ID: 242343
Cookbook: browseurl.jbs
Time: 18:02:31
Date: 30/06/2020
Version: 29.0.0 Ocean Jasper

Table of Contents

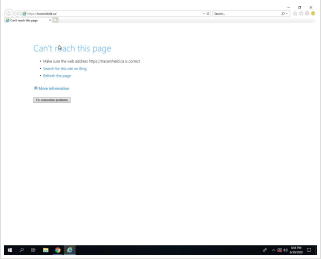
Analysis Report https://tracershield.ca/

Overview

General Information

Sample URL:	http://https://tracershield.ca/

Most interesting Screenshot:



Errors

URL not reachable

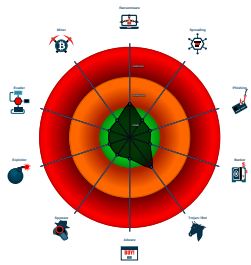
Detection

Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Tries to resolve domain names, but n…

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 3284 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 3472 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3284 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

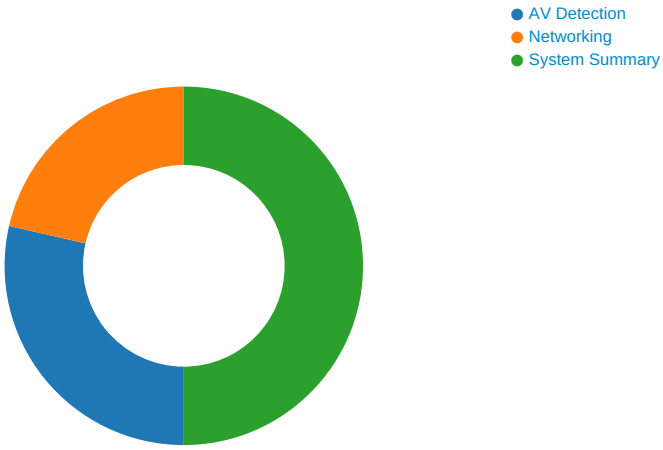
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

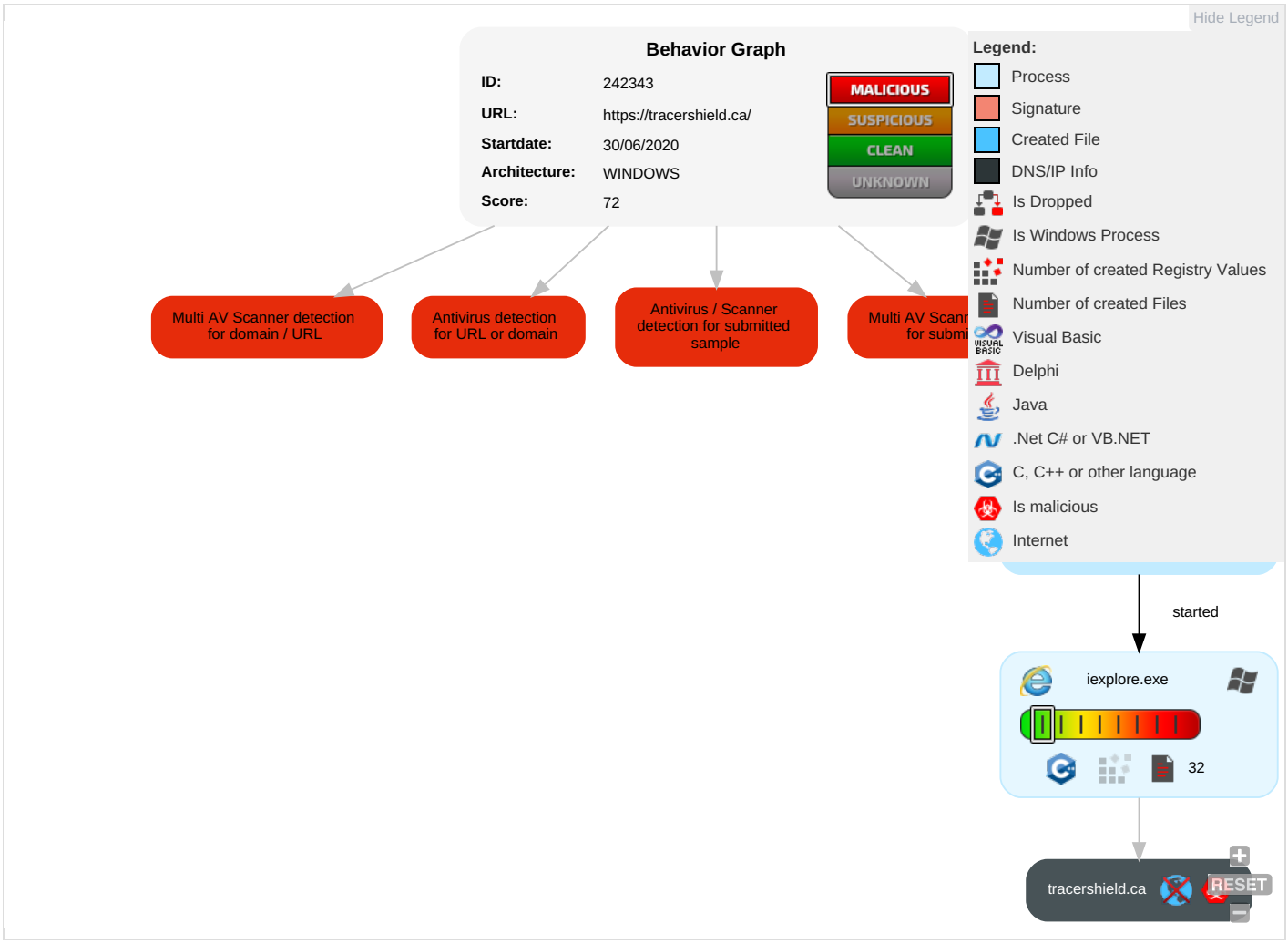
Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Graphical User Interface 1	Winlogon Helper DLL	Process Injection 1	Masquerading 1	Credential Dumping	File and Directory Discovery 1	Application Deployment Software	Data from Local System	Data Compressed	Standard Non-Application Layer Protocol 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
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 Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

