ID: 396513
Cookbook: browseurl.jbs
Time: 14:09:51
Date: 23/04/2021
Version: 31.0.0 Emerald

Table of Contents

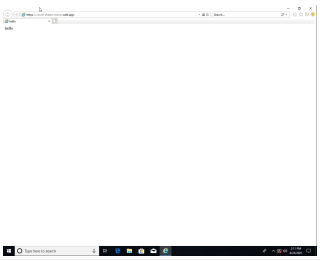
Analysis Report http://covid-sheets-mirror.web.app

Overview

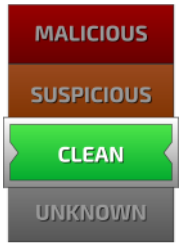
General Information

Sample URL:	http://covid-sheets-mirror.web.app
Analysis ID:	396513
Infos:	

Most interesting Screenshot:



Detection

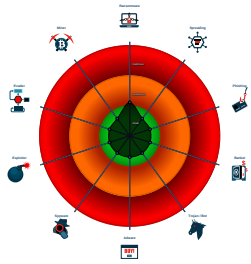


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 5772 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 4808 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5772 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

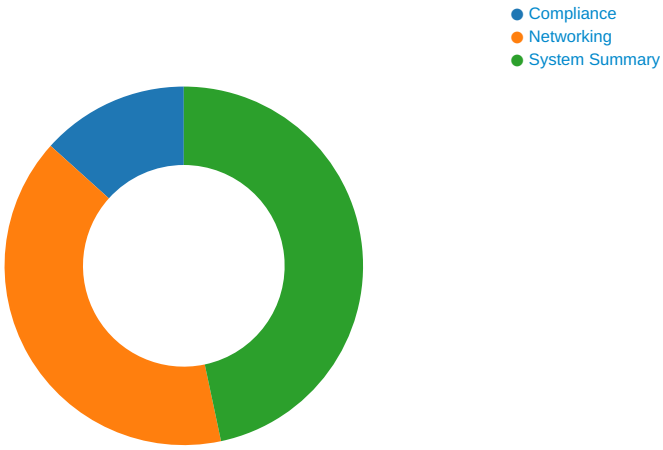
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



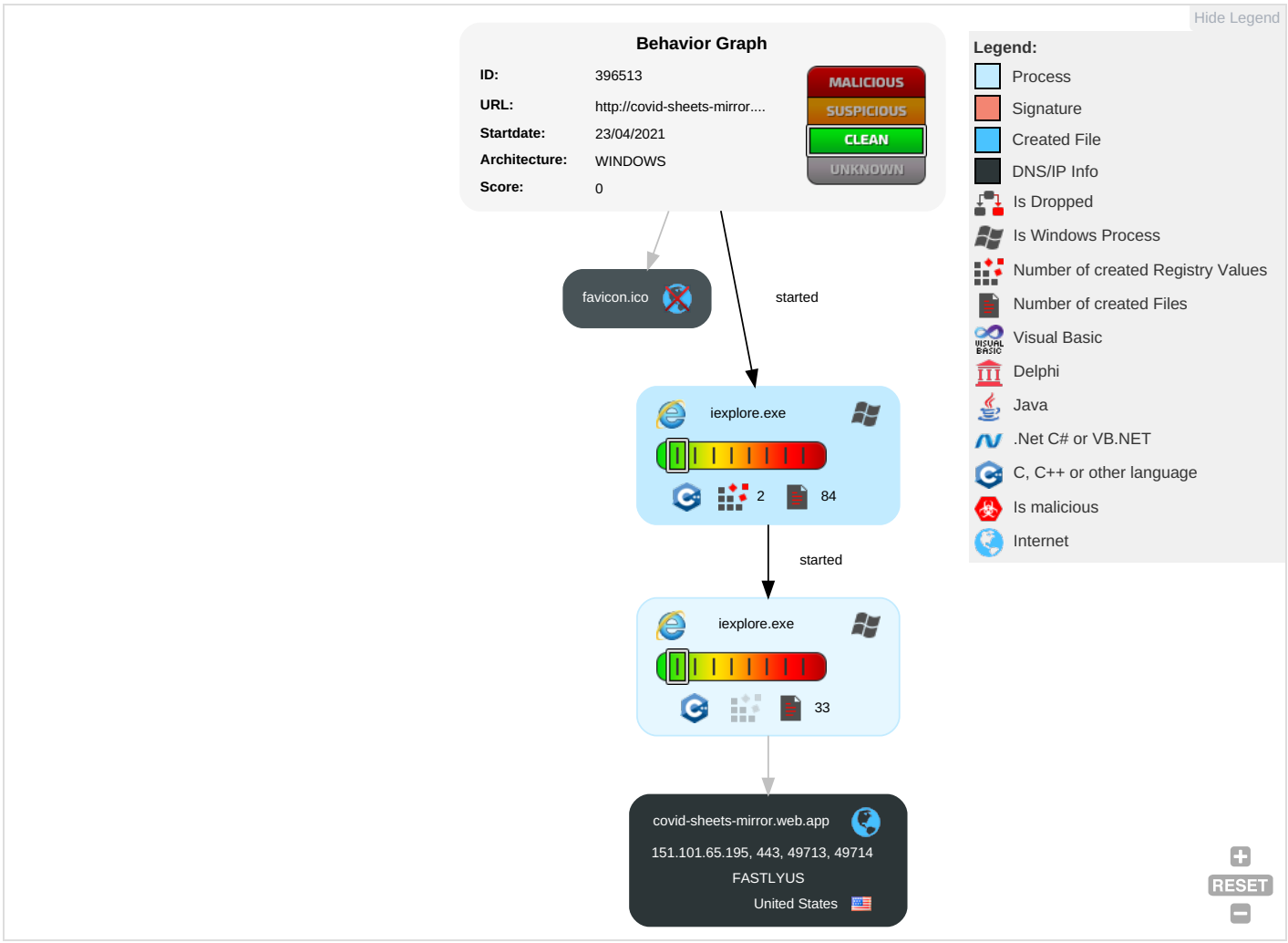
Click to jump to signature section

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

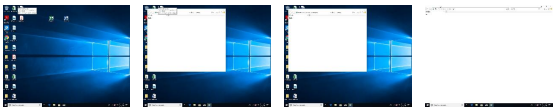
Behavior Graph

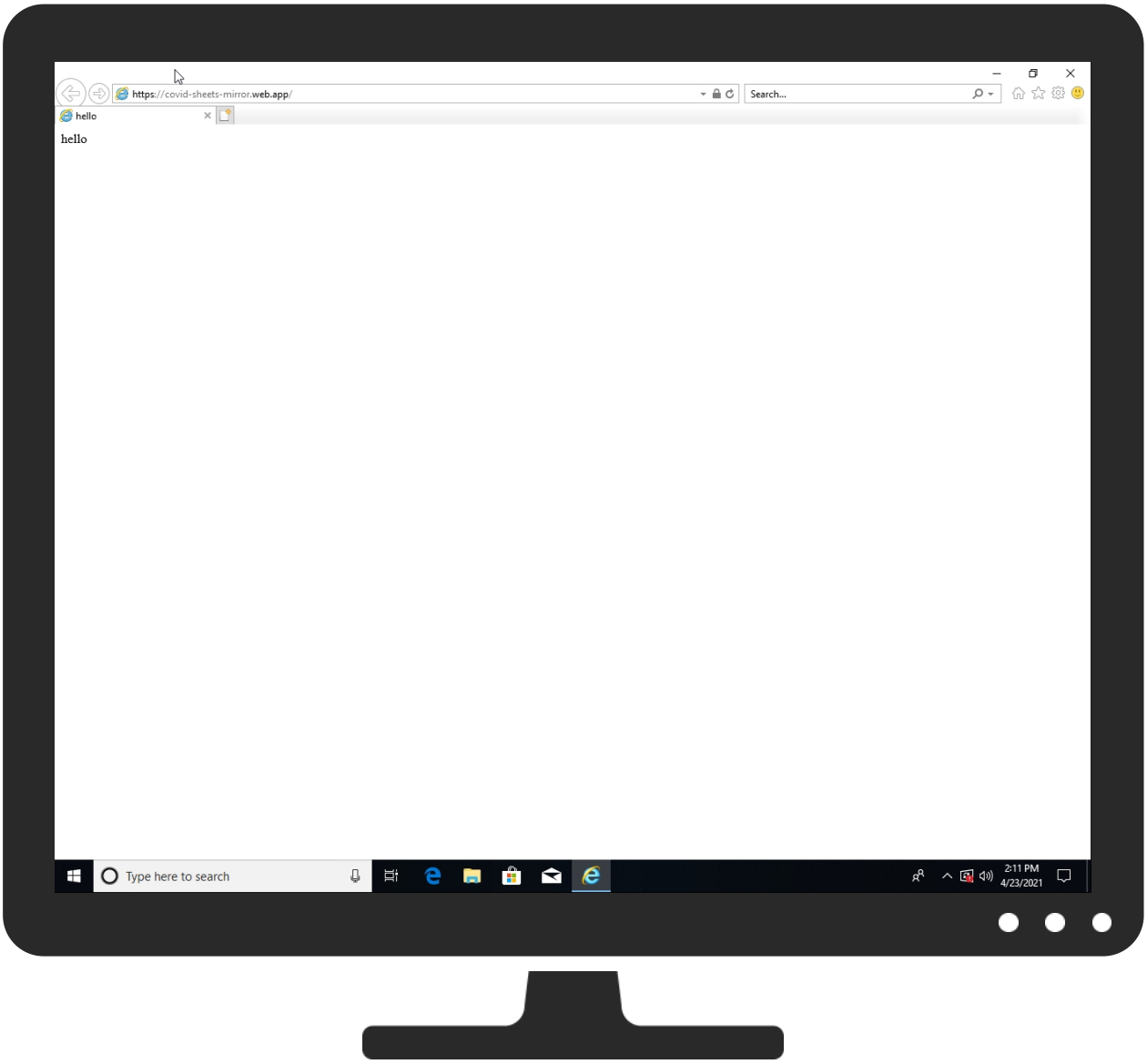


Screenshots

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://covid-sheets-mirror.web.app	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	
http://covid-sheets-mirror.web.app/	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://covid-sheets-mirror.web.app/Root	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
covid-sheets-mirror.web.app	151.101.65.195	true	false		unknown
favicon.ico	unknown	unknown	false		unknown

