ID: 241054
Cookbook: browseurl.jbs
Time: 04:12:37
Date: 24/06/2020
Version: 29.0.0 Ocean Jasper

Table of Contents

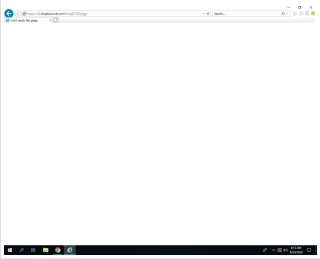
Analysis Report http://laltraimmagine.ss.it/~genio/a53i2....

Overview

General Information

Sample URL:	http://laltraimmagine.ss.it/~genio/a53i2.html

Most interesting Screenshot:



Errors

⚠ URL not reachable

Detection

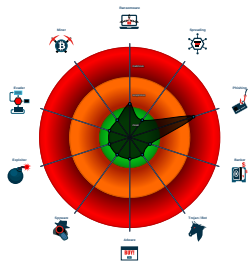
Phisher

Score:	36
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for doma...
- Yara detected Phisher

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 3688 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5028 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3688 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

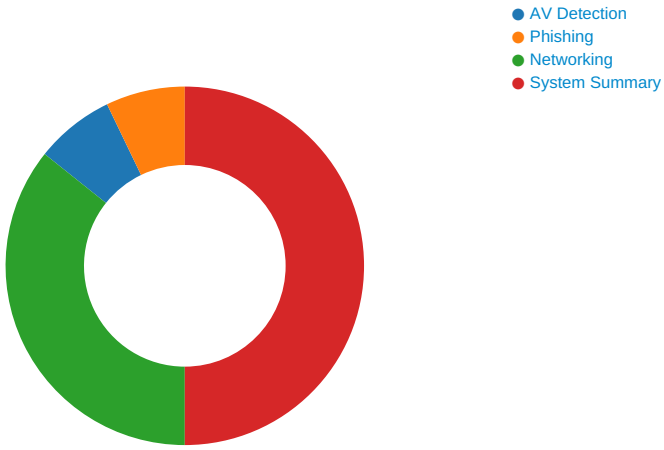
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\5N37O3UG\a53i2[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

AV Detection:

Multi AV Scanner detection for domain / URL

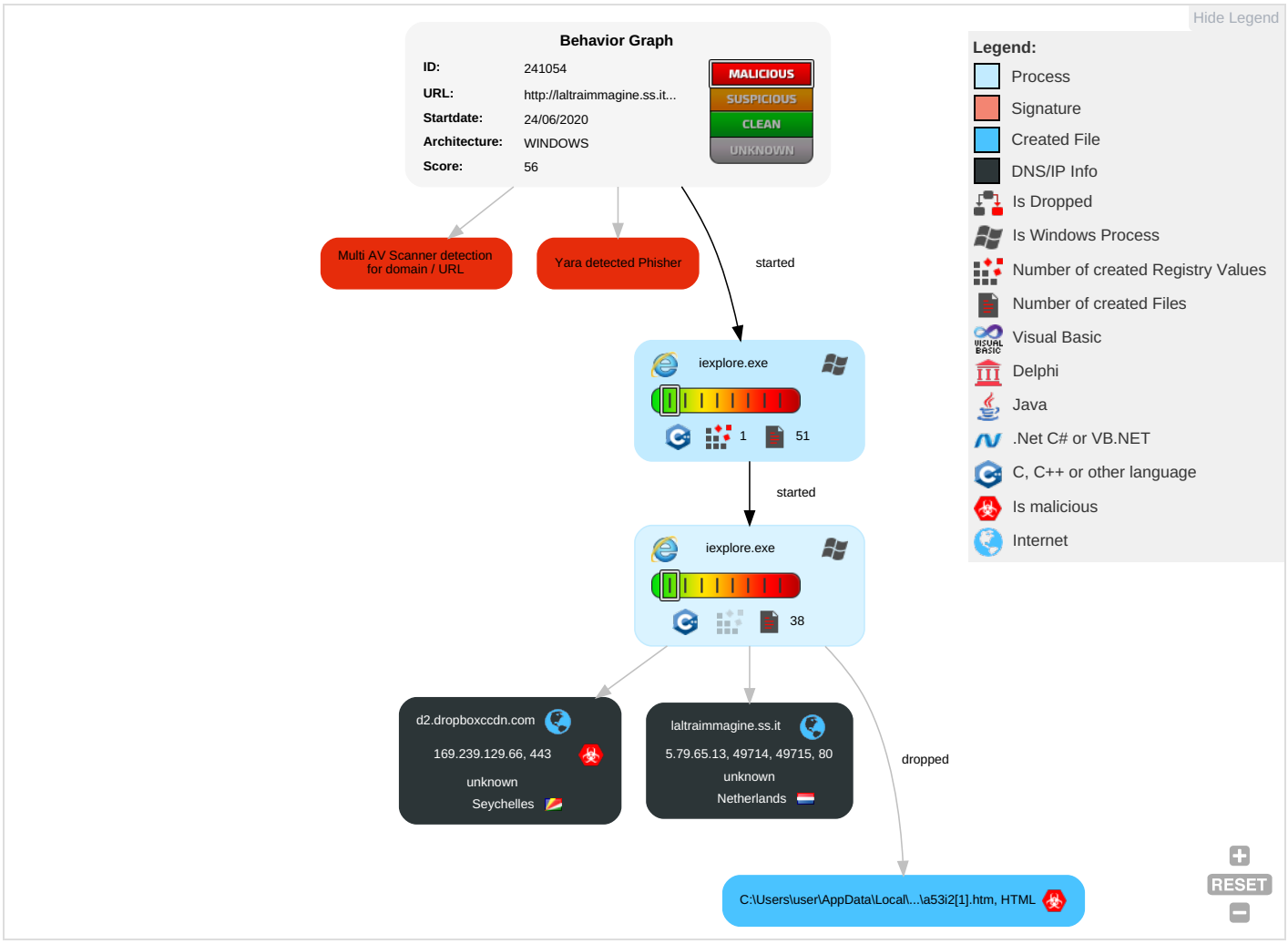
Phishing:

