ID: 348805
Cookbook: browseurl.jbs
Time: 17:08:44
Date: 04/02/2021
Version: 31.0.0 Emerald

Table of Contents

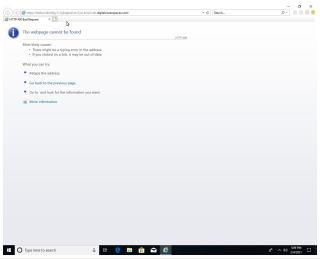
Analysis Report https://testcovidrrddyy1v1ydOppse1Os…

Overview

General Information

Sample URL:	http://https://testcovidrrddyy1v1ydOppse1Osv1ysr.ams3.cdn.digitaloceanspaces.com/
Analysis ID:	348805

Most interesting Screenshot:



Errors

URL not reachable

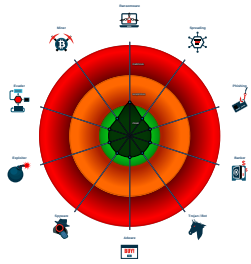
Detection

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

Signatures

No high impact signatures.

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 6812 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6856 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6812 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

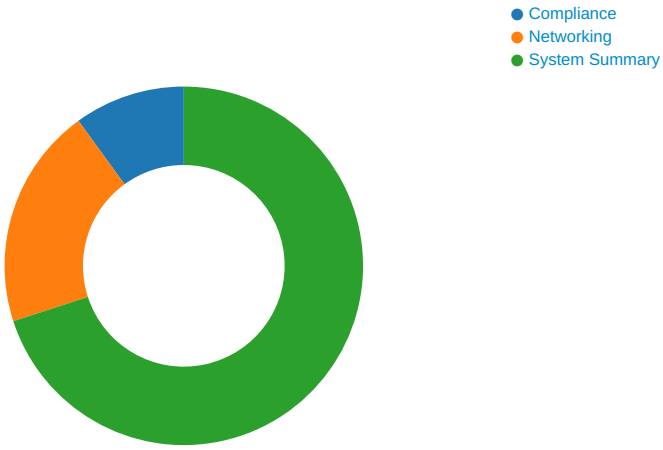
Yara Overview

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.

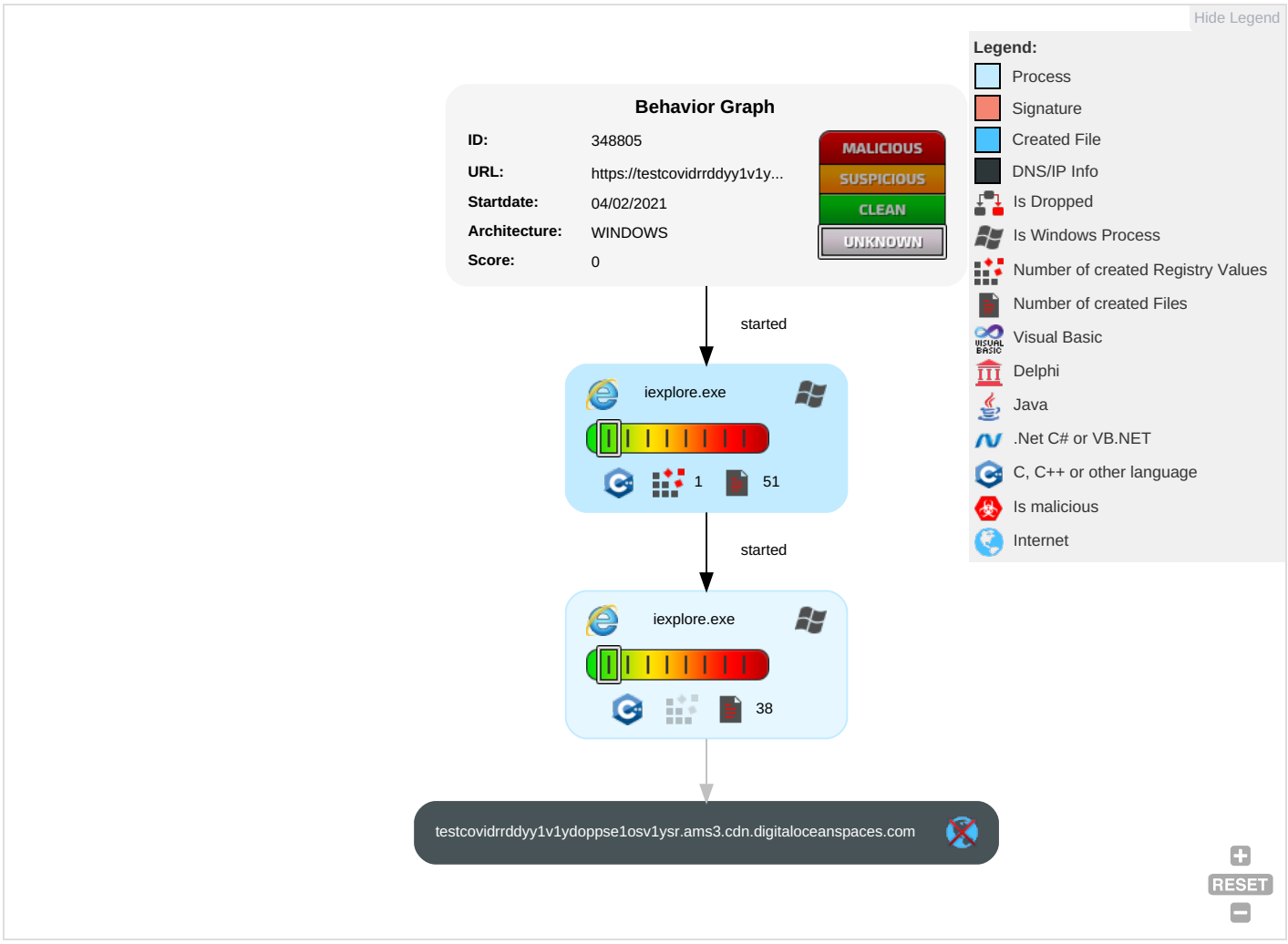
Compliance:

Uses new MSVCR Dlls

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	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

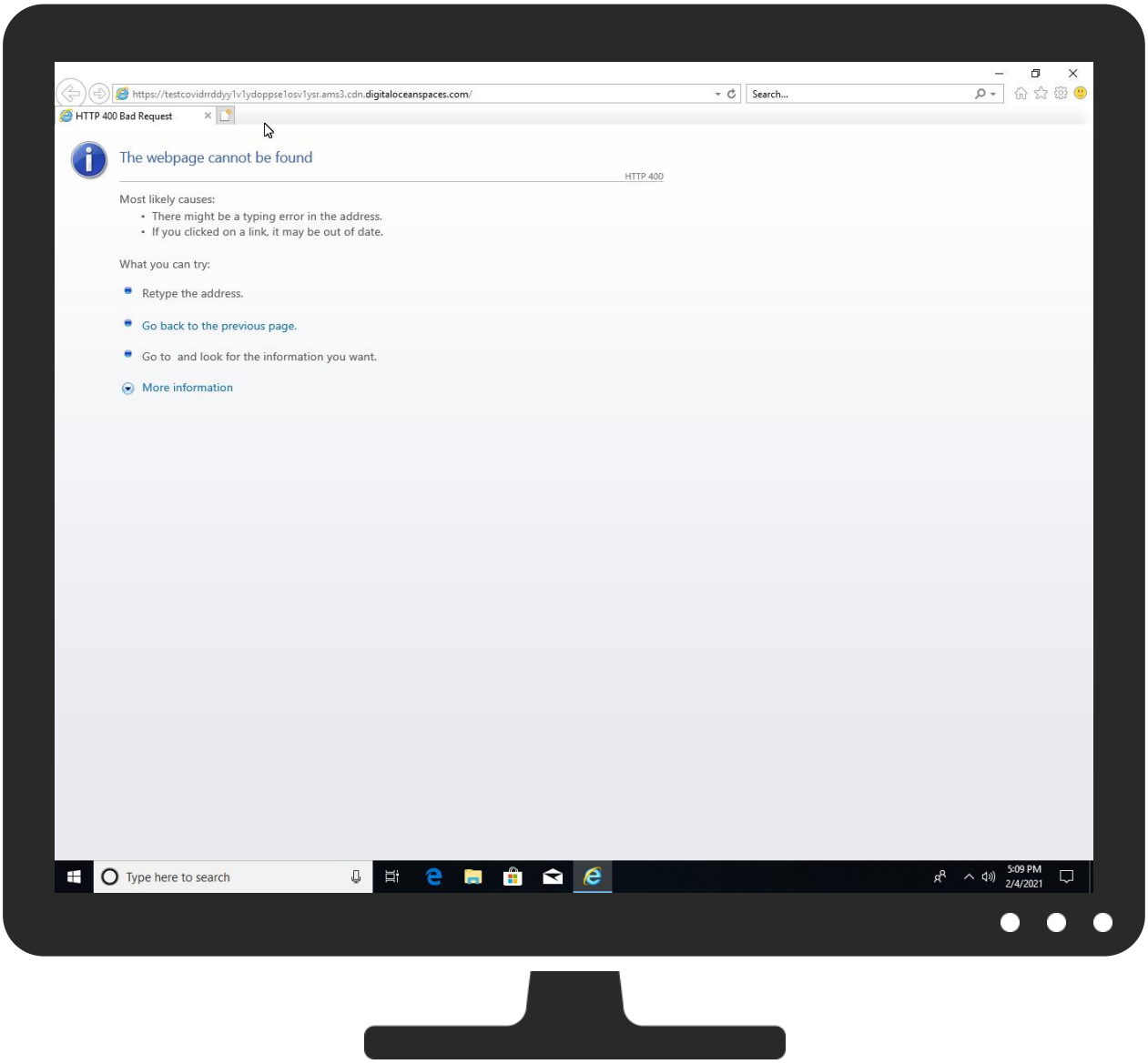
Behavior Graph



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://testcovidrrddyy1v1ydOppse1Osv1ysr.ams3.cdn.digitaloceanspaces.com/	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
testcovidrrddyy1v1ydoppse1osv1ysr.ams3.cdn.digitaloceanspaces.com	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://testcovidrrddyy1v1ydoppse1osv1ysr.ams3.cdn.digitaloceanspaces.com/	~DFA71BDA2BE398EEAD.TMP.1.dr	false		high
http://https://testcovidrrddyy1v1ydoppse1osv1ysr.ams3.cdn.digitaloceanspaces.com/Root	{5C597E50-6703-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false		high

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	348805
Start date:	04.02.2021
Start time:	17:08:44
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://testcovidrrddyy1v1ydOppse1Osv1ysr.ams3.cdn.digitaloceanspaces.com/
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@3/14@1/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • **URL browsing timeout or error**

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 104.42.151.234, 52.147.198.201, 88.221.62.148, 205.185.216.42, 205.185.216.10, 168.61.161.212, 51.104.144.132, 92.122.213.247, 92.122.213.194 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, skypedataprdcolcus17.cloudapp.net, cds.b5g9b8e4.hwcdn.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcoleus16.cloudapp.net, e11290.dspg.akamaiedge.net, go.microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, 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.{5C597E4E-6703-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8473445932816004
Encrypted:	false
SSDEEP:	192:ryZBZO2J9WhtHif/pnzM5vBW1D6sfyp2jX:ruHlJUTgy/qpv

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{5C597E4E-6703-11EB-90EB-ECF4BBEA1588}.dat	
MD5:	C146C86D2B752B86CF9FDD6039A94EE1
SHA1:	5D83F34F0063E32CF64FAD6C096E80CAD8730324
SHA-256:	C7B04E694A2F5BA4D9C8B7FB1315C68E39352A3B68CB554B01F0896766F97FDD
SHA-512:	3EAA6ADEE9FE0959F9288A46F96760386F889F889E0B3E5B656B0A88F5524AA84C8BA70E7A4DC9319CA1F21EF6A47F8861846CEA7907A26FD83EE99D0E955A8
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\{5C597E50-6703-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24260
Entropy (8bit):	1.6462355305937688
Encrypted:	false
SSDEEP:	48:IwmGcpr7GwpaXG4pQ/GrapbSMxrGQpBeGHHpc0sTGUp8OGzYpmOMYGopxkT575GH:r6ZVQZ6DBSMxFjt20kWiMJY3glbg
MD5:	05BE0CC15A29AD7846665554326C4894
SHA1:	A77429A03609F01E8810C51A4435FF8A7267FE02
SHA-256:	7D3938BBBDFE9F59B1405458397DDEF3566251041781E06A07AFD083F51A4741
SHA-512:	20522A110DC618047BED6173293CE034CF638CD2E82B802F891789743DAC585101CF36602F83871197EBC38DDE7F25F32C779618983F910C4C503EF150FC8504
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\{5C597E51-6703-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5650486083403357
Encrypted:	false
SSDEEP:	48:IwyGcprw7GwpaRG4pQxGrapbSvrGQpKvG7HpRWsTGIpG:rGZcQD6BBSvFA+TW4A
MD5:	F3D755DD6E5F11FA1FED63FF20FF98A4
SHA1:	88917C0073989F04ABAABBAE6320F4225319DC83
SHA-256:	5152E5E9742BF5B378246FA642BF89820D5E7C7C5AF2827AE17A9A8E73D4E5EF
SHA-512:	163CFB5E3CC6483A998936AA1216C3475A22F1B9EEBD733649436031C4628CF7A87200E733B6BDD5E1217155D510B87E3E927F2078C506C0E9D761FC81E6FA4A
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\http_400[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):	6410
Entropy (8bit):	3.863492220582535
Encrypted:	false
SSDEEP:	48:upUPinvV4VkBXvLuJyk5N9JXa5TI7kZ3GUsn3GFa7K083GJehBuU1kpd87KxnNst:ufbp69N9JcKktZs36a7x05h427Ow
MD5:	1960097B221E608A79D278C7959B3C59
SHA1:	10C261310CA68C5624185C4F6FEF8AF44EA6FBAF
SHA-256:	1BCAF35CA02140D731E6A3AE3D3D6A5EA49CE7E552728457F790919A540AEC78
SHA-512:	88A5AA0223462A576F07EEDC8182762C1E926B5B91163799FA4357B961ABA28AB94920479C993D30337A3814BE03430437DF9372F9D99743512E7F4152B0DE98
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/http_400.htm

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\http_400[1]	
Preview:	.<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">....<html>.... <head>.. <link rel="stylesheet" type="text/css" href="ErrorPageTemplate.css" >.... <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.... <title>HTTP 400 Bad Request</title>.... <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="javascript:initHomepage(); expandCollapse('infoBlockID', true); initGoBack(); initMoreInfo('infoBlockID');">.... <table width="730" cellpadding="0" cellspacing="0" border="0">.... Error title -->.. <tr>.. <td id="infoIconAlign" width="60" align="left" valign="top" rowspan="2">.. <img src="info_48.png" id="infoIcon" alt="Info icon">..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\info_48[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 47 x 48, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	4113
Entropy (8bit):	7.9370830126943375
Encrypted:	false
SSDEEP:	96:WNTJL8szf79M8FUjE39KJoUUuJPnvmKacs6Uq7qDMj1XPL:WNrzFoQSJPnvzs6rL
MD5:	5565250FCC163AA3A79F0B746416CE69
SHA1:	B97CC66471FCDEE07D0EE36C7FB03F342C231F8F
SHA-256:	51129C6C98A82EA491F89857C31146ECEC14C4AF184517450A7A20C699C84859
SHA-512:	E60EA153B0FECE4D311769391D3B763B14B9A140105A36A13DAD23C2906735EAAB9092236DEB8C68EF078E8864D6E288BEF7EF1731C1E9F1AD9B0170B95AC134
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/info_48.png
Preview:	.PNG.....IHDR.../...0.....#.....IDATx^...pUU..{....KB.....!....F.....jp.Q.....Vg.F..m.Q....{...,m.@.56D...&$d!.<..}....s..K9.....{.....[./<..T..I.I..JR)).9.k.N.%.E.W^}....Po.....X..;.=.P...../...+...9./..s.....9..|.....*.7v.`..V.....-^.$S[[[.....K..z.....3..3....5 ...0.."/n/.c...&.{.ht..?....A..I{.n.....|....t.....N}..%.v...:.E..i....`....a.k.mg.LX..fcFU.fO-..YEfd.}...~.".....}l$....^.re..'^X..*}.?.^U.G..... .30...X.....f[.l0.P`..KC...[..[..6....~..i..Q.|;x..T .....s.5...n+.0..;...H#.2..#.M..m[^3x&E.Ya..\K..{[..M..g...yf0..~....M.]7..ZZZ:..a.O.G64]....9..l[..a...N,,.h.....5...f*.y...}...BX{.G^...?.c.....s^..P.(..G...t.0.:.X.DCs.....]vf...py).....x..>-..Be.a...G...Y!...z...g.{....d.s.o.....%.x.....R.W.....Z.b,....!..6Ub....U.qY(/v..m.a...4.`Qr\.E.G..a)..t..e.j.W.....C<.1.....c..l1w....]3%....tR;,..3..-.NW.5...t..H..h..D..b.....M....)B..2J...)..o..m..M.t....wn./....+Wv....xkg..*..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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..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\Microsoft\Windows\INetCache\IE\9026IKNJ\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\errorPageStrings[1]	
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 connection.";..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\CS6IXJW6\background_gradient[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.02, aspect ratio, density 100x100, segment length 16, baseline, precision 8, 1x800, frames 3
Category:	downloaded
Size (bytes):	453
Entropy (8bit):	5.019973044227213
Encrypted:	false
SSDEEP:	6:3llVuiPjlXJYhg5suRd8PImMo23C/kHrJ8yA/NIeYoWg78C/vTFvbKLAh3:V/XPYhiPRd8j7+9LoIrobtHTdbKi
MD5:	20F0110ED5E4E0D5384A496E4880139B
SHA1:	51F5FC61D8BF19100DF0F8AADAA57FCD9C086255
SHA-256:	1471693BE91E53C2640FE7BAEECBC624530B088444222D93F2815DFCE1865D5B
SHA-512:	5F52C117E346111D99D3B642926139178A80B9EC03147C00E27F07AAB47FE38E9319FE983444F3E0E36DEF1E86DD7C56C25E44B14EFDC3F13B45EDEDA064DB5A
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/background_gradient.jpg
Preview:	......JFIF.....d.d......Ducky.....P......Adobe.d..... ....W..... .....Qa.....?.....%.....x.....s...Z.....j.T.wz.6...X.@... V.3tM...P@.u.%...m..D.25...T...F.....p.....A.....BP..qD.(.....ntH.@.....h?..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\httpErrorPagesScripts[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):	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\OR0WKIO1\ErrorPageTemplate[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):	2168
Entropy (8bit):	5.207912016937144
Encrypted:	false
SSDEEP:	24:5+j5xU5k5N0ndgvoyeP0yyiyQCDr3nowMVworDtX3orKxWxDnCMA0da+hieyuSQK:5Q5K5k5pvFehWrrarrZIrHd3FIQfOS6
MD5:	F4FE1CB77E758E1BA56B8A8EC20417C5
SHA1:	F4EDA06901EDB98633A686B11D02F4925F827BF0
SHA-256:	8D018639281B33DA8EB3CE0B21D11E1D414E59024C3689F92BE8904EB5779B5F
SHA-512:	62514AB345B6648C5442200A8E9530DFB88A0355E262069E0A694289C39A4A1C06C6143E5961074BFAC219949102A416C09733F24E8468984B96843DC222B436
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/ErrorPageTemplate.css

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\ErrorPageTemplate[1]	
Preview:	.body..{...font-family: "Segoe UI", "verdana", "arial";...background-image: url(background_gradient.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;...color: #575757;..}....body.securityError..{...font-family: "Segoe UI", "verdana" , "Arial";...background-image: url(background_gradient_red.jpg);...background-repeat: repeat-x;...background-color: #E8EAEF;...margin-top: 20px;...margin-left: 20px;..}....body.tabInfo..{...background-image: none;...background-color: #F4F4F4;..}.. ..a..{...color: rgb(19,112,171);.font-size: 1em;...font-weight: normal;...text-decoration: none;...margin-left: 0px;...vertical-align: top;..}....a:link, a:visited..{...color: rgb(19,112,171);...text-decoration: none;...vertical-align: top;..}....a:hover..{...color: rgb(7,74,229);...text-decoration: underline;..}....p..{...font-size: 0.9em;..}.....h1 /* used for Title */..{...color: #4465A2;...font-size: 1.1em;...font-weight: normal;...vertical-align

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\bullet[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):	447
Entropy (8bit):	7.304718288205936
Encrypted:	false
SSDEEP:	12:6v/71Cyt/JNTWxGdr+kZDWO7+4dKlv0b1GKuxu+R:/yBJNTqsSk9BTwE05su+R
MD5:	26F971D87CA00E23BD2D064524AEF838
SHA1:	7440BEFF2F4F8FABC9315608A13BF26CABAD27D9
SHA-256:	1D8E5FD3C1FD384C0A7507E7283C7FE8F65015E521B84569132A7EABEDC9D41D
SHA-512:	C62EB51BE301BB96C80539D66A73CD17CA2021D5D816233853A37DB72E04050271E581CC99652F3D8469B390003CA6C62DAD2A9D57164C620B7777AE99AA1B1
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/bullet.png
Preview:	.PNG.....IHDR.....ex....PLTE...(EkFRp&@e&@e)Af)AgANjBNjDNjDNj2Vv-Xz-Y{3XyC\}E_.2j.3l.8p.7q.;j.;l.Zj.\l.5o.7q.<..aw.<..dz.E.....1..@.7..~.....9..:.....A ..B..E..9..:..a..c..b..g.#M.%O.#r.#s.%y.2..4..+..-..?..@..;..p..s...G..H..M.....z`....#tRNS...../,....mIDATx^..C..`.....S....y'...05...|..k.X.....*`.F.K....JQ..u.<.}.. .. [U..m....'r%.....yn.`.7F..).5..b..rX.T.....IEND.B`.

C:\Users\user\AppData\Local\Temp\~DFA71BDA2BE398EEAD.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34453
Entropy (8bit):	0.36518937904144333
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lw89lws9l269l2a9l/Ou:kBqoxKAuvScS+/hDqOlObkT5xNv
MD5:	1880F633AFF3D0E8E97CD064929A4C04
SHA1:	62D5552CB79163708AF7B23EA7E2C04BBE6ED553
SHA-256:	1839215622CD5D77073C6A2EC9AEEFB2C7430019E52896DD7DA452516722134C
SHA-512:	87BDE96B009D5339E96D7705AF2C05BFAA926201825EC7E4E2D31AD9FA9F55DDFEBB911AE2D76787F30F6631F61EE26EB3185392BF5F5BB4EB99A8A9F3681EED
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFC7C1BF063F481040.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.3012563731283957
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laAsVUI:kBqoxxJhHWSVSEabsVUI
MD5:	D8E63DAE84BECD0D1B61E4E27F146FB7
SHA1:	1811115937A37568B6B7F44F196A69298C6D5A63
SHA-256:	A86629F124289D2D134200DBFBF3C9ABB068138447DDF7C37B9973585452AD99
SHA-512:	06C312A9E6515E1EB418CA288E40948D1B1092B04E62B34382B6491542C1886DF1854377DBB2C25EF5452EC58CD97F13461D68E6C784F639F8183DD3F55E3385
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFF8937DCD4090A9AC.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4753938324707004
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lox9loR9lWf//OY5:kBqoI6EHWY5
MD5:	6DB060ADEA0439805205B4C8B7E2AA6B
SHA1:	11935E7A6171A7914D2670E45FFB20330FCF7640
SHA-256:	A3741493C90A03C03FCCB02696B94595C672F25E454DCB57958331880419EE81
SHA-512:	450966FBDAF68CD9EEE06CC64A1C0038BF4D0970636C5EC3C412BEE4E2641762A4D60C3E9FAEA843F8A40E6B1B20B7458948B8887195CF3F481BD7129FCEA8(0
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
Feb 4, 2021 17:09:26.621494055 CET	51726	53	192.168.2.4	8.8.8.8
Feb 4, 2021 17:09:26.667305946 CET	53	51726	8.8.8.8	192.168.2.4
Feb 4, 2021 17:09:27.841783047 CET	56794	53	192.168.2.4	8.8.8.8
Feb 4, 2021 17:09:27.898060083 CET	53	56794	8.8.8.8	192.168.2.4
Feb 4, 2021 17:09:28.705199957 CET	56534	53	192.168.2.4	8.8.8.8
Feb 4, 2021 17:09:28.753746033 CET	53	56534	8.8.8.8	192.168.2.4
Feb 4, 2021 17:09:29.599138975 CET	56627	53	192.168.2.4	8.8.8.8
Feb 4, 2021 17:09:29.645288944 CET	53	56627	8.8.8.8	192.168.2.4
Feb 4, 2021 17:09:30.445597887 CET	56621	53	192.168.2.4	8.8.8.8
Feb 4, 2021 17:09:30.502696037 CET	53	56621	8.8.8.8	192.168.2.4
Feb 4, 2021 17:09:31.215408087 CET	63116	53	192.168.2.4	8.8.8.8
Feb 4, 2021 17:09:31.272572041 CET	53	63116	8.8.8.8	192.168.2.4
Feb 4, 2021 17:09:31.582253933 CET	64078	53	192.168.2.4	8.8.8.8
Feb 4, 2021 17:09:31.638137102 CET	53	64078	8.8.8.8	192.168.2.4
Feb 4, 2021 17:09:32.286883116 CET	64801	53	192.168.2.4	8.8.8.8
Feb 4, 2021 17:09:32.344733000 CET	53	64801	8.8.8.8	192.168.2.4
Feb 4, 2021 17:09:32.912501097 CET	61721	53	192.168.2.4	8.8.8.8
Feb 4, 2021 17:09:32.961791039 CET	53	61721	8.8.8.8	192.168.2.4
Feb 4, 2021 17:09:34.460099936 CET	51255	53	192.168.2.4	8.8.8.8
Feb 4, 2021 17:09:34.508558989 CET	53	51255	8.8.8.8	192.168.2.4
Feb 4, 2021 17:09:35.538669109 CET	61522	53	192.168.2.4	8.8.8.8
Feb 4, 2021 17:09:35.584433079 CET	53	61522	8.8.8.8	192.168.2.4
Feb 4, 2021 17:09:36.370537996 CET	52337	53	192.168.2.4	8.8.8.8
Feb 4, 2021 17:09:36.427592993 CET	53	52337	8.8.8.8	192.168.2.4
Feb 4, 2021 17:09:37.507256985 CET	55046	53	192.168.2.4	8.8.8.8
Feb 4, 2021 17:09:37.556010008 CET	53	55046	8.8.8.8	192.168.2.4
Feb 4, 2021 17:09:38.691828012 CET	49612	53	192.168.2.4	8.8.8.8
Feb 4, 2021 17:09:38.739572048 CET	53	49612	8.8.8.8	192.168.2.4
Feb 4, 2021 17:09:40.082771063 CET	49285	53	192.168.2.4	8.8.8.8
Feb 4, 2021 17:09:40.131465912 CET	53	49285	8.8.8.8	192.168.2.4
Feb 4, 2021 17:09:50.394831896 CET	50601	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 4, 2021 17:09:50.445580006 CET	53	50601	8.8.8.8	192.168.2.4
Feb 4, 2021 17:09:53.956485987 CET	60875	53	192.168.2.4	8.8.8.8
Feb 4, 2021 17:09:54.012439013 CET	53	60875	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 4, 2021 17:09:32.286883116 CET	192.168.2.4	8.8.8.8	0x84d9	Standard query (0)	testcovidrrddyy1v1yd oppse1osv1 ysr.ams3.c dn.digital oceanspace s.com	A (IP address)	IN (0x0001)

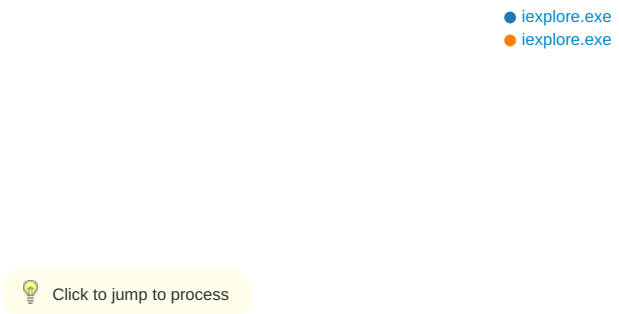
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 4, 2021 17:09:32.344733000 CET	8.8.8.8	192.168.2.4	0x84d9	No error (0)	testcovidrrddyy1v1yd oppse1osv1 ysr.ams3.c dn.digital oceanspace s.com	cds.b5g9b8e4.hwcdn.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: iexplore.exe PID: 6812 Parent PID: 800

General

Start time:	17:09:30
Start date:	04/02/2021

Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff799000000
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: 6856 Parent PID: 6812

General

Start time:	17:09:30
Start date:	04/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6812 CREDAT:17410 /prefetch:2
Imagebase:	0x1390000
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