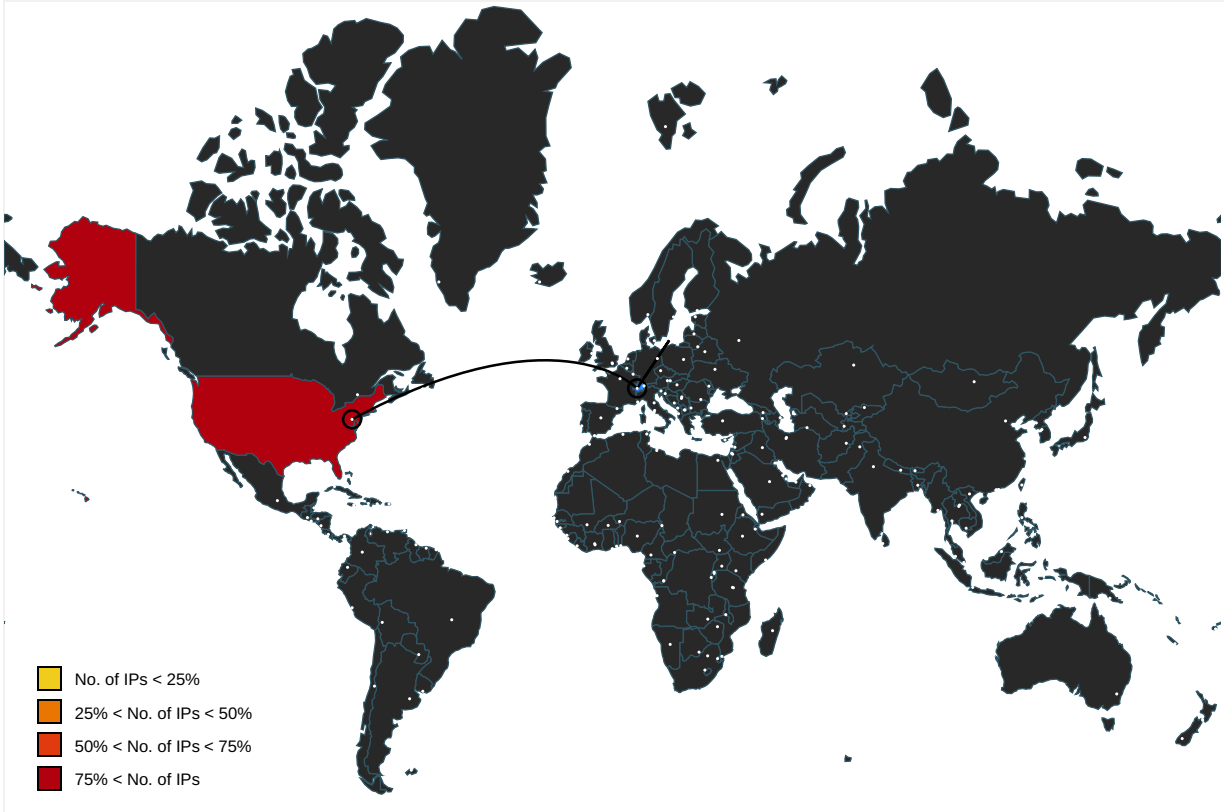
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://covid-sheets-mirror.web.app/	false	• Avira URL Cloud: safe	unknown
http://https://covid-sheets-mirror.web.app/	false		unknown

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	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://https://covid-sheets-mirror.web.app/Root	{5CBE83C7-A478-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://www.youtube.com/	msapplication.xml7.1.dr	false		high
http://https://covid-sheets-mirror.web.app/	~DFEA5ABAD7DD1060EC.TMP.1.dr	false		unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
151.101.65.195	covid-sheets-mirror.web.app	United States		54113	FASTLYUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	396513
Start date:	23.04.2021
Start time:	14:09:51
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://covid-sheets-mirror.web.app
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:	17
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:	CLEAN
Classification:	clean0.win@3/16@2/1
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 52.255.188.83, 92.122.145.220, 13.88.21.125, 13.64.90.137, 88.221.62.148, 184.30.24.56, 20.82.210.154, 152.199.19.161, 92.122.213.194, 92.122.213.247, 8.248.135.254, 8.248.131.254, 8.253.207.121, 67.27.159.126, 67.27.233.254, 51.103.5.186 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, go.microsoft.com, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, ie9comview.vo.msecnd.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus15.cloudapp.net, cs9.wpc.v0cdn.net • VT rate limit hit for: http://covid-sheets-mirror.web.app

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.{5CBE83C5-A478-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8578054712813123
Encrypted:	false
SSDEEP:	48:IwWGcprPGwpLHG/ap80GIpcrZGvnZpvrGGocUqp9ruGo4lx8pmrgGWcKw+9rmGWs:rKZ5ZP20WrGtrlfrZlMrWrgr3sfrbaMX
MD5:	CC7E1E8E8470E90009334F8D90E32559
SHA1:	68DC2B67D3E83D4E21DA76C35E1F4107A9B9E946
SHA-256:	EB04A295DD788AA82319D7B1DA12925C387B0D5BF5AC7972D67C05CA4B0C00AA
SHA-512:	E41FBDFD10AD4A772194EE02199E140A718809F162663C4D4293E095D8FE5B2DC51D8F4ED6A38617F4BFB94EB897EAFEC0E021BED67076E89640E72B6CF64B61
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\{5CBE83C7-A478-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24184
Entropy (8bit):	1.6317420801144664
Encrypted:	false
SSDEEP:	48:IwkGcprhGwpa/G4pQTGrapbS4GQpBqGHHpc7TGUp8WGzYpm6XGopPm0jMGaXpm:r4Z7QR63BSAjx2VWaMO0vg
MD5:	0A1D73735625E6CEEC7E047BCAAC0B77
SHA1:	4651D1D2B0BDF20639AC55ECA49F9544B28B1518
SHA-256:	2274B2457194DB0F7010C53070156E8DE94AF18E3291E1DAC1EE46141EE936E1
SHA-512:	B25CABC7D6BF0CD5B5A99CC860467716CA16F24BF1393BB0C1C524A1719651DAE6BF02ACFCB46ABF1C9D27716B825D10AD7BE36315A59AE676E8E17C273D514
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\{5CBE83C8-A478-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.566224183206568
Encrypted:	false
SSDEEP:	48:IwgiGcprCpGwpajG4pQ3GrapbSAGQpKKG7HpRvTGIpG:rgWZCDQV6LBSoAITNA
MD5:	E1EC7C1C143B2C0CAB7427E309EBF452
SHA1:	64E96D7824BCC2002B1F8A9C535B0C74FAFD9AA9
SHA-256:	E87CDCB05D977842991405640C6175E93BDB8BFE590C609F8A50BAF107448CC7
SHA-512:	09C9CD50FF0AE5103E7C4D2654F5290A313725427EB03DAC76CE2C29580C52B5DC8323AAF72EA355122D5AEAB845D4B9E8833BCDA6A8F15420EA932C71B8CACA
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):	5.131113248807694
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEqHuH3nWimI002EtM3MHdNMNxOEqHuH3nWimI00ObVbkEtMb:2d6NxOnE3SZHKd6NxOnE3SZ76b
MD5:	371CDEFE42CAE8C200D595FB0C495ACB
SHA1:	5AB5CE95115F3CA46CE0894C4DE804E098D41575
SHA-256:	C9ABEA9C8B0D97A63002C3709621D50447AA78868E3D18974DC528968BBEE422
SHA-512:	43E64A5856EDFF0E82E68D88B131B7776998875C424BEB4E0F08FC4FE3C644F711DE0489C571C770B89EF9C3A0EA2B11AB60D08C5F70F2D7E1F98A276B63DEFC
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x32f8f626,0x01d73885</date><accdate>0x32f8f626,0x01d73885</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>0x32f8f626,0x01d73885</date><accdate>0x32f8f626,0x01d73885</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):	5.143199050854845
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kdoHpoH3nWimI002EtM3MHdNMNxe2kdoHlDYH3nWimI00Obkak6Ety:2d6NxrLA3SZHKd6NxrLCH3SZ7Aa7b
MD5:	A6B6A3331C892E49CA4742AAF8C0012E
SHA1:	4C9913FE0A14957FFC932450336AA3F4191BE782
SHA-256:	1A86D3472F383202E91B11976533BCDDE339F9AF0CB8DF8A29ADDC040E7FF0AB
SHA-512:	E1AE7027375BADF45AC574932B8471805D805E2807ECAFDC416B2D89A08B35F7CB055F2389689EBF17D6A31C7E3F669EDB3361CE12075E25606475E5A920BC63
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x32e846cf,0x01d73885</date><accdate>0x32e846cf,0x01d73885</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>0x32e846cf,0x01d73885</date><accdate>0x32eaa854,0x01d73885</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):	5.150784577330843
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLqHuH3nWimI002EtM3MHdNMNxvLqHuH3nWimI00ObmZEtMb:2d6NxvEE3SZHKd6NxvEE3SZ7mb
MD5:	C34B9D63418DB5BF527620562F5F52BC
SHA1:	5E84A58E60955E0CF2BC20C922CF014AD8E1EE3B
SHA-256:	C4644B9A6C7B00FE19D7F8CB49A51D83A4F516FF8F870964315F9BE3745B873C
SHA-512:	23630649DD94F746F3F4A125357B82D26EEE2CD96ED98466548D1E732D054CEE36492D27B3217F0DBF72110CB7A98ACB896A39FBC895FCE157A271BBC629CC2
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x32f8f626,0x01d73885</date><accdate>0x32f8f626,0x01d73885</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>0x32f8f626,0x01d73885</date><accdate>0x32f8f626,0x01d73885</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.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):	5.150456092141202

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Encrypted:	false
SSDEEP:	12:TMHdNMNxihd3nWimI002EtM3MHdNMNxihd3nWimI00Obd5EtMb:2d6Nxsd3SZHKd6Nxsd3SZ7Jjb
MD5:	812414BAB46FD2BCE4CBD4D07809573C
SHA1:	671CC9A3D58A24C4E4E9824D93E897E1C474364B
SHA-256:	D42C6A46BC939107BC062CB69ADB12B2B576C2C30B3BB096846E166B83DE27E5
SHA-512:	57F157FDF106867581FF1F1FF5AC18206E159D7BE6CE18933AD4ACB52FECE97A5B0BA5A6E9BCB4CA6560A94C393A690B2B43B6613AC019FEE6A70605E079D1AC
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x32f693eb,0x01d73885</date><accdate>0x32f693eb,0x01d73885</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>0x32f693eb,0x01d73885</date><accdate>0x32f693eb,0x01d73885</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):	5.162692513473671
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGw6O3nWimI002EtM3MHdNMNxhGw6O3nWimI00Ob8K075EtMb:2d6NxQ9O3SZHKd6NxQ9O3SZ7YKajb
MD5:	02726B0CB164A17C6FDB2DF261C900A0
SHA1:	3D7742B8F4864BF46B5DE4E012FB8B37AF8B7AAD
SHA-256:	19BAEE40EB75BFE9761D90226CFD015B68C9C79850C39AAD085D4C05358DFF29
SHA-512:	6BCA164916B777391DB15CB40C397DF682461237DB480F2E2945372EDC70BD73E32B8494ADF16F1D0943F1B6D84323766C3D7B2E4495FDFC3695C3460DDF9F5
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x32fb5865,0x01d73885</date><accdate>0x32fb5865,0x01d73885</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>0x32fb5865,0x01d73885</date><accdate>0x32fb5865,0x01d73885</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):	5.14115169997254
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nhd3nWimI002EtM3MHdNMNx0nhuH3nWimI00ObxEtMb:2d6Nx0hd3SZHKd6Nx0hE3SZ7nb
MD5:	19A580B0363EDB6561068E88125AC1F1
SHA1:	045B80619C5DFBDD5B602C5B5CF7ECABBE765C75
SHA-256:	A5D60B792E77E35784E0653EE11DBF774B5AF53E0E5161D90DF37E0F04CD9BF8
SHA-512:	0E1BD77E6E89FA622F3BB1ECFA72A519ED2C972400C5A2F6453E3AA1312889DAE752BB2ABCCEDDD977C71AEFD44195FFF018FF4F6481AF8E2F88B28991EE87F3
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x32f693eb,0x01d73885</date><accdate>0x32f693eb,0x01d73885</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>0x32f693eb,0x01d73885</date><accdate>0x32f8f626,0x01d73885</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):	5.174567074706032
Encrypted:	false
SSDEEP:	12:TMHdNMNxxhd3nWimI002EtM3MHdNMNxxhd3nWimI00Ob6Kq5EtMb:2d6Nx3d3SZHKd6Nx3d3SZ7ob
MD5:	F2AF788FB00245E7D5793E546F30C9EE
SHA1:	1707FA46B56D466B78441F4656848118B85374C8

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
SHA-256:	D5CDE0EE0184FC1BBEBB8F7298F627749F09AF1368F9B61C7E49162972374F2A
SHA-512:	88789664E53AD6A97B51CFC56DD1ACBF8CE80F04D4C95CFD5368DE981F8CB5A61176D8D0B0FE81E1E4C35B00BF3F1DE7D068B8043B83E44F335460AE66ECD 05
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x32f693eb,0x01d73885</date> accdate>0x32f693eb,0x01d73885</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>0x32f693eb,0x01d73885</date><accdate>0 x32f693eb,0x01d73885</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):	5.144726615766364
Encrypted:	false
SSDEEP:	12:TMHdNMNxcVEHpEH3nWimI002EtM3MHdNMNxcVEHpEH3nWimI00ObVEtMb:2d6Nx/HuH3SZHKd6Nx/HuH3SZ7Db
MD5:	A24B38BFB1F401C7D686DD9928AE6B27
SHA1:	068C9581C1B021A2B47748511C37D625E7EF5197
SHA-256:	AB50BB7AACA601316CADE938787FBFDAEF4EE5087DF45263ECC3795C37DBFD00
SHA-512:	340ECD8ACC16D1E5AC011B66057B7A0EED156CF1F7F8B1ED1542712FB5142268092755E0AC9023F6917626F3F674834FF190B962E3C6F33171866CD7972776D9
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x32f43144,0x01d73885</date> <accdate>0x32f43144,0x01d73885</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>0x32f43144,0x01d73885</date><accdate >0x32f43144,0x01d73885</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):	5.141230654538224
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnVEHpEH3nWimI002EtM3MHdNMNxfnVEHd3nWimI00Obe5EtMb:2d6NxCHuH3SZHKd6NxCHd3SZ7ijb
MD5:	0E28EA18B7610C3E652BA78BBC60E26D
SHA1:	3183AB9F635676DE81F1D0501FD72433F79BF7B0
SHA-256:	9E945234603D90762AEBA8F4D97A4D6152244C6C3A35716C6A692127124EBBA5
SHA-512:	763A6DA75FC3E50AFC38FCDA92EDFAA41B207EEC73AF60868827A699AB2748D1386D5594A5FDA9160C753507375CAD60BBBE84C75520BE0823014E5E46D7595 E
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x32f43144,0x01d73885</date><a ccdate>0x32f43144,0x01d73885</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>0x32f43144,0x01d73885</date><accdate>0x3 2f693eb,0x01d73885</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile> </msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\ZRIEUREG.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	213
Entropy (8bit):	4.676325552995358
Encrypted:	false
SSDEEP:	6:h4QKxAGSKYkxfVfAbplgSUqoYhAEyXMqH7ZcXfGu:hPa+gC93nWErscPGu
MD5:	CA4061A139C209DD4AF9528B4B9EE895
SHA1:	D14FF75707DF7D8C672599B1005D3B6F728BE68B
SHA-256:	2F96A05DEBBE4E482069B6405FC1D7CF9D8D1E7079A8B49B0220F6C3482566B0
SHA-512:	299E82FF312B620E422570ACE9F0254DE1957F630D001E895F64FCAE34ECCB98D913BC07521A7520691E9598615F2B303D1C6EEFC5B974920EF527C19ECE50AE
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\ZRIEUREG.htm	
IE Cache URL:	http://https://covid-sheets-mirror.web.app/
Preview:	<!DOCTYPE html>..<html>.. <head>.. <meta charset="utf-8">.. <meta name="viewport" content="width=device-width, initial-scale=1">.. <title>hello</title>.... </head>.. <body>..hello.. </body>..</html>..