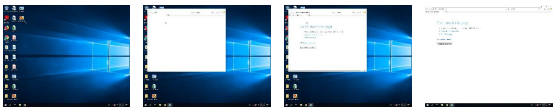
Behavior Graph

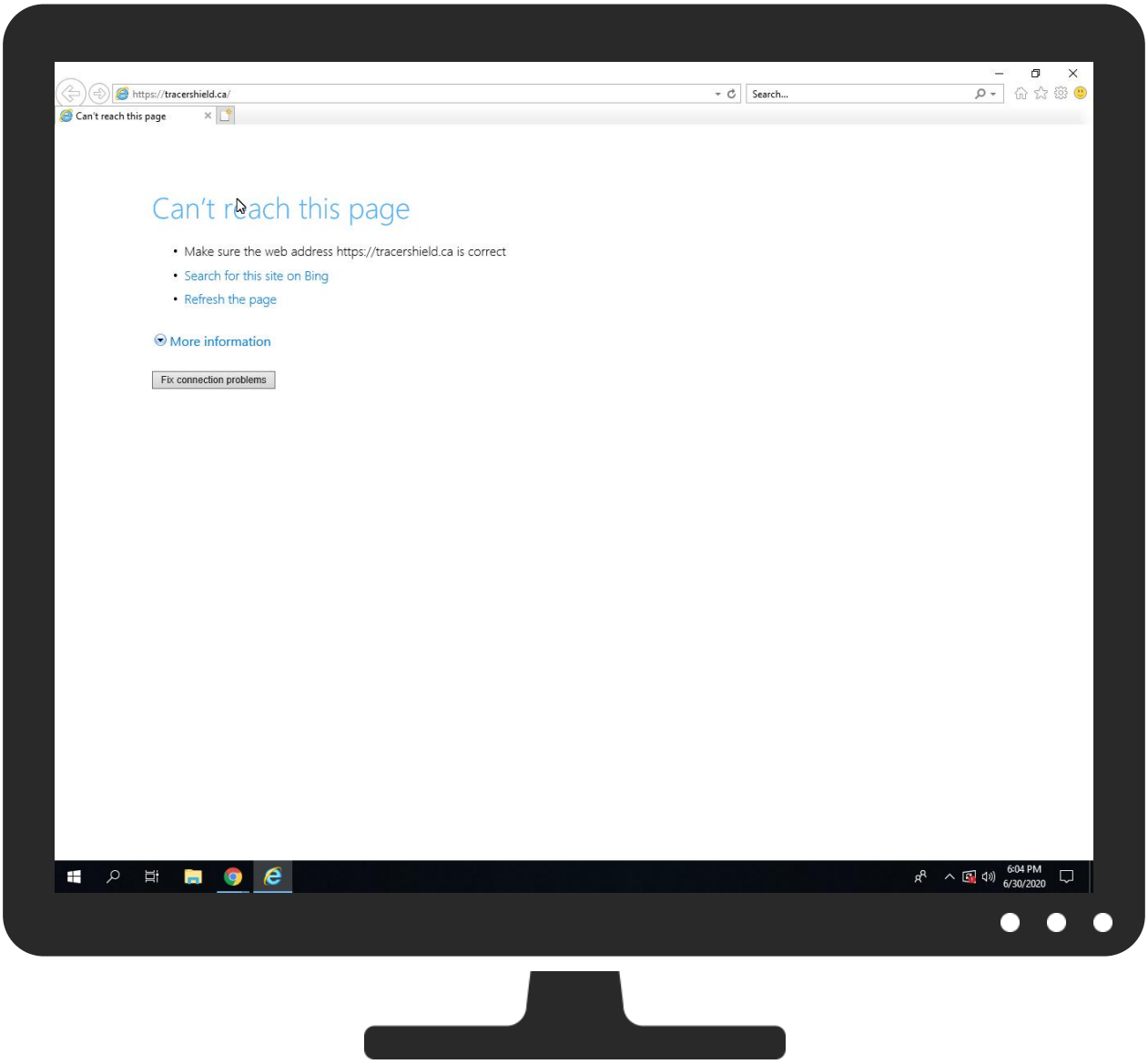


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://tracershield.ca/	10%	Virustotal		Browse
http://https://tracershield.ca/	100%	Avira URL Cloud	malware	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
tracershield.ca	11%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://tracershield.ca/Root	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
tracershield.ca	unknown	unknown	true	• 11%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://tracershield.ca/Root	{49151619-BAEB-11EA-AAE7-9CC1A2A860C6}.dat.1.dr	true	• Avira URL Cloud: malware	unknown
http://https://tracershield.ca/	~DF3277FDDF3D1960CE.TMP.1.dr	true		unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	29.0.0 Ocean Jasper
Analysis ID:	242343
Start date:	30.06.2020
Start time:	18:02:31
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://tracershield.ca/
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:	5
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:	mal72.win@3/11@3/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • **URL browsing timeout or error**
Warnings:	Show All • Exclude process from analysis (whitelisted): ielowutil.exe, SgrmBroker.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 104.83.21.70, 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.{49151617-BAEB-11EA-AAE7-9CC1A2A860C6}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Size (bytes):	30296
Entropy (8bit):	1.8554806867940292
Encrypted:	false
MD5:	F29E942377B2B1D6C11BE3FAF27BAB02
SHA1:	23E7295344AFDF3B6542C27552EFF0B27C7A8658
SHA-256:	95509C6B7E46C2E98B2B328975A6DBEEDFCA282B27C2F1CC452F91BAE64A7E85
SHA-512:	5DC5320D541C4FCE71C11346E565F7B53CC7138AC96ADB0653DE142FE6726E97512922A686F8EF4AC9A2135DBA695C6EC6AB1972B0F44291AEDC975DFF7562 A
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\{49151619-BAEB-11EA-AAE7-9CC1A2A860C6}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Size (bytes):	24160
Entropy (8bit):	1.6249613000883985
Encrypted:	false
MD5:	94CBBB2F00BD5B8BA1907928589EE5F4
SHA1:	0322147A2A0C099B63ECB3D21AD9C9EE71A2ED7B
SHA-256:	38BE936B2A6E20178C90E3E60EA46E5EC5F46BF15375F3AB1BB09641C6D5C421
SHA-512:	4BCF49AAE7E4E73EC7477FA6ECBDF98745626CD774FF561572BE50CD3E2BC9688F7E718437D592460DE538953906975CEC572E27DF1816A9244F28D0ACB871E

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{49151619-BAEB-11EA-AAE7-9CC1A2A860C6}.dat	
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\{4915161A-BAEB-11EA-AAE7-9CC1A2A860C6}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Size (bytes):	16984
Entropy (8bit):	1.5649250013593177
Encrypted:	false
MD5:	EC69CA30C92E836F06E4C5FF126366D6
SHA1:	E69715AA5F36BE2E5F292CD1D138B6BB1311987B
SHA-256:	25C8C7825E5999F8446823063F63AFA5BA4764374CB60D8248A31DBCC696BE2F
SHA-512:	8AA49BEBDA3DC3EA5CDE0786A6030EC9A7F4CEA680AEB8D3BD50505F422ED99AA33B2F3473ED3C762AAD819D8BE2D374ACB66CB4ACE38970FBB40232A5FC 068E
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

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:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493 AC6D
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/dnserror.htm?ErrorStatus=0x800C0005&DNSError=9002
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMo reInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\5N37O3UG\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
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\O0N4T4W6\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:	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: #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\P24S97MI\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\PKAQFTEH\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..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....#+....l..z.....'.ksC...X<.+..J>....%3BmqaV ...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Temp\~DF3277FDDF3D1960CE.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Size (bytes):	34353
Entropy (8bit):	0.34555909389512274
Encrypted:	false
MD5:	B2B064743E11663AE836E85796AE9E1B
SHA1:	DE91CAA17E6DAB6B645A31D8151C20D7B411B5A4

