ID: 348813
Cookbook: browseurl.jbs
Time: 17:22:38
Date: 04/02/2021
Version: 31.0.0 Emerald

Table of Contents

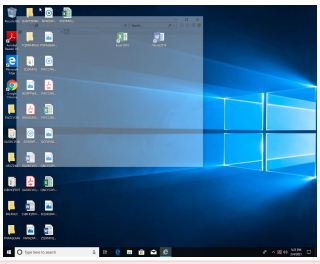
Analysis Report http://noreply@test-for-coronavirus.ser…

Overview

General Information

Sample URL:	http://noreply@test-for-coronavirus.service.gov.uk
Analysis ID:	348813

Most interesting Screenshot:



Errors

URL not reachable

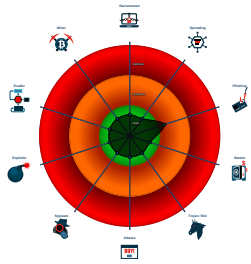
Detection

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

Signatures

URL contains potential PII (phishing…

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 3980 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 3560 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3980 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 5756 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3980 CREDAT:17414 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

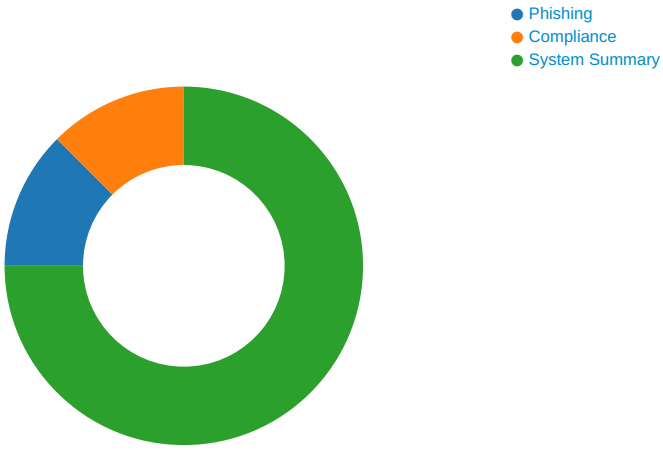
Yara Overview

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.

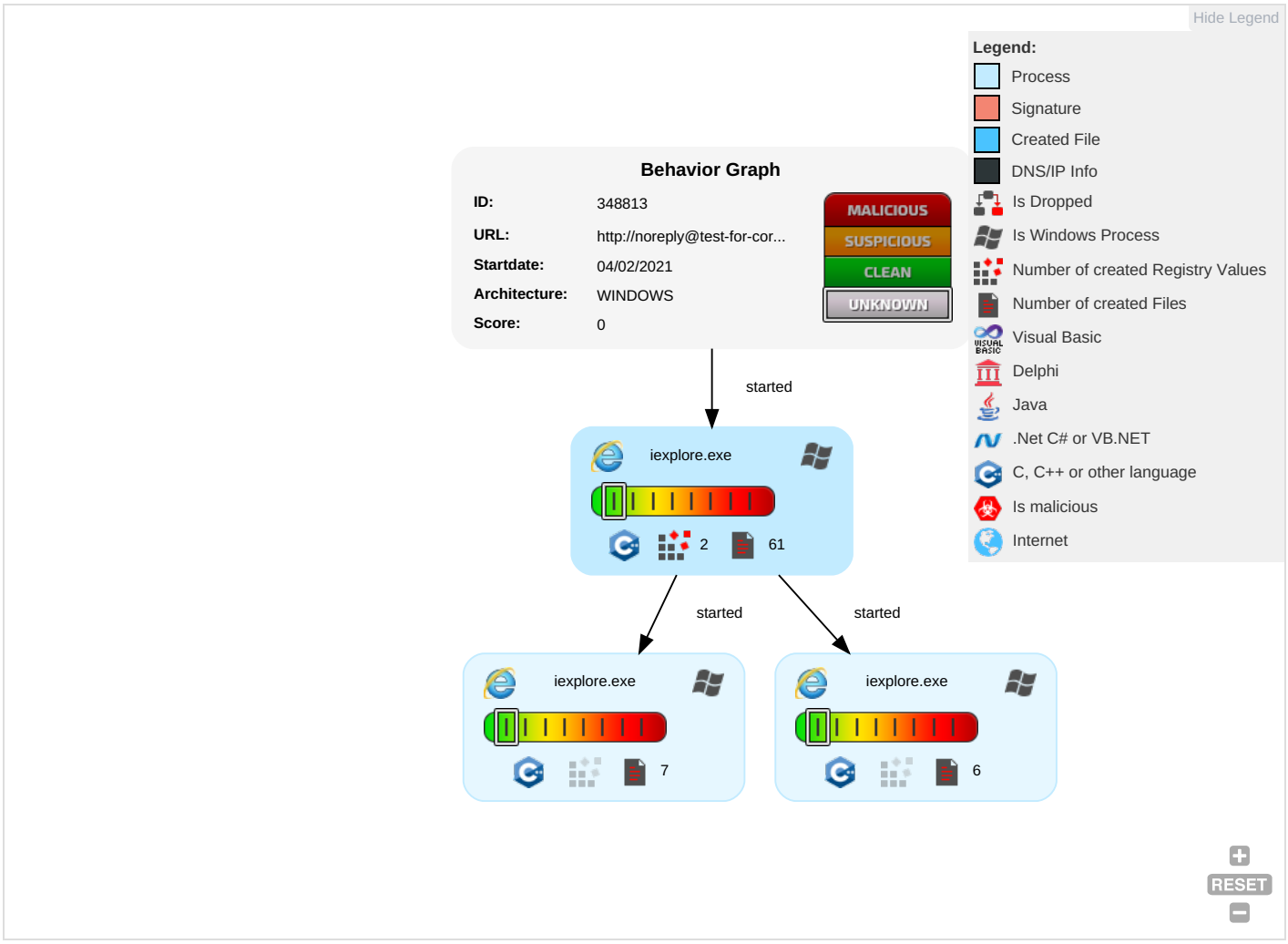
Compliance:

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	Data Obfuscation	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	Junk Data	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://noreply@test-for-coronavirus.service.gov.uk	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

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	348813
Start date:	04.02.2021
Start time:	17:22:38
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 1m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://noreply@test-for-coronavirus.service.gov.uk
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:	4
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	UNKNOWN
Classification:	unknown0.win@5/6@0/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Unable to create IE instance
Warnings:	Show All • Exclude process from analysis (whitelisted): ielowutil.exe • Excluded IPs from analysis (whitelisted): 104.43.139.144, 52.147.198.201, 88.221.62.148 • Excluded domains from analysis (whitelisted): skypedataprdcoleus16.cloudapp.net, e11290.dspg.akamaiedge.net, go.microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolcus16.cloudapp.net, watson.telemetry.microsoft.com
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.{BD952218-6750-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	39624
Entropy (8bit):	1.968084788510127
Encrypted:	false
SSDEEP:	96:rjZkZ72T9WoMtoDfoKtMoOoQoFo6Mp8eWop8vog8R:rjZkZ72T9WdtyfhtMhfK8bW/g
MD5:	4E2A2AE6AF44D6756243D4279869E7AD
SHA1:	9B74EBD350A3175DA69FB2FE5D82BE7D74BB65D5
SHA-256:	FBECDAE25C3900B39B78C83CE97D0AC2C11FC11F3C5A028274D4A6EBAB508405
SHA-512:	3676AC80ACD8C6DD5D273538F78B7CCBA9F63DE9AFBD89FB61FA6B790AB8287AACCF09290D8C8F8217B1AB21F3700BFAA6264235CB79CE0A307FD701D14BAD9
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\{BD95221A-6750-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5733048781893466
Encrypted:	false
SSDEEP:	48:IwuGcpr7GwpaPG4pQjGrapbSPorGQpBaGHHpcAsTGUpG:ryZVQB6HBSPoFjh2AkA
MD5:	A85095686E24FCCABDDC0AD0C45786B4
SHA1:	688E778C3A628FC6DCE3FA4E0B3D01E8009EBE21
SHA-256:	59ABCC215255C2694065F24EAC9F13DCA923B4412693E9C9FD78DE190850BE23
SHA-512:	B2B6EDFAE4620E6AE9122784DE660471AF49F0C82033F1859ED68EF0B839CFF64BB010D6A81B9CD5A5BD45633263832D3738E3592961B6A887AE3891CDD05B0
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\{BD95221C-6750-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5727325912881567
Encrypted:	false
SSDEEP:	48:IwCGcprrGwpafG4pQyGrapbSjrGQpBFoGHHpcF2sTGUpG:r2ZlQx60BSjFjFn2F2kA
MD5:	A2E8C80ED06FC33A9DD687C8ECB73EF8
SHA1:	484145055DE46D963D63042DD770E3C48EC19432
SHA-256:	CE28910CD9FEE1436B33DE2FB724FD9E2463BB774411AE8A07AD13138C3E9FCA
SHA-512:	15F169DD146E2EFAC644FB650B55ED9BE47008CBC242A13F8BC7879BC5C5B6CC377BCE2D31D519A4012CAB2DB4B3DD7AFD46B3B78C9C296B5A401C1186B23C1
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Temp\~DF37EFEE2E2D3513EC.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25657
Entropy (8bit):	0.31389264313232407
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwF49lwFo9l2FD:kBqoxKAuvScS+FrFlFD
MD5:	0B2F428E951D823FF1882C6419C32BD7
SHA1:	B76AD8B72322324642795C4DB35EA70CDCB2A64C
SHA-256:	81121332B4640EB51855AB4F185B8CD77EC908A536F8638AD7DE58DC79B8D57A
SHA-512:	B2363E90EEA04B4C9B7A5A95FC90E1C7A884DCCA1425E31417DA2B24508449B1CC57BA3EF919F7C194D01E7E089FCB29240632139C0B16F7018FB8A3AD9D3EC
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... .....

C:\Users\user\AppData\Local\Temp\~DF3B95DC255F2B2C46.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13285
Entropy (8bit):	0.63067620631711
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lobrF9lobR9lWbQ2+K/r2+4TC+42+40+tA0A2+40+JAy+7:kBqoIOwIKRepk+4+6+o
MD5:	487DABF0ED6763AA69C56A4EA877102E
SHA1:	900DACF9CF54344B24B5DB05725EC8862A624BA7
SHA-256:	A0C8610CE7B933D785E98966D7F95DCC5CDEE8D7C6E4744F533AFC0401EFE65B
SHA-512:	D4917B24F1333360C0069FE7632937925A80344EEF04FC3D5D1FD54047230B37217887C51ABF8A622D32822807883E205A64D298A9E2709B03221D1AA447AEF3
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... .....

C:\Users\user\AppData\Local\Temp\~DFC3663B37B4B83C27.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25657
Entropy (8bit):	0.3139908173815561
Encrypted:	false

C:\Users\user\AppData\Local\Temp\~DFC3663B37B4B83C27.TMP	
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwEz9lwEz9l2E6:kBqoxKAuvScS+XZX
MD5:	01E9FE4BD778A5FACF39C51B396C55BA
SHA1:	A1E382C387DFE679B7BFD76AC1B4CC58EFCE8871
SHA-256:	424EB88AED3110ECD5EF0290106B4A297237F0ED07F02B3B9AFBC30D8F1F4844
SHA-512:	AB011F5C8F489BBE32E120F853AC2AD9D65999F9E4A3FB5B84227C88A1BA453A47BBED072419A0D3242083F65606ADC214EF13C6CFB8B47B5B618DAC0D27BEC
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

No static file info

Network Behavior

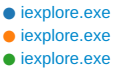
UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 4, 2021 17:23:20.289442062 CET	58361	53	192.168.2.3	8.8.8.8
Feb 4, 2021 17:23:20.335300922 CET	53	58361	8.8.8.8	192.168.2.3
Feb 4, 2021 17:23:21.214654922 CET	63492	53	192.168.2.3	8.8.8.8
Feb 4, 2021 17:23:21.262147903 CET	53	63492	8.8.8.8	192.168.2.3
Feb 4, 2021 17:23:22.183742046 CET	60831	53	192.168.2.3	8.8.8.8
Feb 4, 2021 17:23:22.241548061 CET	53	60831	8.8.8.8	192.168.2.3
Feb 4, 2021 17:23:23.170387983 CET	60100	53	192.168.2.3	8.8.8.8
Feb 4, 2021 17:23:23.216113091 CET	53	60100	8.8.8.8	192.168.2.3
Feb 4, 2021 17:23:24.079062939 CET	53195	53	192.168.2.3	8.8.8.8
Feb 4, 2021 17:23:24.125026941 CET	53	53195	8.8.8.8	192.168.2.3
Feb 4, 2021 17:23:25.050978899 CET	50141	53	192.168.2.3	8.8.8.8
Feb 4, 2021 17:23:25.107064962 CET	53	50141	8.8.8.8	192.168.2.3
Feb 4, 2021 17:23:25.311341047 CET	53023	53	192.168.2.3	8.8.8.8
Feb 4, 2021 17:23:25.357526064 CET	53	53023	8.8.8.8	192.168.2.3
Feb 4, 2021 17:23:26.337198973 CET	49563	53	192.168.2.3	8.8.8.8
Feb 4, 2021 17:23:26.383213997 CET	53	49563	8.8.8.8	192.168.2.3
Feb 4, 2021 17:23:27.618762016 CET	51352	53	192.168.2.3	8.8.8.8
Feb 4, 2021 17:23:27.672357082 CET	53	51352	8.8.8.8	192.168.2.3
Feb 4, 2021 17:23:28.587527990 CET	59349	53	192.168.2.3	8.8.8.8
Feb 4, 2021 17:23:28.636225939 CET	53	59349	8.8.8.8	192.168.2.3
Feb 4, 2021 17:23:29.376858950 CET	57084	53	192.168.2.3	8.8.8.8
Feb 4, 2021 17:23:29.422759056 CET	53	57084	8.8.8.8	192.168.2.3
Feb 4, 2021 17:23:30.307686090 CET	58823	53	192.168.2.3	8.8.8.8
Feb 4, 2021 17:23:30.353607893 CET	53	58823	8.8.8.8	192.168.2.3
Feb 4, 2021 17:23:31.254872084 CET	57568	53	192.168.2.3	8.8.8.8
Feb 4, 2021 17:23:31.309276104 CET	53	57568	8.8.8.8	192.168.2.3
Feb 4, 2021 17:23:32.211746931 CET	50540	53	192.168.2.3	8.8.8.8
Feb 4, 2021 17:23:32.262957096 CET	53	50540	8.8.8.8	192.168.2.3
Feb 4, 2021 17:23:33.356656075 CET	54366	53	192.168.2.3	8.8.8.8
Feb 4, 2021 17:23:33.407926083 CET	53	54366	8.8.8.8	192.168.2.3
Feb 4, 2021 17:23:34.272886992 CET	53034	53	192.168.2.3	8.8.8.8
Feb 4, 2021 17:23:34.321721077 CET	53	53034	8.8.8.8	192.168.2.3

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 3980 Parent PID: 792

General

Start time:	17:23:24
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:	0x7ff777c50000
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: 3560 Parent PID: 3980

General

Start time:	17:23:25
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:3980 CREDAT:17410 /prefetch:2
Imagebase:	0x1190000
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

Analysis Process: iexplore.exe PID: 5756 Parent PID: 3980

General

Start time:	17:23:26
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:3980 CREDAT:17414 /prefetch:2
Imagebase:	0x1190000
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

Disassembly