ID: 322846
Cookbook: browseurl.jbs
Time: 00:15:28
Date: 26/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

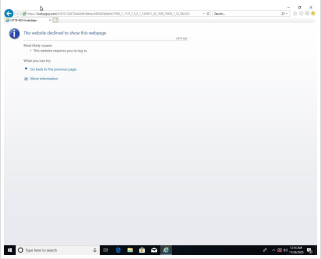
Analysis Report https://lhklzbenyc.objects-us-east-1.dre…

Overview

General Information

Sample URL:	http://https://lhklzbenyc.objects-us-east-1.dream.io/liinkk.html#qs=r-abacacfekhccacaeikheababacafeadbfaccagjdacjekaibfgjacb
Analysis ID:	322846

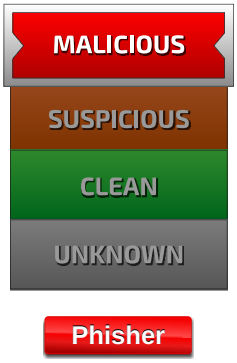
Most interesting Screenshot:



Errors

URL not reachable

Detection

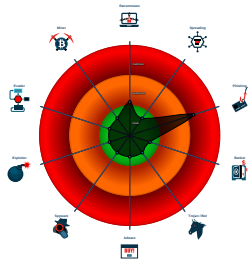


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Yara detected Phisher

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 5892 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5936 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5892 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

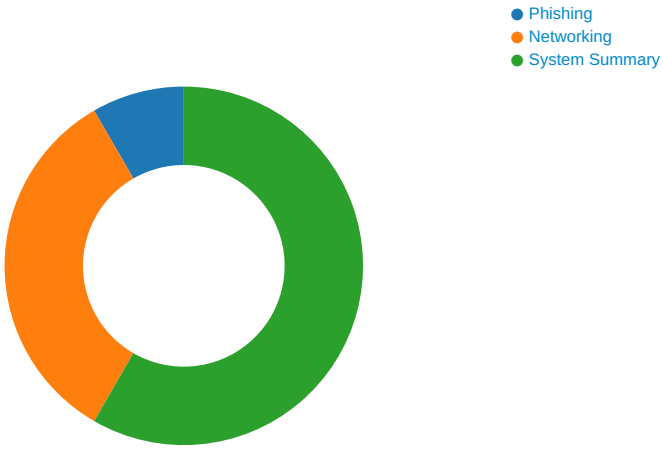
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\liinkk[1].htm	JoeSecurity_Phisher_2	Yara detected Phisher	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

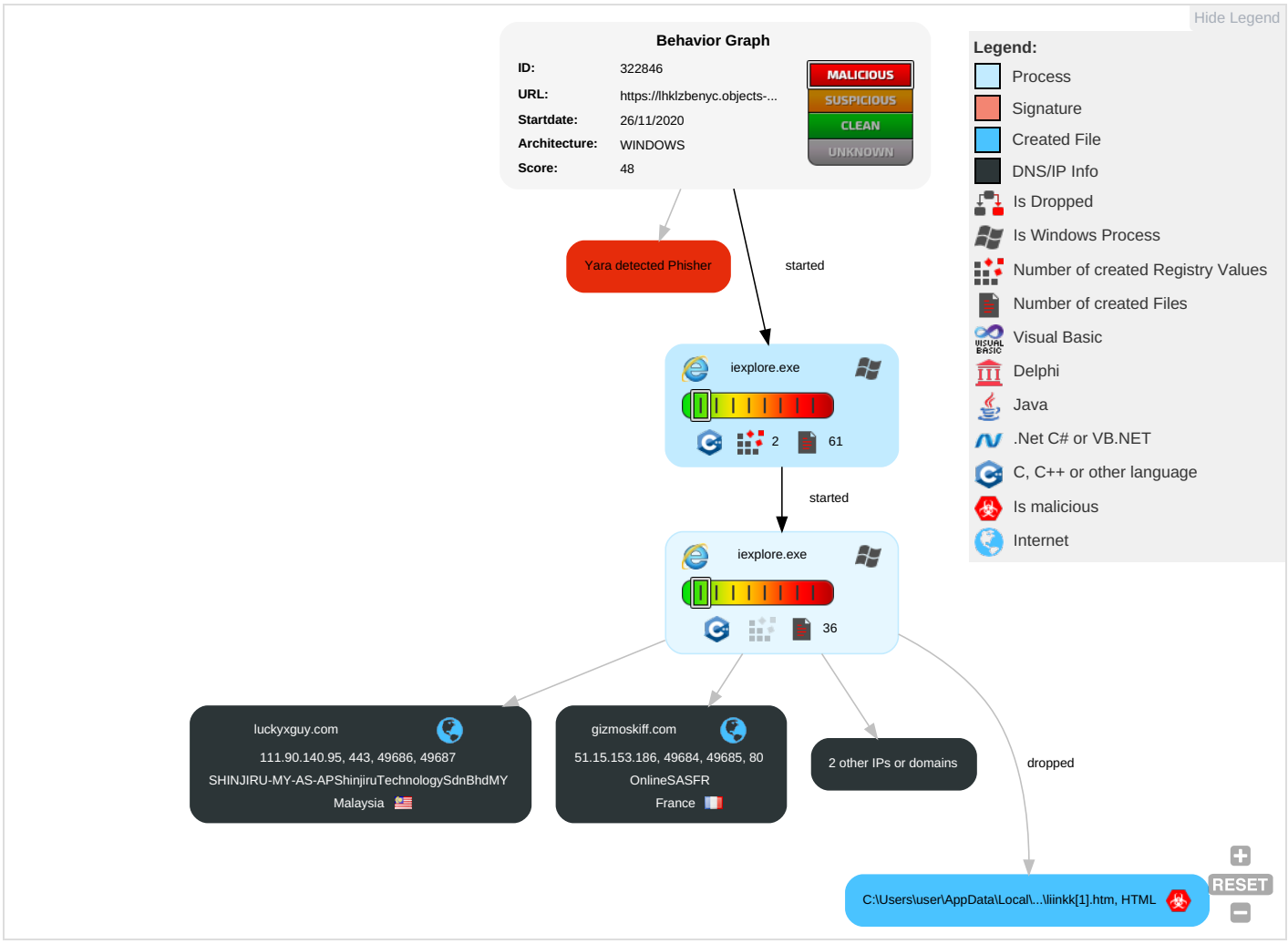
Phishing:

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	Impa
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 Partit
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lock
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM Card Swap		Carri Billing Fraud

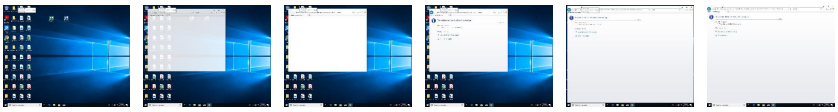
Behavior Graph

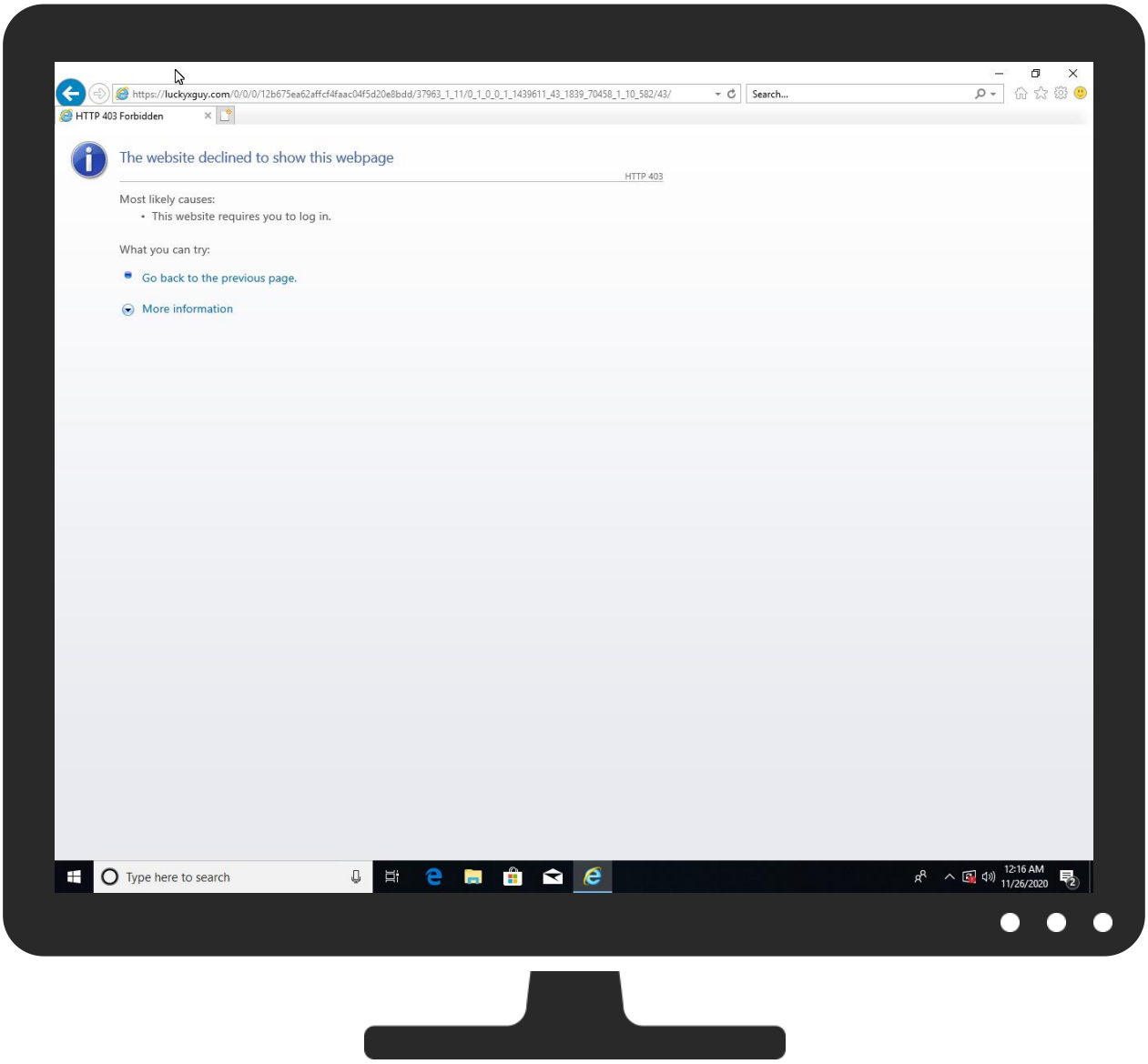


Screenshots

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://lhklzbenyc.objects-us-east-1.dream.io/liinkk.html#qs=r-abacacfekhccacaeikheababacafeadbfaccagjdacjekaibfgjacb	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
luckyxguy.com	0%	Virustotal		Browse
gizmoskiff.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://luckyxguy.com/0/0/0/12b675ea62affcf4faac04f5d20e8bdd/37963_1_11/0_1_0_0_1_1439611_43_1839_70	0%	Avira URL Cloud	safe	
http://https://luckyxguy.com/	0%	Avira URL Cloud	safe	
http://gizmoskiff.com/qs=r-abacacfekhccacaeikheababacafeadbfaccagjdacjekaibfgjacb	0%	Avira URL Cloud	safe	
http://https://lhklzbenyc.obj	0%	Avira URL Cloud	safe	
http://gizmoskiff.com/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
objects-us-east-1.dream.io	208.113.201.33	true	false		high
luckyxguy.com	111.90.140.95	true	false	• 0%, Virustotal, Browse	unknown
gizmoskiff.com	51.15.153.186	true	false	• 0%, Virustotal, Browse	unknown
lhklzbenyc.objects-us-east-1.dream.io	unknown	unknown	false		high

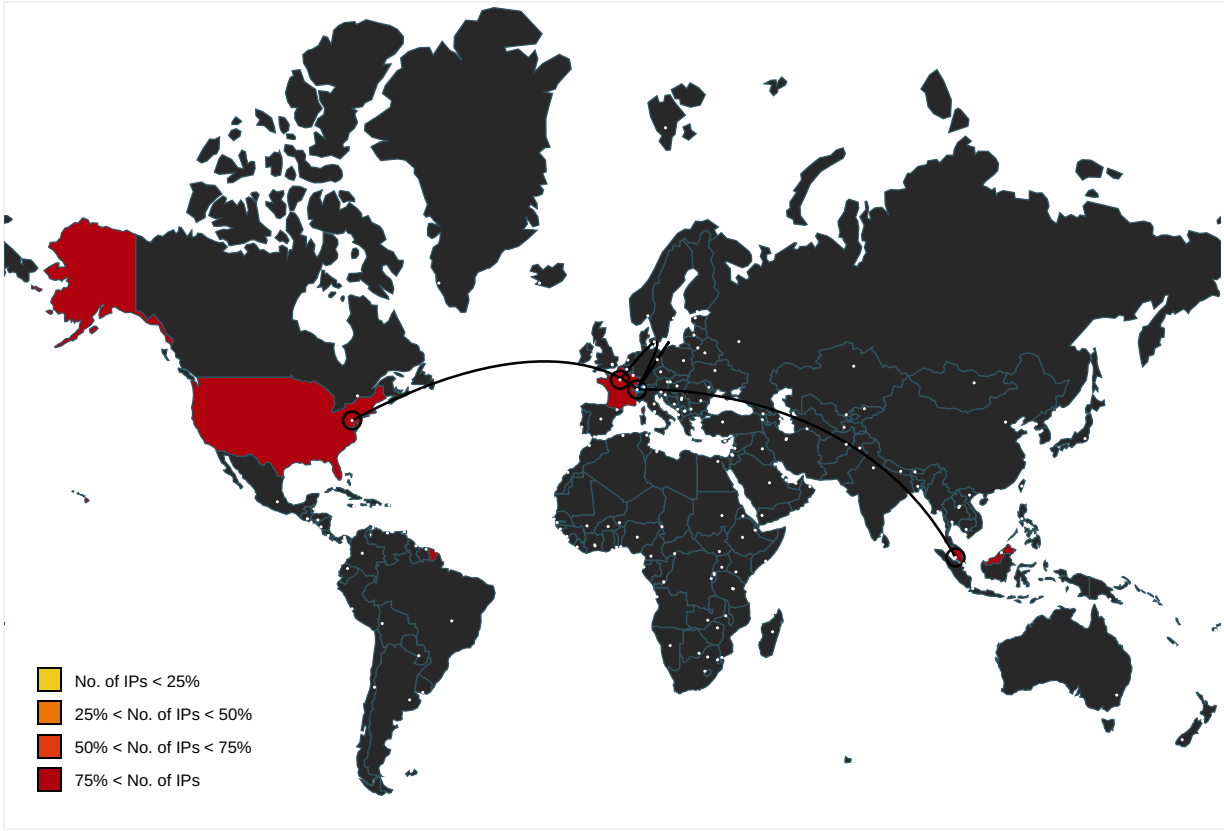
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://gizmoskiff.com/qs=r-abacacfekhccacaeikheababacafeadbfaccagjdacjekaibfgjacb	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://luckyxguy.com/0/0/0/12b675ea62affcf4faac04f5d20e8bdd/37963_1_11/0_1_0_0_1_1439611_43_1839_70	~DF2F607BA7733F9ACF.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://luckyxguy.com/	{A6FA38B5-2FBF-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://lhklzbenyc.objects-us-east-1.dream.io/liinkk.html#qs=r-abacacfekhccacaeikheababacafeadbfacca	~DF2F607BA7733F9ACF.TMP.1.dr, {A6FA38B5-2FBF-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://https://lhklzbenyc.obj	{A6FA38B5-2FBF-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://gizmoskiff.com/	liinkk[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://lhklzbenyc.objects-us-east-1.dream.io/liinkk.html	~DF2F607BA7733F9ACF.TMP.1.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
111.90.140.95	unknown	Malaysia		45839	SHINJIRU-MY-AS-APShinjiruTechnologySdnBhdMY	false
51.15.153.186	unknown	France		12876	OnlineSASFR	false
208.113.201.33	unknown	United States		26347	DREAMHOST-ASUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	322846
Start date:	26.11.2020
Start time:	00:15:28
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://lhklzbenyc.objects-us-east-1.dream.io/liink.html#qs=r-abacacfekhccacaeikheababacafeadbfaccagjdacjekaibfgjacb
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:	4
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.phis.win@3/15@4/3
Cookbook Comments:	• Adjust boot time • Enable AMSI • **URL browsing timeout or error**
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, ielowutil.exe • Excluded IPs from analysis (whitelisted): 104.83.120.32 • Excluded domains from analysis (whitelisted): e11290.dspg.akamaiedge.net, go.microsoft.com, go.microsoft.com.edgekey.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.{A6FA38B3-2FBF-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8578613347742838
Encrypted:	false
SSDEEP:	192:rZZmZ/l2/d9W/0t/rf/77hM/g/B/tf/IsX:rPCklUIj6YptZ
MD5:	E1F0B420E758FE4C7FF194DDF037C669
SHA1:	29C7ABA121994E5E7C2FB76D512E87E4E8C99BE8
SHA-256:	BECA1FBA5A8E7C0F9A2560299EF0B4A6BB5A9829BB260C92B8AE61DBEB5AE221
SHA-512:	6F11A96F22C8778E287774469839D2C496CB03F7C86862C0A44D2046DC03207F6190A9DC472CE0FADCBF0F1E71734864BD912484A535D379C0DAEF5256D7E06E
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{A6FA38B3-2FBF-11EB-90E4-ECF4BB862DED}.dat	
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{A6FA38B5-2FBF-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	35104
Entropy (8bit):	2.0129166806631718
Encrypted:	false
SSDEEP:	384:rAYFB/h84GwmBwUIH0DIqNVw/pN662wkRwBwGsgwt:Li9mA7VSCdUrA
MD5:	A877C17E71EE687BD97F1575B54BB40C
SHA1:	9EDE09E80DEFE69B66F5FE0E979B4404EC332030
SHA-256:	65EF57B3CEC55AACA13B6DDEEBF2704DEB13C850D9238CDCAC545B9F161CB0E7
SHA-512:	3F71309534FDD52FEED10D23CA6938460FD9A779CFF486EF0FCE8E4E3F803AC7A582AF84DBFEDBCC0CC1240C6CEF7897210780F3A4141B8C1B79EE14A0DF32 9
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\{AD7A6107-2FBF-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5653656941340854
Encrypted:	false
SSDEEP:	48:IwxGcproGwpaJG4pQKGrapbSKrGQpKHG7HpRRsTGIpG:rHZwQL68BSKFAmTR4A
MD5:	2F81B3224D8143A6ACDC7FC27054F797
SHA1:	F7AADE38857D3D7645023AD5DDF479B6D0C8C173
SHA-256:	E1AABA221B2139C41F6244B284444532E6B2F5573AB68451CFC98CE804E2DEB4
SHA-512:	F2AB4C43E9C320CB14A12E2138E0A7F74A0E78D8D13B96556CED95359B868975FD5FB0CF296079D9252D466336D1B8A1459843AFE86C91DB8F0D0A7F47F1058
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\http_403[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):	4585
Entropy (8bit):	4.046190045670235
Encrypted:	false
SSDEEP:	48:upUw1V4VOBXvLwSZIPTC5f1a5TI7jn3GFa7KGuc1kpNc7K1rfQy:u3p9ZQw6Kj36a7gG7I
MD5:	3215E2E80AA8B9FABA83D76AEF71F1B9
SHA1:	C7582D414EE6A1DAE098F6DBBBF68ED9641D0023
SHA-256:	D91C22EF6451561F346B8C8BC6F98897E2E5C28135A421EE946800F6C8451B24
SHA-512:	690E4D62229AD14D3D842DABE986651B4CC2E4C873A50E5B7FC4FD539662A703690ECC70649ACEA7751E69CE6046489C0E6B05D24F0030D68773C67B3DCBAE 0
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/http_403.htm

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\http_403[1]	
Preview:	.<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">....<html>.... <head>.. <link rel="stylesheet" type="text/css" href="ErrorPageTemplate.css" />.... <meta http-equiv="Content-Type" content="text/html; charset=UTF-8"/>.... <title>HTTP 403 Forbidden</title>.... <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="javascript:expandCollapse('infoBlockID', true); initGoBack(); initMoreInfo('infoBlockID');">.... <table width="730" cellpadding="0" cellspacing="0" border="0">.... Error title -->.. <tr>.. <td id="infoIconAlign" width="60" align="left" valign="top" rowspan="2">.. <img src="info_48.png" id="infoIcon" alt="Info icon">.. </td>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\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:	E60EA153B0FECE4D311769391D3B763B14B9A140105A36A13DAD23C2906735EAAB9092236DEB8C68EF078E8864D6E288BEF7EF1731C1E9F1AD9B0170B95AC134
Malicious:	false
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\Microsoft\Windows\INetCache\IE\MEEXW4H4\background_gradient[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 1x800, frames 3
Category:	downloaded
Size (bytes):	453
Entropy (8bit):	5.019973044227213
Encrypted:	false
SSDEEP:	6:3llVuiPjlXJYhg5suRd8PImMo23C/kHrJ8yA/NIeYoWg78C/vTFvbKLAh3:V/XPYhiPRd8j7+9LoIrobtHTdbKi
MD5:	20F0110ED5E4E0D5384A496E4880139B
SHA1:	51F5FC61D8BF19100DF0F8AADAA57FCD9C086255
SHA-256:	1471693BE91E53C2640FE7BAEECBC624530B088444222D93F2815DFCE1865D5B
SHA-512:	5F52C117E346111D99D3B642926139178A80B9EC03147C00E27F07AAB47FE38E9319FE983444F3E0E36DEF1E86DD7C56C25E44B14EFDC3F13B45EDEDA064DB5A
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/background_gradient.jpg
Preview:	.....JFIF.....d.d.....Ducky.....P.....Adobe.d..... .....W..... .....Qa.....?.....%.....x.....s...Z.....j.T.wz.6...X.@... V.3tM...P@.u.%...m..D.25...T...F.....p.....A.....BP..qD.(.....ntH.@.....h?..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\httpErrorPagesScripts[1]	
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\PSUEOSZZ\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;...margin-top: 20px;...margin-left: 20px;...color: #575757;..}....body.securityError..{...font-family: "Segoe UI", "verdana" , "Arial";...background-image: url(background_gradient_red.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;..}....body.tabInfo..{...background-image: none;...background-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\PSUEOSZZ\bullet[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	447
Entropy (8bit):	7.304718288205936
Encrypted:	false
SSDEEP:	12:6v/71Cyt/JNTWxGdr+kZDWO7+4dKIv0b1GKuxu+R:/yBJNTqsSk9BTwE05su+R
MD5:	26F971D87CA00E23BD2D064524AEF838
SHA1:	7440BEFF2F4F8FABC9315608A13BF26CABAD27D9
SHA-256:	1D8E5FD3C1FD384C0A7507E7283C7FE8F65015E521B84569132A7EABEDC9D41D
SHA-512:	C62EB51BE301BB96C80539D66A73CD17CA2021D5D816233853A37DB72E04050271E581CC99652F3D8469B390003CA6C62DAD2A9D57164C620B7777AE99AA1B1
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/bullet.png
Preview:	.PNG.....IHDR.....ex....PLTE...(EkFRp&@e&@e)Af)AgANjBNjDNjDNj2Vv-Xz-Y{3XyC\}E_.2j.3l.8p.7q.;j.;l.Zj.\l.5o.7q.<..aw.<..dz.E.....1..@.7..~.....9..:.....A ..B..E..9..:..a..c..b..g.#M.%O.#r.#s.%y.2..4..+..-..?..@..;..p..s...G..H..M.....z`....#tRNS...../,....mIDATx^..C..`.....S....y'...05...|..k.X.....*`.F.K....JQ..u.<.}.. .. [U..m....'r%.....yn.`.7F..).5..b..rX.T.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/down.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\down[1]	
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~..... ....b.....$..s...7tRNS.a.o(,.s....e.....q*..... .....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV ...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\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 connection.";..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\WJ8I2OL4\liinkk[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	102
Entropy (8bit):	4.809296910429262
Encrypted:	false
SSDEEP:	3:gkJR9dBkADFoCDRAZMfI9DNIwSkoOkADLWECGXIM7b:P7YmmTyg9DNt+mfOlb
MD5:	7F4C13A05A98AF88115B54D97338C0BD
SHA1:	7BFA51D43467659FA2965F338E09AA4E899EF3EE
SHA-256:	795F51FBF78F0C6225C58BECDB4D34082D42D1F2266AC75E334F61C0E7E8F491
SHA-512:	44045E76B8D213B506513E919686BB177CC14D7FCD1CD33899A03942348F1BF2AD3FE31018B5A28ED5F400A6F235562189A9A4D7FE851D90657981386CAF181A
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Phisher_2, Description: Yara detected Phisher, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\liinkk[1].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://lhklzbenyc.objects-us-east-1.dream.io/liinkk.html
Preview:	<script>document.location.href = 'http://gizmoskiff.com/'+window.location.href.split('#')[1];</script>

C:\Users\user\AppData\Local\Temp\~DF2F607BA7733F9ACF.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	44409
Entropy (8bit):	0.6266600081976721
Encrypted:	false
SSDEEP:	384:kBqoxKAuqR+1bZILkBwyIH0DIqNVw/pN6LGw6:BjmA7VSx
MD5:	1ED41B158D205CE7EDF5C7CFC5D42A5F
SHA1:	9127694339CBE58131DE5DEE7FE473985F12FE0E
SHA-256:	DB1321FA28A68F3CB2F5EA6DAB00709B31C3A07925EE7B8637D70C48FA523C12
SHA-512:	58FC46E31A823B1D998636A9AB0FE9AF5B53937D24F5927A045E0CE6B0D5859CE136F4B4EDC3CB31BE76071ACC6B2D1347F184ED686B7DD841942859CF569D5
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF55A80DF302D01A96.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.28812825761064564
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA:kBqoxxJhHWSVSEab
MD5:	7DA1144C781AB85AB41C54FF25B1C771
SHA1:	56B6208446BD8498219279A5B68E1FE658BCB5AC
SHA-256:	F16931FFBC6FDBBD1A453AC88CF63B93C1E2D0D6613F5C3D985B7CB5327F9C2C
SHA-512:	37B60B39C9761ACE847FDC221A649AC9C1290C5D92C587E0FCA4E5F9F52BACE2BBF57BE0DE8B1887CCF6737933B950E4FF39A87CE83E8A3798FAACF3B6F0C 9F
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFB7E7B6F16E3436F0.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4825851731874986
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lo/rF9lo/R9lW/DDQVMDQh1G:kBqoI/6/E/oV7h1G
MD5:	E1BEEFF6620ECA40A593B714E778C9E1
SHA1:	5D5EA9F64196E12B0A5923202538DCA5C8A1C16F
SHA-256:	69F4B09B2045A940C0B132C54C6C87FAE522DEB9B1FF7AA543141457C5125BBC
SHA-512:	8954A20DE237A684376199FB8FBC2E348042D517E03DFC1BFFAC5F3F66D0AFFF014462DA6D91D856E58FB1F5A3F4B57A67478378B3494EC72E072802E49F6C49
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

Static File Info

No static file info

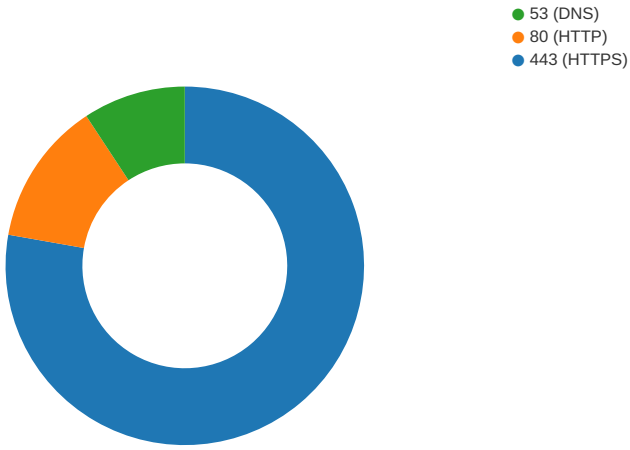
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/26/20-00:16:21.974713	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8

Network Port Distribution

Total Packets: 54



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 00:16:18.147492886 CET	49682	443	192.168.2.3	208.113.201.33
Nov 26, 2020 00:16:18.149163961 CET	49683	443	192.168.2.3	208.113.201.33
Nov 26, 2020 00:16:18.258263111 CET	443	49682	208.113.201.33	192.168.2.3
Nov 26, 2020 00:16:18.258522987 CET	49682	443	192.168.2.3	208.113.201.33
Nov 26, 2020 00:16:18.259718895 CET	443	49683	208.113.201.33	192.168.2.3
Nov 26, 2020 00:16:18.259840965 CET	49683	443	192.168.2.3	208.113.201.33
Nov 26, 2020 00:16:18.270504951 CET	49682	443	192.168.2.3	208.113.201.33
Nov 26, 2020 00:16:18.270745993 CET	49683	443	192.168.2.3	208.113.201.33
Nov 26, 2020 00:16:18.392407894 CET	443	49682	208.113.201.33	192.168.2.3
Nov 26, 2020 00:16:18.392469883 CET	443	49682	208.113.201.33	192.168.2.3
Nov 26, 2020 00:16:18.392509937 CET	443	49682	208.113.201.33	192.168.2.3
Nov 26, 2020 00:16:18.392538071 CET	443	49682	208.113.201.33	192.168.2.3
Nov 26, 2020 00:16:18.392577887 CET	443	49683	208.113.201.33	192.168.2.3
Nov 26, 2020 00:16:18.392626047 CET	443	49683	208.113.201.33	192.168.2.3
Nov 26, 2020 00:16:18.392625093 CET	49682	443	192.168.2.3	208.113.201.33
Nov 26, 2020 00:16:18.392663956 CET	49682	443	192.168.2.3	208.113.201.33
Nov 26, 2020 00:16:18.392669916 CET	443	49683	208.113.201.33	192.168.2.3
Nov 26, 2020 00:16:18.392680883 CET	49682	443	192.168.2.3	208.113.201.33
Nov 26, 2020 00:16:18.392698050 CET	443	49683	208.113.201.33	192.168.2.3
Nov 26, 2020 00:16:18.392720938 CET	49683	443	192.168.2.3	208.113.201.33
Nov 26, 2020 00:16:18.392776012 CET	49683	443	192.168.2.3	208.113.201.33
Nov 26, 2020 00:16:18.392822027 CET	49683	443	192.168.2.3	208.113.201.33
Nov 26, 2020 00:16:18.411511898 CET	443	49682	208.113.201.33	192.168.2.3
Nov 26, 2020 00:16:18.411556959 CET	443	49682	208.113.201.33	192.168.2.3
Nov 26, 2020 00:16:18.411729097 CET	49682	443	192.168.2.3	208.113.201.33
Nov 26, 2020 00:16:18.413368940 CET	443	49683	208.113.201.33	192.168.2.3
Nov 26, 2020 00:16:18.413429022 CET	443	49683	208.113.201.33	192.168.2.3
Nov 26, 2020 00:16:18.413467884 CET	49683	443	192.168.2.3	208.113.201.33
Nov 26, 2020 00:16:18.413526058 CET	49683	443	192.168.2.3	208.113.201.33
Nov 26, 2020 00:16:18.488132954 CET	49683	443	192.168.2.3	208.113.201.33
Nov 26, 2020 00:16:18.488312960 CET	49682	443	192.168.2.3	208.113.201.33
Nov 26, 2020 00:16:18.493895054 CET	49683	443	192.168.2.3	208.113.201.33
Nov 26, 2020 00:16:18.601104975 CET	443	49682	208.113.201.33	192.168.2.3
Nov 26, 2020 00:16:18.601360083 CET	49682	443	192.168.2.3	208.113.201.33
Nov 26, 2020 00:16:18.614700079 CET	443	49683	208.113.201.33	192.168.2.3
Nov 26, 2020 00:16:18.614820004 CET	49683	443	192.168.2.3	208.113.201.33
Nov 26, 2020 00:16:18.618040085 CET	443	49683	208.113.201.33	192.168.2.3
Nov 26, 2020 00:16:18.618316889 CET	49683	443	192.168.2.3	208.113.201.33
Nov 26, 2020 00:16:20.207673073 CET	49684	80	192.168.2.3	51.15.153.186
Nov 26, 2020 00:16:20.209266901 CET	49685	80	192.168.2.3	51.15.153.186
Nov 26, 2020 00:16:20.228477001 CET	80	49684	51.15.153.186	192.168.2.3
Nov 26, 2020 00:16:20.228667021 CET	49684	80	192.168.2.3	51.15.153.186
Nov 26, 2020 00:16:20.229384899 CET	49684	80	192.168.2.3	51.15.153.186
Nov 26, 2020 00:16:20.229885101 CET	80	49685	51.15.153.186	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 00:16:20.229970932 CET	49685	80	192.168.2.3	51.15.153.186
Nov 26, 2020 00:16:20.250077963 CET	80	49684	51.15.153.186	192.168.2.3
Nov 26, 2020 00:16:20.477262020 CET	80	49684	51.15.153.186	192.168.2.3
Nov 26, 2020 00:16:20.477391005 CET	49684	80	192.168.2.3	51.15.153.186
Nov 26, 2020 00:16:20.505105019 CET	49686	443	192.168.2.3	111.90.140.95
Nov 26, 2020 00:16:20.505264044 CET	49687	443	192.168.2.3	111.90.140.95
Nov 26, 2020 00:16:20.693448067 CET	443	49687	111.90.140.95	192.168.2.3
Nov 26, 2020 00:16:20.693492889 CET	443	49686	111.90.140.95	192.168.2.3
Nov 26, 2020 00:16:20.693702936 CET	49686	443	192.168.2.3	111.90.140.95
Nov 26, 2020 00:16:20.693758965 CET	49687	443	192.168.2.3	111.90.140.95
Nov 26, 2020 00:16:20.917037964 CET	49687	443	192.168.2.3	111.90.140.95
Nov 26, 2020 00:16:20.918147087 CET	49686	443	192.168.2.3	111.90.140.95
Nov 26, 2020 00:16:21.108575106 CET	443	49687	111.90.140.95	192.168.2.3
Nov 26, 2020 00:16:21.108633995 CET	443	49687	111.90.140.95	192.168.2.3
Nov 26, 2020 00:16:21.108665943 CET	443	49687	111.90.140.95	192.168.2.3
Nov 26, 2020 00:16:21.108680010 CET	49687	443	192.168.2.3	111.90.140.95
Nov 26, 2020 00:16:21.108709097 CET	49687	443	192.168.2.3	111.90.140.95
Nov 26, 2020 00:16:21.108716965 CET	49687	443	192.168.2.3	111.90.140.95
Nov 26, 2020 00:16:21.109318972 CET	443	49686	111.90.140.95	192.168.2.3
Nov 26, 2020 00:16:21.109360933 CET	443	49686	111.90.140.95	192.168.2.3
Nov 26, 2020 00:16:21.109410048 CET	49686	443	192.168.2.3	111.90.140.95
Nov 26, 2020 00:16:21.109436989 CET	443	49686	111.90.140.95	192.168.2.3
Nov 26, 2020 00:16:21.109442949 CET	49686	443	192.168.2.3	111.90.140.95
Nov 26, 2020 00:16:21.109483957 CET	49686	443	192.168.2.3	111.90.140.95
Nov 26, 2020 00:16:21.118163109 CET	49687	443	192.168.2.3	111.90.140.95
Nov 26, 2020 00:16:21.118469954 CET	49687	443	192.168.2.3	111.90.140.95
Nov 26, 2020 00:16:21.122354031 CET	49686	443	192.168.2.3	111.90.140.95
Nov 26, 2020 00:16:21.308881044 CET	443	49687	111.90.140.95	192.168.2.3
Nov 26, 2020 00:16:21.308996916 CET	49687	443	192.168.2.3	111.90.140.95
Nov 26, 2020 00:16:21.312568903 CET	443	49686	111.90.140.95	192.168.2.3
Nov 26, 2020 00:16:21.312665939 CET	49686	443	192.168.2.3	111.90.140.95
Nov 26, 2020 00:16:22.112649918 CET	443	49687	111.90.140.95	192.168.2.3
Nov 26, 2020 00:16:22.112762928 CET	49687	443	192.168.2.3	111.90.140.95
Nov 26, 2020 00:16:25.481529951 CET	80	49684	51.15.153.186	192.168.2.3
Nov 26, 2020 00:16:25.481623888 CET	49684	80	192.168.2.3	51.15.153.186
Nov 26, 2020 00:16:31.315411091 CET	443	49686	111.90.140.95	192.168.2.3
Nov 26, 2020 00:16:31.315459967 CET	443	49686	111.90.140.95	192.168.2.3
Nov 26, 2020 00:16:31.315655947 CET	49686	443	192.168.2.3	111.90.140.95
Nov 26, 2020 00:16:32.113346100 CET	443	49687	111.90.140.95	192.168.2.3
Nov 26, 2020 00:16:32.113444090 CET	443	49687	111.90.140.95	192.168.2.3
Nov 26, 2020 00:16:32.113574982 CET	49687	443	192.168.2.3	111.90.140.95
Nov 26, 2020 00:16:32.113600016 CET	49687	443	192.168.2.3	111.90.140.95

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 00:16:17.001856089 CET	51904	53	192.168.2.3	8.8.8.8
Nov 26, 2020 00:16:17.019181967 CET	53	51904	8.8.8.8	192.168.2.3
Nov 26, 2020 00:16:18.019845009 CET	61328	53	192.168.2.3	8.8.8.8
Nov 26, 2020 00:16:18.128572941 CET	53	61328	8.8.8.8	192.168.2.3
Nov 26, 2020 00:16:18.795351028 CET	54130	53	192.168.2.3	8.8.8.8
Nov 26, 2020 00:16:19.809458017 CET	54130	53	192.168.2.3	8.8.8.8
Nov 26, 2020 00:16:20.039973974 CET	53	54130	8.8.8.8	192.168.2.3
Nov 26, 2020 00:16:20.485218048 CET	56961	53	192.168.2.3	8.8.8.8
Nov 26, 2020 00:16:20.503166914 CET	53	56961	8.8.8.8	192.168.2.3
Nov 26, 2020 00:16:21.974597931 CET	53	54130	8.8.8.8	192.168.2.3

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Nov 26, 2020 00:16:21.974713087 CET	192.168.2.3	8.8.8.8	d001	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 26, 2020 00:16:18.019845009 CET	192.168.2.3	8.8.8.8	0x5b89	Standard query (0)	lhklzbenyc .objects-us-east-1.dream.io	A (IP address)	IN (0x0001)
Nov 26, 2020 00:16:18.795351028 CET	192.168.2.3	8.8.8.8	0x44be	Standard query (0)	gizmoskiff.com	A (IP address)	IN (0x0001)
Nov 26, 2020 00:16:19.809458017 CET	192.168.2.3	8.8.8.8	0x44be	Standard query (0)	gizmoskiff.com	A (IP address)	IN (0x0001)
Nov 26, 2020 00:16:20.485218048 CET	192.168.2.3	8.8.8.8	0x960a	Standard query (0)	luckyxguy.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 26, 2020 00:16:18.128572941 CET	8.8.8.8	192.168.2.3	0x5b89	No error (0)	lhklzbenyc .objects-us-east-1.dream.io	objects-us-east-1.dream.io		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 00:16:18.128572941 CET	8.8.8.8	192.168.2.3	0x5b89	No error (0)	objects-us-east-1.dream.io		208.113.201.33	A (IP address)	IN (0x0001)
Nov 26, 2020 00:16:20.039973974 CET	8.8.8.8	192.168.2.3	0x44be	No error (0)	gizmoskiff.com		51.15.153.186	A (IP address)	IN (0x0001)
Nov 26, 2020 00:16:20.503166914 CET	8.8.8.8	192.168.2.3	0x960a	No error (0)	luckyxguy.com		111.90.140.95	A (IP address)	IN (0x0001)
Nov 26, 2020 00:16:21.974597931 CET	8.8.8.8	192.168.2.3	0x44be	No error (0)	gizmoskiff.com		51.15.153.186	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- gizmoskiff.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49684	51.15.153.186	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 00:16:20.229384899 CET	16	OUT	GET /qs=r-abacacfekhccacaeikheababacafeadbfaccagjdacjekaibfgjacb 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: gizmoskiff.com Connection: Keep-Alive
Nov 26, 2020 00:16:20.477262020 CET	16	IN	HTTP/1.1 302 Found Date: Wed, 25 Nov 2020 23:16:20 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 X-Powered-By: PHP/5.4.16 location: https://luckyxguy.com/0/0/0/12b675ea62affcf4faac04f5d20e8bdd/37963_1_11/0_1_0_0_1_1439611_43_1839_70458_1_10_582/43/ Content-Length: 0 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8

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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 26, 2020 00:16:18.411511898 CET	208.113.201.33	443	192.168.2.3	49682	CN=*.objects-us-east-1.dream.io CN=USERTrust RSA Domain Validation Secure Server CA, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=USERTrust RSA Domain Validation Secure Server CA, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Jul 21 02:00:00 CEST 2020 Fri Aug 22 02:00:00 CEST 2014 Tue Mar 12 01:00:00 CET 2019	Thu Apr 08 01:59:59 CEST 2021 Wed Aug 22 01:59:59 CEST 2029 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=USERTrust RSA Domain Validation Secure Server CA, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Aug 22 02:00:00 CEST 2014	Wed Aug 22 01:59:59 CEST 2029		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
Nov 26, 2020 00:16:18.413368940 CET	208.113.201.33	443	192.168.2.3	49683	CN=*.objects-us-east-1.dream.io CN=USERTrust RSA Domain Validation Secure Server CA, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=USERTrust RSA Domain Validation Secure Server CA, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Jul 21 02:00:00 CEST 2020 Fri Aug 22 02:00:00 CEST 2014 Tue Mar 12 01:00:00 CET 2019	Thu Apr 08 01:59:59 CEST 2021 Wed Aug 22 01:59:59 CEST 2029 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=USERTrust RSA Domain Validation Secure Server CA, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Aug 22 02:00:00 CEST 2014	Wed Aug 22 01:59:59 CEST 2029		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
Nov 26, 2020 00:16:21.108633995 CET	111.90.140.95	443	192.168.2.3	49687	CN=luckyxguy.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.	Wed Nov 18 20:44:09 CET 2020 Thu Mar 17 17:40:46 CET 2016	Tue Feb 16 20:44:09 CET 2021 Wed Mar 17 17:40:46 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 26, 2020 00:16:21.109360933 CET	111.90.140.95	443	192.168.2.3	49686	CN=luckyxguy.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.	Wed Nov 18 20:44:09 CET 2020 Thu Mar 17 17:40:46 CET 2016	Tue Feb 16 20:44:09 CET 2021 Wed Mar 17 17:40:46 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		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5892 Parent PID: 792

General

Start time:	00:16:15
Start date:	26/11/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff65dd30000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 5936 Parent PID: 5892

General

Start time:	00:16:16
Start date:	26/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5892 CREDAT:17410 /prefetch:2
Imagebase:	0xba0000
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