ID: 392871
Cookbook: browseurl.jbs
Time: 23:09:22
Date: 19/04/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2

Analysis Report http://7lyonline.com/app/feedclick?p=YaNzDr1n8wuMCeH3yeI7_ccZeaeGPnD7yDcN_3ivXIa1ZubyCpAa3MNnA02fFaz8aOuYKJrsTGs1F2mXCl-YVw3jO6VAG9VkBDEK4mzoj_t_qW7ZJPi1e9N5huazfoKx6ICBOkPhmI5elBP0p5ETqgvC4-_dGy4yjqvCmbuyuSMioQEKiPfavdX6-9kT7sye03mG5rN-grEMtCRRqzsm2g 3

- Overview 3
  - General Information 3
  - Detection 3
  - Signatures 3
  - Classification 3
  - Analysis Advice 3
- Startup 3
- Malware Configuration 3
- Yara Overview 3
- Sigma Overview 3
- Signature Overview 4
- Mitre Att&ck Matrix 4
- Behavior Graph 4
- Screenshots 5
  - Thumbnails 5
- Antivirus, Machine Learning and Genetic Malware Detection 6
  - Initial Sample 6
  - Dropped Files 6
  - Unpacked PE Files 6
  - Domains 6
  - URLs 6
- Domains and IPs 7
  - Contacted Domains 7
  - Contacted URLs 7
  - URLs from Memory and Binaries 7
  - Contacted IPs 7
  - Public 7
- General Information 8
- Simulations 8
  - Behavior and APIs 8
- Joe Sandbox View / Context 9
  - IPs 9
  - Domains 9
  - ASN 9
  - JA3 Fingerprints 9
  - Dropped Files 9
- Created / dropped Files 9
- Static File Info 12
  - No static file info 12
- Network Behavior 13
  - Network Port Distribution 13
  - TCP Packets 13
  - UDP Packets 13
  - DNS Queries 14
  - DNS Answers 14
  - HTTP Request Dependency Graph 15
  - HTTP Packets 15
- Code Manipulations 15
- Statistics 15
  - Behavior 15
- System Behavior 15
  - Analysis Process: iexplore.exe PID: 4792 Parent PID: 792 15
    - General 16
    - File Activities 16
    - Registry Activities 16
  - Analysis Process: iexplore.exe PID: 4812 Parent PID: 4792 16
    - General 16
    - File Activities 16
- Disassembly 17

Analysis Report http://7lyonline.com/app/feedclick?p=Y…

Overview

General Information

Sample URL:	7lyonline.com/app/feedclick?p=YaNzDr1n8wuMCeH3yeI7_ccZeaeGPnD7yDcN_3ivXIa1Z...elBP0p5ETqgvC4-_dGy4yjqvCmbuyuSMioQEKiPfavdX6-9kT7sye03mG5rN-grEMtCRRqzsm2g
Analysis ID:	392871
Infos:	
Most interesting Screenshot:	

Errors

URL not reachable

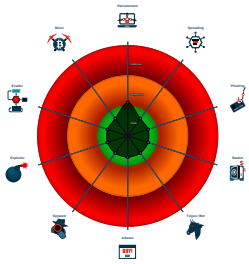
Detection

Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	60%

Signatures

No high impact signatures.

Classification



Analysis Advice

Joe Sandbox was unable to browse the URL (domain or webserver down or HTTPS issue), try to browse the URL again later

Uses HTTPS for network communication, use the 'Proxy HTTPS (port 443) to read its encrypted data' cookbook for further analysis

Startup

- **System is w10x64**
- iexplore.exe (PID: 4792 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 4812 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4792 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

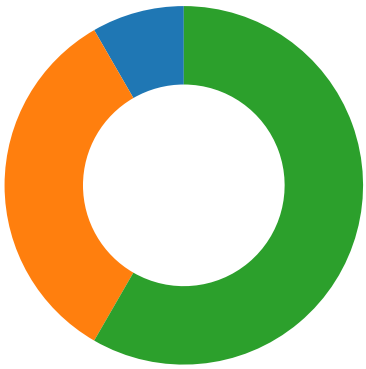
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



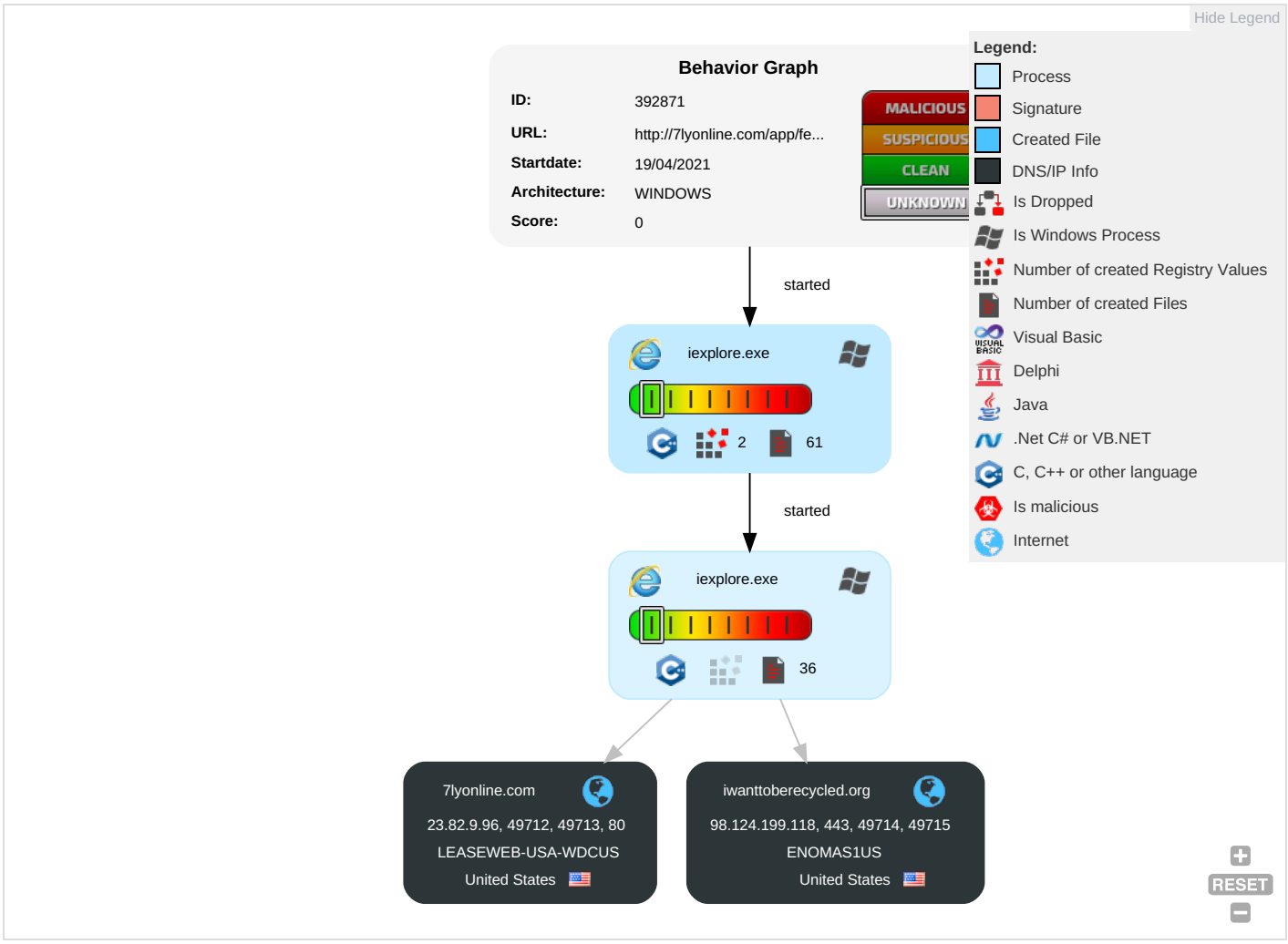
Click to jump to signature section

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	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 Billin Fraud

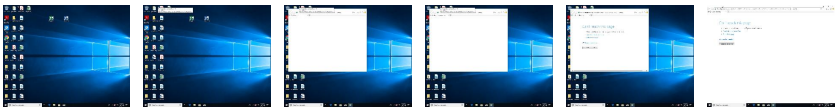
Behavior Graph

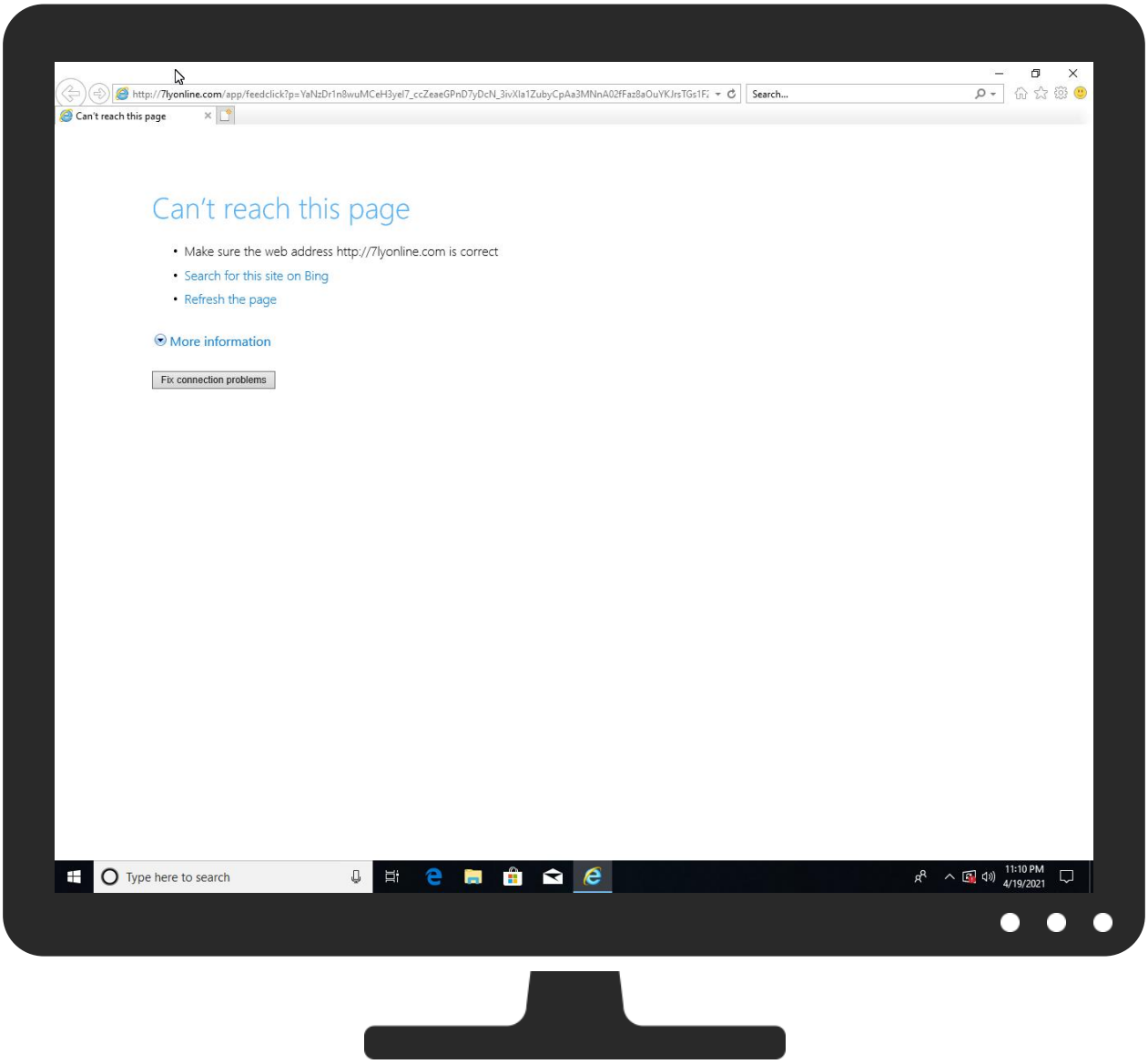


Screenshots

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://7lyonline.com/app/feedclick?p=YaNzDr1n8wuMCeH3yel7_ccZeaeGPnD7yDcN_3ivXIa1ZubyCpAa3MNnA02fFaz8aOuYKJrsTGs1F2mXCl-YVw3jO6VAG9VkBDEK4mzoj_t_qW7ZJPi1e9N5huazfoKx6ICBOkPhmI5elBP0p5ETqgvC4-_dGy4yjqvCmbuyuSMioQEKiPfavdX6-9kT7sye03mG5rN-grEMtCRRqzsm2g	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
7lyonline.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://7lyonline.com/app/feedclick?p=YaNzDr1n8wuMCeH3yeI7_ccZeaeGPnD7yDcN_3ivXIa1ZubyCpAa3MNnA02fFaz	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
iwanttoberecycled.org	98.124.199.118	true	false		high
7lyonline.com	23.82.9.96	true	false	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://7lyonline.com/app/feedclick?p=YaNzDr1n8wuMCeH3yeI7_ccZeaeGPnD7yDcN_3ivXIa1ZubyCpAa3MNnA02fFaz8aOuYKJrsTGs1F2mXCl-YVw3jO6VAG9VkBDEK4mzoj_t_qW7ZJPi1e9N5huazfoKx6ICBOkPhmI5elBP0p5ETqgvC4-_dGy4yjqvCmbuyuSMioQEKiPfavdX6-9kT7sye03mG5rN-grEMtCRRqzsm2g	false		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://7lyonline.com/app/feedclick?p=YaNzDr1n8wuMCeH3yeI7_ccZeaeGPnD7yDcN_3ivXIa1ZubyCpAa3MNnA02fFaz	~DF8CE724674FDD1AE6.TMP.2.dr, {0D3E5F8C-A19F-11EB-90E4-ECF4BB862DED}.dat.2.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
98.124.199.118	iwanttoberecycled.org	United States		21740	ENOMAS1US	false
23.82.9.96	7lyonline.com	United States		30633	LEASEWEB-USA-WDCUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	392871
Start date:	19.04.2021
Start time:	23:09:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://7lyonline.com/app/feedclick?p=YaNzDr1n8wuMCeH3yeI7_ccZeaeGPnD7yDcN_3ivXIa1ZubyCpAa3MNnA02fFaz8aOuYKJrsTGs1F2mXCl-YVw3jO6VAG9VkBDEK4mzoj_t_qW7ZJPi1e9N5huazfoKx6ICBOkPhmI5elBP0p5ETqgvC4-_dGy4yjqvCmbuyuSMioQEKiPfavdX6-9kT7sye03mG5rN-grEMtCRRqzsm2g
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	7
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	UNKNOWN
Classification:	unknown0.win@3/11@3/2
Cookbook Comments:	• Adjust boot time • Enable AMSI • **URL browsing timeout or error**
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 52.255.188.83, 104.42.151.234, 204.79.197.200, 13.107.21.200, 23.211.6.115, 168.61.161.212, 104.43.193.48, 88.221.62.148 • Excluded domains from analysis (whitelisted): www.bing.com, dual-a-0001.a-msedge.net, store-images.s-microsoft.com-c.edgekey.net, skypedataprdcolcus17.cloudapp.net, skypedataprdcolcus15.cloudapp.net, e11290.dspg.akamaiedge.net, e12564.dspb.akamaiedge.net, skypedataprdcoleus17.cloudapp.net, go.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, www-bing-com.dual-a-0001.a-msedge.net, go.microsoft.com.edgekey.net, watson.telemetry.microsoft.com, skypedataprdcolwus16.cloudapp.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.{0D3E5F8A-A19F-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8565697379443642
Encrypted:	false
SSDEEP:	48:IwRGcprwGwpLvhG/ap8EGIpcrg3WGvnZpvrgRGoGqp9rgjGo4Vpmr7GWU09r+GWn:rnZYZvl2EWrQztrifrJVMrVr4refrVMX
MD5:	C3845010495594DC45B7CF848E955147
SHA1:	121E6C2AF85003F2D0412BE926ADD34C77DCC67E
SHA-256:	DD01B0A6E0D0D9AED9D680EF2916854A2B05A734AB17A7B404533483F78BF6B9
SHA-512:	D55DB7A1946B16C23ECF399791B3CA1637A73C9DECBAC6CDE1A75E85E4A671DFA78F9663A34178AFF5F5A084796A4850E40E83714783A82438830A788C8EB94
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\{0D3E5F8C-A19F-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24612
Entropy (8bit):	1.723277129300364
Encrypted:	false
SSDEEP:	48:IwqGcprXGwpa4G4pQAhGrapbSyGQpBVNWGHHpcVhTGUp8VZUGzYpmVDavGopUHDq:rOZBQo6AxBSajPV2RW0McGiSD7x8kcwg
MD5:	C0BD87C48346B7E209B047CC7710386D
SHA1:	BDC8D4ABA33D75460BAE800BAB0EF6CFBE5976B8
SHA-256:	C3B8383EE3E570B5CEBA9DB52B63DBB9EDC5FEE120BE6BBA001E5BF361C077BA
SHA-512:	17FF098326BB197E314DD8779ABC7DE1C29F65E3FE1F5D0AC539EB8F1FD8886C0749814842961F18C703C5835ECE73AE5C232F77B6BBBA03B51219EE3E12C3A
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\{13E24B38-A19F-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5657160964476846
Encrypted:	false
SSDEEP:	48:Iw4GcprlGwpaXG4pQnGrapbSRGQpKvG7HpRdTGIpG:rMZvQZ67BSrA+TbA
MD5:	06092EAF84CCB5B719787460C2557B9C
SHA1:	A5E49C6EC56153477EEB210BC754F84775656C1B
SHA-256:	96DD2508D19BFBE16A80EE019F404C15A8AEFF5CC4BE06DAC64023413C54E2D2
SHA-512:	8D4867F85A2D19678182925529A2528068D295D06E11B715CDD6A880DCB9809C799D8480250F4BB9F4557D7A0DCEC2DB3379043EF066AE67822D0139B92FED5D
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/errorPageStrings.js
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts ";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet conn ection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";..../used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284F D
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/NewErrorPageTemplate.css
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #00 0000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt; ..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\httpErrorPagesScripts[1]	
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/httpErrorPagesScripts.js
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vIlJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/dnserror.htm?ErrorStatus=0x800C0005&DNSError=9002
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); 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\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
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\Temp\~DF3E8B2475FB85CB4F.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data

C:\Users\user\AppData\Local\Temp\~DF3E8B2475FB85CB4F.TMP	
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.48285589057210837
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loyDF9loyJ9lWyxbGgzObGJtnwGJ6cOc2:kBqoINLLgFPrM
MD5:	F1047ACA1144811BA1F5CD931184E548
SHA1:	BE58432F1D5277BB1097450DB611E612A569A07A
SHA-256:	635F0D47F6F51546511BEF733EA6399A65832D4D5A4746B7F0822B344CE8A79C
SHA-512:	19000574C0B4EABEC4CA6C32D181D811521A64BF8D60AA346FFDCF175CA372FB4F991641775072E918D9B773F310CEF2E4D13657629FAD99A0A3D9CF7A4D5A1
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF8CE724674FDD1AE6.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34805
Entropy (8bit):	0.4317346303545725
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+VaV8VmVvVDIVDqHDGDODfTiK8kGlF:kBqoxKAuvScS+IOEV+ciSD7x8kcF
MD5:	EB5A6B0C3DCBDCDF214D32B2D41C89A6
SHA1:	685C7022CC4979BDDCE97D56D0C4706D38620268
SHA-256:	2B9AC1EB460292E52A89BAC26E53437814131FC6FFF7BE648B915AD32BBDB360
SHA-512:	279DCD8DADFE3DCB414DACDA0CBB3359BE2683D532C32B9A739FC3937EB34E7281985C34554E00D19ED49EBF7AA42B6830D443EBC6930071F49FEA97704A1 A2
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

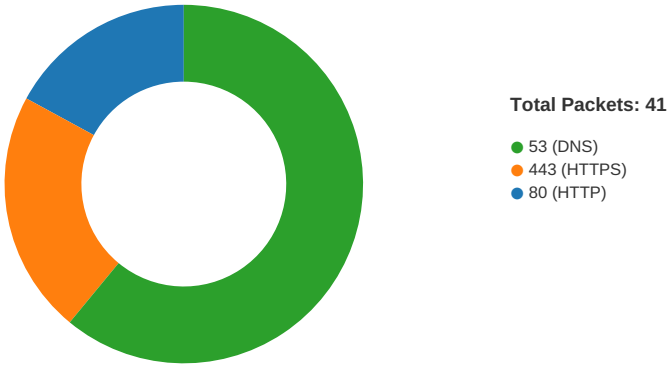
C:\Users\user\AppData\Local\Temp\~DFB28D409A66DF3C47.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.27918767598683664
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA:kBqoxxJhHWSVSEab
MD5:	AB889A32AB9ACD33E816C2422337C69A
SHA1:	1190C6B34DED2D295827C2A88310D10A8B90B59B
SHA-256:	4D6EC54B8D244E63B0F04FBE2B97402A3DF722560AD12F218665BA440F4CEFDA
SHA-512:	BD250855747BB4CEC61814D0E44F810156D390E3E9F120A12935EFDF80ACA33C4777AD66257CCA4E4003FEF0741692894980B9298F01C4CDD2D8A9C7BB522FB
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 19, 2021 23:10:09.340655088 CEST	49712	80	192.168.2.3	23.82.9.96
Apr 19, 2021 23:10:09.340975046 CEST	49713	80	192.168.2.3	23.82.9.96
Apr 19, 2021 23:10:09.478661060 CEST	80	49713	23.82.9.96	192.168.2.3
Apr 19, 2021 23:10:09.478828907 CEST	49713	80	192.168.2.3	23.82.9.96
Apr 19, 2021 23:10:09.479538918 CEST	49713	80	192.168.2.3	23.82.9.96
Apr 19, 2021 23:10:09.482728958 CEST	80	49712	23.82.9.96	192.168.2.3
Apr 19, 2021 23:10:09.482830048 CEST	49712	80	192.168.2.3	23.82.9.96
Apr 19, 2021 23:10:09.620309114 CEST	80	49713	23.82.9.96	192.168.2.3
Apr 19, 2021 23:10:09.621481895 CEST	80	49713	23.82.9.96	192.168.2.3
Apr 19, 2021 23:10:09.621583939 CEST	49713	80	192.168.2.3	23.82.9.96
Apr 19, 2021 23:10:09.708466053 CEST	49714	443	192.168.2.3	98.124.199.118
Apr 19, 2021 23:10:09.709809065 CEST	49715	443	192.168.2.3	98.124.199.118
Apr 19, 2021 23:10:09.905718088 CEST	443	49714	98.124.199.118	192.168.2.3
Apr 19, 2021 23:10:09.913774967 CEST	443	49715	98.124.199.118	192.168.2.3
Apr 19, 2021 23:10:10.418226004 CEST	49714	443	192.168.2.3	98.124.199.118
Apr 19, 2021 23:10:10.418241978 CEST	49715	443	192.168.2.3	98.124.199.118
Apr 19, 2021 23:10:10.615894079 CEST	443	49714	98.124.199.118	192.168.2.3
Apr 19, 2021 23:10:10.622736931 CEST	443	49715	98.124.199.118	192.168.2.3
Apr 19, 2021 23:10:11.262023926 CEST	49714	443	192.168.2.3	98.124.199.118
Apr 19, 2021 23:10:11.264168978 CEST	49715	443	192.168.2.3	98.124.199.118
Apr 19, 2021 23:10:11.459172964 CEST	443	49714	98.124.199.118	192.168.2.3
Apr 19, 2021 23:10:11.468085051 CEST	443	49715	98.124.199.118	192.168.2.3
Apr 19, 2021 23:10:11.469414949 CEST	49717	443	192.168.2.3	98.124.199.118
Apr 19, 2021 23:10:11.670187950 CEST	443	49717	98.124.199.118	192.168.2.3
Apr 19, 2021 23:10:12.262088060 CEST	49717	443	192.168.2.3	98.124.199.118
Apr 19, 2021 23:10:12.468914032 CEST	443	49717	98.124.199.118	192.168.2.3
Apr 19, 2021 23:10:13.153462887 CEST	49717	443	192.168.2.3	98.124.199.118
Apr 19, 2021 23:10:13.354099989 CEST	443	49717	98.124.199.118	192.168.2.3
Apr 19, 2021 23:10:14.618917942 CEST	80	49713	23.82.9.96	192.168.2.3
Apr 19, 2021 23:10:14.619007111 CEST	49713	80	192.168.2.3	23.82.9.96

