ID: 383821
Cookbook: browseurl.jbs
Time: 10:32:22
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

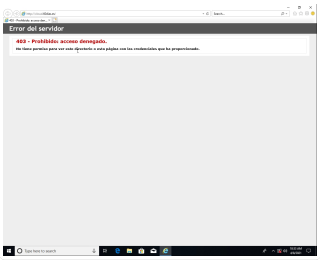
Analysis Report http://cloud.60dias.es

Overview

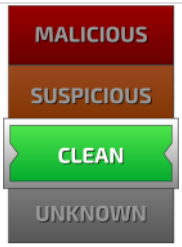
General Information

Sample URL:	http://cloud.60dias.es
Analysis ID:	383821
Infos:	

Most interesting Screenshot:



Detection

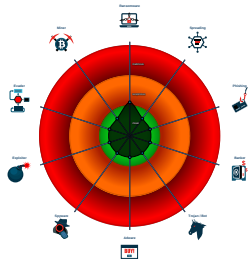


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 5828 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 1056 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5828 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

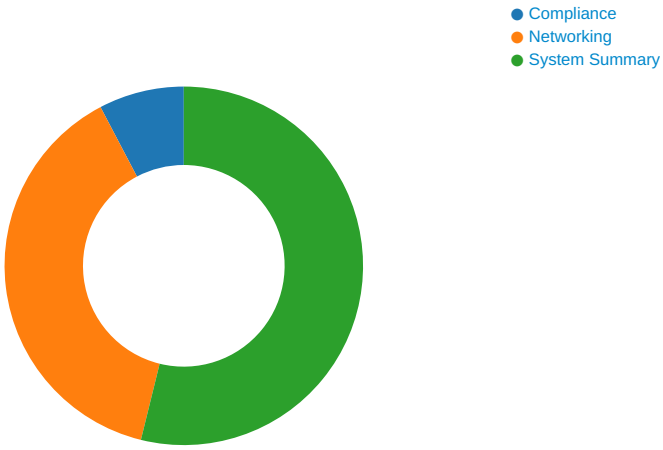
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



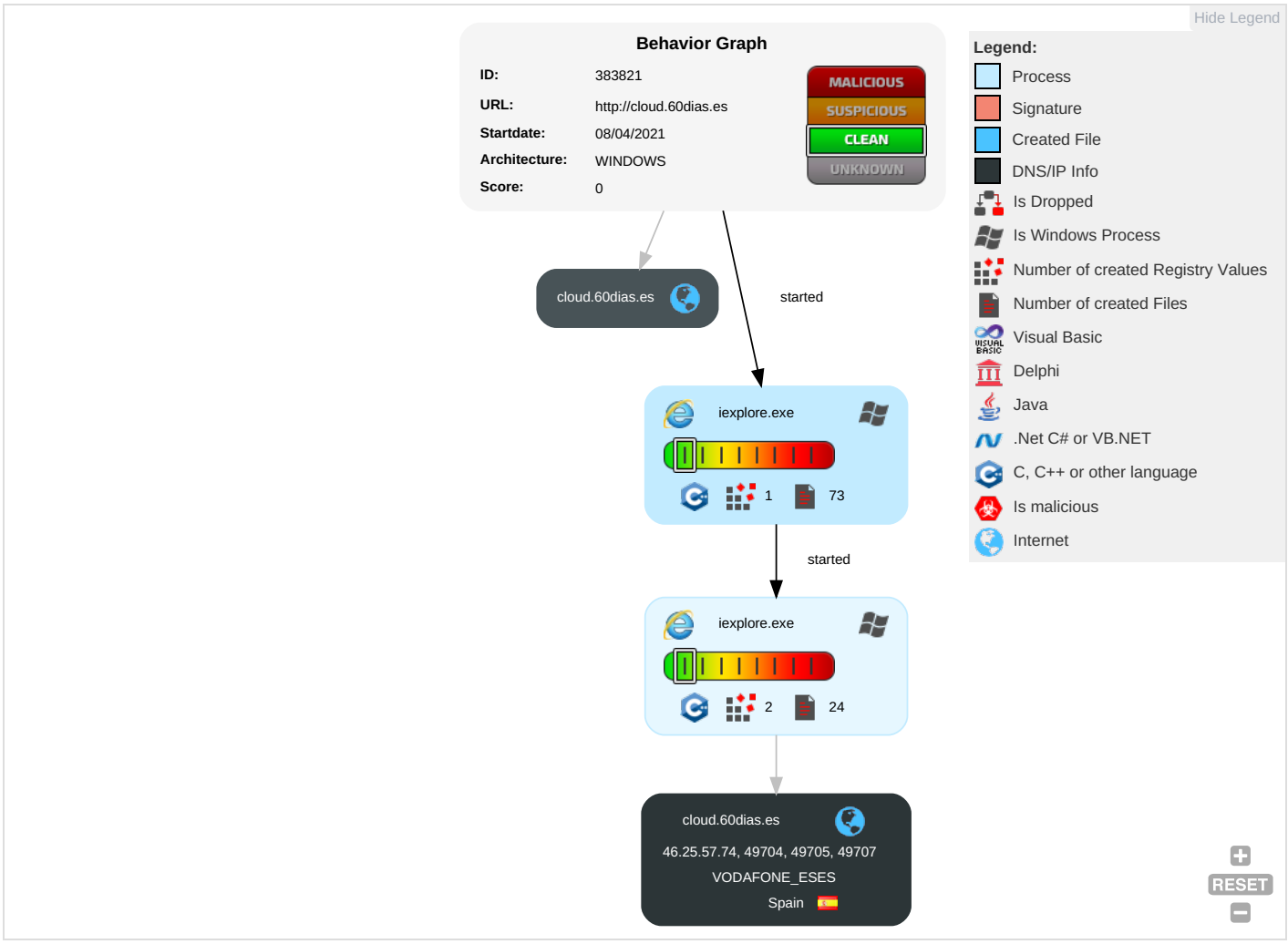
Click to jump to signature section

There are no malicious signatures, click here to show all signatures.

Mitre Att&ck Matrix

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

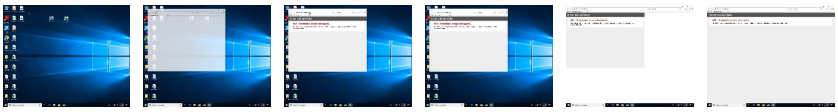
Behavior Graph

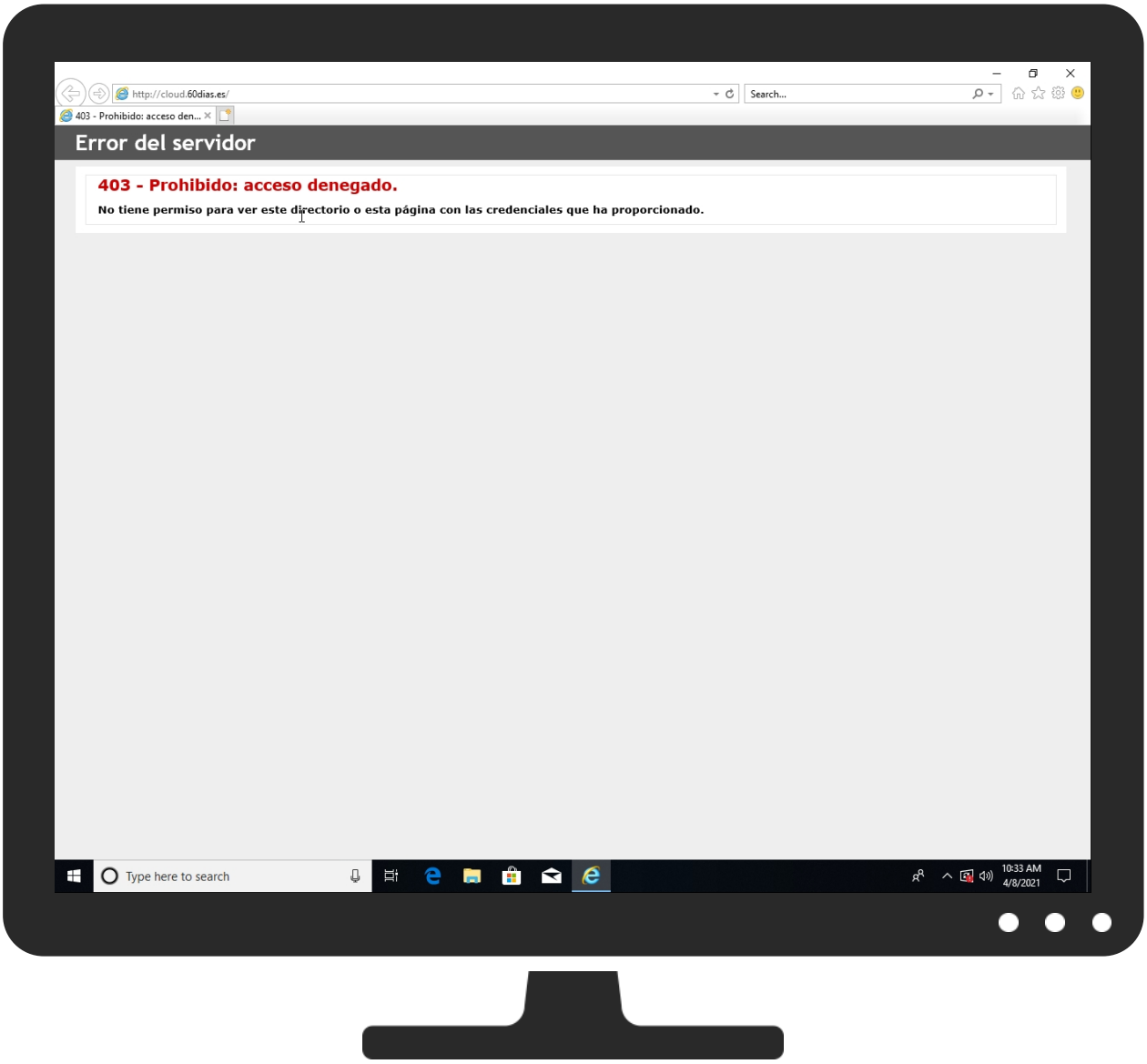


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://cloud.60dias.es	0%	Virustotal		Browse
http://cloud.60dias.es	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.wikipedia.com/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cloud.60dias.es	46.25.57.74	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://cloud.60dias.es/	false		high
http://cloud.60dias.es/favicon.ico	false		high
http://cloud.60dias.es/	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.wikipedia.com/	msapplication.xml6.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.amazon.com/	msapplication.xml.1.dr	false		high
http://www.nytimes.com/	msapplication.xml3.1.dr	false		high
http://www.live.com/	msapplication.xml2.1.dr	false		high
http://www.reddit.com/	msapplication.xml4.1.dr	false		high
http://www.twitter.com/	msapplication.xml5.1.dr	false		high
http://www.youtube.com/	msapplication.xml7.1.dr	false		high
http://cloud.60dias.es/Root	{0A7BCE5F-9845-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
46.25.57.74	cloud.60dias.es	Spain		12430	VODAFONE_ESES	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383821
Start date:	08.04.2021
Start time:	10:32:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://cloud.60dias.es
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:	3
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:	CLEAN
Classification:	clean0.win@3/15@2/1
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): ielowutil.exe • Excluded IPs from analysis (whitelisted): 13.88.21.125, 104.43.193.48, 104.83.120.32, 13.64.90.137, 152.199.19.161 • Excluded domains from analysis (whitelisted): e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, skypedataprdcolwus17.cloudapp.net, go.microsoft.com, ie9comview.vo.msecnd.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, watson.telemetry.microsoft.com, skypedataprdcolwus15.cloudapp.net, skypedataprdcolcus15.cloudapp.net, cs9.wpc.v0cdn.net

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.{0A7BCE5D-9845-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.855444716283116
Encrypted:	false
SSDEEP:	192:raZdZW2gWDtVifHnpzMiBBcbDLsfVnkjX:rGTt3h6+QOWq
MD5:	2E8FE54A21400BD43B416EB665B827AE
SHA1:	8D0F3B4ABC4A71A5653F8DE6297504C3467F3AA5
SHA-256:	7A27D1044446C09E3FC28D58F57CB6835877179448BE8466B86D4D89C2FE8B82
SHA-512:	042BDD41AE375A1739C9EF4B398A8A14DC30B02BD489616FF8C8A714B06AB38D5CE297DCE9DF5677269CA49BA453371B2491D1F8770D6B7A46D4EE382C20ED1
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\{0A7BCE5F-9845-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24156
Entropy (8bit):	1.6273384035903418
Encrypted:	false
SSDEEP:	48:Iw3GcprCGwpaiG4pQmGrapbSNjGQpByGHHpcc5ETGUp8+GzYpms+QGopq+PsGuXg:r9ZqQS6oBSNdjJ2i8WyMVQgBg
MD5:	ECAB6481D3C63E5D0A445AD805ADB67E
SHA1:	E3093A1EE9DC8361E3DF993EEE05D33B74B96A3C
SHA-256:	C66A89F7678394F46A9E8A752E7085406253457BFB568256DF75CFFEE79B9CEF
SHA-512:	311E3F6AD2139D7150AD81D8408E1FD7FCDEE00C07FD13E3F2EF0481B91BA119EA8321CBE805C7D5946A3B69D5CF7E53B2F16BA5CA7521D55FD707B58427894
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\{0A7BCE60-9845-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{0A7BCE60-9845-11EB-90EB-ECF4BBEA1588}.dat	
Size (bytes):	16984
Entropy (8bit):	1.5667901292330468
Encrypted:	false
SSDEEP:	48:Iw/GcprSGwpabG4pQ/GrapbSEjGQpKuG7HpRYETGIpG:rVZaQ96DBSEdApTYAA
MD5:	661F4EA6FF904A17BD7C7435B9A1F258
SHA1:	20223488A89C7DBBA9629EED0D93833343FEDB53
SHA-256:	E4E7FEF14B9E80BE64416A33038E4327D278CE1943287955BD41D0E731CFD2F2
SHA-512:	66CE2603267E2A8E1A1B32A2F85F343D84C85C8C4E741DDBDE71CDB81F9071FA9394BBDC9F276867440F8A3456D3D16EE551265A72396D2A79BA6F1D76BED18A
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r.y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.0546905665623205
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEFLlnWimI002EtM3MHdNMNxOEFLlnWimI00OYGVbkEtMb:2d6NxOiSZHKd6NxOiSZ7YLb
MD5:	315A7C88A86E63674B43B3C607996F33
SHA1:	526F9F51297272C487DAE578F8B9BF0EA2C34718
SHA-256:	92A83C8307FA28A54548DB820BA0A9724D650AB733F17CCBA634151060575E74
SHA-512:	B4D02466CE22F2CB8C78F3CB215B2945F339BC5ABB9F2E93F11542713A003A6DB4722D03B2BFB96141A7D6A72CF4AF2294C747F5260C6D786BEB435FF0BD650
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xe02732e3,0x01d72c51</date><accdate>0xe02732e3,0x01d72c51</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xe02732e3,0x01d72c51</date><accdate>0xe02732e3,0x01d72c51</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.0949461064970425
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kzibowibownWimI002EtM3MHdNMNxe2kzibowibownWimI00OYGkan:2d6NxrLboRbowSZHKd6NxrLboRbowSZN
MD5:	805834ED2EE4860055521D07335F15FF
SHA1:	30CC4D172C388AE4F3F64DB0203B19B70455A5E3
SHA-256:	7BEC3CB27FD346107BE337D7E304DAFEAE798AA2483DFF57A73D7D58838DE399
SHA-512:	0F5346832390534943 68AC5FAF621B225A70A19EA46C6665ED3045EAA0544B837FE146AA1A1E63044BC247E3D70669BC276BB7B6086CBF1AD620DC50DDDA91E
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xe0200b74,0x01d72c51</date><accdate>0xe0200b74,0x01d72c51</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xe0200b74,0x01d72c51</date><accdate>0xe0200b74,0x01d72c51</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	662
Entropy (8bit):	5.105747861492968
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLF5J3nWimI002EtM3MHdNMNxvLF41BwnWimI00OYGmZEtMb:2d6NxvNSZHKd6Nxv2BwSZ7Yjb
MD5:	3D24B5D5F6B207AB44588DC4EC061472
SHA1:	8C7FAC5D105C752B45B3F1F4631E12B6A5D409B7

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
SHA-256:	E0D86404F7343D87C7E487393BE2A40BD5331EE8E93F849561CDFB77721687E6
SHA-512:	4DEFEB69EFE8F3EFF685340C0F7C3CC45D91A0DE972D12D28DE68E94E41D073B612DB29A193D248C3FD3266328C2959BA20113DF7ADBFE158F9140BDA6F5AE A5
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xe02732e3,0x01d72c51</date> <accdate>0xe02994d8,0x01d72c51</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xe02732e3,0x01d72c51</date><accda te>0xe02e599d,0x01d72c51</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipe dia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	5.09252084469492
Encrypted:	false
SSDEEP:	12:TMHdNMNxiznWimI002EtM3MHdNMNxiznWimI00OYGd5EtMb:2d6NxESZHKd6NxESZ7YEjb
MD5:	FE8909B52560EA1C1481E29A5072B849
SHA1:	1BB0AB2291AC39BB4EDEFA4B5B6BEEB16DF4FC94
SHA-256:	2FA6D9657C414667CF81AB3F2F72B8691262CCC90A3888FAD81CBF553394B996
SHA-512:	80CC0E5F6B5036F8EAD7C19D4BB6620B095026604E622D23B26913533D5268C6C1F28A45E15E0A226F45D5987D33C7B25642B3F58ECCC4DFABCE27B02E4F348
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xe024d04b,0x01d72c51</date><acc date>0xe024d04b,0x01d72c51</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xe024d04b,0x01d72c51</date><accdate>0xe024d 04b,0x01d72c51</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile> </msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.106803339969711
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwa1Bp1BwnWimI002EtM3MHdNMNxhGwa1Bp1BwnWimI00OYG8K075Es:2d6NxQtBzBwSZHKd6NxQtBzBwSZ7YrKG
MD5:	1C299F1C5E52A0B4695ADC6418BDDC66
SHA1:	4D3AA325B356C992249D919C2124F65D62091C46
SHA-256:	5D04E1670A8B5660CA73BD3D9A43E96F75911E495F9CD9CB569163A2F04E8D56
SHA-512:	491E1A7BB0ECADD8DA071B5D354FECFEC4FD7B7D75244FC8D47A88B065799BEFC37A900A2DB75D41C5F7AAB8163E08B286AA6D23D358EB00AA9E1007D3EC 7F5
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xe02e599d,0x01d72c51</date>< accdate>0xe02e599d,0x01d72c51</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xe02e599d,0x01d72c51</date><accdate>0 xe02e599d,0x01d72c51</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/> </tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.058272524153906
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nFLlnWimI002EtM3MHdNMNx0nFLlnWimI00OYGxEtMb:2d6Nx0LSZHKd6Nx0LSZ7Ygb
MD5:	B8B0F664CB188B7ECBD4DCA5C2E3B9A5
SHA1:	1B2F46107080093C94B76CF088BA3F65DDC00DEA
SHA-256:	897B98F88E21FB8F4CE7C5F71764B4FD72AA1D89B5F915714959DB813D373EC6
SHA-512:	A8C723D5413DD6ED0EA66108AA3F927ECDEFC4973536EE7F283322E15A71B6503F00F173FA68564BC9B78448A1379E438F5F6152E31461ADD7489DAB8D2D6775
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xe02732e3,0x01d72c51</date><accdate>0xe02732e3,0x01d72c51</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xe02732e3,0x01d72c51</date><accdate>0xe02732e3,0x01d72c51</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.11692555809491
Encrypted:	false
SSDEEP:	12:TMHdNMNxxznWimI002EtM3MHdNMNxxznWimI00OYG6Kq5EtMb:2d6NxVSZHKd6NxVSZ7Yhb
MD5:	04966944527E9605A8DFFFF1D6368D6E
SHA1:	E7EDCD6BC0F58EA31FF11F094BBEC3CFB9D5D9EA
SHA-256:	44E045DCB623A6B1FEEEDF73C312D44E7267F299E018379C06CF7974550F2033
SHA-512:	00CCE8D5447E50FF35701261EF3627D1B98E6A7E53FEE1877F9C77091CF60AD20D84D2CFD39AFAE5D5D5D8DD43A29FF6C198F474E7C22B78DF8395A904184E
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xe024d04b,0x01d72c51</date><accdate>0xe024d04b,0x01d72c51</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xe024d04b,0x01d72c51</date><accdate>0xe024d04b,0x01d72c51</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.088488557580741
Encrypted:	false
SSDEEP:	12:TMHdNMNxcRGbG5nWimI002EtM3MHdNMNxcRGbG5nWimI00OYGVEtMb:2d6NxDi5SZHKd6NxDi5SZ7Ykb
MD5:	A38A2EB37EE65A62C0CEE481A7A12FD0
SHA1:	46B8A0B8EB993DAD8B2A9C38FE8812C336A1AABE
SHA-256:	DCBABD0FD823BF55D14BCEEF36A2F3CC3846DB1427CBDF9C09FF4C213C62FEF9
SHA-512:	F2A22657DEF76F6CE25CBD0EC66B41C9167234F8946C30B46CAD6530274A6BB808D5F12886FFF735DB2631FB7962962B005477B9AB30D76BBE7CDA049E03AF6
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xe0226dcb,0x01d72c51</date><accdate>0xe0226dcb,0x01d72c51</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xe0226dcb,0x01d72c51</date><accdate>0xe0226dcb,0x01d72c51</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.078019079722306
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnznWimI002EtM3MHdNMNxfnznWimI00OYGe5EtMb:2d6Nx7SZHKd6Nx7SZ7YLjb
MD5:	D81D6E4AEA37D5F24CED4F72624379E2
SHA1:	9749BDA940207A3CF4A0D2CDBDD1EFDD2CF57B4D
SHA-256:	358067457C442D506FFB554BA45D3BC1D6B0C73E6C81B0A8D2D47737AECB16BE
SHA-512:	3A39CC98BCCF3F3CC251577392A5E3537DC10D0E6A212849AA32D286163087C6B3AA41666F2847D181E430A240D6656104C37484BE74D7B53233EC7F390CBB03
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xe024d04b,0x01d72c51</date><accdate>0xe024d04b,0x01d72c51</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xe024d04b,0x01d72c51</date><accdate>0xe024d04b,0x01d72c51</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Temp\~DF842C372FCF4BE378.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.27918767598683664
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA:kBqoxxJhHWSVSEab
MD5:	AB889A32AB9ACD33E816C2422337C69A
SHA1:	1190C6B34DED2D295827C2A88310D10A8B90B59B
SHA-256:	4D6EC54B8D244E63B0F04FBE2B97402A3DF722560AD12F218665BA440F4CEFDA
SHA-512:	BD250855747BB4CEC61814D0E44F810156D390E3E9F120A12935EFDF80ACA33C4777AD66257CCA4E4003FEF0741692894980B9298F01C4CDD2D8A9C7BB522FB
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFA194DF819C6EE39B.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34349
Entropy (8bit):	0.34800235401706053
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwv+99lwvy9l2vE9l2vj:kBqoxKAuvScS+GejBgsIsU+Px
MD5:	802A2289D05BE4845440A5480A4E0A8C
SHA1:	DE9568211C14C6A123F7B278E0BB2F870C3DCB72
SHA-256:	010AC7D3A5773203602D36B5EC8E3F5D5BEAC5865507D75B604ADF09310DEDF5
SHA-512:	65C861F80F628F9E758A591FAA95D6E0D20A218A974C032F28B13D5DA91E28C5B9CBACB9FD97D631EA4673B26829457FB17A4992D7AF4D14B0166433F18A577
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFB2C8B416DC11612E.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.47582027989183606
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loz99lozd9lWzzbU:kBqoIzmz4zs
MD5:	5A1F05F99ED9F1BBDA6EBEDBE36A286E
SHA1:	FF9E1533187046D1E9AD6D5E26684714412AD6DC
SHA-256:	28C777B4AFBD1D79F02873ADB8C1CD72210F6DA05AB75BDD4C45B513EF8F63D8
SHA-512:	0550ABD29EEBD2C6821517F7549B4A7F3F792CE70EAEA49DA1FCCD1794EB3A42F7956685709D432C4B8B50139270F146C8B9D175C229D64FD700B4496707FC3
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

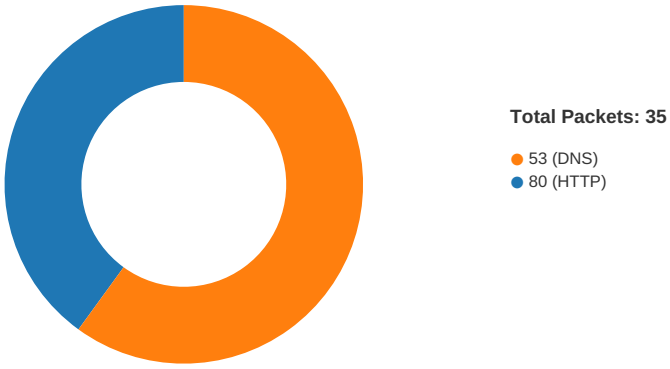
No static file info

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/08/21-10:33:08.955164	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49705	46.25.57.74	192.168.2.4

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 10:33:08.311757088 CEST	49704	80	192.168.2.4	46.25.57.74
Apr 8, 2021 10:33:08.312611103 CEST	49705	80	192.168.2.4	46.25.57.74
Apr 8, 2021 10:33:08.366228104 CEST	80	49705	46.25.57.74	192.168.2.4
Apr 8, 2021 10:33:08.366337061 CEST	49705	80	192.168.2.4	46.25.57.74
Apr 8, 2021 10:33:08.367726088 CEST	49705	80	192.168.2.4	46.25.57.74
Apr 8, 2021 10:33:08.372184038 CEST	80	49704	46.25.57.74	192.168.2.4
Apr 8, 2021 10:33:08.372298002 CEST	49704	80	192.168.2.4	46.25.57.74
Apr 8, 2021 10:33:08.416208029 CEST	80	49705	46.25.57.74	192.168.2.4
Apr 8, 2021 10:33:08.955163956 CEST	80	49705	46.25.57.74	192.168.2.4
Apr 8, 2021 10:33:08.955336094 CEST	49705	80	192.168.2.4	46.25.57.74
Apr 8, 2021 10:33:08.956178904 CEST	80	49705	46.25.57.74	192.168.2.4
Apr 8, 2021 10:33:08.956324100 CEST	49705	80	192.168.2.4	46.25.57.74
Apr 8, 2021 10:33:24.976656914 CEST	49707	80	192.168.2.4	46.25.57.74
Apr 8, 2021 10:33:25.040033102 CEST	80	49707	46.25.57.74	192.168.2.4
Apr 8, 2021 10:33:25.040175915 CEST	49707	80	192.168.2.4	46.25.57.74
Apr 8, 2021 10:33:25.040314913 CEST	49707	80	192.168.2.4	46.25.57.74
Apr 8, 2021 10:33:25.089231968 CEST	80	49707	46.25.57.74	192.168.2.4
Apr 8, 2021 10:33:25.095752001 CEST	80	49707	46.25.57.74	192.168.2.4
Apr 8, 2021 10:33:25.095798016 CEST	80	49707	46.25.57.74	192.168.2.4
Apr 8, 2021 10:33:25.095849037 CEST	49707	80	192.168.2.4	46.25.57.74
Apr 8, 2021 10:33:25.095885038 CEST	49707	80	192.168.2.4	46.25.57.74
Apr 8, 2021 10:33:25.096088886 CEST	49707	80	192.168.2.4	46.25.57.74
Apr 8, 2021 10:33:25.096158981 CEST	49707	80	192.168.2.4	46.25.57.74

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 10:32:59.298455000 CEST	56483	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:32:59.310214996 CEST	53	56483	8.8.8.8	192.168.2.4
Apr 8, 2021 10:33:00.273766994 CEST	51025	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:33:00.286176920 CEST	53	51025	8.8.8.8	192.168.2.4
Apr 8, 2021 10:33:07.152489901 CEST	61516	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:33:07.171089888 CEST	53	61516	8.8.8.8	192.168.2.4
Apr 8, 2021 10:33:08.244632006 CEST	49182	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 10:33:08.302061081 CEST	53	49182	8.8.8.8	192.168.2.4
Apr 8, 2021 10:33:22.958586931 CEST	59920	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:33:22.972811937 CEST	53	59920	8.8.8.8	192.168.2.4
Apr 8, 2021 10:33:24.933012009 CEST	57458	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:33:24.973526001 CEST	53	57458	8.8.8.8	192.168.2.4
Apr 8, 2021 10:33:25.130399942 CEST	50579	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:33:25.144102097 CEST	53	50579	8.8.8.8	192.168.2.4
Apr 8, 2021 10:33:33.553307056 CEST	51703	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:33:33.565994978 CEST	53	51703	8.8.8.8	192.168.2.4
Apr 8, 2021 10:33:35.810189962 CEST	65248	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:33:35.822825909 CEST	53	65248	8.8.8.8	192.168.2.4
Apr 8, 2021 10:33:36.861268044 CEST	53723	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:33:36.873900890 CEST	53	53723	8.8.8.8	192.168.2.4
Apr 8, 2021 10:33:37.145855904 CEST	64646	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:33:37.159142017 CEST	53	64646	8.8.8.8	192.168.2.4
Apr 8, 2021 10:33:37.821991920 CEST	65298	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:33:37.834598064 CEST	53	65298	8.8.8.8	192.168.2.4
Apr 8, 2021 10:33:38.155375004 CEST	64646	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:33:38.162177086 CEST	59123	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:33:38.169019938 CEST	53	64646	8.8.8.8	192.168.2.4
Apr 8, 2021 10:33:38.174639940 CEST	53	59123	8.8.8.8	192.168.2.4
Apr 8, 2021 10:33:38.827016115 CEST	65298	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:33:38.840203047 CEST	53	65298	8.8.8.8	192.168.2.4
Apr 8, 2021 10:33:39.173413038 CEST	64646	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:33:39.186728001 CEST	53	64646	8.8.8.8	192.168.2.4
Apr 8, 2021 10:33:39.855179071 CEST	65298	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:33:39.868319988 CEST	53	65298	8.8.8.8	192.168.2.4
Apr 8, 2021 10:33:41.303740025 CEST	64646	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:33:41.316955090 CEST	53	64646	8.8.8.8	192.168.2.4
Apr 8, 2021 10:33:41.842935085 CEST	65298	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:33:41.856256962 CEST	53	65298	8.8.8.8	192.168.2.4
Apr 8, 2021 10:33:45.296324968 CEST	64646	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:33:45.309592009 CEST	53	64646	8.8.8.8	192.168.2.4
Apr 8, 2021 10:33:45.861478090 CEST	65298	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:33:45.874919891 CEST	53	65298	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 10:33:08.244632006 CEST	192.168.2.4	8.8.8.8	0x11e	Standard query (0)	cloud.60dias.es	A (IP address)	IN (0x0001)
Apr 8, 2021 10:33:24.933012009 CEST	192.168.2.4	8.8.8.8	0xe4	Standard query (0)	cloud.60dias.es	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 10:33:08.302061081 CEST	8.8.8.8	192.168.2.4	0x11e	No error (0)	cloud.60dias.es		46.25.57.74	A (IP address)	IN (0x0001)
Apr 8, 2021 10:33:24.973526001 CEST	8.8.8.8	192.168.2.4	0xe4	No error (0)	cloud.60dias.es		46.25.57.74	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- cloud.60dias.es

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49705	46.25.57.74	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 10:33:08.367726088 CEST	113	OUT	GET / 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: cloud.60dias.es Connection: Keep-Alive
Apr 8, 2021 10:33:08.955163956 CEST	114	IN	HTTP/1.1 403 Forbidden Content-Type: text/html Server: Microsoft-IIS/10.0 X-Powered-By: ASP.NET Date: Thu, 08 Apr 2021 08:33:07 GMT Content-Length: 1237

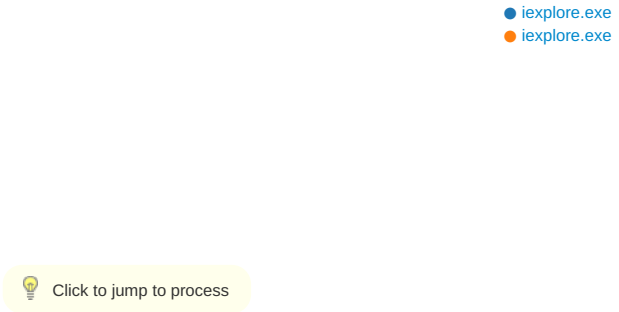
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49707	46.25.57.74	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 10:33:25.040314913 CEST	311	OUT	GET /favicon.ico HTTP/1.1 User-Agent: AutoIt Host: cloud.60dias.es
Apr 8, 2021 10:33:25.095752001 CEST	311	IN	HTTP/1.1 404 Not Found Content-Type: text/html Server: Microsoft-IIS/10.0 X-Powered-By: ASP.NET Date: Thu, 08 Apr 2021 08:33:24 GMT Content-Length: 1282

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: iexplore.exe PID: 5828 Parent PID: 800

General

Start time:	10:33:06
Start date:	08/04/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff69ac30000
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: 1056 Parent PID: 5828

General

Start time:	10:33:07
Start date:	08/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5828 CREDAT:17410 /prefetch:2
Imagebase:	0x13d0000
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	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly