ID: 424073
Cookbook: browseurl.jbs
Time: 16:20:46
Date: 25/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

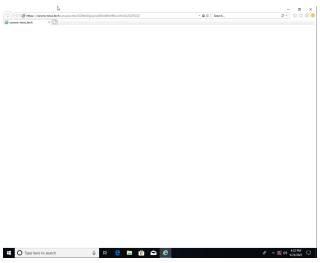
Analysis Report https://corona-news.tech/unsubscribe/…

Overview

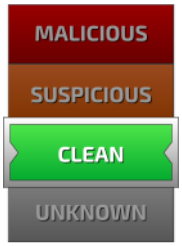
General Information

Sample URL:	http://https://corona-news.tech/unsubscribe/ZG9taW5pay5zdXRlckBheHBvLmNvbQ%3D%3D
Analysis ID:	424073
Infos:	

Most interesting Screenshot:



Detection

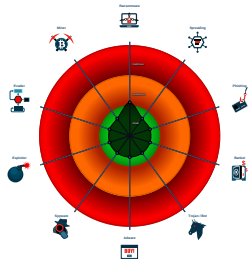


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- **System is w10x64**
- iexplore.exe (PID: 5424 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5628 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5424 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

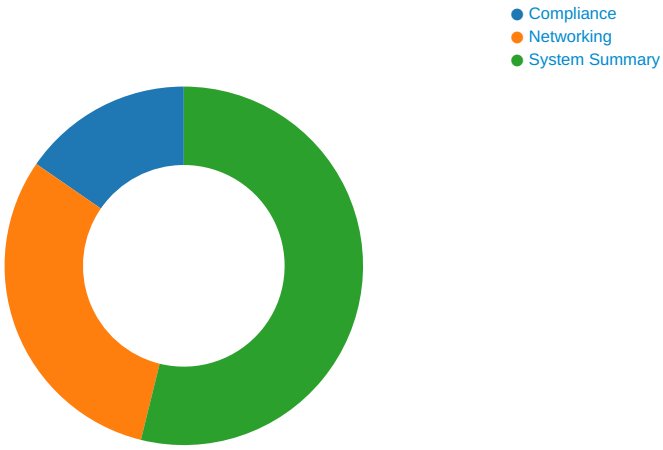
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



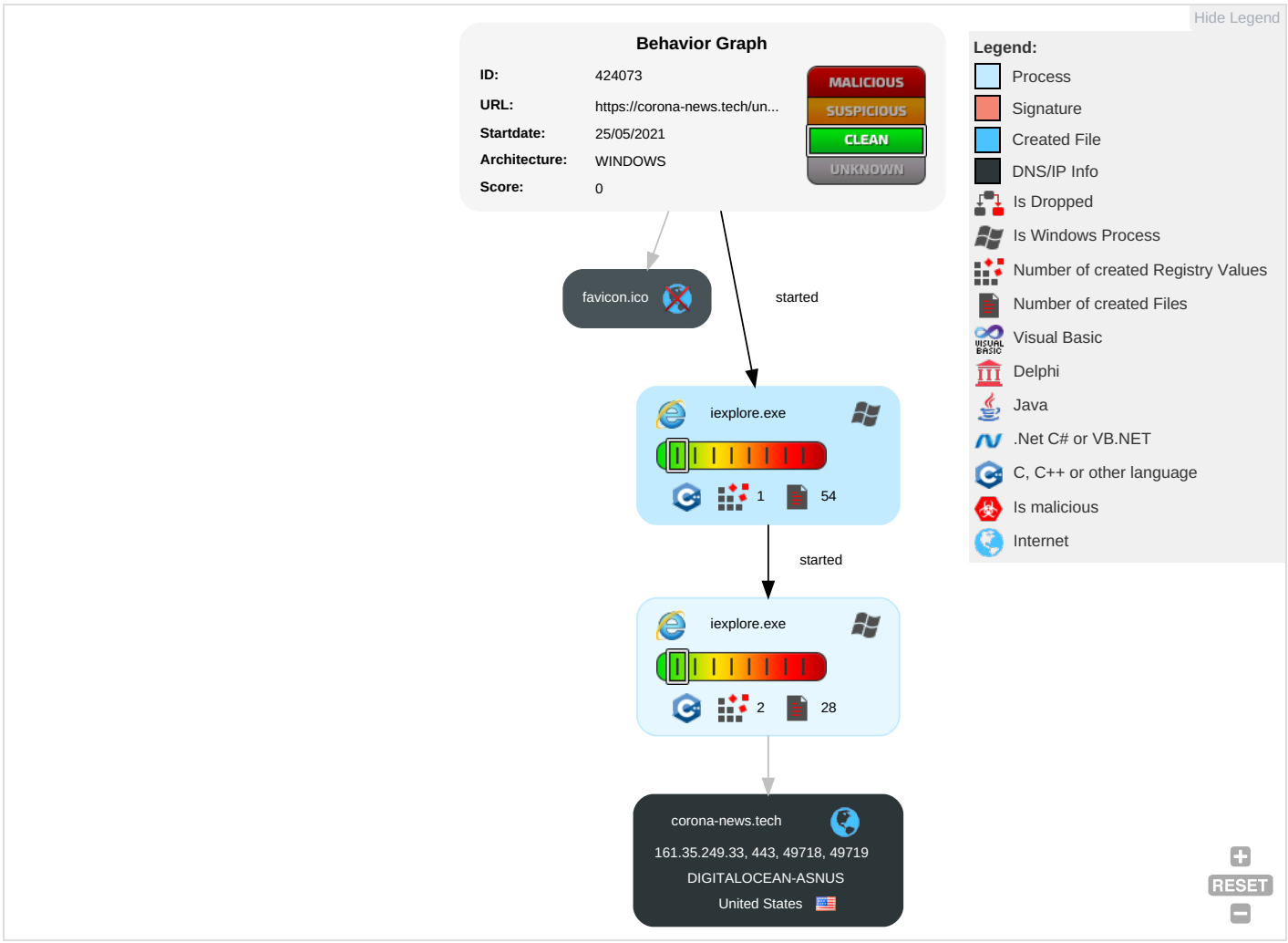
Click to jump to signature section

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

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impac
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modif Syste Partiti
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lockc
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data

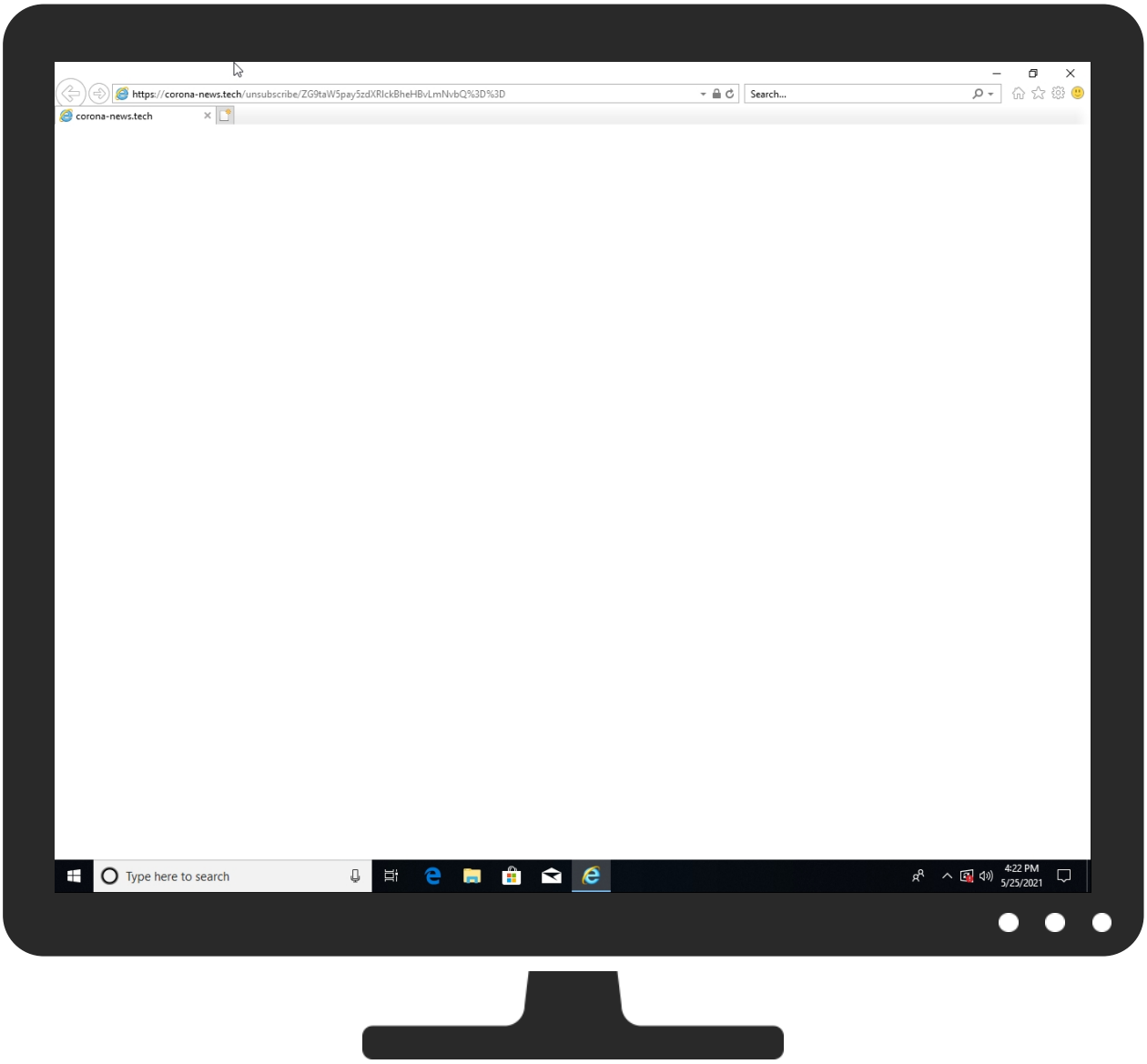
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://corona-news.tech/unsubscribe/ZG9taW5pay5zdXRlckBheHBvLmNvbQ%3D%3D	1%	Virustotal		Browse
http://https://corona-news.tech/unsubscribe/ZG9taW5pay5zdXRlckBheHBvLmNvbQ%3D%3D	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
corona-news.tech	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://corona-news.tech/unsubscribe/ZG9taW5pay5zdXRlckBheHBvLmNvbQ%3D%3DRoot	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
corona-news.tech	161.35.249.33	true	false	• 0%, Virustotal, Browse	unknown
favicon.ico	unknown	unknown	false		unknown

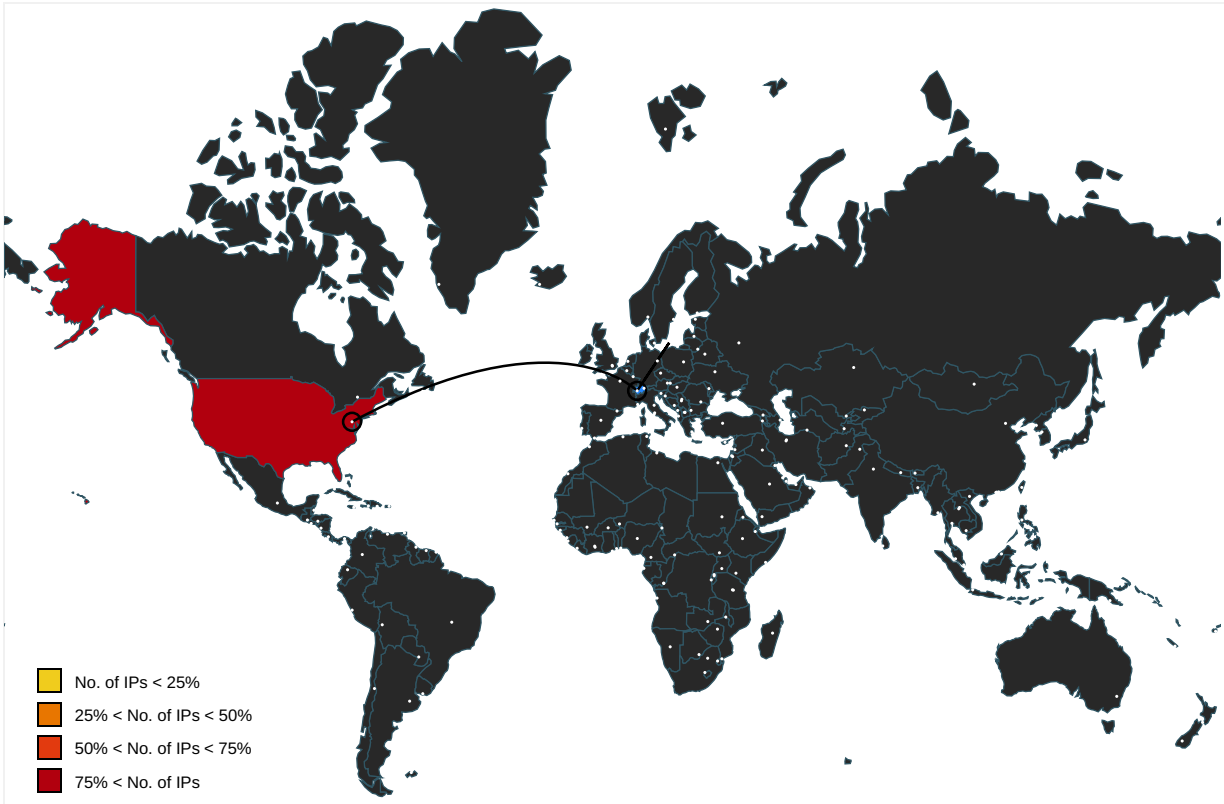
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://corona-news.tech/unsubscribe/ZG9taW5pay5zdXRlckBheHBvLmNvbQ%3D%3D	false		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://corona-news.tech/unsubscribe/ZG9taW5pay5zdXRlckBheHBvLmNvbQ%3D%3DRoot	{F39CEA8E-BDAF-11EB-90E5-ECF4BB570DC9}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://corona-news.tech/unsubscribe/ZG9taW5pay5zdXRlckBheHBvLmNvbQ%3D%3D	~DF5F5139FBE8D279C0.TMP.1.dr	false		unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
161.35.249.33	corona-news.tech	United States		14061	DIGITALOCEAN-ASNUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	424073
Start date:	25.05.2021
Start time:	16:20:46
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://corona-news.tech/unsubscribe/ZG9taW5pay5zdXRlckBheHBvLmNvbQ%3D%3D
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:	15
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@3/6@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): 93.184.220.29, 92.122.145.220, 13.88.21.125, 88.221.62.148, 104.43.193.48, 92.122.144.200, 20.82.210.154, 152.199.19.161, 2.20.142.209, 2.20.143.16, 51.103.5.159, 92.122.213.194, 92.122.213.247 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, cs9.wac.phicdn.net, store-images.s-microsoft.com-c.edgekey.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, 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, ocsp.digicert.com, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, client.wns.windows.com, fs.microsoft.com, ie9comview.vo.msecnd.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus15.cloudapp.net, cs9.wpc.v0cdn.net

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{F39CEA8C-BDAF-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8564562803384559
Encrypted:	false
SSDEEP:	96:rrZYZl2zWNtXbf5hCKM9aq00QAxfZhD6X:rrZYZl2zWNtrf5RMzcOfZMX
MD5:	8F7D8C0B026F6F7E86DABF97EBEB31B9
SHA1:	44265C1A4BC3315FE9D21ECED1A27967A22B5EB1
SHA-256:	7216B567FCF11C6B247749154FD8E16A6C3B3760B210525D2F28139340B4C4AE
SHA-512:	C377408479D0E2C507AF8F93C4CC4CFA8C152CED5F38E05CDF6D7A9D7C138F50B4CB6AE197925558E0F01D12EE50E24EA53905602C6983807981310FF7D1F79
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\{F39CEA8E-BDAF-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24256
Entropy (8bit):	1.650199349610017
Encrypted:	false
SSDEEP:	48:IwzGcpr2GwpaJG4pQ9GrapbSrGQpBnGHHpcqTGUp8YGzYpm9aGopV78TEZGSNpm:rJZuQL6dBSFjS26W8Msbfng
MD5:	29AB0C9938D91732450A06C4768D0F6E
SHA1:	E86D2C6883A600B0F3ABBC4A3381A03C96C75795
SHA-256:	308657399534C2AC7CD9CD1E0B8CB0E22A11C37C0026D0650B26C6ECF0DA7E72
SHA-512:	15BAE953DE1BF22BCB055B2CD2EAF37E3DD9FA2C69CFF91ECC4414C03C51FB3751E9B447FD51E3798F5FAEA4290626DF92FCBA52842C49559ED09E33D857B5 04
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{F39CEA8E-BDAF-11EB-90E5-ECF4BB570DC9}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{FD58632A-BDAF-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5659222782875168
Encrypted:	false
SSDEEP:	48:IwKGcprrGwpahG4pQBGrapbSvGQpKcG7HpRHTGIpG:ruZlQz6RBS5A3T1A
MD5:	84781A322EA876BB550EEE2BC71EE3CC
SHA1:	028E8CC5A3BA7F6DFC253AE33FDAA4816EF5493E
SHA-256:	8432259BB74827E33866B62C5AECF12CCDBB2BDEE0F93FA3D4ADE06ECEF7B2E3
SHA-512:	4A34BDFB5E35C332E59A62AF34AE26C9441EE8FF44256698294D95AB1C992963B8C3455BE71888BFD4C3E20ADE29F008315B972792283E3C4293BAD04DDB87B
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Temp\~DF5F5139FBE8D279C0.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34449
Entropy (8bit):	0.36683324364657494
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwT9lwT9l2l9l2l9l/9m:kBqoxKAuvScS+sKQx9I9378TEJ
MD5:	B698E16400D5639563844E6E81C6E742
SHA1:	6C5840F52E6C62A060B0404D99EAFB4135B065D3
SHA-256:	939ABEC9F8DCB6DF616A6175E63E07C1738E159F8FC5698742F8A5E37008AD60
SHA-512:	AE057EAB6B5A75F86695431E7DEE93656CC3E3AED3C6D40B1DEAE1F09BAA79950674B0C58427D30561033040D65257A38A62F119DA65F566171725CDAC87A83
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFA4B83D12B410FB30.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4832349124351087
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lo/9lo/9lWS9wPU57:kBqoIg+S9ws57
MD5:	DAF7F1C05B743F51C84E971AE0470F9C
SHA1:	9AF6A8CD24A54D3BF9CEC9B51329921A64915593
SHA-256:	5B22CE86DBA084D461EF662EE962B7B2FB6925FACB7C9D5BE3C5DBC864AC48FD
SHA-512:	B2052D9AD41ED74FE22D844CADFA9D473E004D7984823B7D102BCFFED2261888CB0536074FFE920B3F8F7794DADDFA2B530213F11E4C3D8F189E7D8F5D0580
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFBCF9A634093BE3CA.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data

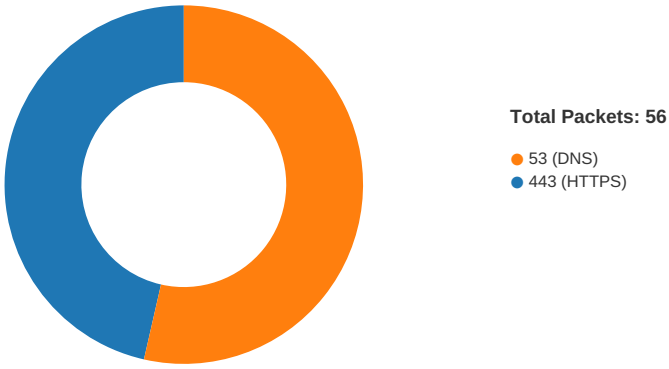
C:\Users\user\AppData\Local\Temp\~DFBCF9A634093BE3CA.TMP	
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.3940030802848299
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laAggpPTQMug/:kBqoxxJhHWSVSEabhxb
MD5:	13F0F1F65B7A3C1D0999EF7C277B0463
SHA1:	93FBFF4545A2BF454A90AF315694B10B02149ABC
SHA-256:	8AEC8A8D3C90AC9AE3F6F1D0891855D42E3299447C99FD4BF7436D2473F99F83
SHA-512:	515B2565FC85B3C13A3FF353F1DA82EE3176DF5A749F25C358542432B683CF85405C8F6A09B21CEF5C4ED64F1A57B671A43F533DD35CF77A506B75A6985C29AE
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
May 25, 2021 16:21:39.392576933 CEST	49718	443	192.168.2.5	161.35.249.33
May 25, 2021 16:21:39.394439936 CEST	49719	443	192.168.2.5	161.35.249.33
May 25, 2021 16:21:39.520654917 CEST	443	49718	161.35.249.33	192.168.2.5
May 25, 2021 16:21:39.521343946 CEST	49718	443	192.168.2.5	161.35.249.33
May 25, 2021 16:21:39.522048950 CEST	443	49719	161.35.249.33	192.168.2.5
May 25, 2021 16:21:39.522166967 CEST	49719	443	192.168.2.5	161.35.249.33
May 25, 2021 16:21:39.526681900 CEST	49718	443	192.168.2.5	161.35.249.33
May 25, 2021 16:21:39.526714087 CEST	49719	443	192.168.2.5	161.35.249.33
May 25, 2021 16:21:39.657084942 CEST	443	49718	161.35.249.33	192.168.2.5
May 25, 2021 16:21:39.657119989 CEST	443	49718	161.35.249.33	192.168.2.5
May 25, 2021 16:21:39.657145977 CEST	443	49718	161.35.249.33	192.168.2.5
May 25, 2021 16:21:39.657161951 CEST	443	49718	161.35.249.33	192.168.2.5
May 25, 2021 16:21:39.657179117 CEST	49718	443	192.168.2.5	161.35.249.33
May 25, 2021 16:21:39.657181978 CEST	443	49718	161.35.249.33	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 25, 2021 16:21:39.657238007 CEST	49718	443	192.168.2.5	161.35.249.33
May 25, 2021 16:21:39.660262108 CEST	443	49719	161.35.249.33	192.168.2.5
May 25, 2021 16:21:39.660295010 CEST	443	49719	161.35.249.33	192.168.2.5
May 25, 2021 16:21:39.660321951 CEST	443	49719	161.35.249.33	192.168.2.5
May 25, 2021 16:21:39.660336971 CEST	49719	443	192.168.2.5	161.35.249.33
May 25, 2021 16:21:39.660342932 CEST	443	49719	161.35.249.33	192.168.2.5
May 25, 2021 16:21:39.660358906 CEST	49719	443	192.168.2.5	161.35.249.33
May 25, 2021 16:21:39.660362959 CEST	443	49719	161.35.249.33	192.168.2.5
May 25, 2021 16:21:39.660387039 CEST	49719	443	192.168.2.5	161.35.249.33
May 25, 2021 16:21:39.660412073 CEST	49719	443	192.168.2.5	161.35.249.33
May 25, 2021 16:21:39.660491943 CEST	49719	443	192.168.2.5	161.35.249.33
May 25, 2021 16:21:39.692184925 CEST	49718	443	192.168.2.5	161.35.249.33
May 25, 2021 16:21:39.694672108 CEST	49719	443	192.168.2.5	161.35.249.33
May 25, 2021 16:21:39.698719025 CEST	49718	443	192.168.2.5	161.35.249.33
May 25, 2021 16:21:39.821301937 CEST	443	49718	161.35.249.33	192.168.2.5
May 25, 2021 16:21:39.821409941 CEST	49718	443	192.168.2.5	161.35.249.33
May 25, 2021 16:21:39.823519945 CEST	443	49719	161.35.249.33	192.168.2.5
May 25, 2021 16:21:39.823622942 CEST	49719	443	192.168.2.5	161.35.249.33
May 25, 2021 16:21:39.868987083 CEST	443	49718	161.35.249.33	192.168.2.5
May 25, 2021 16:22:39.824668884 CEST	443	49719	161.35.249.33	192.168.2.5
May 25, 2021 16:22:39.826035976 CEST	49719	443	192.168.2.5	161.35.249.33
May 25, 2021 16:22:39.826045036 CEST	443	49719	161.35.249.33	192.168.2.5
May 25, 2021 16:22:39.826122046 CEST	49719	443	192.168.2.5	161.35.249.33
May 25, 2021 16:22:39.829587936 CEST	443	49718	161.35.249.33	192.168.2.5
May 25, 2021 16:22:39.829726934 CEST	49718	443	192.168.2.5	161.35.249.33
May 25, 2021 16:22:40.246503115 CEST	49719	443	192.168.2.5	161.35.249.33
May 25, 2021 16:22:40.247297049 CEST	49719	443	192.168.2.5	161.35.249.33
May 25, 2021 16:22:40.248486996 CEST	49718	443	192.168.2.5	161.35.249.33
May 25, 2021 16:22:40.373558044 CEST	443	49719	161.35.249.33	192.168.2.5
May 25, 2021 16:22:40.373708010 CEST	49719	443	192.168.2.5	161.35.249.33
May 25, 2021 16:22:40.375833035 CEST	443	49718	161.35.249.33	192.168.2.5
May 25, 2021 16:22:40.379618883 CEST	443	49718	161.35.249.33	192.168.2.5
May 25, 2021 16:22:40.379775047 CEST	49718	443	192.168.2.5	161.35.249.33

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 25, 2021 16:21:27.271135092 CEST	54795	53	192.168.2.5	8.8.8.8
May 25, 2021 16:21:27.323276043 CEST	53	54795	8.8.8.8	192.168.2.5
May 25, 2021 16:21:28.132626057 CEST	49557	53	192.168.2.5	8.8.8.8
May 25, 2021 16:21:28.193675995 CEST	53	49557	8.8.8.8	192.168.2.5
May 25, 2021 16:21:28.363732100 CEST	61733	53	192.168.2.5	8.8.8.8
May 25, 2021 16:21:28.417289972 CEST	53	61733	8.8.8.8	192.168.2.5
May 25, 2021 16:21:29.822879076 CEST	65447	53	192.168.2.5	8.8.8.8
May 25, 2021 16:21:29.874293089 CEST	53	65447	8.8.8.8	192.168.2.5
May 25, 2021 16:21:30.979235888 CEST	52441	53	192.168.2.5	8.8.8.8
May 25, 2021 16:21:31.028963089 CEST	53	52441	8.8.8.8	192.168.2.5
May 25, 2021 16:21:32.415137053 CEST	62176	53	192.168.2.5	8.8.8.8
May 25, 2021 16:21:32.465653896 CEST	53	62176	8.8.8.8	192.168.2.5
May 25, 2021 16:21:34.543663979 CEST	59596	53	192.168.2.5	8.8.8.8
May 25, 2021 16:21:34.593041897 CEST	53	59596	8.8.8.8	192.168.2.5
May 25, 2021 16:21:36.812438965 CEST	65296	53	192.168.2.5	8.8.8.8
May 25, 2021 16:21:36.865326881 CEST	53	65296	8.8.8.8	192.168.2.5
May 25, 2021 16:21:37.955298901 CEST	63183	53	192.168.2.5	8.8.8.8
May 25, 2021 16:21:38.017707109 CEST	53	63183	8.8.8.8	192.168.2.5
May 25, 2021 16:21:38.224860907 CEST	60151	53	192.168.2.5	8.8.8.8
May 25, 2021 16:21:38.274178028 CEST	53	60151	8.8.8.8	192.168.2.5
May 25, 2021 16:21:39.145023108 CEST	56969	53	192.168.2.5	8.8.8.8
May 25, 2021 16:21:39.379641056 CEST	53	56969	8.8.8.8	192.168.2.5
May 25, 2021 16:21:39.492075920 CEST	55161	53	192.168.2.5	8.8.8.8
May 25, 2021 16:21:39.542303085 CEST	53	55161	8.8.8.8	192.168.2.5
May 25, 2021 16:21:40.388914108 CEST	54757	53	192.168.2.5	8.8.8.8
May 25, 2021 16:21:40.447354078 CEST	53	54757	8.8.8.8	192.168.2.5
May 25, 2021 16:21:41.278615952 CEST	49992	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 25, 2021 16:21:41.328169107 CEST	53	49992	8.8.8.8	192.168.2.5
May 25, 2021 16:21:58.123661995 CEST	60075	53	192.168.2.5	8.8.8.8
May 25, 2021 16:21:58.213941097 CEST	53	60075	8.8.8.8	192.168.2.5
May 25, 2021 16:22:07.525724888 CEST	55016	53	192.168.2.5	8.8.8.8
May 25, 2021 16:22:07.583666086 CEST	53	55016	8.8.8.8	192.168.2.5
May 25, 2021 16:22:08.016684055 CEST	64345	53	192.168.2.5	8.8.8.8
May 25, 2021 16:22:08.076773882 CEST	53	64345	8.8.8.8	192.168.2.5
May 25, 2021 16:22:08.704226971 CEST	57128	53	192.168.2.5	8.8.8.8
May 25, 2021 16:22:08.762134075 CEST	53	57128	8.8.8.8	192.168.2.5
May 25, 2021 16:22:09.006998062 CEST	64345	53	192.168.2.5	8.8.8.8
May 25, 2021 16:22:09.056512117 CEST	53	64345	8.8.8.8	192.168.2.5
May 25, 2021 16:22:09.788331985 CEST	57128	53	192.168.2.5	8.8.8.8
May 25, 2021 16:22:09.837726116 CEST	53	57128	8.8.8.8	192.168.2.5
May 25, 2021 16:22:10.022970915 CEST	64345	53	192.168.2.5	8.8.8.8
May 25, 2021 16:22:10.072165966 CEST	53	64345	8.8.8.8	192.168.2.5
May 25, 2021 16:22:10.829804897 CEST	57128	53	192.168.2.5	8.8.8.8
May 25, 2021 16:22:10.880718946 CEST	53	57128	8.8.8.8	192.168.2.5
May 25, 2021 16:22:12.037208080 CEST	64345	53	192.168.2.5	8.8.8.8
May 25, 2021 16:22:12.088709116 CEST	53	64345	8.8.8.8	192.168.2.5
May 25, 2021 16:22:12.818694115 CEST	57128	53	192.168.2.5	8.8.8.8
May 25, 2021 16:22:12.869805098 CEST	53	57128	8.8.8.8	192.168.2.5
May 25, 2021 16:22:16.053632975 CEST	64345	53	192.168.2.5	8.8.8.8
May 25, 2021 16:22:16.103003979 CEST	53	64345	8.8.8.8	192.168.2.5
May 25, 2021 16:22:16.879224062 CEST	57128	53	192.168.2.5	8.8.8.8
May 25, 2021 16:22:16.928673029 CEST	53	57128	8.8.8.8	192.168.2.5
May 25, 2021 16:22:22.302351952 CEST	54791	53	192.168.2.5	8.8.8.8
May 25, 2021 16:22:22.363655090 CEST	53	54791	8.8.8.8	192.168.2.5
May 25, 2021 16:22:23.406016111 CEST	50463	53	192.168.2.5	8.8.8.8
May 25, 2021 16:22:23.463814020 CEST	53	50463	8.8.8.8	192.168.2.5
May 25, 2021 16:22:34.325551987 CEST	50394	53	192.168.2.5	8.8.8.8
May 25, 2021 16:22:34.388235092 CEST	53	50394	8.8.8.8	192.168.2.5
May 25, 2021 16:22:40.676449060 CEST	58530	53	192.168.2.5	8.8.8.8
May 25, 2021 16:22:40.734395027 CEST	53	58530	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 25, 2021 16:21:39.145023108 CEST	192.168.2.5	8.8.8.8	0xd4c8	Standard query (0)	corona-news.tech	A (IP address)	IN (0x0001)
May 25, 2021 16:22:40.676449060 CEST	192.168.2.5	8.8.8.8	0xbb0b	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
May 25, 2021 16:21:39.379641056 CEST	8.8.8.8	192.168.2.5	0xd4c8	No error (0)	corona-news.tech		161.35.249.33	A (IP address)	IN (0x0001)
May 25, 2021 16:22:40.734395027 CEST	8.8.8.8	192.168.2.5	0xbb0b	Name error (3)	favicon.ico	none	none	A (IP address)	IN (0x0001)

HTTPS Packets

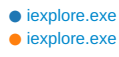
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 25, 2021 16:21:39.657181978 CEST	161.35.249.33	443	192.168.2.5	49718	CN=corona-news.tech CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Fri May 21 01:03:15 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Thu Aug 19 01:03:15 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	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=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		
May 25, 2021 16:21:39.660362959 CEST	161.35.249.33	443	192.168.2.5	49719	CN=corona-news.tech CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Fri May 21 01:03:15 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Thu Aug 19 01:03:15 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	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=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5424 Parent PID: 792

General

Start time:	16:21:37
Start date:	25/05/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7c9db0000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 5628 Parent PID: 5424

General

Start time:	16:21:38

Start date:	25/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5424 CREDAT:17410 /prefetch:2
Imagebase:	0xd80000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly