ID: 365435
Cookbook: browseurl.jbs
Time: 15:35:42
Date: 09/03/2021
Version: 31.0.0 Emerald

Table of Contents

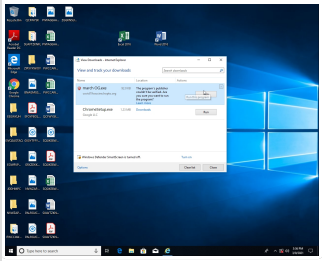
Analysis Report http://covid19vaccine.hopto.org/march …

Overview

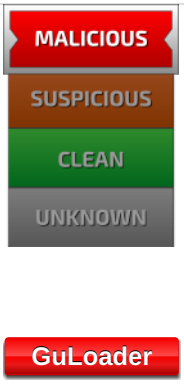
General Information

Sample URL:	http://covid19vaccine.hopto.org/march OG.exe
Analysis ID:	365435
Infos:	

Most interesting Screenshot:



Detection



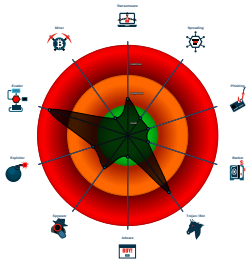
GuLoader

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

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Contains functionality to detect hard…
- Contains functionality to hide a threa…
- Detected RDTSC dummy instruction…
- Hides threads from debuggers
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 3476 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5588 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3476 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - march OG.exe (PID: 3652 cmdline: 'C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\march OG.exe' MD5: B75B990AC5990F1B6B0127540DE4EC30)
    - march OG.exe (PID: 6092 cmdline: 'C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\march OG.exe' MD5: B75B990AC5990F1B6B0127540DE4EC30)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

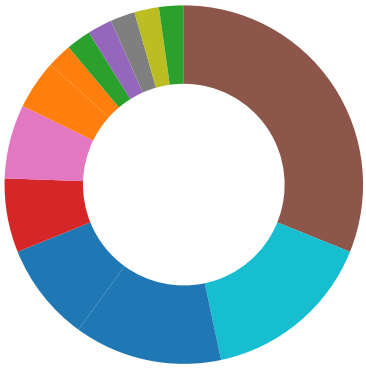
Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: march OG.exe PID: 3652	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: march OG.exe PID: 3652	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	
Process Memory Space: march OG.exe PID: 6092	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: march OG.exe PID: 6092	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Data Obfuscation:

Yara detected GuLoader

Yara detected VB6 Downloader Generic

Malware Analysis System Evasion:

Contains functionality to detect hardware virtualization (CPUID execution measurement)

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Tries to detect Any.run

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

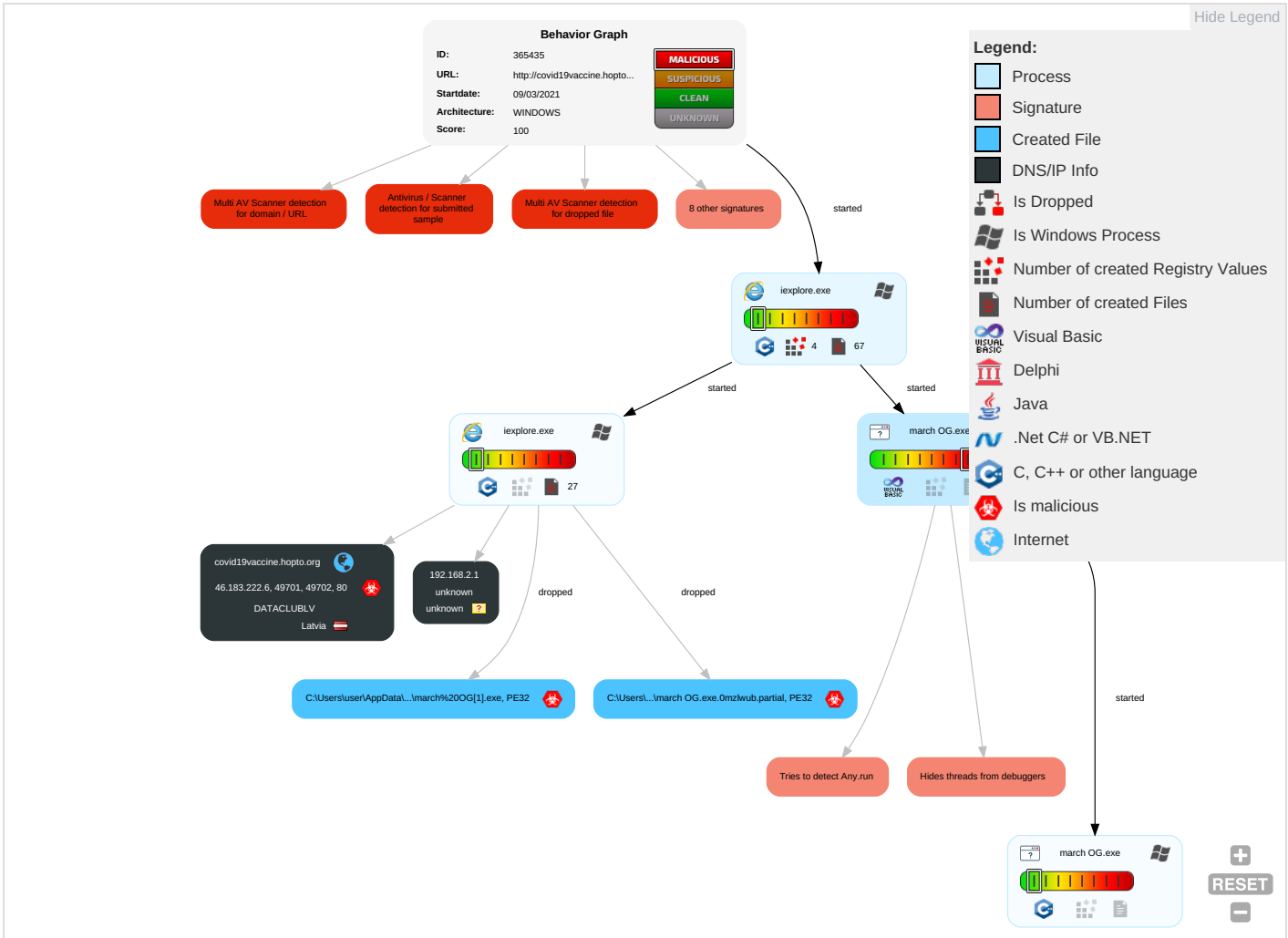
Contains functionality to hide a thread from the debugger

Hides threads from debuggers

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Re Se Eff
Valid Accounts	Exploitation for Client Execution 1	Path Interception	Process Injection 1 2	Masquerading 1	Input Capture 1	Security Software Discovery 8 2 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Re Tra Wi Au
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2 1	LSASS Memory	Virtualization/Sandbox Evasion 2 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 1	Exploit SS7 to Redirect Phone Calls/SMS	Re Wi Wi Au
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 2	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 to Track Device Location	Ob De Cl Ba
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	File and Directory Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	System Information Discovery 3 1 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

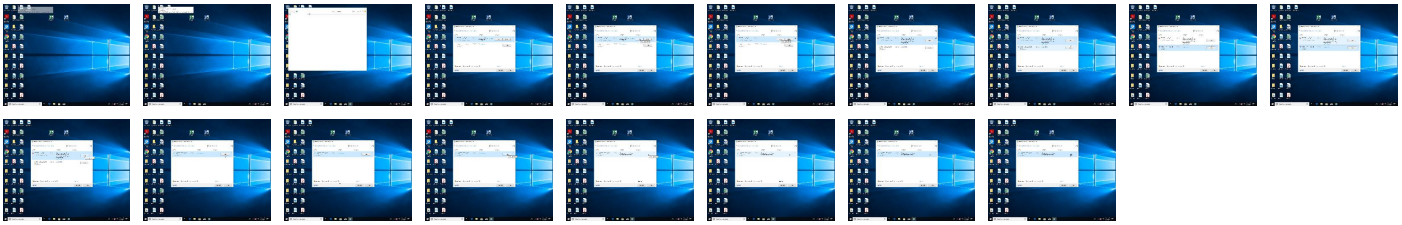
Behavior Graph

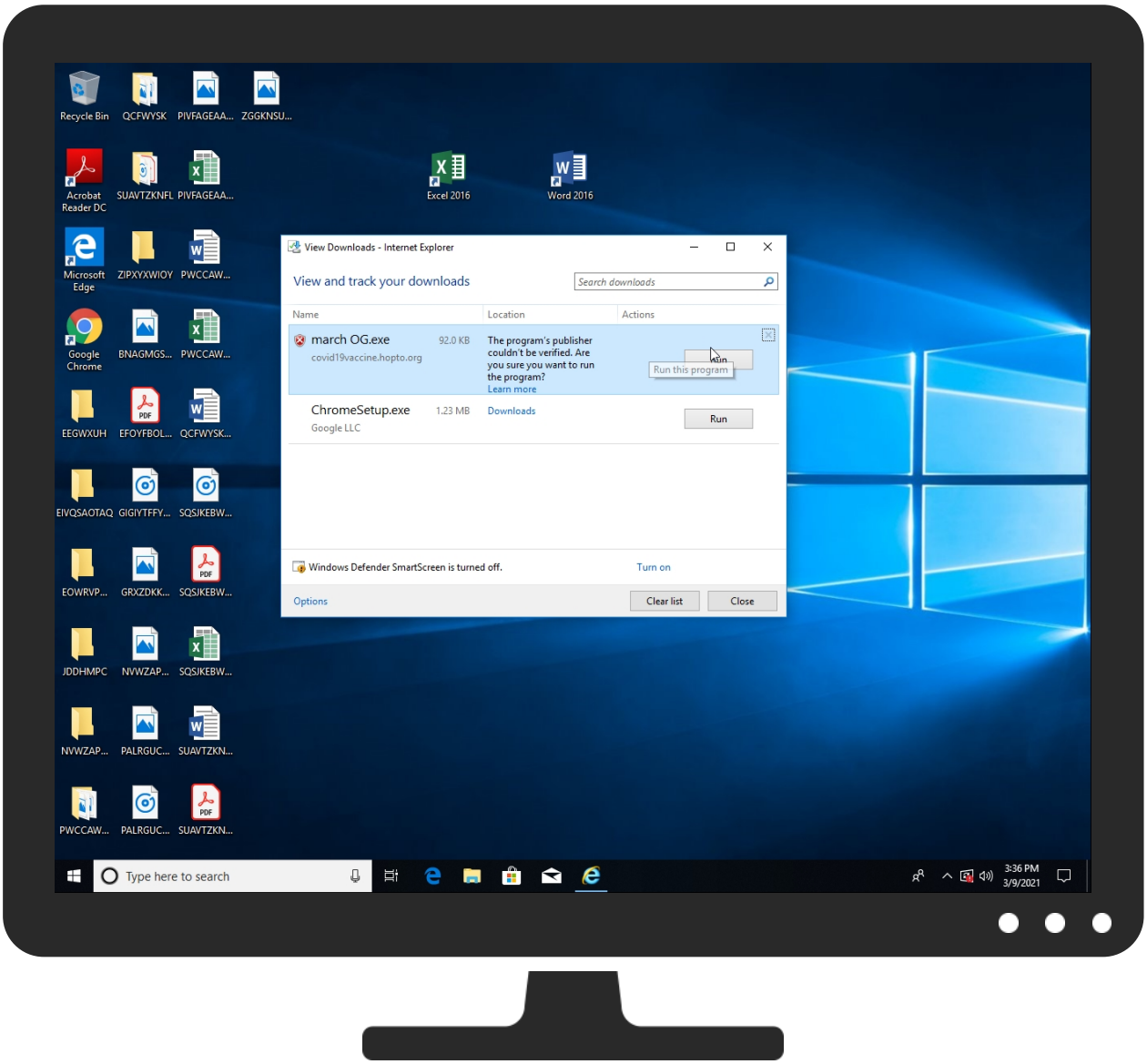


Screenshots

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://covid19vaccine.hopto.org/march%20OG.exe	18%	Virustotal		Browse
http://covid19vaccine.hopto.org/march%20OG.exe	100%	Avira URL Cloud	malware	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\march OG.exe.0mzlwub.partial	76%	Virustotal		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\march OG.exe.0mzlwub.partial	24%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\march OG.exe.0mzlwub.partial	82%	ReversingLabs	Win32.Trojan.VBObfuse	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\march%20OG[1].exe	24%	Metadefender		Browse

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\march%20OG[1].exe	82%	ReversingLabs	Win32.Trojan.VBObfuse	

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
covid19vaccine.hopto.org	13%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
0	1%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
covid19vaccine.hopto.org	46.183.222.6	true	true	• 13%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://covid19vaccine.hopto.org/march%20OG.exe	true		unknown
0	true	• 1%, Virustotal, Browse	low

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
46.183.222.6	covid19vaccine.hopto.org	Latvia		52048	DATACLUBLV	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	365435
Start date:	09.03.2021
Start time:	15:35:42
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://covid19vaccine.hopto.org/march OG.exe
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:	27
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:	MAL
Classification:	mal100.troj.evad.win@7/9@1/2
EGA Information:	• Successful, ratio: 50%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 184.30.21.219, 92.122.145.220, 88.221.62.148, 13.64.90.137, 2.18.68.82, 51.104.144.132, 152.199.19.161, 168.61.161.212, 2.20.142.209, 2.20.142.210, 20.54.26.129, 131.253.33.200, 13.107.22.200, 92.122.213.247, 92.122.213.194, 13.88.21.125, 104.42.151.234 • Excluded domains from analysis (whitelisted): storeedgefd.dsx.mp.microsoft.com.edgekey.net.globalredir.akadns.net, au.download.windowsupdate.com.edgesuite.net, 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, storeedgefd.xbetservices.akadns.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, e12564.dspb.akamaiedge.net, go.microsoft.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, storeedgefd.dsx.mp.microsoft.com, www.bing.com, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, dual-a-0001.a-msedge.net, ie9comview.vo.msecnd.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, storeedgefd.dsx.mp.microsoft.com.edgekey.net, ris.api.iris.microsoft.com, dual-a-0001.dc-msedge.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, go.microsoft.com.edgekey.net, blobcollector.events.data.trafficmanager.net, e16646.dscg.akamaiedge.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.net, cs9.wpc.v0cdn.net • Execution Graph export aborted for target march OG.exe, PID 6092 because there are no executed function

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.{493F8842-8130-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	32344
Entropy (8bit):	1.7991357474314675
Encrypted:	false
SSDEEP:	48:IwQGcprSGwpLZG/ap8XGIpcwMUGvnZpvw/Gohqp9wWGo4xpmw95GWD59wE0GW55t:rUZaZ92JWwwtwwfwRxMw9XwEhdrEgn2
MD5:	E05F8B9026F6AB4A3BCA3481B5A45DF8
SHA1:	3CDF3E87CEFAA47ACB356905D9B92EBCA66C79C0
SHA-256:	9D56214120EEBBEDACE33EA337A717E048EDE3510B29CE26ED7D23CD902C8264
SHA-512:	DDBFFA59A3531388AEDFB558C4F5B805F65F10EFF8248D8E001ECD58D81A66EFE3894DC6B7ACF00702B133505544B0BE9254D34E4E0DB4A6455F7F51757C54D9
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\{493F8844-8130-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	19032
Entropy (8bit):	1.5992342785899085
Encrypted:	false
SSDEEP:	48:Iw1GcprIGwpa8G4pQMGrapbS8GQpBKNDGHHpcKD8TGUpQKyYGcpm:rrZQQc6KBSUjKNG2KD06Kvg
MD5:	7CEF46956A143ED51FF3A627748817BA
SHA1:	71672762BE40C842285BA8E03647829B0CF13CD7
SHA-256:	EA349A91319FFED1164CB070B8BEFBE8BE55647B6642C948748740CA48781D08
SHA-512:	1D972E682883EC574ED1ED6CB871C5201BCC642770164233A7F6B6E82EF09C1FD3F279AD1B00E82F9BBEAAAB460FBE016255445B258A3B435CA00FC448AA7533
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\march OG.exe.0mzlwub.partial	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	5.559510350020854
Encrypted:	false
SSDEEP:	1536:61oJy7aGTvIaUZNcddsm3dE+WE2i5JjyI+h91mR4E:6v7aGTUcddaMrjyIA1jE
MD5:	B75B990AC5990F1B6B0127540DE4EC30
SHA1:	66DD5A9D359FAF4ABDFF9B53B8E96280EFF58038
SHA-256:	F7ABA1C5E66938EFC7A722F98344A70A2443391668283F08DA1202BDE6C9B925

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\march OG.exe.0mzlwub.partial	
SHA-512:	E2009B8E6AD35C60F08EFB6514C18C650929F343B01A14F2AAB8D5EAEC880520C67BCF6795ED21BE8C462A2C32EB31E80A7A3A1C9767776CE18F208B4F89FF4 5
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 76%, Browse • Antivirus: Metadefender, Detection: 24%, Browse • Antivirus: ReversingLabs, Detection: 82%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L....]/M..... ...@...0.....P....@.....gw.....F..(....p.....(... .....text...,=.....@..... ..... ..`.data.....P.....P.....@....rsrc.....p.....`.....@..@...I.....MSVBVM60.DLL..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\march OG.exe.0mzlwub.partial:Zone.Identifier	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:gAWY3n:qY3n
MD5:	FBCCF14D504B7B2DBCB5A5BDA75BD93B
SHA1:	D59FC84CDD5217C6CF74785703655F78DA6B582B
SHA-256:	EACD09517CE90D34BA562171D15AC40D302F0E691B439F91BE1B6406E25F5913
SHA-512:	AA1D2B1EA3C9DE3CCADB319D4E3E3276A2F27DD1A5244FE72DE2B6F94083DDDC762480482C5C2E53F803CD9E3973DDEFC68966F974E124307B5043E654443E 8
Malicious:	false
Reputation:	low
Preview:	[ZoneTransfer]..ZoneId=3..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\march OG.exe:Zone.Identifier	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	very short file (no magic)
Category:	modified
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:W:W
MD5:	ECCBC87E4B5CE2FE28308FD9F2A7BAF3
SHA1:	77DE68DAECD823BABBB58EDB1C8E14D7106E83BB
SHA-256:	4E07408562BEDB8B60CE05C1DECFE3AD16B72230967DE01F640B7E4729B49FCE
SHA-512:	3BAFBF08882A2D10133093A1B8433F50563B93C14ACD05B79028EB1D1279902724145098065199450142 3A66C276AE26C43B739BC65C4E16B10C3AF6C202AEBB
Malicious:	false
Reputation:	low
Preview:	3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\march%20OG[1].exe	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	5.559510350020854
Encrypted:	false
SSDEEP:	1536:61oJy7aGTvlaUZNcddsm3dE+WE2i5JjyI+h91mR4E:6v7aGTUcddaMrjyIA1jE
MD5:	B75B990AC5990F1B6B0127540DE4EC30
SHA1:	66DD5A9D359FAF4ABDFF9B53B8E96280EFF58038
SHA-256:	F7ABA1C5E66938EFC7A722F98344A70A2443391668283F08DA1202BDE6C9B925
SHA-512:	E2009B8E6AD35C60F08EFB6514C18C650929F343B01A14F2AAB8D5EAEC880520C67BCF6795ED21BE8C462A2C32EB31E80A7A3A1C9767776CE18F208B4F89FF4 5
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 24%, Browse • Antivirus: ReversingLabs, Detection: 82%
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\march%20OG[1].exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L....]/M..... ...@...0.....P....@.....gw.....F..(....p.....(... .....text...,=.....@..... ..... ..`.data.....P.....P.....@....rsrc.....p.....`.....@..@...I.....MSVBVM60.DLL..... ....

C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	89
Entropy (8bit):	4.530422375380909
Encrypted:	false
SSDEEP:	3:oVXU045U4FqH8JOGXnE045U4Fp+n:o9Ur5iqEr5g
MD5:	817557F2DB45C216F5A59F2376362473
SHA1:	9380C2684926B21BE23A939F4AB2590154DAA9C1
SHA-256:	722CE801E7793DCE8BB9E4B3CC8468F6169BD7E5ACF96262FBA076335BF1BC47
SHA-512:	1A81275CA731EBE765370D9C57157EEB161C6C67DD8559110426E1D02BC2D04E6104E0FB37E9C89D9EA4C40A5C364B2E6E6BE88687AC795C2724B0902E0266D
Malicious:	false
Reputation:	low
Preview:	[2021/03/09 15:36:37.381] Latest deploy version: ..[2021/03/09 15:36:37.381] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\~DF9FFFDC171AAF0B67.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12981
Entropy (8bit):	0.4434537083961431
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lofrF9lofR9lWfgy+AhLy+QHG+QqyBe:kBqolysQUsEA
MD5:	7FE43CF9F07CD890DF825FD8886CF8B5
SHA1:	C5EDA05D06A046A9631260A233344E1CF00E944D
SHA-256:	449A0263467C3F3C2B94FB42B57CF4CE628891893D13EA639B323EB2CF9D7EE5
SHA-512:	BFAC3BCA847E931113FC67BD2F06DEAA20AD90E5ABDD42C19623F1B461E978ACAD801C5D3C5FFB58E911798735F9A6C8067D5F9341E167D8451EC72CE26B78 F5
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

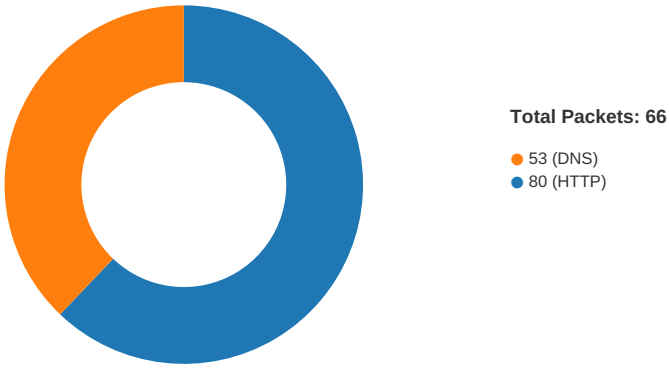
C:\Users\user\AppData\Local\Temp\~DFB4A747BCDB3C3464.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	29989
Entropy (8bit):	0.33004936311962413
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwKo/9lwKg9l2K2/9l29:kBqoxKAuvScS+KTKtK2+KTKyy
MD5:	8D36A92224CE46D9DA8D1E66E91FF1BB
SHA1:	B0D2DBBE0C2A09BE4F4F0C8F3E655A2AFA70C36D
SHA-256:	9F516C3E632C0E6695FB7C564CF04B8B6A39863A2A0BEA6E31663748BC3E60F0
SHA-512:	FD49C473DE4F7897EC120260E25E628361E521EB7F3C05B2A2B65322E1E5C36CDA729DE8015F7854D54144279B75E0EAC534E7497654D2EE1CFF30800C9A41B
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
Mar 9, 2021 15:36:38.324227095 CET	49701	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:36:38.325638056 CET	49702	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:36:38.393903971 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.393937111 CET	80	49701	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.394047022 CET	49702	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:36:38.394094944 CET	49701	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:36:38.394871950 CET	49702	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:36:38.466542959 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.466579914 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.467020035 CET	49702	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:36:38.534555912 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.534600019 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.534617901 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.534636021 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.534753084 CET	49702	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:36:38.534810066 CET	49702	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:36:38.605431080 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.605468988 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.605487108 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.605503082 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.605519056 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.605534077 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.605546951 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.605573893 CET	49702	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:36:38.605592966 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.605648994 CET	49702	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:36:38.677581072 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.677614927 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.677633047 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.677649021 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.677665949 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.677684069 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.677700996 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.677717924 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.677733898 CET	49702	80	192.168.2.3	46.183.222.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 9, 2021 15:36:38.677764893 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.677793980 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.677817106 CET	49702	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:36:38.677855015 CET	49702	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:36:38.677895069 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.677918911 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.677938938 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.677951097 CET	49702	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:36:38.677969933 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.677998066 CET	49702	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:36:38.678034067 CET	49702	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:36:38.747087002 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.747153997 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.747179985 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.747201920 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.747225046 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.747239113 CET	49702	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:36:38.747266054 CET	49702	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:36:38.747279882 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.747302055 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.747324944 CET	49702	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:36:38.747334003 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.747351885 CET	49702	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:36:38.747395992 CET	49702	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:36:38.747421980 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.747445107 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.747474909 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.747483015 CET	49702	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:36:38.747504950 CET	49702	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:36:38.747517109 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.747544050 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.747554064 CET	49702	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:36:38.747572899 CET	49702	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:36:38.747586966 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.747601032 CET	49702	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:36:38.747626066 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.747632980 CET	49702	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:36:38.747658968 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.747675896 CET	49702	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:36:38.747694016 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.747703075 CET	49702	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:36:38.747728109 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.747737885 CET	49702	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:36:38.747760057 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.747770071 CET	49702	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:36:38.747795105 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.747805119 CET	49702	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:36:38.747829914 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.747839928 CET	49702	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:36:38.747863054 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.747874975 CET	49702	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:36:38.747894049 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.747910976 CET	49702	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:36:38.747926950 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.747935057 CET	49702	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:36:38.747957945 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.747972012 CET	49702	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:36:38.747989893 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.748013020 CET	49702	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:36:38.748030901 CET	49702	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:36:38.816648006 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.816682100 CET	80	49702	46.183.222.6	192.168.2.3
Mar 9, 2021 15:36:38.816729069 CET	49702	80	192.168.2.3	46.183.222.6
Mar 9, 2021 15:36:38.816770077 CET	49702	80	192.168.2.3	46.183.222.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 9, 2021 15:36:38.817224026 CET	80	49702	46.183.222.6	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 9, 2021 15:36:23.719480038 CET	58643	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:36:23.773894072 CET	53	58643	8.8.8.8	192.168.2.3
Mar 9, 2021 15:36:24.463095903 CET	60985	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:36:24.520833015 CET	53	60985	8.8.8.8	192.168.2.3
Mar 9, 2021 15:36:26.329641104 CET	50200	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:36:26.385292053 CET	53	50200	8.8.8.8	192.168.2.3
Mar 9, 2021 15:36:36.735038042 CET	51281	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:36:36.791449070 CET	53	51281	8.8.8.8	192.168.2.3
Mar 9, 2021 15:36:38.247195005 CET	49199	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:36:38.304399014 CET	53	49199	8.8.8.8	192.168.2.3
Mar 9, 2021 15:36:50.737313032 CET	50620	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:36:50.787389040 CET	53	50620	8.8.8.8	192.168.2.3
Mar 9, 2021 15:36:59.617201090 CET	64938	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:36:59.674304008 CET	53	64938	8.8.8.8	192.168.2.3
Mar 9, 2021 15:37:02.738008022 CET	60152	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:37:02.786905050 CET	53	60152	8.8.8.8	192.168.2.3
Mar 9, 2021 15:37:06.763540983 CET	57544	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:37:06.810987949 CET	53	57544	8.8.8.8	192.168.2.3
Mar 9, 2021 15:37:07.760843992 CET	57544	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:37:07.808106899 CET	53	57544	8.8.8.8	192.168.2.3
Mar 9, 2021 15:37:08.781852961 CET	57544	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:37:08.829157114 CET	53	57544	8.8.8.8	192.168.2.3
Mar 9, 2021 15:37:10.263906956 CET	55984	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:37:10.309812069 CET	53	55984	8.8.8.8	192.168.2.3
Mar 9, 2021 15:37:10.777937889 CET	57544	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:37:10.823820114 CET	53	57544	8.8.8.8	192.168.2.3
Mar 9, 2021 15:37:11.388683081 CET	64185	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:37:11.436532974 CET	53	64185	8.8.8.8	192.168.2.3
Mar 9, 2021 15:37:14.792624950 CET	57544	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:37:14.847003937 CET	53	57544	8.8.8.8	192.168.2.3
Mar 9, 2021 15:37:17.968511105 CET	65110	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:37:18.025552988 CET	53	65110	8.8.8.8	192.168.2.3
Mar 9, 2021 15:37:28.588829994 CET	58361	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:37:28.634722948 CET	53	58361	8.8.8.8	192.168.2.3
Mar 9, 2021 15:37:30.339835882 CET	63492	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:37:30.385863066 CET	53	63492	8.8.8.8	192.168.2.3
Mar 9, 2021 15:37:32.505307913 CET	60831	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:37:32.570585966 CET	53	60831	8.8.8.8	192.168.2.3
Mar 9, 2021 15:37:41.719213009 CET	60100	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:37:41.764954090 CET	53	60100	8.8.8.8	192.168.2.3
Mar 9, 2021 15:37:48.150382996 CET	53195	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:37:48.206485987 CET	53	53195	8.8.8.8	192.168.2.3
Mar 9, 2021 15:37:57.925112009 CET	50141	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:37:57.973954916 CET	53	50141	8.8.8.8	192.168.2.3
Mar 9, 2021 15:38:18.275732040 CET	53023	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:38:18.321680069 CET	53	53023	8.8.8.8	192.168.2.3
Mar 9, 2021 15:38:25.975334883 CET	49563	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:38:26.044024944 CET	53	49563	8.8.8.8	192.168.2.3
Mar 9, 2021 15:38:30.108715057 CET	51352	53	192.168.2.3	8.8.8.8
Mar 9, 2021 15:38:30.157547951 CET	53	51352	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 9, 2021 15:36:38.247195005 CET	192.168.2.3	8.8.8.8	0xc324	Standard query (0)	covid19vaccine.hopto.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 9, 2021 15:36:38.304399014 CET	8.8.8.8	192.168.2.3	0xc324	No error (0)	covid19vaccine.hopto.org		46.183.222.6	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- covid19vaccine.hopto.org

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49702	46.183.222.6	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 15:36:38.394871950 CET	958	OUT	GET /march%20OG.exe 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: covid19vaccine.hopto.org Connection: Keep-Alive
Mar 9, 2021 15:36:38.466542959 CET	959	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 14:36:37 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1h PHP/8.0.2 Last-Modified: Wed, 03 Mar 2021 00:26:30 GMT ETag: "17000-5bc96e70c1a4b" Accept-Ranges: bytes Content-Length: 94208 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 8b 23 c4 db cf 42 aa 88 cf 42 aa 88 cf 42 aa 88 4c 5e a4 88 ce 42 aa 88 80 60 a3 88 cd 42 aa 88 f9 64 a7 88 ce 42 aa 88 52 69 63 68 cf 42 aa 88 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 8c 5d 2f 4d 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 40 01 00 00 30 00 00 00 00 00 00 14 17 00 00 00 10 00 00 00 50 01 00 00 00 40 00 00 10 00 00 00 10 00 00 04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 80 01 00 00 10 00 00 67 77 01 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 f4 46 01 00 28 00 00 00 00 70 01 00 ac 09 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 28 02 00 00 20 00 00 00 00 10 00 00 90 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 2c 3d 01 00 00 10 00 00 00 40 01 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 64 61 74 61 00 00 00 08 12 00 00 00 50 01 00 00 10 00 00 00 50 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 ac 09 00 00 00 70 01 00 00 10 00 00 00 60 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 c3 1f b0 49 10 00 00 00 00 00 00 00 00 00 00 4d 53 56 42 56 4d 36 30 2e 44 4c 4c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$#BBBL^B`BdBRichBPEL]/M@0P@gwF(p( .text,=@ `.dataPP@.rsrcp`@@IMSVBVM60.DLL

Code Manipulations

Statistics

Behavior

- iexplore.exe
- iexplore.exe
- march OG.exe
- march OG.exe

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 3476 Parent PID: 792

General

Start time:	15:36:35
Start date:	09/03/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff6a9080000
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: 5588 Parent PID: 3476

General

Start time:	15:36:36
Start date:	09/03/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:3476 CREDAT:17410 /prefetch:2
Imagebase:	0x1260000
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

Analysis Process: march OG.exe PID: 3652 Parent PID: 3476

General

Start time:	15:37:19
Start date:	09/03/2021
Path:	C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\march OG.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\march OG.exe'
Imagebase:	0x400000
File size:	94208 bytes
MD5 hash:	B75B990AC5990F1B6B0127540DE4EC30
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: march OG.exe PID: 6092 Parent PID: 3652

General

Start time:	15:38:25
Start date:	09/03/2021
Path:	C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\march OG.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\march OG.exe'
Imagebase:	0x400000
File size:	94208 bytes
MD5 hash:	B75B990AC5990F1B6B0127540DE4EC30
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

Code Analysis