C:\Users\user\AppData\Local\Temp\~DF3277FDDF3D1960CE.TMP	
SHA-256:	D4563D675DCFBB0D913922ABE209AB9B0A4328D150CA712F5C3A0789BA15DC6C
SHA-512:	AD17AD9FB8B96A5100C5A5DB9EF6427F5B4020C270A347C88FE13AEFF164634A59A5D35293CA564DEE53F54F9FF21691998D9B8AAADA489101816D2C00D12DC 4
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFB4DC5491F9A1180D.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Size (bytes):	13029
Entropy (8bit):	0.4810139375598866
Encrypted:	false
MD5:	C92ECC58DEBA1078F99BCFC5A75CE01E
SHA1:	6F6630A8C3BEBE8A2FB9DA9E4BA5BD2E2D6C3DF2
SHA-256:	A9A4577A5223971100095CB57177E2E44051A67968CD78E12F39200CD1AAFE39
SHA-512:	128E9DFD659EAA8248A9682DF44964C9861C29D065888F124D1699BE35D628C32739217DF9C95314D15C72BECB5BEC546863083C879348C2ACA082BD25613CD
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFF753BF2E092F638E.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Size (bytes):	25441
Entropy (8bit):	0.27918767598683664
Encrypted:	false
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

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 30, 2020 18:03:51.420176029 CEST	60679	53	192.168.2.6	8.8.8.8
Jun 30, 2020 18:03:51.455312967 CEST	53	60679	8.8.8.8	192.168.2.6
Jun 30, 2020 18:03:53.321444988 CEST	59670	53	192.168.2.6	8.8.8.8
Jun 30, 2020 18:03:53.356720924 CEST	53	59670	8.8.8.8	192.168.2.6
Jun 30, 2020 18:03:53.363142014 CEST	50342	53	192.168.2.6	8.8.8.8
Jun 30, 2020 18:03:53.397068024 CEST	53	50342	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 30, 2020 18:03:53.445960045 CEST	57707	53	192.168.2.6	8.8.8.8
Jun 30, 2020 18:03:53.479760885 CEST	53	57707	8.8.8.8	192.168.2.6
Jun 30, 2020 18:04:10.479617119 CEST	51048	53	192.168.2.6	8.8.8.8
Jun 30, 2020 18:04:10.514882088 CEST	53	51048	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 30, 2020 18:03:53.321444988 CEST	192.168.2.6	8.8.8.8	0x89bd	Standard query (0)	tracershield.ca	A (IP address)	IN (0x0001)
Jun 30, 2020 18:03:53.363142014 CEST	192.168.2.6	8.8.8.8	0x5964	Standard query (0)	tracershield.ca	A (IP address)	IN (0x0001)
Jun 30, 2020 18:03:53.445960045 CEST	192.168.2.6	8.8.8.8	0xcc93	Standard query (0)	tracershield.ca	A (IP address)	IN (0x0001)

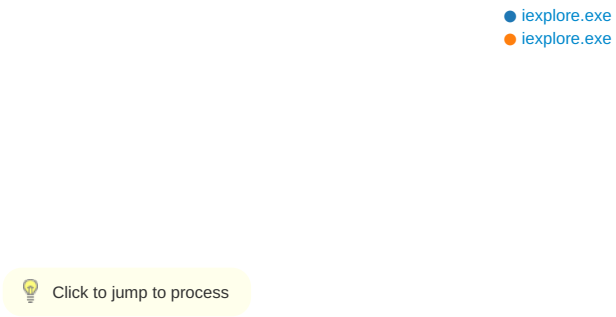
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 30, 2020 18:03:53.356720924 CEST	8.8.8.8	192.168.2.6	0x89bd	Name error (3)	tracershield.ca	none	none	A (IP address)	IN (0x0001)
Jun 30, 2020 18:03:53.397068024 CEST	8.8.8.8	192.168.2.6	0x5964	Name error (3)	tracershield.ca	none	none	A (IP address)	IN (0x0001)
Jun 30, 2020 18:03:53.479760885 CEST	8.8.8.8	192.168.2.6	0xcc93	Server failure (2)	tracershield.ca	none	none	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: iexplore.exe PID: 3284 Parent PID: 696

General

Start time:	18:03:50
Start date:	30/06/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff6e8aa0000
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: 3472 Parent PID: 3284

General

Start time:	18:03:51
Start date:	30/06/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3284 CREDAT:17410 /prefetch:2
Imagebase:	0xa50000
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