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
Valid Accounts	Graphical User Interface 1	Winlogon Helper DLL	Process Injection 1	Masquerading 1	Credential Dumping	File and Directory Discovery 1	Remote File Copy 2	Data from Local System	Data Compressed	Standard Cryptographic Protocol 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
Replication Through Removable Media	Service Execution	Port Monitors	Accessibility Features	Process Injection 1	Network Sniffing	Application Window Discovery	Remote Services	Data from Removable Media	Exfiltration Over Other Network Medium	Standard Non-Application Layer Protocol 3	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
External Remote Services	Windows Management Instrumentation	Accessibility Features	Path Interception	Rootkit	Input Capture	Query Registry	Windows Remote Management	Data from Network Shared Drive	Automated Exfiltration	Standard Application Layer Protocol 4	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Drive-by Compromise	Scheduled Task	System Firmware	DLL Search Order Hijacking	Obfuscated Files or Information	Credentials in Files	System Network Configuration Discovery	Logon Scripts	Input Capture	Data Encrypted	Remote File Copy 2	SIM Card Swap	

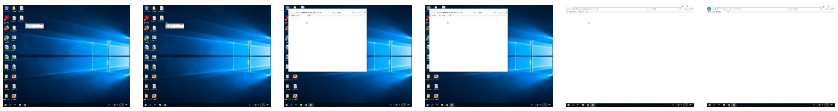
Behavior Graph

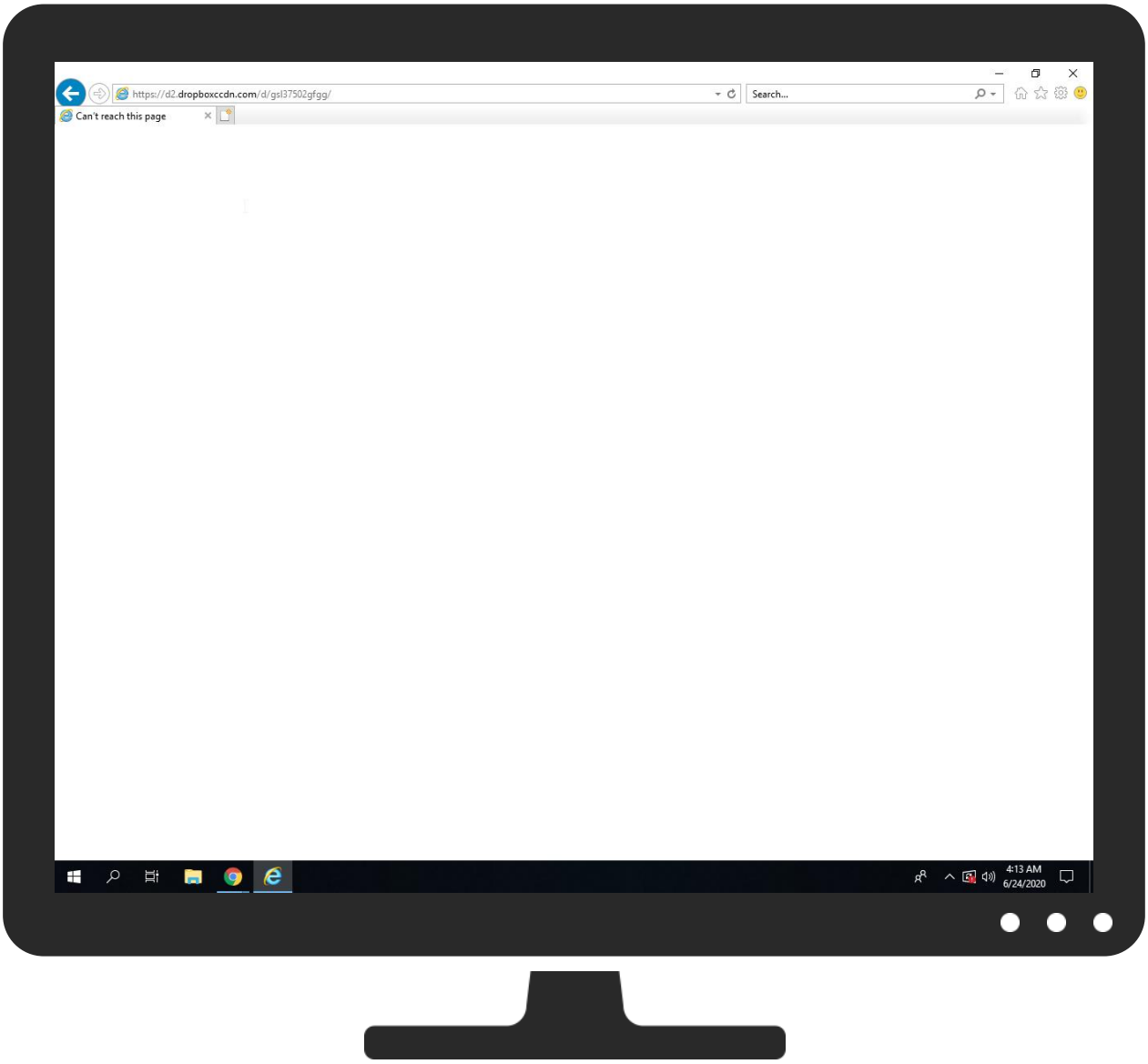


Screenshots

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://laltraimmagine.ss.it/~genio/a53i2.html	0%	Virustotal		Browse
http://laltraimmagine.ss.it/~genio/a53i2.html	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
laltraimmagine.ss.it	0%	Virustotal		Browse
d2.dropboxccdn.com	11%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://laltraimmagine.ss.it/~genio/a53i2.htmlZ.com/d/gsl37502gfgg/lRoot	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://laltraimmagine.ss.it/~genio/a53i2.htmlZRoot	0%	Avira URL Cloud	safe	
http://https://d2.dropboxccdn.com/d/gsl37502gfgg/	10%	Virustotal		Browse
http://https://d2.dropboxccdn.com/d/gsl37502gfgg/	0%	Avira URL Cloud	safe	
http://https://d2.dropboxccdn	0%	Avira URL Cloud	safe	
http://laltraimmagine.ss.it/favicon.ico	0%	Avira URL Cloud	safe	
http://laltraimmagine.ss.it/~genio/a53i2.htmlRoot	0%	Avira URL Cloud	safe	
http://laltraimmagine.ss.it/~genio/a53i2.htmlZhttp://laltraimmagine.ss.it/~genio/a53i2.html	0%	Avira URL Cloud	safe	
http://laltraimmagine.ss.it/~genio/a53i2.htmlZss.it/~genio/a53i2.htmlRoot	0%	Avira URL Cloud	safe	
http://laltraimmagine.ss.it/favicon.ico~	0%	Avira URL Cloud	safe	
http://https://d2.dropboxccdn.com/d/gsl37502gfgg/l	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
laltraimmagine.ss.it	5.79.65.13	true	false	• 0%, Virustotal, Browse	unknown
d2.dropboxccdn.com	169.239.129.66	true	true	• 11%, Virustotal, Browse	unknown

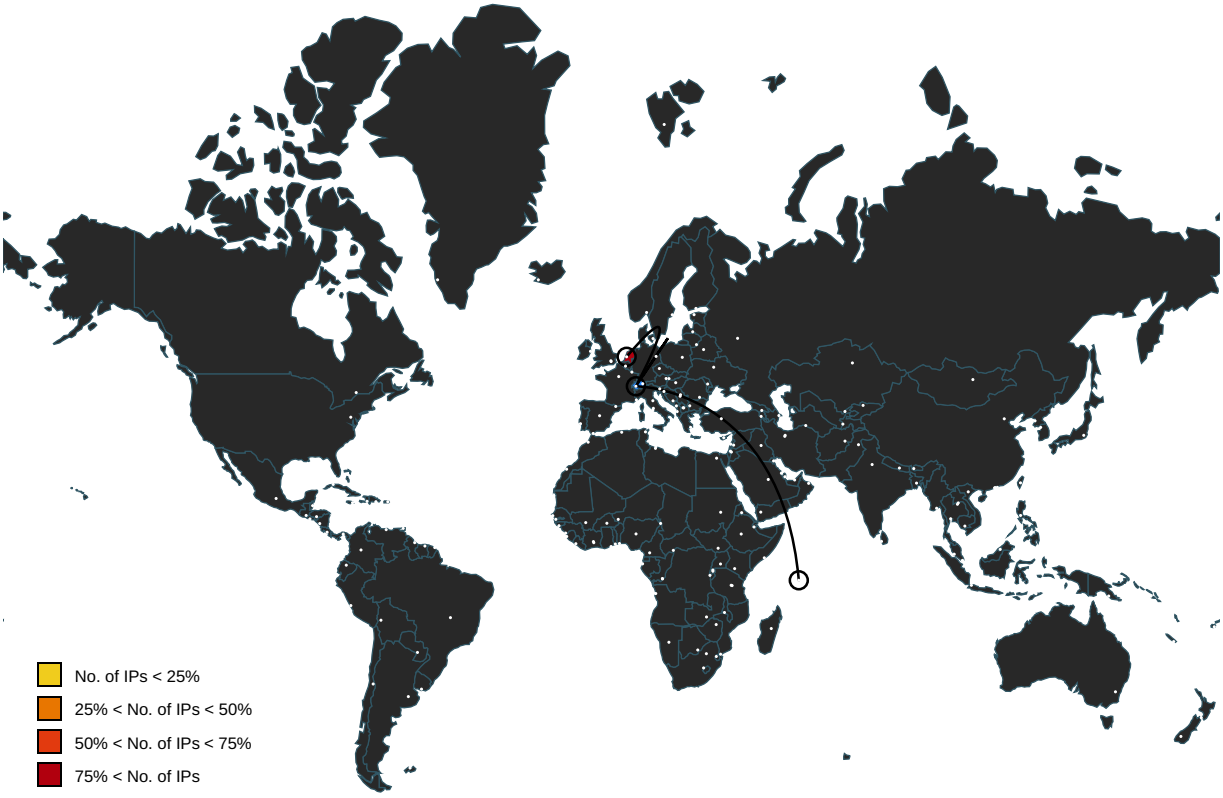
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://laltraimmagine.ss.it/~genio/a53i2.html	false		unknown
http://laltraimmagine.ss.it/favicon.ico	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://laltraimmagine.ss.it/~genio/a53i2.htmlZ.com/d/gsl37502gfgg/lRoot	{3C5B2859-B5C0-11EA-AAE7-9CC1A2A860C6}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://laltraimmagine.ss.it/~genio/a53i2.htmlZRoot	{3C5B2859-B5C0-11EA-AAE7-9CC1A2A860C6}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://d2.dropboxccdn.com/d/gsl37502gfgg/	a53i2[1].htm.2.dr	true	• 10%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://d2.dropboxccdn	{3C5B2859-B5C0-11EA-AAE7-9CC1A2A860C6}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://laltraimmagine.ss.it/~genio/a53i2.htmlRoot	{3C5B2859-B5C0-11EA-AAE7-9CC1A2A860C6}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://laltraimmagine.ss.it/~genio/a53i2.htmlZhttp://laltraimmagine.ss.it/~genio/a53i2.html	~DF247769AC85A63711.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://laltraimmagine.ss.it/~genio/a53i2.htmlZss.it/~genio/a53i2.htmlRoot	{3C5B2859-B5C0-11EA-AAE7-9CC1A2A860C6}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://laltraimmagine.ss.it/favicon.ico~	imagestore.dat.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://d2.dropboxccdn.com/d/gsl37502gfgg/l	~DF247769AC85A63711.TMP.1.dr	true	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Country	Flag	ASN	ASN Name	Malicious
169.239.129.66	Seychelles		61138	unknown	true
5.79.65.13	Netherlands		60781	unknown	false

General Information

Joe Sandbox Version:	29.0.0 Ocean Jasper
Analysis ID:	241054
Start date:	24.06.2020
Start time:	04:12:37
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 1m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://laltraimmagine.ss.it/~genio/a53i2.html
Analysis system description:	Windows 10 64 bit (version 1803) with **Office 2016**, Adobe Reader DC 19, Chrome 70, Firefox 63, Java 8.171, Flash 30.0.0.113
Number of analysed new started processes analysed:	6
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:	• EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal56.phis.win@3/14@3/2
Cookbook Comments:	• Adjust boot time • Enable AMSI • **URL browsing timeout or error**

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, ielowutil.exe, SgrmBroker.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 104.103.98.58, 2.18.68.82 • Excluded domains from analysis (whitelisted): e11290.dspg.akamaiedge.net, go.microsoft.com, fs.microsoft.com, go.microsoft.com.edgekey.net, e1723.g.akamaiedge.net, prod.fs.microsoft.com.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.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.{3C5B2857-B5C0-11EA-AAE7-9CC1A2A860C6}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Size (bytes):	30296
Entropy (8bit):	1.8522608714100992
Encrypted:	false
MD5:	A2BE833E27782917DB2BBF10328BEAD9
SHA1:	16B300E70ED5F94CC3F32266C578B85E60D2D832
SHA-256:	73F07E49AD88086BF672073AA35FCAA5753852B4AB12C43CE720DB73F4435103
SHA-512:	8B723DE4D014856BB09CB41F00B06767F76C8D207DCE8123ED0A6B6855A55EF46341664A4B6250099974ADCE332BA1E706D143BEEBDECF0775EC558D1BE24DE
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{3C5B2857-B5C0-11EA-AAE7-9CC1A2A860C6}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y... ....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{3C5B2859-B5C0-11EA-AAE7-9CC1A2A860C6}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Size (bytes):	34284
Entropy (8bit):	1.8868131425747547
Encrypted:	false
MD5:	062E4BFF982B49F474BB95FA9A0771CC
SHA1:	C6CD0D379D2E3C01F768D7ABCD786683F902EAE6
SHA-256:	CD3CD63ABBFA0180AED23ADC84D941954A9D2B87D0F4D635D72E6667496E57A8
SHA-512:	63FEDE4CBB6FB85665D83E6F46A8F3DCA939C9D77A4692EFB8EE0F7026F6424C1E90ED957B849458C332253927C6290DBB13A9F2EA3C329C39C0169F17B5466
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\{4666282B-B5C0-11EA-AAE7-9CC1A2A860C6}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Size (bytes):	16984
Entropy (8bit):	1.5669451044759182
Encrypted:	false
MD5:	6309BA07400FC885D4C2CD10E7DE354A
SHA1:	E63C422B2D02E5E265A2FB97AADD240FC29BB200
SHA-256:	A0E7A3741CA1BD125D24171FAE9E468E94DE93563F28D6C1CB4EC6A9D86AE3F0
SHA-512:	1BFDECF0C15FBB51D6A1C4C8F490E8D77118D9C1253A8A2F0AC1C0924466FF5F02B00FEE9AB2D3AF90B1C07D972523BF20DB99AC49EF041DCAAFFF6BF94A290
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y... ....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\v8bxa9r\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Size (bytes):	18024
Entropy (8bit):	5.8069155409836135
Encrypted:	false
MD5:	2A57FA22C7B0A4F60AA90AE91180C1B8
SHA1:	0D8CCFB5FC4D519C4AF33383E124EEBB9EC9F2E2
SHA-256:	CA336ABEEAA14E0369E86F93CB0E2F2D83037181FAC3801652E9B8156CB6551B
SHA-512:	D4A33A8DA00BAD81D1E4BDFB9B5B56D8F22E7DEEA17015AF8AECABF16E7DFE6D76F558B501A19BA5B5E88DD41F224AD0EFC7C8E7321BB814714EEF3ED2948A66
Malicious:	false
Reputation:	low
Preview:	'.h.t.t.p.:././.l.a.l.t.r.a.i.m.m.a.g.i.n.e...s.s...i.t./.f.a.v.i.c.o.n...i.c.o..%........00.... ..%......(...0...`..... ......%..@@@.@@@.@@@. @@@+@@@2@@@3@@@3@@@3@@@3@@@3@@@3@@@3@@@3@@@3@@@3@@@3@@@3@@@3@@@3@@@3@@@3 @@@3@@@3@@@3@@@3@@@3@@@3@@@3@@@3@@@3@@@.@@@ @@@...@@@.@@@.@@@N@@@p@@@| @@@~@@@~@@@~@@@~@@@~@@@~@@@~@@@~@@@~@@@~@@@~@@@~@@@~@@@~@@@~@@@~@@@~@@@~ @@@~@@@~@@@~@@@~@@@~@@@~@@@~@@@w@@@]@@@ ....@@@.@@@..M..[..Y..V..T...R...O...N...L..~K..|J..zI.. yH..xH..xG..xG..xG..xG..xH..yH..zI..|J..~K...L...N...O...Q..S..V..Y..[..Q.@@@w@@@.........................@@@.@@@.@@@.@@@.@@@.@@@.@@@.@@@..H.......... ....X.@@@~@@@3@@@.@@@.@@@.@@@.@@@.@@@.@@@.@@@.@@@.@@@ %@@@,@@@3@@@A@@@R.uB..........................

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\5N37O3UG\a53i2[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with no line terminators
Size (bytes):	150
Entropy (8bit):	5.00292094111295

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\5N37O3UG\a53i2[1].htm	
Encrypted:	false
MD5:	17A61C51A518D1BFAB0BD47F8CC70BD6
SHA1:	B324B96B40FEB3EB34318EBA7D7089A016228D6F
SHA-256:	EA221DB01A8686BF340168C42178D8DF66531A01E5105990DEC514748D49F175
SHA-512:	9504FD11BEF8F3076382D833F4C9FF475FE327E5CE61455BD802E5706FA3FC08668149574C22D660A6A6CEC96F1A11525913FC6DA74B9E7274DF0BD2DF8D76B
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Phisher_2, Description: Yara detected Phisher, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\5N37O3UG\a53i2[1].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://laltraimmagine.ss.it/~genio/a53i2.html
Preview:	<head/><script type="text/javascript">var delay=0000;setTimeout("document.location.href='https://d2.dropboxccdn.com/d/gsl37502gfgg/'",delay);</script>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\5N37O3UG\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
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/dnserror.htm?ErrorStatus=0x800C0005&DNSError=0
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMoreInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\5N37O3UG\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
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\O0N4T4W6\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 4 icons, 48x48, 32 bits/pixel, 32x32, 32 bits/pixel
Size (bytes):	17542
Entropy (8bit):	5.81165239030264
Encrypted:	false
MD5:	DCEA02A5797CE9E36F19B7590752563E
SHA1:	39C5523F02F3F3F164F2CCB2B42DAF225644129B
SHA-256:	BDA29A52D3518EE35A06C77639C02879CBA30D3B20953D7BEE2F2349DC0F67E5
SHA-512:	C9C050E95EEEA02C42B82EAB99820F378BCE6145842A177D73A3A3DF2470C049CAE5E9BAE0F578723F62C0E13FEAF5AF64B21052F88D031B5720D3852130E29
Malicious:	false
Reputation:	low
IE Cache URL:	http://laltraimmagine.ss.it/favicon.ico

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\O0N4T4W6\favicon[1].ico	
Preview:	......00.... ..%..F... ....%........ ......6........ .h....@..(...0...`..... ......%..@@@.@@@.@@@.@@@+@@@2@@@3@@@3 @@@3@@@3@@@3@@@3@@@3@@@3@@@3@@@3@@@3@@@3@@@3@@@3@@@3@@@3@@@3@@@3@@@3@@@3@@@3 @@@3@@@3@@@3@@@3@@@3@@@.@@@ @@@..@@@.@@@.@@@N@@@p@@@|@@@~@@@~@@@~@@@~ @@@~ @@@~@@@~@@@~@@@w@@@]@@@ ....@@@.@@@..M..[..Y..V..T...R...O...N...L..~K..|J..zI..yH..xH..xG..xG..xG..xH..yH..zI.. |J..~K...L...N...O...Q..S..V..Y..[..Q.@@@w@@@.........................@@@.@@@.@@@.@@@.@@@.@@@.@@@.@@@..H.. ....X.@@@~@@@3@@@.@@@.@@@.@@@.@@@.@@@.@@@.@@@.@@@.@@@%@@@,@@@3@@@A@@@R.uB...... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\O0N4T4W6\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
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\Microsoft\Windows\INetCache\IE\P24S97MI\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284FD
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/NewErrorPageTemplate.css
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt; ..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PKAQFTEH\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/errorPageStrings.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PKAQFTEH\errorPageStrings[1]	
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 website you are trying to visit.";..var L

C:\Users\user\AppData\Local\Temp\~DF247769AC85A63711.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Size (bytes):	43493
Entropy (8bit):	0.7953826637621513
Encrypted:	false
MD5:	5378F92FEC38A219EE02E40699E61854
SHA1:	0E7823636C219485DB7C93E14B80B638ACC757BA
SHA-256:	71569AAC29FD0F4094C3EEFBB6A14A25F03F93BD098805918B57F6BED9C41139
SHA-512:	EB54DB373ED45F88A5AE80AB3B34E9600F3B6664177F6A1EC68D242128B8D27006841E8C697407C2B8D5A681A0F00DD13879379DAB42E8377FEBAE03D9593FD
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF4DB819B4189A5210.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Size (bytes):	13029
Entropy (8bit):	0.481069220318935
Encrypted:	false
MD5:	987658F9EE88BD835CEEDBE2A59E715D
SHA1:	2E8F78B9B1BFD7D4A4D183FF4C7F991A6392F806
SHA-256:	A982B227E0D7A050DC2F3811DF680D362F404FBD9E61AA6EA424BB1FA58B814C
SHA-512:	D4F7DCB6C7FC0F6DB1967B66DCC4249759DEE919B9BF6D323BE258234DB05EA8C8A4BDB3A54F7DC5EEDD7A236828A8E657431AA5DBD4E69E1B70EA9398DB84D
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

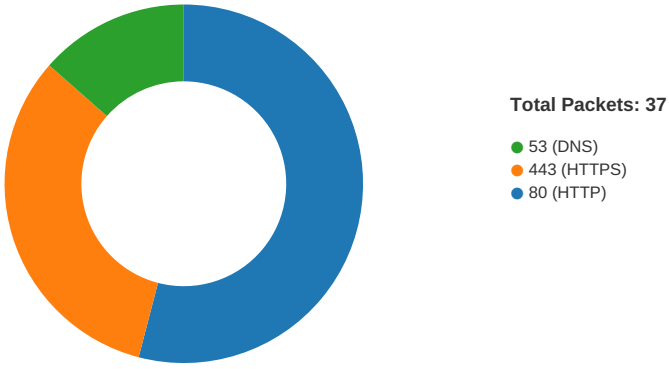
C:\Users\user\AppData\Local\Temp\~DFE95E197F59997B4F.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Size (bytes):	25441
Entropy (8bit):	0.2885839700600326
Encrypted:	false
MD5:	C969501A46040166207B410170802083
SHA1:	680C9F543B3B2D06B58678C66F83220853BF25EB
SHA-256:	98E0DBFAE12734E4BCFFEC5A718335A7A1557E5BA43363BCF276C6A29FBB9052
SHA-512:	C4B7899156AA1C65C7CADE0D534C305E3B76B85074DB789B520B5B4123AE09771141CAA571AF2974AAC418458D4FAF567DC48938EC57D79972B07627F2285A7I
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
Jun 24, 2020 04:13:06.970482111 CEST	49714	80	192.168.2.6	5.79.65.13
Jun 24, 2020 04:13:06.971950054 CEST	49715	80	192.168.2.6	5.79.65.13
Jun 24, 2020 04:13:06.997503996 CEST	80	49714	5.79.65.13	192.168.2.6
Jun 24, 2020 04:13:06.997709990 CEST	49714	80	192.168.2.6	5.79.65.13
Jun 24, 2020 04:13:06.998475075 CEST	80	49715	5.79.65.13	192.168.2.6
Jun 24, 2020 04:13:06.998591900 CEST	49715	80	192.168.2.6	5.79.65.13
Jun 24, 2020 04:13:07.003498077 CEST	49714	80	192.168.2.6	5.79.65.13
Jun 24, 2020 04:13:07.030220032 CEST	80	49714	5.79.65.13	192.168.2.6
Jun 24, 2020 04:13:07.033560038 CEST	80	49714	5.79.65.13	192.168.2.6
Jun 24, 2020 04:13:07.033586979 CEST	80	49714	5.79.65.13	192.168.2.6
Jun 24, 2020 04:13:07.033674955 CEST	49714	80	192.168.2.6	5.79.65.13
Jun 24, 2020 04:13:07.043056011 CEST	49714	80	192.168.2.6	5.79.65.13
Jun 24, 2020 04:13:07.069766045 CEST	80	49714	5.79.65.13	192.168.2.6
Jun 24, 2020 04:13:07.485191107 CEST	49715	80	192.168.2.6	5.79.65.13
Jun 24, 2020 04:13:07.511811972 CEST	80	49715	5.79.65.13	192.168.2.6
Jun 24, 2020 04:13:07.512896061 CEST	80	49715	5.79.65.13	192.168.2.6
Jun 24, 2020 04:13:07.512985945 CEST	80	49715	5.79.65.13	192.168.2.6
Jun 24, 2020 04:13:07.513062000 CEST	49715	80	192.168.2.6	5.79.65.13
Jun 24, 2020 04:13:07.513161898 CEST	49715	80	192.168.2.6	5.79.65.13
Jun 24, 2020 04:13:07.513169050 CEST	80	49715	5.79.65.13	192.168.2.6
Jun 24, 2020 04:13:07.513283014 CEST	49715	80	192.168.2.6	5.79.65.13
Jun 24, 2020 04:13:07.513360023 CEST	80	49715	5.79.65.13	192.168.2.6
Jun 24, 2020 04:13:07.513463974 CEST	49715	80	192.168.2.6	5.79.65.13
Jun 24, 2020 04:13:07.513534069 CEST	80	49715	5.79.65.13	192.168.2.6
Jun 24, 2020 04:13:07.513559103 CEST	80	49715	5.79.65.13	192.168.2.6
Jun 24, 2020 04:13:07.513633966 CEST	49715	80	192.168.2.6	5.79.65.13
Jun 24, 2020 04:13:07.513715029 CEST	80	49715	5.79.65.13	192.168.2.6
Jun 24, 2020 04:13:07.513806105 CEST	49715	80	192.168.2.6	5.79.65.13
Jun 24, 2020 04:13:07.513904095 CEST	80	49715	5.79.65.13	192.168.2.6
Jun 24, 2020 04:13:07.513921022 CEST	80	49715	5.79.65.13	192.168.2.6
Jun 24, 2020 04:13:07.514012098 CEST	49715	80	192.168.2.6	5.79.65.13
Jun 24, 2020 04:13:07.514086008 CEST	80	49715	5.79.65.13	192.168.2.6
Jun 24, 2020 04:13:07.514206886 CEST	49715	80	192.168.2.6	5.79.65.13
Jun 24, 2020 04:13:07.539805889 CEST	80	49715	5.79.65.13	192.168.2.6
Jun 24, 2020 04:13:07.539918900 CEST	80	49715	5.79.65.13	192.168.2.6
Jun 24, 2020 04:13:07.540021896 CEST	49715	80	192.168.2.6	5.79.65.13
Jun 24, 2020 04:13:07.540103912 CEST	80	49715	5.79.65.13	192.168.2.6
Jun 24, 2020 04:13:07.540124893 CEST	80	49715	5.79.65.13	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 24, 2020 04:13:07.540124893 CEST	49715	80	192.168.2.6	5.79.65.13
Jun 24, 2020 04:13:07.540143967 CEST	80	49715	5.79.65.13	192.168.2.6
Jun 24, 2020 04:13:07.540215015 CEST	49715	80	192.168.2.6	5.79.65.13
Jun 24, 2020 04:13:07.541250944 CEST	49715	80	192.168.2.6	5.79.65.13
Jun 24, 2020 04:13:07.567760944 CEST	80	49715	5.79.65.13	192.168.2.6
Jun 24, 2020 04:13:07.965075016 CEST	49716	443	192.168.2.6	169.239.129.66
Jun 24, 2020 04:13:07.966381073 CEST	49717	443	192.168.2.6	169.239.129.66
Jun 24, 2020 04:13:08.967411041 CEST	49717	443	192.168.2.6	169.239.129.66
Jun 24, 2020 04:13:08.967464924 CEST	49716	443	192.168.2.6	169.239.129.66
Jun 24, 2020 04:13:10.972830057 CEST	49717	443	192.168.2.6	169.239.129.66
Jun 24, 2020 04:13:10.974353075 CEST	49716	443	192.168.2.6	169.239.129.66
Jun 24, 2020 04:13:14.996269941 CEST	49718	443	192.168.2.6	169.239.129.66
Jun 24, 2020 04:13:14.996342897 CEST	49719	443	192.168.2.6	169.239.129.66
Jun 24, 2020 04:13:15.989494085 CEST	49718	443	192.168.2.6	169.239.129.66
Jun 24, 2020 04:13:15.989558935 CEST	49719	443	192.168.2.6	169.239.129.66
Jun 24, 2020 04:13:17.994159937 CEST	49718	443	192.168.2.6	169.239.129.66
Jun 24, 2020 04:13:17.994204044 CEST	49719	443	192.168.2.6	169.239.129.66

