD2B014D7F0B7B682E76DD
SHA-512:	A4B1B02EDB37D5D02655AFD84D989FF9681BD39B2474162460756DA6639B2685C2BB4AD0D881AD9B297EEF5DF195C197AD0614F48A7C962740384B07030620222
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\~DF56FE44C79C55CB47.TMP	
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF9C8CC8F981501DD5.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34405
Entropy (8bit):	0.35732495996627217
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwC9lwS9l2GV9l2GV9l4:kBqoxKAuvScS+FrGAGhGNIGNrUN9g
MD5:	308291654322E8D621EBB8BD0DAAC69A
SHA1:	13C0A2B6D15C77D1B546BF974FF21233605B7086
SHA-256:	16226A298967D71B21E7C707BBEE13085E72816AE5102D0F18355000A96821A1
SHA-512:	B869AC5A625526E1A619CF5FF4BEB8119B705831C57580B2C0B3D3FE92D5852A4BE97E7849E031A127BD35C26F0E6277FA54F426A49D366105A7C57AEEEABE4
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

No static file info

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:50:14.088824034 CET	55411	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:50:14.148663998 CET	53	55411	8.8.8.8	192.168.2.7
Feb 23, 2021 17:50:14.762492895 CET	63668	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:50:14.821083069 CET	53	63668	8.8.8.8	192.168.2.7
Feb 23, 2021 17:50:14.869460106 CET	54640	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:50:14.920192957 CET	53	54640	8.8.8.8	192.168.2.7
Feb 23, 2021 17:50:15.733531952 CET	58739	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:50:15.790869951 CET	53	58739	8.8.8.8	192.168.2.7
Feb 23, 2021 17:50:16.709494114 CET	60338	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:50:16.771826029 CET	53	60338	8.8.8.8	192.168.2.7
Feb 23, 2021 17:50:17.767123938 CET	58717	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:50:17.815850019 CET	53	58717	8.8.8.8	192.168.2.7
Feb 23, 2021 17:50:19.015187979 CET	59762	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:50:19.072199106 CET	53	59762	8.8.8.8	192.168.2.7
Feb 23, 2021 17:50:19.908703089 CET	54329	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:50:19.957338095 CET	53	54329	8.8.8.8	192.168.2.7
Feb 23, 2021 17:50:20.951492071 CET	58052	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:50:21.008574009 CET	53	58052	8.8.8.8	192.168.2.7
Feb 23, 2021 17:50:21.897435904 CET	54008	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:50:21.955745935 CET	53	54008	8.8.8.8	192.168.2.7
Feb 23, 2021 17:50:22.260745049 CET	59451	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:50:22.312283039 CET	53	59451	8.8.8.8	192.168.2.7
Feb 23, 2021 17:50:23.253957033 CET	52914	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:50:23.325082064 CET	53	52914	8.8.8.8	192.168.2.7
Feb 23, 2021 17:50:23.332840919 CET	64569	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:50:23.379527092 CET	52816	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:50:23.395154953 CET	53	64569	8.8.8.8	192.168.2.7
Feb 23, 2021 17:50:23.407108068 CET	50781	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:50:23.431224108 CET	53	52816	8.8.8.8	192.168.2.7
Feb 23, 2021 17:50:23.467032909 CET	53	50781	8.8.8.8	192.168.2.7
Feb 23, 2021 17:50:24.661395073 CET	54230	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:50:24.712858915 CET	53	54230	8.8.8.8	192.168.2.7
Feb 23, 2021 17:50:26.200211048 CET	54911	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:50:26.248887062 CET	53	54911	8.8.8.8	192.168.2.7
Feb 23, 2021 17:50:27.183206081 CET	49958	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:50:27.231946945 CET	53	49958	8.8.8.8	192.168.2.7
Feb 23, 2021 17:50:28.338660955 CET	50860	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:50:28.390305996 CET	53	50860	8.8.8.8	192.168.2.7
Feb 23, 2021 17:50:29.536531925 CET	50452	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:50:29.586503029 CET	53	50452	8.8.8.8	192.168.2.7
Feb 23, 2021 17:50:32.544779062 CET	59730	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:50:32.593575954 CET	53	59730	8.8.8.8	192.168.2.7
Feb 23, 2021 17:50:33.383183002 CET	59310	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:50:33.434628010 CET	53	59310	8.8.8.8	192.168.2.7
Feb 23, 2021 17:50:34.576373100 CET	51919	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:50:34.625114918 CET	53	51919	8.8.8.8	192.168.2.7
Feb 23, 2021 17:50:35.378457069 CET	64296	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:50:35.427479982 CET	53	64296	8.8.8.8	192.168.2.7
Feb 23, 2021 17:50:42.558177948 CET	56680	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:50:42.618704081 CET	53	56680	8.8.8.8	192.168.2.7
Feb 23, 2021 17:50:49.029365063 CET	58820	53	192.168.2.7	8.8.8.8
Feb 23, 2021 17:50:49.080852032 CET	53	58820	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 17:50:23.253957033 CET	192.168.2.7	8.8.8.8	0xcad4	Standard query (0)	rizma.appa rtamentima stromario.com	A (IP address)	IN (0x0001)
Feb 23, 2021 17:50:23.332840919 CET	192.168.2.7	8.8.8.8	0xc22d	Standard query (0)	rizma.appa rtamentima stromario.com	A (IP address)	IN (0x0001)
Feb 23, 2021 17:50:23.407108068 CET	192.168.2.7	8.8.8.8	0x6951	Standard query (0)	rizma.appa rtamentima stromario.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 17:50:23.325082064 CET	8.8.8.8	192.168.2.7	0xcad4	Name error (3)	rizma.appa rtamentima stromario.com	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 17:50:23.395154953 CET	8.8.8.8	192.168.2.7	0xc22d	Name error (3)	rizma.appa rtamentima stromario.com	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 17:50:23.467032909 CET	8.8.8.8	192.168.2.7	0x6951	Server failure (2)	rizma.appa rtamentima stromario.com	none	none	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

● iexplore.exe
● iexplore.exe

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5784 Parent PID: 792

General

Start time:	17:50:21
Start date:	23/02/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff6db240000
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: 5228 Parent PID: 5784

General

Start time:	17:50:21

Start date:	23/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5784 CREDAT:17410 /prefetch:2
Imagebase:	0x20000
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