C:\Users\user\AppData\Local\Temp\~DFD4F5A23495EC46F8.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.34192789266646456
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laAFtMk7KtWI:kBqoxxJhHWSVSEabFtpsWI
MD5:	3CE591BBA39102B08835D2E1C137F5ED
SHA1:	9C45AA88ADE0B6F909D656838215F813EECCBED1
SHA-256:	A702D42E09869FB25EC234F19C90A13EA0B9C48650185E6EC8E0C9B0C4E6DE9B
SHA-512:	D366ABE33E9C806497C1CBCF92A3DB5FA379E761785A73E54E6A4FC16966337DDCAFB79BB3A5DE3CF98E0856D3B006B13BE3BD9611F3181ADB8DDF72EC3AB099
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFEA5ABAD7DD1060EC.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34377
Entropy (8bit):	0.3522917804508176
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwI9lw49l2W9l229l/6C:kBqoxKAuvScS+71nO6I6xm0j8
MD5:	F5DA0C1B643CEEAAFF2D5C7A12725E9E
SHA1:	AF75814DF8F44EEC497CAD29B689CFECD3B7E80D
SHA-256:	FBAF55DBBEF0E27442B9E00263A815C01B80D477254223AE7D9652E3EF4AC2A4
SHA-512:	0C78DDCD52263B7000FCDFE6F8A577874B2279B020B3496A5F794929EAF8A3975006D90AE28F0AEEC60AB2C100CF8BB737EC2A13C06ECB3AA492C51AD5C815EE
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

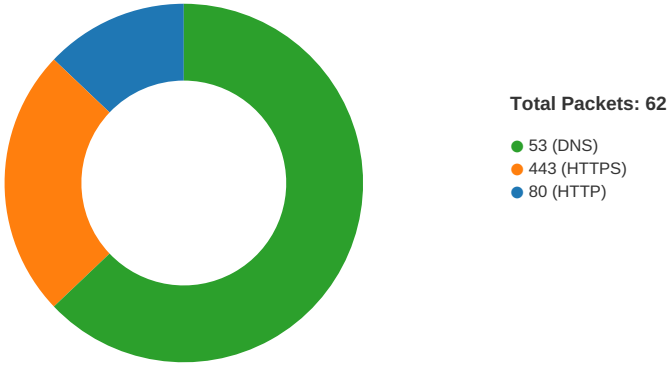
C:\Users\user\AppData\Local\Temp\~DFFBC719CFCCCFFAFC.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4809874128304595
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loKF9loG9lWLSd3yK:kBqoIRXLSd3yK
MD5:	5692C9BAA7EAB60BAECBDCF7DC2FDD92
SHA1:	611D3DBA4B4667D60921E57FD76C7BE7FF3817B7
SHA-256:	FACF750FD206F359D9B2AE36D16ECE984FE817B67952CE77B6563ED92660735D
SHA-512:	0E637C5A45D3478970A276510787763CBA461192516E422880876D3172E462B1D4C680BD458C5232E10E9501B31A9DB58B4FF3AB24DEDEFDA720E8403DFF8432
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 23, 2021 14:10:45.382936001 CEST	49713	80	192.168.2.3	151.101.65.195
Apr 23, 2021 14:10:45.383811951 CEST	49714	80	192.168.2.3	151.101.65.195
Apr 23, 2021 14:10:45.426325083 CEST	80	49713	151.101.65.195	192.168.2.3
Apr 23, 2021 14:10:45.426441908 CEST	49713	80	192.168.2.3	151.101.65.195
Apr 23, 2021 14:10:45.427074909 CEST	80	49714	151.101.65.195	192.168.2.3
Apr 23, 2021 14:10:45.427196980 CEST	49714	80	192.168.2.3	151.101.65.195
Apr 23, 2021 14:10:45.428792953 CEST	49713	80	192.168.2.3	151.101.65.195
Apr 23, 2021 14:10:45.472166061 CEST	80	49713	151.101.65.195	192.168.2.3
Apr 23, 2021 14:10:45.472213030 CEST	80	49713	151.101.65.195	192.168.2.3
Apr 23, 2021 14:10:45.472295046 CEST	80	49713	151.101.65.195	192.168.2.3
Apr 23, 2021 14:10:45.472369909 CEST	49713	80	192.168.2.3	151.101.65.195
Apr 23, 2021 14:10:45.472408056 CEST	49713	80	192.168.2.3	151.101.65.195
Apr 23, 2021 14:10:45.472553015 CEST	49713	80	192.168.2.3	151.101.65.195
Apr 23, 2021 14:10:45.482476950 CEST	49715	443	192.168.2.3	151.101.65.195
Apr 23, 2021 14:10:45.515908957 CEST	80	49713	151.101.65.195	192.168.2.3
Apr 23, 2021 14:10:45.525863886 CEST	443	49715	151.101.65.195	192.168.2.3
Apr 23, 2021 14:10:45.526108980 CEST	49715	443	192.168.2.3	151.101.65.195
Apr 23, 2021 14:10:45.535027027 CEST	49715	443	192.168.2.3	151.101.65.195
Apr 23, 2021 14:10:45.578368902 CEST	443	49715	151.101.65.195	192.168.2.3
Apr 23, 2021 14:10:45.580003977 CEST	443	49715	151.101.65.195	192.168.2.3
Apr 23, 2021 14:10:45.580040932 CEST	443	49715	151.101.65.195	192.168.2.3
Apr 23, 2021 14:10:45.580063105 CEST	443	49715	151.101.65.195	192.168.2.3
Apr 23, 2021 14:10:45.580080032 CEST	443	49715	151.101.65.195	192.168.2.3
Apr 23, 2021 14:10:45.580137968 CEST	49715	443	192.168.2.3	151.101.65.195
Apr 23, 2021 14:10:45.580185890 CEST	49715	443	192.168.2.3	151.101.65.195
Apr 23, 2021 14:10:45.626297951 CEST	49715	443	192.168.2.3	151.101.65.195
Apr 23, 2021 14:10:45.635253906 CEST	49715	443	192.168.2.3	151.101.65.195
Apr 23, 2021 14:10:45.635406971 CEST	49715	443	192.168.2.3	151.101.65.195
Apr 23, 2021 14:10:45.669883966 CEST	443	49715	151.101.65.195	192.168.2.3
Apr 23, 2021 14:10:45.670063019 CEST	49715	443	192.168.2.3	151.101.65.195
Apr 23, 2021 14:10:45.697458982 CEST	443	49715	151.101.65.195	192.168.2.3
Apr 23, 2021 14:10:45.697489977 CEST	443	49715	151.101.65.195	192.168.2.3
Apr 23, 2021 14:10:45.697599888 CEST	49715	443	192.168.2.3	151.101.65.195

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 23, 2021 14:10:45.697910070 CEST	49715	443	192.168.2.3	151.101.65.195
Apr 23, 2021 14:10:45.788424969 CEST	443	49715	151.101.65.195	192.168.2.3
Apr 23, 2021 14:10:45.954411030 CEST	443	49715	151.101.65.195	192.168.2.3
Apr 23, 2021 14:10:45.954583883 CEST	49715	443	192.168.2.3	151.101.65.195
Apr 23, 2021 14:10:46.403342009 CEST	49715	443	192.168.2.3	151.101.65.195
Apr 23, 2021 14:10:46.446680069 CEST	443	49715	151.101.65.195	192.168.2.3
Apr 23, 2021 14:10:46.673516989 CEST	443	49715	151.101.65.195	192.168.2.3
Apr 23, 2021 14:10:46.673662901 CEST	49715	443	192.168.2.3	151.101.65.195
Apr 23, 2021 14:10:46.674305916 CEST	443	49715	151.101.65.195	192.168.2.3
Apr 23, 2021 14:10:46.674514055 CEST	49715	443	192.168.2.3	151.101.65.195

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 23, 2021 14:10:37.019797087 CEST	50620	53	192.168.2.3	8.8.8.8
Apr 23, 2021 14:10:37.068432093 CEST	53	50620	8.8.8.8	192.168.2.3
Apr 23, 2021 14:10:37.642507076 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 23, 2021 14:10:37.711415052 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 23, 2021 14:10:37.916222095 CEST	60152	53	192.168.2.3	8.8.8.8
Apr 23, 2021 14:10:37.966700077 CEST	53	60152	8.8.8.8	192.168.2.3
Apr 23, 2021 14:10:40.725169897 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 23, 2021 14:10:40.773777962 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 23, 2021 14:10:41.951009989 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 23, 2021 14:10:41.999550104 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 23, 2021 14:10:43.182924986 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 23, 2021 14:10:43.243848085 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 23, 2021 14:10:43.976178885 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 23, 2021 14:10:44.033844948 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 23, 2021 14:10:44.738712072 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 23, 2021 14:10:44.787422895 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 23, 2021 14:10:45.295485973 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 23, 2021 14:10:45.370389938 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 23, 2021 14:10:46.094820023 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 23, 2021 14:10:46.145075083 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 23, 2021 14:10:49.473581076 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 23, 2021 14:10:49.525021076 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 23, 2021 14:10:50.695944071 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 23, 2021 14:10:50.744695902 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 23, 2021 14:10:51.908287048 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 23, 2021 14:10:51.961042881 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 23, 2021 14:10:52.817595959 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 23, 2021 14:10:52.866347075 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 23, 2021 14:10:53.998076916 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 23, 2021 14:10:54.051080942 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 23, 2021 14:10:54.974711895 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 23, 2021 14:10:55.026254892 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 23, 2021 14:10:55.736090899 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 23, 2021 14:10:55.785558939 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 23, 2021 14:10:56.534202099 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 23, 2021 14:10:56.582906008 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 23, 2021 14:11:00.548641920 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 23, 2021 14:11:00.597563982 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 23, 2021 14:11:01.719312906 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 23, 2021 14:11:01.777318001 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 23, 2021 14:11:02.703984022 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 23, 2021 14:11:02.753901005 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 23, 2021 14:11:03.560473919 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 23, 2021 14:11:03.609575033 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 23, 2021 14:11:08.893302917 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 23, 2021 14:11:08.972076893 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 23, 2021 14:11:11.892043114 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 23, 2021 14:11:11.945847034 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 23, 2021 14:11:14.014657974 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 23, 2021 14:11:14.063355923 CEST	53	55435	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 23, 2021 14:11:14.684401035 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 23, 2021 14:11:14.733036041 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 23, 2021 14:11:15.007190943 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 23, 2021 14:11:15.064589024 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 23, 2021 14:11:15.695420980 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 23, 2021 14:11:15.757361889 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 23, 2021 14:11:16.025254011 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 23, 2021 14:11:16.087250948 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 23, 2021 14:11:16.694875002 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 23, 2021 14:11:16.745696068 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 23, 2021 14:11:18.038948059 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 23, 2021 14:11:18.103725910 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 23, 2021 14:11:18.710671902 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 23, 2021 14:11:18.759454966 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 23, 2021 14:11:19.188448906 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 23, 2021 14:11:19.250159979 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 23, 2021 14:11:22.039028883 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 23, 2021 14:11:22.100903034 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 23, 2021 14:11:22.726444006 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 23, 2021 14:11:22.783696890 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 23, 2021 14:11:30.384692907 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 23, 2021 14:11:30.433247089 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 23, 2021 14:11:31.836992025 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 23, 2021 14:11:31.899733067 CEST	53	56579	8.8.8.8	192.168.2.3
Apr 23, 2021 14:11:51.415041924 CEST	60633	53	192.168.2.3	8.8.8.8
Apr 23, 2021 14:11:51.465854883 CEST	53	60633	8.8.8.8	192.168.2.3
Apr 23, 2021 14:11:55.235836983 CEST	61292	53	192.168.2.3	8.8.8.8
Apr 23, 2021 14:11:55.297214031 CEST	53	61292	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 23, 2021 14:10:45.295485973 CEST	192.168.2.3	8.8.8.8	0x4f6f	Standard query (0)	covid-sheets-mirror.web.app	A (IP address)	IN (0x0001)
Apr 23, 2021 14:11:01.719312906 CEST	192.168.2.3	8.8.8.8	0x674b	Standard query (0)	favicon.ico	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 23, 2021 14:10:45.370389938 CEST	8.8.8.8	192.168.2.3	0x4f6f	No error (0)	covid-sheets-mirror.web.app		151.101.65.195	A (IP address)	IN (0x0001)
Apr 23, 2021 14:10:45.370389938 CEST	8.8.8.8	192.168.2.3	0x4f6f	No error (0)	covid-sheets-mirror.web.app		151.101.1.195	A (IP address)	IN (0x0001)
Apr 23, 2021 14:11:01.777318001 CEST	8.8.8.8	192.168.2.3	0x674b	Name error (3)	favicon.ico	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- covid-sheets-mirror.web.app

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49713	151.101.65.195	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Apr 23, 2021 14:10:45.428792953 CEST	871	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: covid-sheets-mirror.web.app Connection: Keep-Alive
Apr 23, 2021 14:10:45.472213030 CEST	897	IN	HTTP/1.1 301 Moved Permanently Server: Varnish Retry-After: 0 Location: https://covid-sheets-mirror.web.app/ Content-Length: 0 Accept-Ranges: bytes Date: Fri, 23 Apr 2021 12:10:45 GMT Connection: close X-Served-By: cache-hhn4080-HHN X-Cache: HIT X-Cache-Hits: 0 X-Timer: S1619179845.464808,VS0,VE0

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 23, 2021 14:10:45.580080032 CEST	151.101.65.195	443	192.168.2.3	49715	CN=web.app CN=GTS CA 1D4, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1D4, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Wed Mar 17 19:54:48 CET 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Tue Jun 15 20:54:47 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1D4, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		

Code Manipulations

Statistics

Behavior

● iexplore.exe
● iexplore.exe

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5772 Parent PID: 792

General

Start time:	14:10:42
Start date:	23/04/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff683af0000
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: 4808 Parent PID: 5772

General

Start time:	14:10:43
Start date:	23/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5772 CREDAT:17410 /prefetch:2
Imagebase:	0x990000
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