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 24, 2020 04:13:05.177968979 CEST	50342	53	192.168.2.6	8.8.8.8
Jun 24, 2020 04:13:05.213182926 CEST	53	50342	8.8.8.8	192.168.2.6
Jun 24, 2020 04:13:06.904500008 CEST	57707	53	192.168.2.6	8.8.8.8
Jun 24, 2020 04:13:06.953644037 CEST	53	57707	8.8.8.8	192.168.2.6
Jun 24, 2020 04:13:07.632426977 CEST	51048	53	192.168.2.6	8.8.8.8
Jun 24, 2020 04:13:07.962373018 CEST	53	51048	8.8.8.8	192.168.2.6
Jun 24, 2020 04:13:22.018345118 CEST	60693	53	192.168.2.6	8.8.8.8
Jun 24, 2020 04:13:22.033348083 CEST	60308	53	192.168.2.6	8.8.8.8
Jun 24, 2020 04:13:22.066993952 CEST	53	60308	8.8.8.8	192.168.2.6
Jun 24, 2020 04:13:22.072098970 CEST	53	60693	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 24, 2020 04:13:06.904500008 CEST	192.168.2.6	8.8.8.8	0x7906	Standard query (0)	laltraimmagine.ss.it	A (IP address)	IN (0x0001)
Jun 24, 2020 04:13:07.632426977 CEST	192.168.2.6	8.8.8.8	0x9815	Standard query (0)	d2.dropboxccdn.com	A (IP address)	IN (0x0001)
Jun 24, 2020 04:13:22.033348083 CEST	192.168.2.6	8.8.8.8	0xe396	Standard query (0)	d2.dropboxccdn.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 24, 2020 04:13:06.953644037 CEST	8.8.8.8	192.168.2.6	0x7906	No error (0)	laltraimmagine.ss.it		5.79.65.13	A (IP address)	IN (0x0001)
Jun 24, 2020 04:13:07.962373018 CEST	8.8.8.8	192.168.2.6	0x9815	No error (0)	d2.dropboxccdn.com		169.239.129.66	A (IP address)	IN (0x0001)
Jun 24, 2020 04:13:22.066993952 CEST	8.8.8.8	192.168.2.6	0xe396	No error (0)	d2.dropboxccdn.com		169.239.129.66	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- laltraimmagine.ss.it

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49714	5.79.65.13	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Jun 24, 2020
04:13:07.003498077 CEST</td><td>1</td><td>OUT</td><td>GET /~genio/a53i2.html 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: laltraimmagine.ss.it
Connection: Keep-Alive</td></tr>
<tr><td>Jun 24, 2020
04:13:07.033560038 CEST</td><td>2</td><td>IN</td><td>HTTP/1.1 200 OK
Date: Wed, 24 Jun 2020 02:13:07 GMT
Server: Apache
Accept-Ranges: bytes
X-Mod-Pagespeed: 1.13.35.2-0
X-Powered-By: PleskLin
Vary: Accept-Encoding
Content-Encoding: gzip
Cache-Control: max-age=0, no-cache, s-maxage=10
Content-Length: 146
Connection: close
Content-Type: text/html
Data Raw: 1f 8b 08 00 00 00 00 00 00 03 25 8d 5b 0a 83 30 10 00 af 22 f9 b1 85 92 15 4b 29 d4 c7 29 bc 40 9a 5d a3 c5 64 43 b2 8a de be a5 ce e7 7c cc b4 13 19 84 be cd 36 cd 51 0a 39 22 75 4a 68 17 f8 98 cd 9c 56 f5 9b 49 05 d2 62 8e ae fa d1 64 92 61 f6 c4 ab 5c 14 b2 5d 3d 05 d1 0b 5b 23 33 07 3d 25 1a bb 72 12 89 f9 05 80 b5 c6 c4 f1 cd bb b5 18 b4 65 0f 08 2e 2f f7 e7 a3 aa dd e8 1c 94 ea f6 6f 5f 9b 16 ce 61 ff 05 ae 40 cd 53 96 00 00 00
Data Ascii: %[0"K))@]dC|6Q9"uJhVIbda\]=[#3=%re./o_a@S</td></tr>
</table>

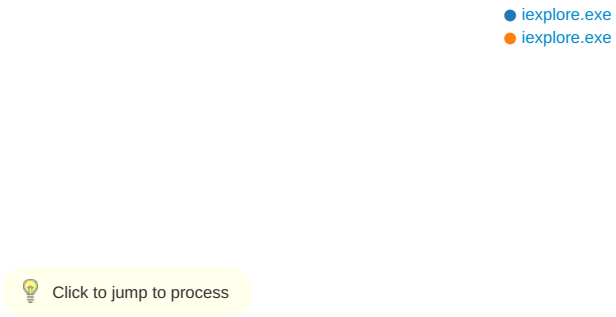
<table>
<tr><th>Session ID</th><th>Source IP</th><th>Source Port</th><th>Destination IP</th><th>Destination Port</th><th>Process</th></tr>
<tr><td>1</td><td>192.168.2.6</td><td>49715</td><td>5.79.65.13</td><td>80</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
</table>

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Jun 24, 2020
04:13:07.485191107 CEST</td><td>2</td><td>OUT</td><td>GET /favicon.ico HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: laltraimmagine.ss.it
Connection: Keep-Alive</td></tr>
<tr><td>Jun 24, 2020
04:13:07.512896061 CEST</td><td>4</td><td>IN</td><td>HTTP/1.1 200 OK
Date: Wed, 24 Jun 2020 02:13:07 GMT
Server: Apache
Last-Modified: Fri, 28 May 2010 22:33:46 GMT
ETag: "4be114a-4486-487af19a34680"
Accept-Ranges: bytes
Content-Length: 17542
X-Powered-By: PleskLin
Cache-Control: s-maxage=10
Connection: close
Content-Type: image/vnd.microsoft.icon
Data Raw: 00 00 01 00 04 00 30 30 00 00 01 00 20 00 a8 25 00 00 46 00 00 00 20 20 00 00 01 00 20 00 a8 10 00 00 ee 25 00 00 18 18 00 00 01 00 20 00 88 09 00 00 96 36 00 00 10 10 00 00 01 00 20 00 68 04 00 00 1e 40 00 00 28 00 00 00 30 00 00 00 60 00 00 00 01 00 20 00 00 00 00 00 80 25 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 40 40 03 40 40 40 0e 40 40 40 1c 40 40 40 2b 40 40 40 32 40 40 40 33 40 40 40 2e 40 40 40 20 40 40 40 12 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 40 40 04 40 40 40 19 40 40 40 4e 40 40 40 70 40 40 40 7c 40 40 40 7e 40 40 40 7e 40 40 40 7e 40 40 40 7e 40 40 40 7e 40 40 40 7e 40 40 40 7e 40 40 40 7e 40 40 40 7e 40 40 40 7e 40 40 40 7e 40 40 40 7e 40 40 40 7e 40 40 40 7e 40 40 40 7e 40 40 40 7e 40 40 40 7e 40 40 40 7e 40 40 40 7e 40 40 40 7e 40 40 40 7e 40 40 40 7e 40 40 40 7e 40 40 40 7e 40 40 40 7e 40 40 40 7e 40 40 40 77 40 40 40 5d 40 40 40 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 40 40 02 40 40 40 09 e6 8a 4d c9 f1 97 5b ff f1 93 59 ff f1 8f 56 ff f1 8b 54 ff f0 88 52 ff f0 85 4f ff f0 82 4e ff f0 80 4c ff f0 7e 4b ff f0 7c 4a ff f0 7a 49 ff f0 79 48 ff f0 78 48 ff f0 78 47 ff f0 78 47 ff f0 78 47 ff f0 78 47 ff f0 78 48 ff f0 79 48 ff f0 7a 49 ff f0 7c 4a ff f0 7e 4b ff f0 80 4c ff f0 82 4e ff f0 85 4f ff f0 88 51 ff f1 8b 53 ff f1 8e 56 ff f1 93 59 ff f1 97 5b ff f0 90 51 ff 40 40 40 77 40 40 40 2e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 40 40 01 40 40 40 02 40 40 40 04 40 40 40 07 40 40 40 09 40 40 40 0d 40 40 40 12 40 40 40 1f e1 81 48 cf f7 ba 90 ff fb d9 c1 ff fb d9 c1 ff fb d9 c1 ff fb d9 c1 ff fb d9 c1 ff fb d9 c1 ff fb d9 c1 ff fb d9 c1 ff fb d9 c1 ff fb d9 c1 ff fb d9 c1 ff fb d9 c1 ff fb d9 c1 ff fb d9 c1 ff fb d9 c1 ff fb d9 c1 ff fb d9 c1 ff fb d9 c1 ff fb d9 c1 ff fb d9 c1 ff fb d9 c1 ff fb d9 c1 ff fb d9 c1 ff fb d9 c1 ff fb d9 c1 ff fb d9 c1 ff f9 c4 a1 ff f1 91 58 ff 40 40 40 7e 40 40 40 33 40 40 40 01 40 40 40 02 40 40 40 04 40 40 40 06 40 40 40 08 40 40 40 0a 40 40 40 0f 40 40 40 16 40 40 40 1d 40 40 40 25 40 40 40 2c 40 40 40 33 40 40 40 41 40 40 40 52 d9 75 42 da f8 b9 8f ff fe f4 d5 ff fe f5 d7 ff fe f5 d8 ff fe f5 da ff fe f6 dc ff fe f6 dd ff fe f7 de ff fe f7 df ff fe f7 e0 ff fe f7 e1 ff fe f7 e1 ff fe f7 e2 ff fe f7 e2 ff fe f7 e2 ff fe f7 e2 ff fe f7 e2 ff fe f7 e2 ff fe f7 e1 ff fe f7 e1 ff fe f7 e0 ff fe f7 df ff fe f6 df ff fe f6 dd ff fe f6 dc ff fe f5 db ff fe f5 d9 ff fe f5
Data Ascii: 00 %F   % 6 h@(0` %@@@@@@@@@@@@@+@@@2@@@3@@@3@@@3@@@3@@@3@@
@3@@@3@@@3@@@3@@@3@@@3@@@3@@@3@@@3@@@3@@@3@@@3@@@3@@@3@@@3@@
@3@@@3@@@3@@@3@@@3@@@3@@@3@@@.@@@ @@@@@@@@@@@@@@N@@@p@@@|@@@~@
@@~@@@~@@@~@@@~@@@~@@@~@@@~@@@~@@@~@@@~@@@~@@@~@@@
~@@@~@@@~@@@~@@@~@@@~@@@~@@@~@@@~@@@~@@@~@@@~@@@~@
@@~@@@w@@@]@@@ @@@@@@M[YVTRONL~K|JzIyHxHxGxGxGxGxHyHzI|J~KLNOQSVY[Q@@@
w@@@.@@@@@@@@@@@@@@@@@@@@@@@@@HX@@@~@@@3@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@%@@@,@@@3@@@A@@@RuB</td></tr>
</table>

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: iexplore.exe PID: 3688 Parent PID: 696

General

Start time:	04:13:04
Start date:	24/06/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff6a3400000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 5028 Parent PID: 3688

General

Start time:	04:13:05
Start date:	24/06/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3688 CREDAT:17410 /prefetch:2
Imagebase:	0x2b0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly