ID: 365439
Cookbook: browseurl.jbs
Time: 15:37:23
Date: 09/03/2021
Version: 31.0.0 Emerald

Table of Contents

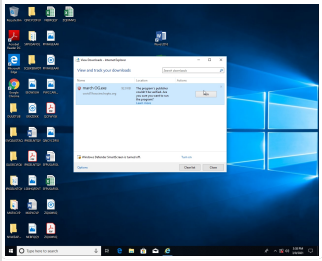
Analysis Report http://covid19vaccine.hopto.org/march …

Overview

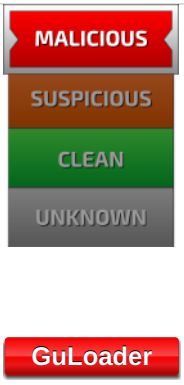
General Information

Sample URL:	http://covid19vaccine.hopto.org/march OG.exe
Analysis ID:	365439
Infos:	

Most interesting Screenshot:



Detection

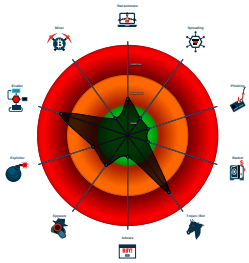


Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Detected RDTSC dummy instruction…
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…
- Yara detected VB6 Downloader Gen…
- Abnormal high CPU Usage
- Contains functionality for execution …
- Contains functionality to call native f…
- Contains functionality to query CPU …

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 4340 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 4436 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4340 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - march OG.exe (PID: 4844 cmdline: 'C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\march OG.exe' MD5: B75B990AC5990F1B6B0127540DE4EC30)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

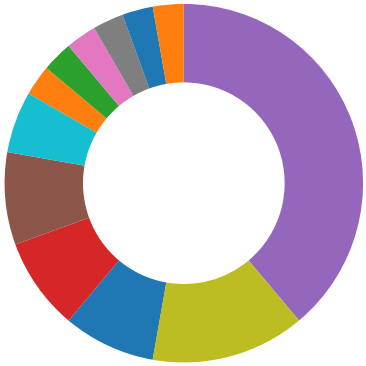
Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: march OG.exe PID: 4844	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: march OG.exe PID: 4844	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- 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 dropped file

Multi AV Scanner detection for submitted file

Data Obfuscation:

Yara detected GuLoader

Yara detected VB6 Downloader Generic

Malware Analysis System Evasion:

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

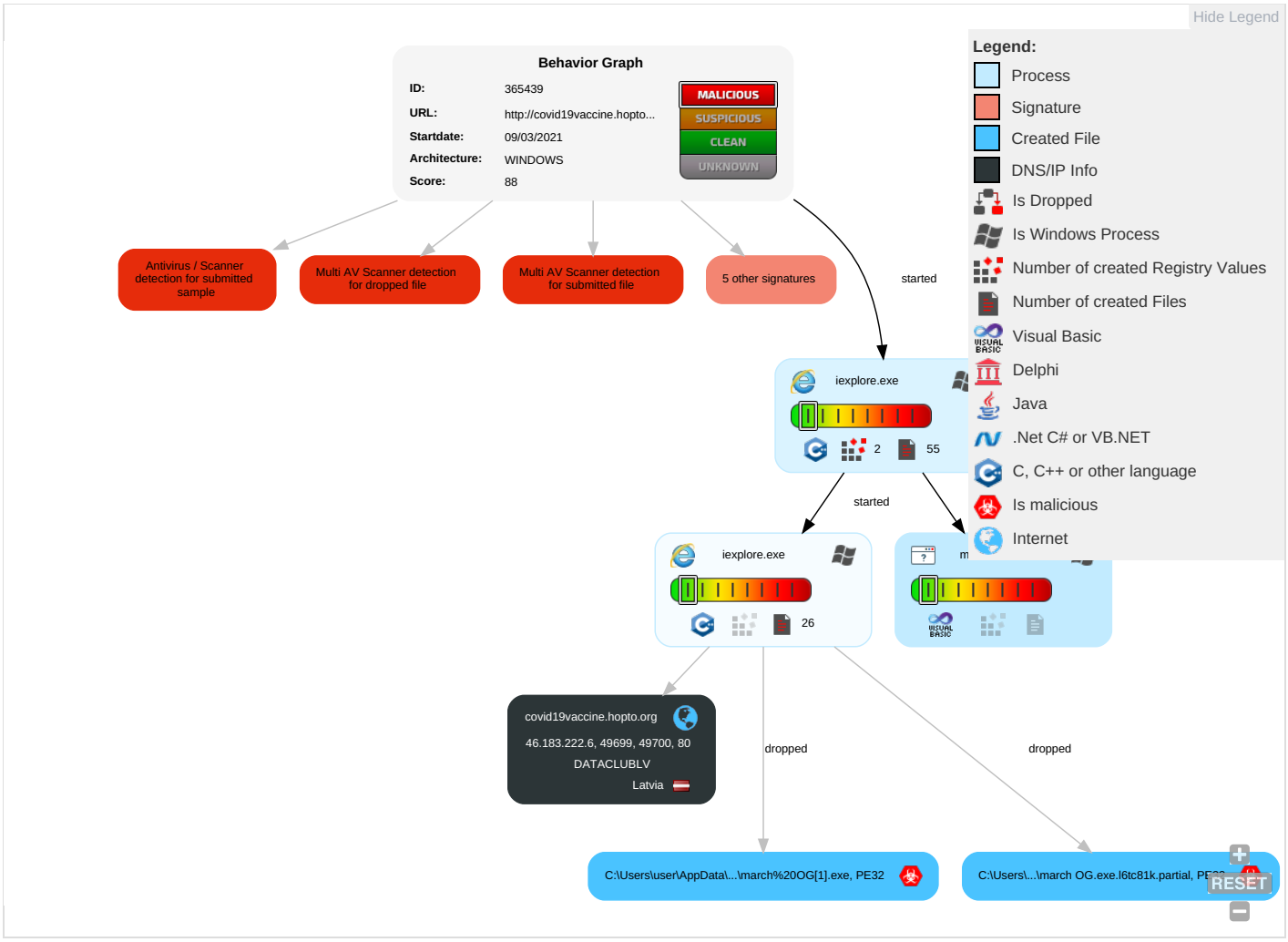
Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Tries to detect virtualization through RDTSC time measurements

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
Valid Accounts	Exploitation for Client Execution 1	Path Interception	Process Injection 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 4 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 2	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 2 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Card Swap	

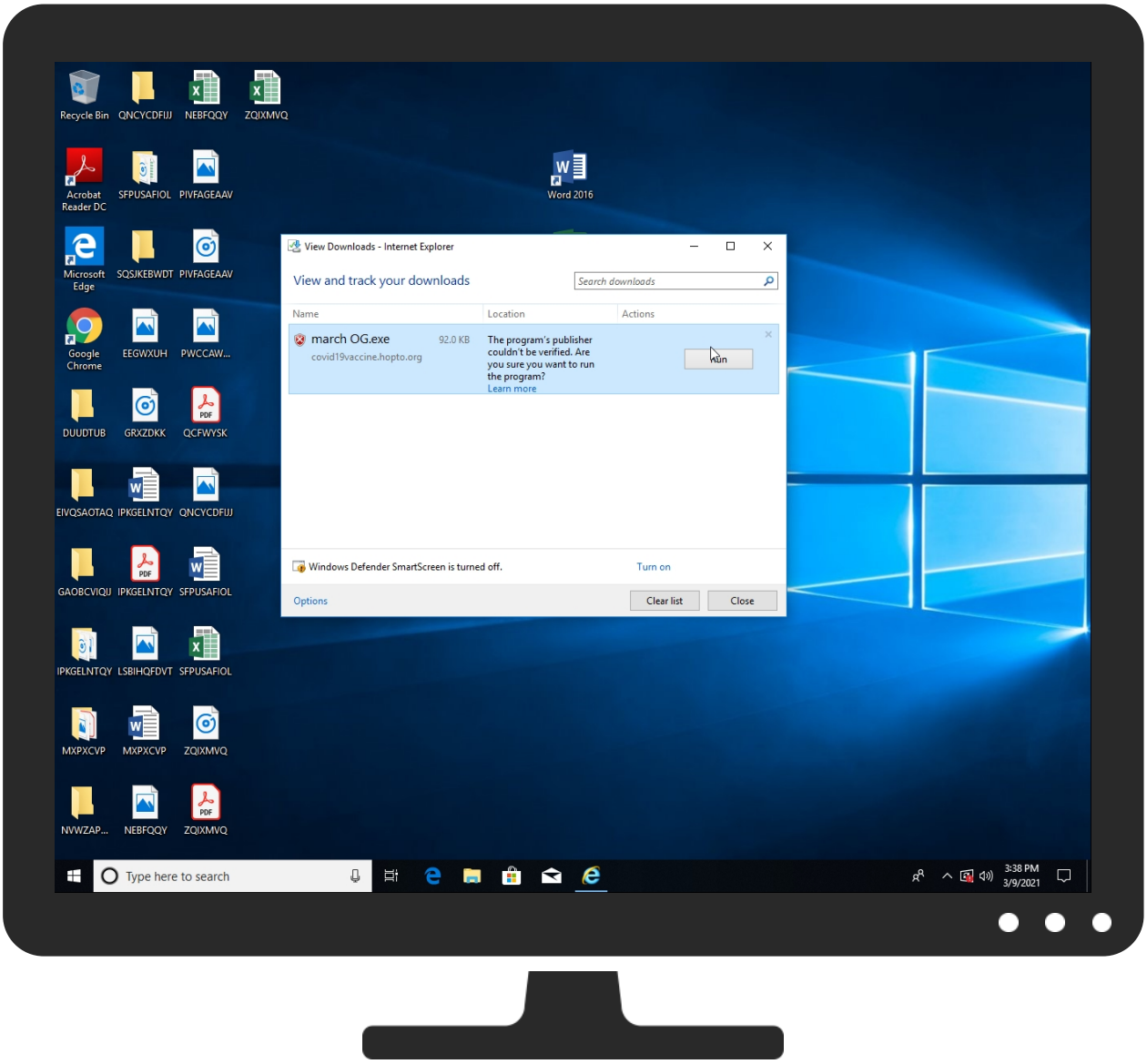
Behavior Graph



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\0MX4YUS9\march OG.exe.l6tc81k.partial	24%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\march OG.exe.l6tc81k.partial	82%	ReversingLabs	Win32.Trojan.VBObfuse	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\march%20OG[1].exe	24%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\march%20OG[1].exe	82%	ReversingLabs	Win32.Trojan.VBObfuse	

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
covid19vaccine.hopto.org	46.183.222.6	true	false		unknown

Contacted URLs

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

Contacted IPs

Public

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

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	365439
Start date:	09.03.2021
Start time:	15:37:23
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 5m 22s
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:	mal88.troj.evad.win@5/9@1/1
EGA Information:	• Successful, ratio: 100%
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, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 92.122.145.220, 104.108.39.131, 23.57.80.111, 13.64.90.137, 51.104.144.132, 152.199.19.161, 104.42.151.234, 2.20.142.210, 2.20.142.209, 51.103.5.186, 40.88.32.150, 92.122.213.247, 92.122.213.194, 52.155.217.156, 20.54.26.129, 13.88.21.125, 168.61.161.212 • Excluded domains from analysis (whitelisted): 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, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, wns.notify.trafficmanager.net, go.microsoft.com, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, ie9comview.vo.msecnd.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus17.cloudapp.net, a767.dscg3.akamai.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, go.microsoft.com.edgekey.net, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net, vip2-par02p.wns.notify.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.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.{813E1F67-8130-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	32344
Entropy (8bit):	1.7940541219870676
Encrypted:	false
SSDEEP:	192:rUZbZ22KWXt0if6j9zM61BPv/k1WAl5p2:rENNJ9Jn80o
MD5:	C6362859B5CB475AADB05A8FF8A63B82
SHA1:	197324A4CCE901D243928ED5ABA0E0311E2DFF0D
SHA-256:	EE4D461DBE6EE3B57F9AEB3BC792EA6543A18D018B42B52CC917D24E6629332E
SHA-512:	6A48B3D6B62D5DE0BF6C531B2538E125981B741AD8520A60D2BA6DAB2478C174D63A71ECB832F69529AC73FD6D38946B06B13B28C1E068D968267548C501ADE
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\{813E1F69-8130-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	19032
Entropy (8bit):	1.599271845016993
Encrypted:	false
SSDEEP:	48:IwEGcprdGwpaxG4pQOGrapbSsGQpBGGHHpc3TGUpQweGcpm:rYZHQj6ABSkjF2B6vg
MD5:	80481B7A27B1D6C0DEF3782C8DE52A26

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{813E1F69-8130-11EB-90E6-ECF4BB82F7E0}.dat	
SHA1:	EC36C5CDABB593C404B5F3908A18029A893B04F4
SHA-256:	DBF8D767C2220C5B9EB6A760EBD206A7A5F8A6515C5CF652E6A9FF5BE690C90C
SHA-512:	8972A04D820B5E433E8B197EC5BF266E3C5B63CD8C43F321826A02189A8B3EA851726BA8298F5CBB3CB11EA980C3AE486EED27280F009E1705BDAA35B8FCC25 1
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\march OG.exe.l6tc81k.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
SHA-512:	E2009B8E6AD35C60F08EFB6514C18C650929F343B01A14F2AAB8D5EAEC880520C67BCF6795ED21BE8C462A2C32EB31E80A7A3A1C9767776CE18F208B4F89FF4 5
Malicious:	**true**
Antivirus:	• 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\0MX4YUS9\march OG.exe.l6tc81k.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\0MX4YUS9\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\march OG.exe:Zone.Identifier	
Preview:	3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\6M6D1PMD\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:	1536:61oJy7aGTvIaUZNcddsm3dE+WE2i5JjyI+h91mR4E:6v7aGTUcddaMrjyIA1jE
MD5:	B75B990AC5990F1B6B0127540DE4EC30
SHA1:	66DD5A9D359FAF4ABDFF9B53B8E96280EFF58038
SHA-256:	F7ABA1C5E66938EFC7A722F98344A70A2443391668283F08DA1202BDE6C9B925
SHA-512:	E2009B8E6AD35C60F08EFB6514C18C650929F343B01A14F2AAB8D5EAEC880520C67BCF6795ED21BE8C462A2C32EB31E80A7A3A1C9767776CE18F208B4F89FF45
Malicious:	**true**
Antivirus:	• 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\Temp\JavaDeployReg.log	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	89
Entropy (8bit):	4.366670544419046
Encrypted:	false
SSDEEP:	3:oVXU0NFUNW8JOGXnE0NFpULun:o9UoqEqUC
MD5:	967DEE776D313F3030F12D257AC94577
SHA1:	AC966037240676B799CDF5FE28716255C1B4303B
SHA-256:	DF6ACB284F6483CE0D3914A5A0985D7F0DC1613DE0F645F6A982F8D109F284F3
SHA-512:	17F91D81F08AF61C7C94490399F09D3F6FE89E1C895DD7E685050026CB017AF48C264A689713FE529740B9EA8F174605E20A7AECF054C767BBEB25F2BDBE8614
Malicious:	false
Reputation:	low
Preview:	[2021/03/09 15:38:11.105] Latest deploy version: ..[2021/03/09 15:38:11.105] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\~DF27A6466E5B9B4110.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12981
Entropy (8bit):	0.4430559335601269
Encrypted:	false
SSDEEP:	12:c9lCg5/9lCgeK9l26an9l26an9l8fR+k9l8fR+09lTq+CVduiryUuNsqNxrt:c9lLh9lLh9lIn9lIn9loL9loL9lWjDoZ
MD5:	1895B7B06EBF1C0546E5EFA39D637A9D
SHA1:	3FC35A4F370B898F686C0B48A1FEBC564772E619
SHA-256:	C94BD6E9E78D006EFC4EDCFDEA87C15220EFA0DBEFC9371A4857BF2B8F1AEDB6
SHA-512:	8A9EE4BFE5AD0632B4E2A81390D64EBBF917C8BBC2660722D21D9D9EFB9CF32849F2814E642C728ED01AD78A79407D5E21C0B2E1D7FA9F63FE26D1E2B9C3EE82
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF761A8E80D89A84E5.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data

C:\Users\user\AppData\Local\Temp\~DF761A8E80D89A84E5.TMP	
Category:	dropped
Size (bytes):	29989
Entropy (8bit):	0.3309272852524987
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwTK/9lwTi9l2Tc/9l2d:kBqoxKAuvScS+B/I+hwy
MD5:	F5EBE47B4CE8A5D9978C360417688828
SHA1:	1D3A7AE1BD8B90F828A0EC66CB23A58CA2AB2AEE
SHA-256:	FE4D22A9CDA7116C1FF6417B55D84C78FBA5C5A6415D8495E79FD1ED59A8BB42
SHA-512:	2DA20731BA721409FA74CD8F14755B90A0BA4F7990CA41A966BB1E70A8BE80B2BB5A79BE9DE9929B2635B1846DF2659E78BB2EAC28800F3691E3ABC4E1C26FF4
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

Total Packets: 76

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 9, 2021 15:38:12.546500921 CET	49700	80	192.168.2.7	46.183.222.6
Mar 9, 2021 15:38:12.546504021 CET	49699	80	192.168.2.7	46.183.222.6
Mar 9, 2021 15:38:12.614873886 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.615099907 CET	49699	80	192.168.2.7	46.183.222.6
Mar 9, 2021 15:38:12.615778923 CET	80	49700	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.616731882 CET	49700	80	192.168.2.7	46.183.222.6
Mar 9, 2021 15:38:12.622627020 CET	49699	80	192.168.2.7	46.183.222.6
Mar 9, 2021 15:38:12.690965891 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.691025019 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.691123962 CET	49699	80	192.168.2.7	46.183.222.6
Mar 9, 2021 15:38:12.691157103 CET	49699	80	192.168.2.7	46.183.222.6
Mar 9, 2021 15:38:12.758311033 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.758338928 CET	80	49699	46.183.222.6	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 9, 2021 15:38:12.758357048 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.758373976 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.758438110 CET	49699	80	192.168.2.7	46.183.222.6
Mar 9, 2021 15:38:12.825692892 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.825736046 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.825762033 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.825787067 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.825809956 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.825817108 CET	49699	80	192.168.2.7	46.183.222.6
Mar 9, 2021 15:38:12.825834990 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.825859070 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.825881004 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.825892925 CET	49699	80	192.168.2.7	46.183.222.6
Mar 9, 2021 15:38:12.825932980 CET	49699	80	192.168.2.7	46.183.222.6
Mar 9, 2021 15:38:12.893600941 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.893641949 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.893672943 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.893692970 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.893712044 CET	49699	80	192.168.2.7	46.183.222.6
Mar 9, 2021 15:38:12.893722057 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.893745899 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.893762112 CET	49699	80	192.168.2.7	46.183.222.6
Mar 9, 2021 15:38:12.893768072 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.893790960 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.893812895 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.893824100 CET	49699	80	192.168.2.7	46.183.222.6
Mar 9, 2021 15:38:12.893841028 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.893851995 CET	49699	80	192.168.2.7	46.183.222.6
Mar 9, 2021 15:38:12.893874884 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.893897057 CET	49699	80	192.168.2.7	46.183.222.6
Mar 9, 2021 15:38:12.893908024 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.893909931 CET	49699	80	192.168.2.7	46.183.222.6
Mar 9, 2021 15:38:12.893934011 CET	49699	80	192.168.2.7	46.183.222.6
Mar 9, 2021 15:38:12.893939018 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.893963099 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.893965960 CET	49699	80	192.168.2.7	46.183.222.6
Mar 9, 2021 15:38:12.893985033 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.893997908 CET	49699	80	192.168.2.7	46.183.222.6
Mar 9, 2021 15:38:12.894006968 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.894016981 CET	49699	80	192.168.2.7	46.183.222.6
Mar 9, 2021 15:38:12.894043922 CET	49699	80	192.168.2.7	46.183.222.6
Mar 9, 2021 15:38:12.894073963 CET	49699	80	192.168.2.7	46.183.222.6
Mar 9, 2021 15:38:12.961520910 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.961580992 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.961627007 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.961630106 CET	49699	80	192.168.2.7	46.183.222.6
Mar 9, 2021 15:38:12.961657047 CET	49699	80	192.168.2.7	46.183.222.6
Mar 9, 2021 15:38:12.961683989 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.961688042 CET	49699	80	192.168.2.7	46.183.222.6
Mar 9, 2021 15:38:12.961740017 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.961755991 CET	49699	80	192.168.2.7	46.183.222.6
Mar 9, 2021 15:38:12.961796045 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.961810112 CET	49699	80	192.168.2.7	46.183.222.6
Mar 9, 2021 15:38:12.961839914 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.961857080 CET	49699	80	192.168.2.7	46.183.222.6
Mar 9, 2021 15:38:12.961874008 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.961884975 CET	49699	80	192.168.2.7	46.183.222.6
Mar 9, 2021 15:38:12.961909056 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.961924076 CET	49699	80	192.168.2.7	46.183.222.6
Mar 9, 2021 15:38:12.961945057 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.961987019 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.961992025 CET	49699	80	192.168.2.7	46.183.222.6
Mar 9, 2021 15:38:12.962029934 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.962038994 CET	49699	80	192.168.2.7	46.183.222.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 9, 2021 15:38:12.962080956 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.962083101 CET	49699	80	192.168.2.7	46.183.222.6
Mar 9, 2021 15:38:12.962135077 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.962150097 CET	49699	80	192.168.2.7	46.183.222.6
Mar 9, 2021 15:38:12.962188005 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.962193012 CET	49699	80	192.168.2.7	46.183.222.6
Mar 9, 2021 15:38:12.962229013 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.962235928 CET	49699	80	192.168.2.7	46.183.222.6
Mar 9, 2021 15:38:12.962265968 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.962272882 CET	49699	80	192.168.2.7	46.183.222.6
Mar 9, 2021 15:38:12.962302923 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.962325096 CET	49699	80	192.168.2.7	46.183.222.6
Mar 9, 2021 15:38:12.962344885 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.962351084 CET	49699	80	192.168.2.7	46.183.222.6
Mar 9, 2021 15:38:12.962383032 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.962388992 CET	49699	80	192.168.2.7	46.183.222.6
Mar 9, 2021 15:38:12.962418079 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.962434053 CET	49699	80	192.168.2.7	46.183.222.6
Mar 9, 2021 15:38:12.962452888 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.962466955 CET	49699	80	192.168.2.7	46.183.222.6
Mar 9, 2021 15:38:12.962505102 CET	49699	80	192.168.2.7	46.183.222.6
Mar 9, 2021 15:38:12.962503910 CET	80	49699	46.183.222.6	192.168.2.7
Mar 9, 2021 15:38:12.962558031 CET	80	49699	46.183.222.6	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 9, 2021 15:38:04.209747076 CET	60501	53	192.168.2.7	8.8.8.8
Mar 9, 2021 15:38:04.268192053 CET	53	60501	8.8.8.8	192.168.2.7
Mar 9, 2021 15:38:11.293840885 CET	53775	53	192.168.2.7	8.8.8.8
Mar 9, 2021 15:38:11.350908995 CET	53	53775	8.8.8.8	192.168.2.7
Mar 9, 2021 15:38:12.472520113 CET	51837	53	192.168.2.7	8.8.8.8
Mar 9, 2021 15:38:12.534859896 CET	53	51837	8.8.8.8	192.168.2.7
Mar 9, 2021 15:38:30.674083948 CET	55411	53	192.168.2.7	8.8.8.8
Mar 9, 2021 15:38:30.732253075 CET	53	55411	8.8.8.8	192.168.2.7
Mar 9, 2021 15:38:33.830120087 CET	63668	53	192.168.2.7	8.8.8.8
Mar 9, 2021 15:38:33.876199007 CET	53	63668	8.8.8.8	192.168.2.7
Mar 9, 2021 15:38:41.172713995 CET	54640	53	192.168.2.7	8.8.8.8
Mar 9, 2021 15:38:41.219281912 CET	53	54640	8.8.8.8	192.168.2.7
Mar 9, 2021 15:38:41.298634052 CET	58739	53	192.168.2.7	8.8.8.8
Mar 9, 2021 15:38:41.345556021 CET	53	58739	8.8.8.8	192.168.2.7
Mar 9, 2021 15:38:42.301479101 CET	58739	53	192.168.2.7	8.8.8.8
Mar 9, 2021 15:38:42.348711967 CET	53	58739	8.8.8.8	192.168.2.7
Mar 9, 2021 15:38:43.330921888 CET	58739	53	192.168.2.7	8.8.8.8
Mar 9, 2021 15:38:43.376823902 CET	53	58739	8.8.8.8	192.168.2.7
Mar 9, 2021 15:38:45.346986055 CET	58739	53	192.168.2.7	8.8.8.8
Mar 9, 2021 15:38:45.392901897 CET	53	58739	8.8.8.8	192.168.2.7
Mar 9, 2021 15:38:49.363078117 CET	58739	53	192.168.2.7	8.8.8.8
Mar 9, 2021 15:38:49.409126997 CET	53	58739	8.8.8.8	192.168.2.7
Mar 9, 2021 15:38:54.034775019 CET	60338	53	192.168.2.7	8.8.8.8
Mar 9, 2021 15:38:54.080661058 CET	53	60338	8.8.8.8	192.168.2.7
Mar 9, 2021 15:38:59.562648058 CET	58717	53	192.168.2.7	8.8.8.8
Mar 9, 2021 15:38:59.619684935 CET	53	58717	8.8.8.8	192.168.2.7
Mar 9, 2021 15:39:02.104366064 CET	59762	53	192.168.2.7	8.8.8.8
Mar 9, 2021 15:39:02.159679890 CET	53	59762	8.8.8.8	192.168.2.7
Mar 9, 2021 15:39:02.893915892 CET	54329	53	192.168.2.7	8.8.8.8
Mar 9, 2021 15:39:02.940005064 CET	53	54329	8.8.8.8	192.168.2.7
Mar 9, 2021 15:39:26.152199030 CET	58052	53	192.168.2.7	8.8.8.8
Mar 9, 2021 15:39:26.207998991 CET	53	58052	8.8.8.8	192.168.2.7
Mar 9, 2021 15:39:33.796916008 CET	54008	53	192.168.2.7	8.8.8.8
Mar 9, 2021 15:39:33.851068974 CET	53	54008	8.8.8.8	192.168.2.7
Mar 9, 2021 15:39:44.002993107 CET	59451	53	192.168.2.7	8.8.8.8
Mar 9, 2021 15:39:44.072282076 CET	53	59451	8.8.8.8	192.168.2.7
Mar 9, 2021 15:39:44.924587965 CET	52914	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 9, 2021 15:39:44.981726885 CET	53	52914	8.8.8.8	192.168.2.7
Mar 9, 2021 15:39:46.029555082 CET	64569	53	192.168.2.7	8.8.8.8
Mar 9, 2021 15:39:46.084809065 CET	53	64569	8.8.8.8	192.168.2.7
Mar 9, 2021 15:39:47.728049994 CET	52816	53	192.168.2.7	8.8.8.8
Mar 9, 2021 15:39:47.805243015 CET	53	52816	8.8.8.8	192.168.2.7
Mar 9, 2021 15:39:48.353799105 CET	50781	53	192.168.2.7	8.8.8.8
Mar 9, 2021 15:39:48.411199093 CET	53	50781	8.8.8.8	192.168.2.7
Mar 9, 2021 15:39:49.070045948 CET	54230	53	192.168.2.7	8.8.8.8
Mar 9, 2021 15:39:49.117367029 CET	53	54230	8.8.8.8	192.168.2.7
Mar 9, 2021 15:39:49.791652918 CET	54911	53	192.168.2.7	8.8.8.8
Mar 9, 2021 15:39:49.846575975 CET	53	54911	8.8.8.8	192.168.2.7
Mar 9, 2021 15:39:51.306799889 CET	49958	53	192.168.2.7	8.8.8.8
Mar 9, 2021 15:39:51.363261938 CET	53	49958	8.8.8.8	192.168.2.7
Mar 9, 2021 15:39:52.744709969 CET	50860	53	192.168.2.7	8.8.8.8
Mar 9, 2021 15:39:52.801925898 CET	53	50860	8.8.8.8	192.168.2.7
Mar 9, 2021 15:39:53.230261087 CET	50452	53	192.168.2.7	8.8.8.8
Mar 9, 2021 15:39:53.286919117 CET	53	50452	8.8.8.8	192.168.2.7
Mar 9, 2021 15:39:53.457514048 CET	59730	53	192.168.2.7	8.8.8.8
Mar 9, 2021 15:39:53.525835991 CET	53	59730	8.8.8.8	192.168.2.7
Mar 9, 2021 15:40:06.724911928 CET	59310	53	192.168.2.7	8.8.8.8
Mar 9, 2021 15:40:06.773703098 CET	53	59310	8.8.8.8	192.168.2.7
Mar 9, 2021 15:40:11.621453047 CET	51919	53	192.168.2.7	8.8.8.8
Mar 9, 2021 15:40:11.667619944 CET	53	51919	8.8.8.8	192.168.2.7
Mar 9, 2021 15:40:22.522402048 CET	64296	53	192.168.2.7	8.8.8.8
Mar 9, 2021 15:40:22.568308115 CET	53	64296	8.8.8.8	192.168.2.7
Mar 9, 2021 15:40:24.529536009 CET	56680	53	192.168.2.7	8.8.8.8
Mar 9, 2021 15:40:24.586733103 CET	53	56680	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 9, 2021 15:38:12.472520113 CET	192.168.2.7	8.8.8.8	0xe69e	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 15:38:12.534859896 CET	8.8.8.8	192.168.2.7	0xe69e	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	192.168.2.7	49699	46.183.222.6	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 15:38:12.622627020 CET	915	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

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 15:38:12.690965891 CET	917	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 14:38:11 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 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 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 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 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 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 40 00 00 40 c3 1f b0 49 10 00 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 4340 Parent PID: 792

General

Start time:	15:38:09
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:	0x7ff6bb910000
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: 4436 Parent PID: 4340

General

Start time:	15:38:10
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:4340 CREDAT:17410 /prefetch:2
Imagebase:	0xde0000
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: 4844 Parent PID: 4340

General

Start time:	15:38:41
Start date:	09/03/2021
Path:	C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\march OG.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\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

Disassembly

Code Analysis