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 19, 2021 23:09:59.689755917 CEST	51281	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:09:59.751813889 CEST	53	51281	8.8.8.8	192.168.2.3
Apr 19, 2021 23:10:00.547797918 CEST	49199	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:10:00.596312046 CEST	53	49199	8.8.8.8	192.168.2.3
Apr 19, 2021 23:10:00.660540104 CEST	50620	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:10:00.729171991 CEST	53	50620	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 19, 2021 23:10:01.324986935 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:10:01.387996912 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 19, 2021 23:10:01.693368912 CEST	60152	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:10:01.744041920 CEST	53	60152	8.8.8.8	192.168.2.3
Apr 19, 2021 23:10:02.468656063 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:10:02.517735958 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 19, 2021 23:10:03.415977001 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:10:03.465799093 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 19, 2021 23:10:04.479376078 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:10:04.531167030 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 19, 2021 23:10:05.643893957 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:10:05.696331024 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 19, 2021 23:10:06.765279055 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:10:06.814018965 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 19, 2021 23:10:07.840667009 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:10:07.882400036 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:10:07.903310061 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 19, 2021 23:10:07.933552980 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 19, 2021 23:10:09.248965025 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:10:09.261406898 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:10:09.318205118 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 19, 2021 23:10:09.325550079 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 19, 2021 23:10:09.643485069 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:10:09.703933954 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 19, 2021 23:10:10.694667101 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:10:10.743237972 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 19, 2021 23:10:12.080921888 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:10:12.132467031 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 19, 2021 23:10:13.012685061 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:10:13.064053059 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 19, 2021 23:10:13.376231909 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:10:13.433073044 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 19, 2021 23:10:13.918159008 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:10:13.967897892 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 19, 2021 23:10:14.813102007 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:10:14.873008013 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 19, 2021 23:10:15.752227068 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:10:15.801218033 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 19, 2021 23:10:16.868623018 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:10:16.929856062 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 19, 2021 23:10:19.901432991 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:10:19.952056885 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 19, 2021 23:10:20.823664904 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 19, 2021 23:10:20.875170946 CEST	53	53034	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 19, 2021 23:10:09.248965025 CEST	192.168.2.3	8.8.8.8	0x2b6b	Standard query (0)	7lyonline.com	A (IP address)	IN (0x0001)
Apr 19, 2021 23:10:09.643485069 CEST	192.168.2.3	8.8.8.8	0xb9f2	Standard query (0)	iwanttoberecycled.org	A (IP address)	IN (0x0001)
Apr 19, 2021 23:10:13.376231909 CEST	192.168.2.3	8.8.8.8	0x688d	Standard query (0)	7lyonline.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 19, 2021 23:10:09.325550079 CEST	8.8.8.8	192.168.2.3	0x2b6b	No error (0)	7lyonline.com		23.82.9.96	A (IP address)	IN (0x0001)
Apr 19, 2021 23:10:09.703933954 CEST	8.8.8.8	192.168.2.3	0xb9f2	No error (0)	iwanttoberecycled.org		98.124.199.118	A (IP address)	IN (0x0001)
Apr 19, 2021 23:10:13.433073044 CEST	8.8.8.8	192.168.2.3	0x688d	Server failure (2)	7lyonline.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 7lyonline.com

HTTP Packets

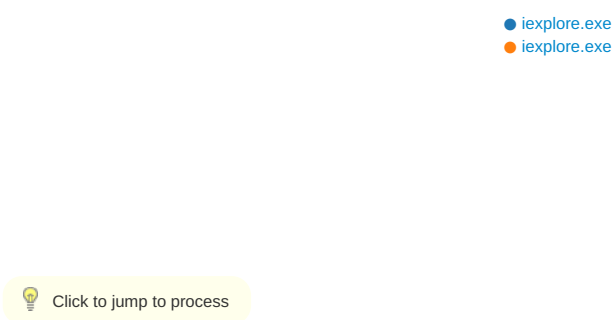
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49713	23.82.9.96	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Apr 19, 2021 23:10:09.479538918 CEST	1304	OUT	GET /app/feedclick?p=YaNzDr1n8wuMCeH3yeI7_ccZeaeGPnD7yDcN_3ivXIa1ZubyCpAa3MNnA02fFaz8aOuYK JrsTGs1F2mXCl-YVw3jO6VAG9VkBDEK4mzoj_t_qW7ZJPi1e9N5huazfoKx6ICBOkPhmI5elBP0p5ETqgvC4-_dGy4 yjqvCmbuyuSMioQEKiPfavdX6-9kT7sye03mG5rN-grEMtCRRqzsm2g 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: 7lyonline.com Connection: Keep-Alive
Apr 19, 2021 23:10:09.621481895 CEST	1304	IN	HTTP/1.1 302 Server: nginx Date: Mon, 19 Apr 2021 21:10:09 GMT Content-Length: 0 Connection: keep-alive Keep-Alive: timeout=5 Location: https://iwanttoberecycled.org/

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: iexplore.exe PID: 4792 Parent PID: 792

General

Start time:	23:10:06
Start date:	19/04/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff6f90b0000
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: 4812 Parent PID: 4792

General

Start time:	23:10:07
Start date:	19/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4792 CREDAT:17410 /prefetch:2
Imagebase:	0x1050000
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