ID: 383193
Sample Name: RFQ #46200058149.exe
Cookbook: default.jbs
Time: 13:01:16
Date: 07/04/2021
Version: 31.0.0 Emerald

Table of Contents

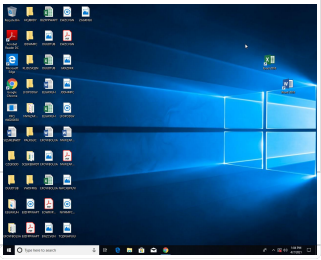
Analysis Report RFQ #46200058149.exe

Overview

General Information

Sample Name:	RFQ #46200058149.exe
Analysis ID:	383193
MD5:	67b96dc502b0c7..
SHA1:	a7c79eeaaafb23e.
SHA256:	ef5cb0bfe2d23b7..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

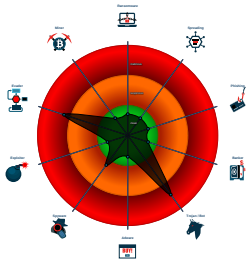
Nanocore

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

Signatures

- Detected Nanocore Rat
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Snort IDS alert for network traffic (e.…
- Yara detected Nanocore RAT
- Hides that the sample has been dow…
- Hides threads from debuggers
- Binary contains a suspicious time st…
- Checks if Antivirus/Antispyware/Fire…
- Checks if the current process is bein…
- Contains capabilities to detect virtua…
- Contains long sleeps (>= 3 min)

Classification



Startup

- **System is w10x64**
- RFQ #46200058149.exe (PID: 5340 cmdline: 'C:\Users\user\Desktop\RFQ #46200058149.exe' MD5: 67B96DC502B0C7A496092D7E6D1DA6C5)
  - cmd.exe (PID: 5912 cmdline: 'C:\Windows\System32\cmd.exe' /c timeout 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 5964 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 5504 cmdline: timeout 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
  - RFQ #46200058149.exe (PID: 5972 cmdline: C:\Users\user\Desktop\RFQ #46200058149.exe MD5: 67B96DC502B0C7A496092D7E6D1DA6C5)
  - WerFault.exe (PID: 5416 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5340 -s 2672 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.301376960.000000000505E000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x105d5:$x1: NanoCore.ClientPluginHost • 0x10612:$x2: IClientNetworkHost • 0x14145:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.301376960.000000000505E000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.301376960.000000000505E000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x1033d:$a: NanoCore • 0x1034d:$a: NanoCore • 0x10581:$a: NanoCore • 0x10595:$a: NanoCore • 0x105d5:$a: NanoCore • 0x1039c:$b: ClientPlugin • 0x1059e:$b: ClientPlugin • 0x105de:$b: ClientPlugin • 0x104c3:$c: ProjectData • 0x10eca:$d: DESCrypto • 0x18896:$e: KeepAlive • 0x16884:$g: LogClientMessage • 0x12a7f:$i: get_Connected • 0x11200:$j: #=q • 0x11230:$j: #=q • 0x1124c:$j: #=q • 0x1127c:$j: #=q • 0x11298:$j: #=q • 0x112b4:$j: #=q • 0x112e4:$j: #=q • 0x11300:$j: #=q
00000000.00000003.240375757.000000000507F000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x223f5:$x1: NanoCore.ClientPluginHost • 0x55015:$x1: NanoCore.ClientPluginHost • 0x22432:$x2: IClientNetworkHost • 0x55052:$x2: IClientNetworkHost • 0x25f65:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x58b85:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000003.240375757.000000000507F000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 4 entries				

Unpacked PEs

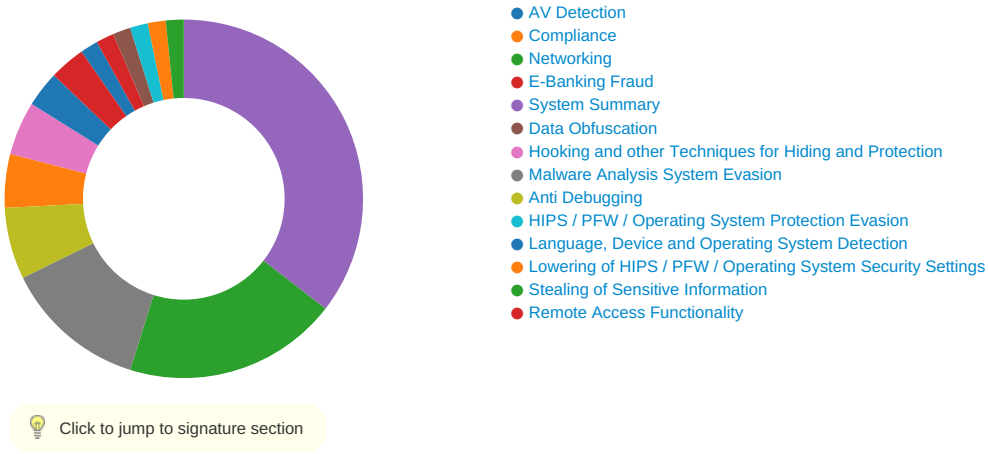
Source	Rule	Description	Author	Strings
0.2.RFQ #46200058149.exe.505e448.10.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0.2.RFQ #46200058149.exe.505e448.10.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
0.2.RFQ #46200058149.exe.505e448.10.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0.2.RFQ #46200058149.exe.505e448.10.raw.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q
0.2.RFQ #46200058149.exe.505e448.10.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 7 entries				

Sigma Overview

System Summary:

Sigma detected: NanoCore

Signature Overview



Click to jump to signature section

AV Detection:

Yara detected Nanocore RAT

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection:

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

Anti Debugging:

Hides threads from debuggers

Stealing of Sensitive Information:

Yara detected Nanocore RAT

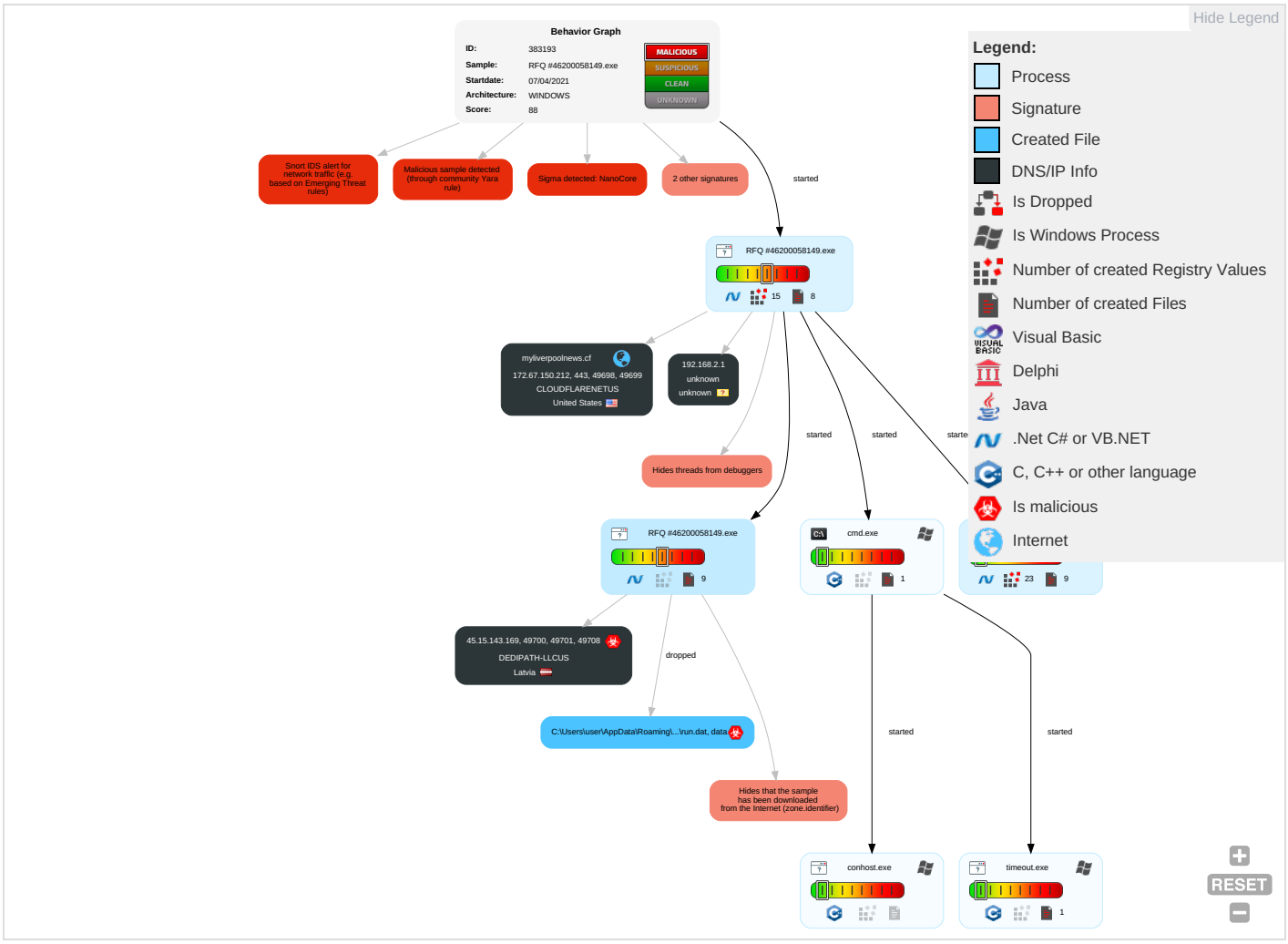
Remote Access Functionality:

Detected Nanocore Rat

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation 1	Path Interception	Process Injection 1 1	Masquerading 1	OS Credential Dumping	Query Registry 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdr Insecure Network Commur
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 1 3 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Remote Access Software 1	Exploit S Redirect Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 4 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 1	Exploit S Track De Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1	NTDS	Virtualization/Sandbox Evasion 1 4 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 2	SIM Car Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Files and Directories 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 3	Manipula Device Commur
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Timestomp 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial o Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue W Access F
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 1 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgra Insecure Protocol

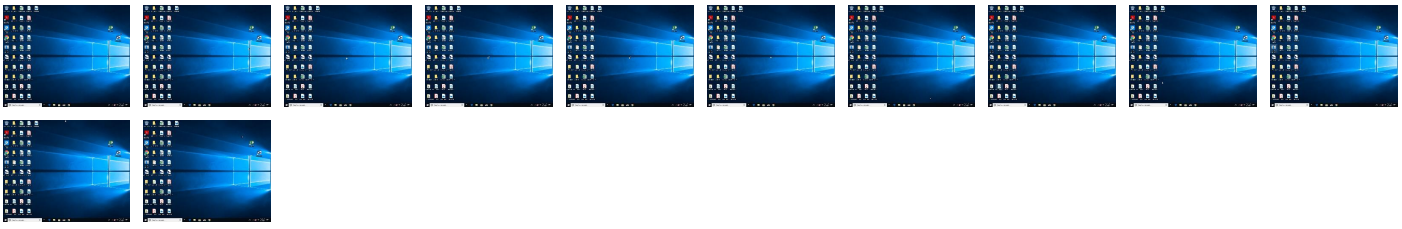
Behavior Graph



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

No Antivirus matches

Domains

No Antivirus matches

URLs

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

Source	Detection	Scanner	Label	Link
http://https://i2-prod.liverpool.com/incoming/article19957561.ece/ALTERNATES/s458/1_FreeAgentPlayers.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19957561.ece/ALTERNATES/s458/1_FreeAgentPlayers.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19957561.ece/ALTERNATES/s458/1_FreeAgentPlayers.jpg	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-arsenal-klopp-lijnders-carabao-171668	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-arsenal-klopp-lijnders-carabao-171668	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-arsenal-klopp-lijnders-carabao-171668	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-02-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-02-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-02-	0%	URL Reputation	safe	
http://https://i2-prod.liverpoolecho.co.uk/incoming/article17165318.ece/ALTERNATES/s615/2_GettyImages-11837	0%	URL Reputation	safe	
http://https://i2-prod.liverpoolecho.co.uk/incoming/article17165318.ece/ALTERNATES/s615/2_GettyImages-11837	0%	URL Reputation	safe	
http://https://i2-prod.liverpoolecho.co.uk/incoming/article17165318.ece/ALTERNATES/s615/2_GettyImages-11837	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s220b/0_GettyImages-1273716690	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s220b/0_GettyImages-1273716690	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s220b/0_GettyImages-1273716690	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961953.ece/ALTERNATES/s180/0_GettyImages-1302496803.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961953.ece/ALTERNATES/s180/0_GettyImages-1302496803.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961953.ece/ALTERNATES/s180/0_GettyImages-1302496803.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s270b/0_Salah-Goal-vs-Leeds.jp	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s270b/0_Salah-Goal-vs-Leeds.jp	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s270b/0_Salah-Goal-vs-Leeds.jp	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19960478.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19960478.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19960478.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://www.liverpool.com/all-about/premier-league	0%	URL Reputation	safe	
http://https://www.liverpool.com/all-about/premier-league	0%	URL Reputation	safe	
http://https://www.liverpool.com/all-about/premier-league	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s180/0_Salah-Pressing.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s180/0_Salah-Pressing.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s180/0_Salah-Pressing.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s615/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s615/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s615/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19963923.ece/ALTERNATES/s180/1_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19963923.ece/ALTERNATES/s180/1_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19963923.ece/ALTERNATES/s180/1_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/	0%	URL Reputation	safe	
http://https://www.liverpool.com/schedule/liverpool-arsenal-carabao-cup-klopp-17166154	0%	URL Reputation	safe	
http://https://www.liverpool.com/schedule/liverpool-arsenal-carabao-cup-klopp-17166154	0%	URL Reputation	safe	
http://https://www.liverpool.com/schedule/liverpool-arsenal-carabao-cup-klopp-17166154	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s615/0_GettyImages-1231353837.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s615/0_GettyImages-1231353837.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s615/0_GettyImages-1231353837.	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-psg-transfer-news-19957850	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-psg-transfer-news-19957850	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-psg-transfer-news-19957850	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s220b/0_WhatsApp-Image-2021-02	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s220b/0_WhatsApp-Image-2021-02	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s220b/0_WhatsApp-Image-2021-02	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s180/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s180/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s180/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s270b/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s270b/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s270b/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/fsg-liverpool-gini-wijnaldum-transfer-1876	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/fsg-liverpool-gini-wijnaldum-transfer-1876	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/fsg-liverpool-gini-wijnaldum-transfer-1876	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s615/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s615/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s615/0_RobertsonCross1.jpg	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/jurgen-klopp-liverpool-transfer-targets-1996166	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/jurgen-klopp-liverpool-transfer-targets-1996166	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/jurgen-klopp-liverpool-transfer-targets-1996166	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/liverpool-erling-haaland-transfer-weghorst	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/liverpool-erling-haaland-transfer-weghorst	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/liverpool-erling-haaland-transfer-weghorst	0%	URL Reputation	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%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s220b/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s220b/0_Curtis-10.png	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19960206.ece/ALTERNATES/s180/0_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19960206.ece/ALTERNATES/s180/0_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19960206.ece/ALTERNATES/s180/0_WhatsApp-Image-2021-03-	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s615/0_GettyImages-1304940818.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s615/0_GettyImages-1304940818.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s615/0_GettyImages-1304940818.	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s270b/0_GettyImages-1273716690	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s270b/0_GettyImages-1273716690	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s270b/0_GettyImages-1273716690	0%	URL Reputation	safe	
http://https://s2-prod.liverpool.com	0%	URL Reputation	safe	
http://https://s2-prod.liverpool.com	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://s2-prod.liverpool.com	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/mohamed-salah-liverpool-goal-flaw-19945816	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/mohamed-salah-liverpool-goal-flaw-19945816	0%	URL Reputation	safe	
http://https://www.liverpool.com/liverpool-fc-news/features/mohamed-salah-liverpool-goal-flaw-19945816	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s270b/0_GettyImages-1231353837	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s270b/0_GettyImages-1231353837	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s270b/0_GettyImages-1231353837	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com	0%	URL Reputation	safe	
http://https://i2-prod.liverpool.com	0%	URL Reputation	safe	
http://https://felix.data.tm-awx.com/felix.min.js	0%	URL Reputation	safe	
http://https://felix.data.tm-awx.com/felix.min.js	0%	URL Reputation	safe	
http://https://felix.data.tm-awx.com/felix.min.js	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
myliverpoolnews.cf	172.67.150.212	true	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-FE6EFB3AED9F05224C930BEF8BE1CC20.html	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dateofbirthhttp://schemas.xmlsoap.org/ws/2005	WerFault.exe, 0000000B.00000003.256378861.0000000005B20000.00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s458/0_GettyImages-1304940818.	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddressxhttp://schemas.xmlsoap.org/ws/200	WerFault.exe, 0000000B.00000003.256378861.0000000005B20000.00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19957561.ece/ALTERNATES/s458/1_FreeAgentPlayers.jpg	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://c.amazon-adsystem.com/aax2/apstag.js	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false		high
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-arsenal-klopp-lijnders-carabao-171668	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-02-	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpoolecho.co.uk/incoming/article17165318.ece/ALTERNATES/s615/2_GettyImages-11837	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/stateorprovince	WerFault.exe, 0000000B.00000003.256378861.0000000005B20000.00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s220b/0_GettyImages-1273716690	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19961953.ece/ALTERNATES/s180/0_GettyImages-1302496803.	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/authentication	WerFault.exe, 0000000B.00000003.256378861.0000000005B20000.00000004.00000001.sdmp	false		high

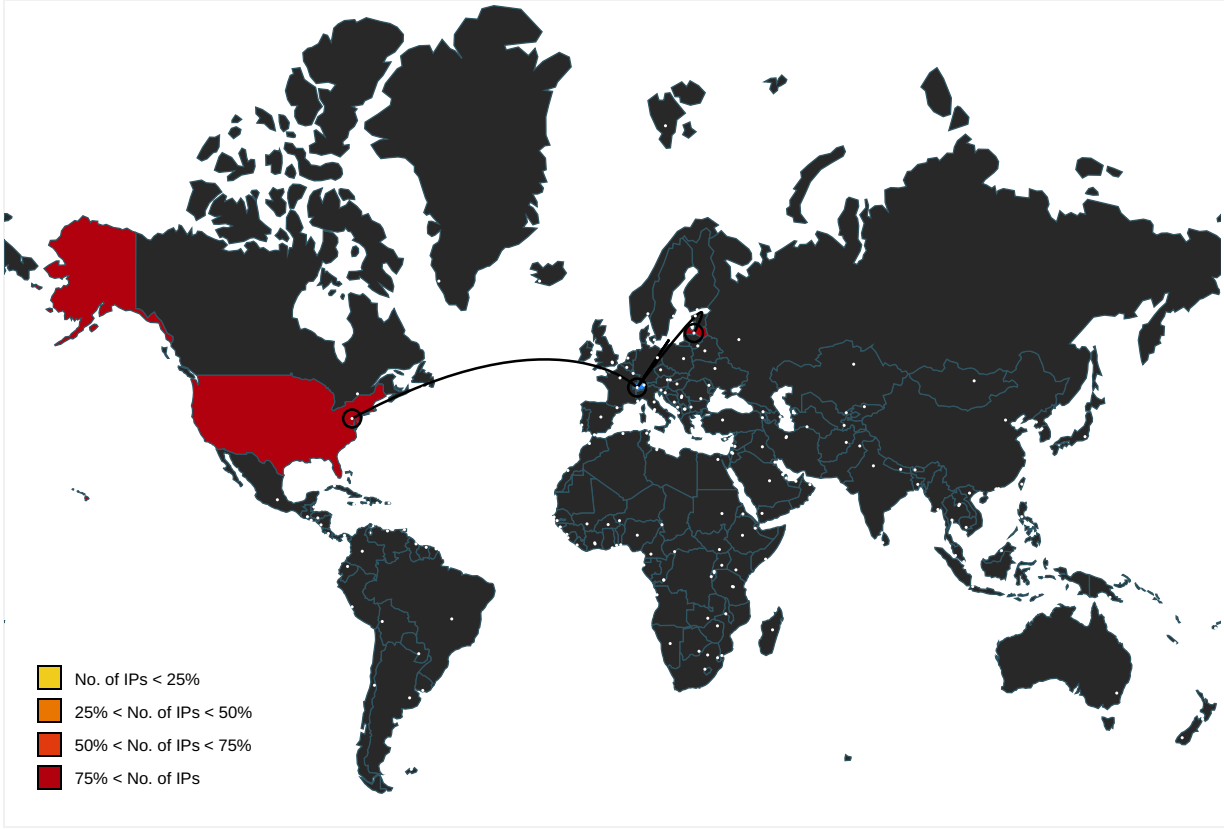
Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/x500distinguishednamejhttp://schemas.xmlsoap.o	WerFault.exe, 0000000B.00000003.256378861.0000000005B20000.00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s270b/0_Salah-Goal-vs-Leeds.jp	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/denyonlysid	WerFault.exe, 0000000B.00000003.256378861.0000000005B20000.00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19960478.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-03-	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/all-about/premier-league	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s180/0_Salah-Pressing.jpg	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp, RFQ #46200058149.exe, 00000000.00000002.296661281.000000000032FE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s615/0_Curtis-10.png	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19963923.ece/ALTERNATES/s180/1_WhatsApp-Image-2021-03-	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/authorizationdecisionzhttp://schemas.xmlsoap.o	WerFault.exe, 0000000B.00000003.256378861.0000000005B20000.00000004.00000001.sdmp	false		high
http://https://www.liverpool.com/schedule/liverpool-arsenal-carabao-cup-klopp-17166154	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s615/0_GettyImages-1231353837.	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-psg-transfer-news-19957850	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s220b/0_WhatsApp-Image-2021-02	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	RFQ #46200058149.exe, 00000000.00000002.296513368.0000000003291000.00000004.00000001.sdmp, WerFault.exe, 0000000B.00000003.256378861.0000000005B20000.00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s180/0_RobertsonCross1.jpg	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ads.pubmatic.com/AdServer/js/pwt/156997/3236/pwt.js	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19940968.ece/ALTERNATES/s270b/0_Curtis-10.png	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/fsg-liverpool-gini-wijnaldum-transfer-1876	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	WerFault.exe, 0000000B.00000003.256378861.0000000005B20000.00000004.00000001.sdmp	false		high
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s615/0_RobertsonCross1.jpg	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/jurgen-klopp-liverpool-transfer-targets-1996166	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/transfer-news/liverpool-erling-haaland-transfer-weghorst	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://reachplc.hub.loginradius.com"	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.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	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19960206.ece/ALTERNATES/s180/0_WhatsApp-Image-2021-03-	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s615/0_GettyImages-1304940818.	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s270b/0_GettyImages-1273716690	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://s2-prod.liverpool.com	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/mohamed-salah-liverpool-goal-flaw-19945816	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s270b/0_GettyImages-1231353837	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://felix.data.tm-awx.com/felix.min.js	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s180/0_Salah-Goal-vs-Leeds.jpg	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19960478.ece/ALTERNATES/s180/0_WhatsApp-Image-2021-03-	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s270b/0_RobertsonCross1.jpg	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s458/0_GettyImages-1273716690.	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/all-about/ozan-kabak	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://s2-prod.mirror.co.uk/	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-	RFQ #46200058149.exe, 00000000.00000002.296513368.0000000003291000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s180/0_WhatsApp-Image-2021-02-	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/all-about/champions-league	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/all-about/curtis-jones	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp, RFQ #46200058149.exe, 00000000.00000002.296661281.000000000032FE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19960206.ece/ALTERNATES/s615/0_WhatsApp-Image-2021-03-	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/all-about/steven-gerrard	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-ozan-kabak-future-audition-19954616	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19963923.ece/ALTERNATES/s458/1_WhatsApp-Image-2021-03-	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-penalties-premier-league-var-17171391	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schema.org/NewsArticle	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.liverpool.com/schedule/	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schema.org/BreadcrumbList	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false		high
http://https://securepubads.g.doubleclick.net/tag/js/gpt.js	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false		high
http://https://s2-prod.liverpool.com/	RFQ #46200058149.exe, 00000000.00000002.296661281.0000000032FE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-champions-league-jurgen-klopp-1996194	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s220b/0_GettyImages-1231353837	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19961953.ece/ALTERNATES/s458/0_GettyImages-1302496803.	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://felix.data.tm-awx.com/ampconfig.json"	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19961704.ece/ALTERNATES/s615/0_GettyImages-1273716690.	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s270b/0_Salah-Pressing.jpg	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp, RFQ #46200058149.exe, 00000000.00000002.296661281.000000000032FE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19945821.ece/ALTERNATES/s615/0_Salah-Goal-vs-Leeds.jpg	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19936064.ece/ALTERNATES/s270b/0_WhatsApp-Image-2021-02	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19946983.ece/ALTERNATES/s220b/0_RobertsonCross1.jpg	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/streetaddressz http://schemas.xmlsoap.org/ws/20	WerFault.exe, 0000000B.00000003.256378861.0000000005B20000.00000004.00000001.sdmp	false		high
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-andy-robertson-valuable-quality-19946	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp, RFQ #46200058149.exe, 00000000.00000002.296661281.000000000032FE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-jurgen-klopp-pressing-tactics-1993836	RFQ #46200058149.exe, 00000000.00000002.296661281.0000000032FE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19938370.ece/ALTERNATES/s615/0_Salah-Pressing.jpg	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp, RFQ #46200058149.exe, 00000000.00000002.296661281.000000000032FE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schema.org/ListItem	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false		high
http://https://www.liverpool.com/all-about/georginio-wijnaldum	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://myliverpoolnews.cf4	RFQ #46200058149.exe, 00000000.00000002.296563326.0000000032CF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://mab.data.tm-awx.com/rhs"	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19955390.ece/ALTERNATES/s180/0_GettyImages-1231353837.	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://felix.data.tm-awx.com	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.liverpool.com/all-about/andrew-robertson	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article17166876.ece/ALTERNATES/s615/0_GettyImages-1175998874.	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-gini-wijnaldum-rumours-fitness-199533	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish-199590	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19955855.ece/ALTERNATES/s180/0_GettyImages-1304940818.	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://myliverpoolnews.cf	RFQ #46200058149.exe, 00000000.00000002.296513368.0000000003291000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.liverpool.com/all-about/transfers	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.liverpool.com/liverpool-fc-news/features/rhian-brewster-liverpool-arsenal-team-17172763&	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19957561.ece/ALTERNATES/s615/1_FreeAgentPlayers.jpg	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19957561.ece/ALTERNATES/s180/1_FreeAgentPlayers.jpg	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://i2-prod.liverpool.com/incoming/article19960206.ece/ALTERNATES/s458/0_WhatsApp-Image-2021-03-	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://reach-id.orbit.tm-awx.com/analytics.js.gz	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/ded/script.js	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false		high
http://https://www.liverpool.com/liverpool-fc-news/features/liverpool-barcelona-real-madrid-psg-17164868	RFQ #46200058149.exe, 00000000.00000003.225747726.0000000004479000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.15.143.169	unknown	Latvia		35913	DEDIPATH-LLCUS	true
172.67.150.212	myliverpoolnews.cf	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383193
Start date:	07.04.2021
Start time:	13:01:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RFQ #46200058149.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:	33
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:	mal88.troj.evad.winEXE@9/11@2/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 76.9% (good quality ratio 52.3%) • Quality average: 31.8% • Quality standard deviation: 22%
HCA Information:	• Successful, ratio: 100% • 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 • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, WerFault.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 93.184.220.29, 20.50.102.62, 23.54.113.53, 23.0.174.200, 23.0.174.185, 95.100.54.203, 104.42.151.234, 104.43.193.48, 13.88.21.125, 23.10.249.26, 23.10.249.43, 20.54.26.129 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, cs9.wac.phicdn.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e12564.dspb.akamaiedge.net, ocsp.digicert.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, fs.microsoft.com, dual-a-0001.a-msedge.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net • Report size getting too big, too many NtAllocateVirtualMemory 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
13:02:05	API Interceptor	1015x Sleep call for process: RFQ #46200058149.exe modified
13:02:36	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
172.67.150.212	Payment Slip E05060_47.doc	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-3764A540BD56887B40989BBA8472B701.html
	New Orders.exe	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-28D56F639751140E7A008217BE126C8D.html
	DHL_document11022020680908911.exe	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-531418C06045F4175229827941 4DE528.html
	BL8846545545363.exe	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-B7B18D8B53846C51E3D2182818196100.html
	BL84995005038483.exe	Get hash	malicious	Browse	• myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-994F3BB06F4A7FE8F60B83F74A076F10.html

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
myliverpoolnews.cf	Payment Slip E05060_47.doc	Get hash	malicious	Browse	• 104.21.56.119
	New Orders.exe	Get hash	malicious	Browse	• 172.67.150.212
	Download Report.06.05.2021.exe	Get hash	malicious	Browse	• 104.21.56.119
	BL836477488575.exe	Get hash	malicious	Browse	• 104.21.56.119
	DHL_document11022020680908911.exe	Get hash	malicious	Browse	• 172.67.150.212
	BL8846545545363.exe	Get hash	malicious	Browse	• 172.67.150.212
	VMtEguRH.exe	Get hash	malicious	Browse	• 104.21.56.119
	BL84995005038483.exe	Get hash	malicious	Browse	• 172.67.150.212

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DEDIPATH-LLCUS	LM_QUOTE757860PDF.exe	Get hash	malicious	Browse	• 45.15.143.178
	PO_4000010871_RFQ_PRS_1000024753_RM.exe	Get hash	malicious	Browse	• 213.59.118.134
	OBJEDNAT.scr.exe	Get hash	malicious	Browse	• 45.144.225.107
	QFSN0331PDF.exe	Get hash	malicious	Browse	• 45.144.225.66
	GBNv7C8xNt.exe	Get hash	malicious	Browse	• 45.144.225.167
	SWIFTCOPY_110255293303484_SANTANDER.doc	Get hash	malicious	Browse	• 45.144.225.167
	receiptpdf.exe	Get hash	malicious	Browse	• 74.201.28.50
	4FNTlzlu10.exe	Get hash	malicious	Browse	• 45.133.1.139
	7Q1bVVkIIL.exe	Get hash	malicious	Browse	• 45.133.1.139
	GMC772739922773829 93PDF.exe	Get hash	malicious	Browse	• 45.133.1.59
	ajESKclz8f.exe	Get hash	malicious	Browse	• 45.133.1.139
	7ua1kNyteq.exe	Get hash	malicious	Browse	• 45.144.225.66
	mHL0xKXQHT.exe	Get hash	malicious	Browse	• 74.201.28.35
	receiptpdf.exe	Get hash	malicious	Browse	• 74.201.28.35
	QGFG0322PDF.exe	Get hash	malicious	Browse	• 45.144.225.66
	h6uc8EaDQX.exe	Get hash	malicious	Browse	• 74.201.28.35
	9MyoOYNXKe.exe	Get hash	malicious	Browse	• 103.124.10 6.203
	iz8AtqlQeh.exe	Get hash	malicious	Browse	• 103.124.10 6.203
	dd7211d8c5d8b0e6290b9eb79787d64b73a91bde129cc.exe	Get hash	malicious	Browse	• 103.124.10 6.203
	862e41d1ddfa72722af62eb35aac11970ed21b6a7f01c.exe	Get hash	malicious	Browse	• 103.124.10 6.203
CLOUDFLARENETUS	Invoice,PDF.exe.exe	Get hash	malicious	Browse	• 172.67.188.154
	606d810b8ff92.pdf.dll	Get hash	malicious	Browse	• 104.20.185.68
	Lista e porosive te blerjes.exe	Get hash	malicious	Browse	• 162.159.13 4.233
	testfile_load.docm	Get hash	malicious	Browse	• 104.23.99.190
	testfile_load.docm	Get hash	malicious	Browse	• 104.23.99.190
	testfile_load.docm	Get hash	malicious	Browse	• 104.23.98.190
	syscshost.dll	Get hash	malicious	Browse	• 104.20.185.68
	invoice.exe	Get hash	malicious	Browse	• 172.67.160.234
	syscshost.dll	Get hash	malicious	Browse	• 104.20.184.68
	Payment Slip E05060_47.doc	Get hash	malicious	Browse	• 172.67.188.154
	New Orders.exe	Get hash	malicious	Browse	• 172.67.150.212
	Download Report.06.05.2021.exe	Get hash	malicious	Browse	• 104.21.56.119
	PROFORMA INVOICE.exe	Get hash	malicious	Browse	• 104.21.19.200
	payment.exe	Get hash	malicious	Browse	• 104.21.48.97
	BL836477488575.exe	Get hash	malicious	Browse	• 104.21.56.119
	RFQ_AP65425652_032421 v#U00e1#U00ba#U00a5n #U00c4#U2018#U00e1#U00bb ,pdf.exe	Get hash	malicious	Browse	• 172.65.227.72
	DHL_document11022020680908911.exe	Get hash	malicious	Browse	• 172.67.150.212
	DHL_document11022020680908911.doc.exe	Get hash	malicious	Browse	• 104.21.15.11
	Confirmation_(#1422) DEKRA order,pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	BL8846545545363.exe	Get hash	malicious	Browse	• 172.67.150.212

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54328bd36c14bd82ddaa0c04b25ed9ad	Invoice,PDF.exe.exe	Get hash	malicious	Browse	• 172.67.150.212
	testfile_load.docm	Get hash	malicious	Browse	• 172.67.150.212
	New Orders.exe	Get hash	malicious	Browse	• 172.67.150.212
	Download Report.06.05.2021.exe	Get hash	malicious	Browse	• 172.67.150.212
	PROFORMA INVOICE.exe	Get hash	malicious	Browse	• 172.67.150.212
	BL836477488575.exe	Get hash	malicious	Browse	• 172.67.150.212
	DHL_document11022020680908911.exe	Get hash	malicious	Browse	• 172.67.150.212
	Confirmation_(#1422) DEKRA order,pdf.exe	Get hash	malicious	Browse	• 172.67.150.212
	BL8846545545363.exe	Get hash	malicious	Browse	• 172.67.150.212
	ATTACHED.exe	Get hash	malicious	Browse	• 172.67.150.212
	Urgent RFQ_AP65425652_040621,pdf.exe	Get hash	malicious	Browse	• 172.67.150.212
	OVERVIEW .pdf.exe	Get hash	malicious	Browse	• 172.67.150.212
	PURCHASE ORDER - XIFFA55.PDF.exe	Get hash	malicious	Browse	• 172.67.150.212

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	doc20192910887888001990.exe	Get hash	malicious	Browse	• 172.67.150.212
	BL84995005038483.exe	Get hash	malicious	Browse	• 172.67.150.212
	ATTACHED.exe	Get hash	malicious	Browse	• 172.67.150.212
	ej 9999999.exe	Get hash	malicious	Browse	• 172.67.150.212
	DHL FINAL REMINDER PDF.exe	Get hash	malicious	Browse	• 172.67.150.212
	WSU0LJSL.exe	Get hash	malicious	Browse	• 172.67.150.212
	RFQ 100400806 SUPPLY.exe	Get hash	malicious	Browse	• 172.67.150.212

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_RFQ #46200058149_b4d3e1611dc98a70f1fcdf76f5b66818af29bc_427b5a83_156ea880\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	17670
Entropy (8bit):	3.7667567847033796
Encrypted:	false
SSDEEP:	192:EsusamHBUZMXiaKswHQ7V+N/u7sKS274ItEj:nusLBUZMXiafVq/u7sKX4ItEj
MD5:	5888DFCFA3A345C6C0ED4A4C0AE3669C
SHA1:	9AE3573BD8339DFCB3A0A4D80B83E1A4322B583B
SHA-256:	5AC91C9A6D9D61265AA99FB8ABDAA7E5A03519AE22E2281846A86B1DAEF0E972
SHA-512:	1F2FAB5B222A3042E060E51101468BDD0FAA0EB429A87D44A346AD901A15ECC10D6A64D19047D7A7658ECC4CBD15DF438ADBB2C26F94AE86968C6008D4FE91E0
Malicious:	false
Reputation:	low
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.=.1.3.2.6.2.2.9.9.3.3.7.9.6.1.2.1.4.7.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.6.2.2.9.9.3.4.6.9.6.1.2.0.9.1.....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.=.d.7.7.d.2.4.8.2.-.c.6.b.e.-.4.2.f.f.-.a.f.b.4.-.f.7.d.5.5.8.4.4.7.6.6.f.....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.=.d.d.6.6.5.7.b.4.-.9.3.f.7.-.4.a.3.d.-.9.0.4.0.-.c.4.8.d.6.9.8.a.e.2.2.a.....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.=.R.F.Q. .#.4.6.2.0.0.0.5.8.1.4.9...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.4.d.c.-.0.0.0.1.-.0.0.1.6.-.1.4.9.0.-.2.d.e.1.e.8.2.b.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.5.0.f.9.2.6.1.f.e.0.9.3.f.0.9.6.7.f.4.0.3.5.d.3.c.4.e.d.3.d.a.f.0.0.0.0.0.0.0.0.!.0.0.0.0.a.7.c.7.9.e.e.a.a.a.f.b.2.3.e.8.e.4.0.4.5.7.c.d.5.d.4.4.c.6.1.1.4.8.c.d.1.f.5.f.!.R.F.Q. .#.4.6.2.0.0.0.5.8.1.4.9...

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5FCE.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Wed Apr 7 20:02:21 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	340719
Entropy (8bit):	3.5620041721378817
Encrypted:	false
SSDEEP:	3072:6HZoYCbg0Sjd+pMQb2jJy3ykjL9gIOgF5iH770E2UCgURsv46cSvg:65B0/pMQCjJyL9RpDu77aTjC4PS4
MD5:	69DDCB125A35756BE7455B158AC8DAF4
SHA1:	6600B884D4998A872C19A9769B0BD0CDB0DC64CB
SHA-256:	477F80FAED13F4DEC72F161D5EC9137D9B9180711A4263F60F3829E0B40106D9
SHA-512:	EDB6FE968D7448ED4FB8E46679B9FA0454E8B7DB4502B5830A550FECBAB0E46C44E2359F04A8B5D756713E82F2C96031EEE5D58F53023C01D07058D7C975269
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....n`.....U.....B.....t2.....GenuineIntelW.....T.....n`.....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\WER7357.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):	8446

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	
Entropy (8bit):	3.699510585522676
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiEB68W6YI+SUzWgmfZjS8CprS389bpGIsf0jm:RrlsNi6616YxSUzWgmfdS2opG7ft
MD5:	BAF97A62AF5099FE2DB41A84129D1031
SHA1:	6006C7931A377B8CEFE399C665BD77BCEC0A76DB
SHA-256:	7BC029A886D38196F155DD4139935F106538DFF03AE26962923E58BC9C0CC269
SHA-512:	29E433A564A995800226574893BF52051246A32FDD2BDB65D44D090761ED2B83707A35C7B45671230B0947BB47E4D66C3C73B16334DAF296890F760D2B45F029
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.3.4.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER758B.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4731
Entropy (8bit):	4.482281240674152
Encrypted:	false
SSDEEP:	48:cvIwSD8zstJgtWI9k6WSC8BP8fm8M4JIedFFxd2+q8vCdt82t0tFd:uITfHL7SNGJlePd2KCb82t0tFd
MD5:	1E1EC12AA951A86B2FA813C6E3F36375
SHA1:	1C0AD65B2C7E1E0FE56CDFE10D1D1FA09E575407
SHA-256:	6A4987CE144499CF985F971C29CCB1E12F8C7BB2F4DE3FBE050A727145DF8227
SHA-512:	E062A1BED8B9CEA071C707D1EB055CF13DE1E9534CDF66A66A0FD955CCC37BEF516CA84E6DA2421260FD25338E4C9B32697493CFF9D081553136D97142DCA50
Malicious:	false
Reputation:	low
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="936313" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Users\user\Desktop\RFQ #46200058149.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
Reputation:	high, very likely benign file
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\RFQ #46200058149.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.1292511123011737
Encrypted:	false
SSDEEP:	6:kKPekO/kwTJ0N+SkQlPlEGYRMY9z+4KlDA3RUe0ht:nekO/kwTJrkPlE99SNxAhUe0ht

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
MD5:	566306A7B32BC696CCCB0443B513A4B5
SHA1:	769810CD8F1F25E0FAD2CF6221B42918FA6B1972
SHA-256:	06DFE7E16529D27A6405F5D9DBAC3B31AB779717365A0EFD53CA64C413191525
SHA-512:	34C0BED6B312B088C44E7DAF4CA80B0DBAF2162E4838536663F1DA5E944B21AB49D820F04CF26024D67CDFA8228BA7273CE592A4CA09A68455E6028CF1F4AE 1
Malicious:	false
Reputation:	low
Preview:	p..... .....+..(..... .....$.....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\??????????????????????????\RFQ_#46200058149.exe_Url_ctkhc4ktipcqngjefh42yihypvjrfm5z\3.371.288.95\a3kbdic0.newcfg	
Process:	C:\Users\user\Desktop\RFQ #46200058149.exe
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	modified
Size (bytes):	945388
Entropy (8bit):	3.114389457588161
Encrypted:	false
SSDEEP:	12288:67bFG6l5E7Vf8aHI8gbSzj4Dhnnp04aHLlw9FuU/y3gZWa1upW35rhlQTK38Fc1d:sPGp+Ho+g2ES
MD5:	1B71DDAEDCDCF1617179B1495973F5A7
SHA1:	AB9175FA1026C6A2464B34B7A920E5934280539E
SHA-256:	27839F3489FDCF1E603F4AF3997C1FE53C05F1E45E50119EBE14F090C53DD9A3
SHA-512:	C0C5B70CC395614F754C115F96ACF48DECA3773AE83EDC8A211D88BB8BD1D8D214F814777E643A43448AA071A92D3D72161D1938613CC43F44B2A756C86255F
Malicious:	false
Reputation:	low
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="....._x148A__x1484__x1475__x147F__x148A__x1487__x1483__x1469__x1462__x1455__x1454__x1453__x1456__x145F__x1461__x1469__x1484__x146B__x1453__x1462__x1488__x145D__x1456__x1487__x147A__x147C__x1457__x1460__x1480__x1462__x1466__x1479__x147C__x1453__x147A__x148B__x147B__x1467__x1481__x1475__x1474__x148B__x145A__x1489__x1459__x147D_" type="System.Configuration.ClientSettingsSection, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" allowExeDefinition="MachineToLocalUser" requirePermission="false" />.. </sectionGroup>.. </configSections>.. <userSettings>.. <.....

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\RFQ #46200058149.exe
File Type:	data
Category:	dropped
Size (bytes):	1856
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	48:Ik/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrw8:flC0IIC0IIC0IIC0IIC0IIC0IIC0IICr
MD5:	838CD9DBC78EA45A5406EAE23962086D
SHA1:	C8273AACDEE03AC0CDCDDBAA83F51D04D6A4203C
SHA-256:	6E11A62511C5BBC0413128305069B780C448684B54FAA3E8DD0B4FD3DB8C9867
SHA-512:	F7D25EF1FA6F50667DD6785CC774E0AA6BC52A2231FE96E7C59D14EFDFDDA076F6399288CF6EAC8EFA8A75727893432AA155DA0E392F8CD1F26C5C5871EAC6 B5
Malicious:	false
Reputation:	low
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0. :e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7.." .hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E..... {...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\RFQ #46200058149.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:EP:0
MD5:	AB92503DEE5748FC157D27383948CF90
SHA1:	0862273CB0A15EBF25A202CB5133CFD7AC3CA046
SHA-256:	BACCF15FA5F39978F57BB22FF66B9891401442DA29DD4E3B3E2C70E4B762F76C
SHA-512:	B58988E01FEF2E02B80268A13FC03086508BA297FD77B8BB592E7924812321B8982E0FF05D19C70B60A48B31A6DD11C7B7A935FD27F66610FBE690DBAF24E16C
Malicious:	**true**

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Reputation:	low
Preview:	3.s....H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\Desktop\RFQ #46200058149.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.221928094887364
Encrypted:	false
SSDEEP:	3:9bzY6oRDMjmPl:RzWDMCd
MD5:	AE0F5E6CE7122AF264EC533C6B15A27B
SHA1:	1265A495C42EED76CC043D50C60C23297E76CCE1
SHA-256:	73B0B92179C61C26589B47E9732CE418B07EDEE3860EE5A2A5FB06F3B8AA9B26
SHA-512:	DD44C2D24D4E3A0F0B988AD3D04683B5CB1282980431346498BE33B2512CE0C9B1A8E7D893B9F66FBBCDD901E2B0646C4533FB6C0C8C4AFCB95A0EFB95D44F8
Malicious:	false
Preview:	9iH...}Z.4..f..... 8.j....|.&X..e.F.*.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\Desktop\RFQ #46200058149.exe
File Type:	data
Category:	dropped
Size (bytes):	327432
Entropy (8bit):	**7.99938831605763**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3Pl6nGV4bfD6wXPIZ9iBj0UeprGm2d7Tm:LkjYGsfGUc9iB4UeprKdnm
MD5:	7E8F4A764B981D5B82D1CC49D341E9C6
SHA1:	D9F0685A028FB219E1A6286AEFB7D6FCFC778B85
SHA-256:	0BD3AAC12623520C4E2031C8B96B4A154702F36F97F643158E91E987D317B480
SHA-512:	880E46504FCFB4B15B86B9D8087BA88E6C4950E433616EBB637799F42B081ABF6F07508943ECB1F786B2A89E751F5AE62D750BDCFFDDF535D600CF66EC44E92
Malicious:	false
Preview:	pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i.....~...|..fX_...Xf.p^.....>a..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..HF7g...I.*3.{.n....L.y;i..s-....(5i.....J.5b7}..fK..HV..,...0.... ....n.w6PMl.....v.'".v.....#..X.a...../...cC...i..l{>5n.._+.e.d'..}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&.jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.QI..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.....Vg.2xC.....O...jc.....z..~.P...q../.-.'.h.._.cj.=..B.x.Q9.pu.\|i4...i...;O...n.?.,. ....v?.5}.OY@.dG\|<.._[.69@.2..m..I..oP=...xrK.?.....b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$...d...|m...N..1.R..B.i.....$....$.....CY}..$....r.....H...8...li.....7 P.....?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. l..&<}....`|.B....3.....I..o...u1..8i=.z.W..7

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.914857977057756
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:	RFQ #46200058149.exe
File size:	55488
MD5:	67b96dc502b0c7a496092d7e6d1da6c5
SHA1:	a7c79eeaaafb23e8e40457cd5d44c61148cd1f5f
SHA256:	ef5cb0bfe2d23b7a13b685f43dc9a100dac402023e11dce7991173bde63b298e
SHA512:	56ea1e779902e8a51de0d20f5d4ea3a4d4e5a441e16666 8fadfbc25bd14715b388296f7d9d44b01499001d71612a7 3e858c0d0ad8d1fd473e3843169e8f60aab
SSDEEP:	768:b/LA9K0Ubu5O9ooy+bwEbcpo31EKGSBAmoSOh:bzIKS5uAmoS

General

File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...$ ....."...0.....>.... ....@.. ....I7.. ..@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x40d53e
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:	0xB5100D24 [Mon Apr 5 21:20:36 2066 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=cJGypErFTYiIKZrVRPaZESbD, S=YzrefMybHjDaqHbkToqPfxOqnUOifyYQU, L=GrmKqYXcIpqu, T=lhjOxKoqQZNoFhwaegDYkMfihogoajYDuqQHU, E=TjleyVAYSBdZejEgZMvkyncOeuPXZHOXQXVxRYDxHdW, OU=NljTHpvqDvYN, O=vXrtPKPHdcshcP, CN=DgYLGpwPLUvEHXHFAFtskroWZlsMsMtPTwOYljdPOsBdPanwm
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	• 4/7/2021 3:24:46 AM 4/7/2022 3:24:46 AM
Subject Chain	• C=cJGypErFTYiIKZrVRPaZESbD, S=YzrefMybHjDaqHbkToqPfxOqnUOifyYQU, L=GrmKqYXcIpqu, T=lhjOxKoqQZNoFhwaegDYkMfihogoajYDuqQHU, E=TjleyVAYSBdZejEgZMvkyncOeuPXZHOXQXVxRYDxHdW, OU=NljTHpvqDvYN, O=vXrtPKPHdcshcP, CN=DgYLGpwPLUvEHXHFAFtskroWZlsMsMtPTwOYljdPOsBdPanwm
Version:	3
Thumbprint MD5:	FB6C7A2D94E91E9FF30697013C5B69D5
Thumbprint SHA-1:	FE02D73BF104783555975688A868009D5570EB73
Thumbprint SHA-256:	BF63495CB82B667811FF374D33F61D640122D1FF75F5B9C359536F194FF72F44
Serial:	00F3D510D4C10F5E02E90D4C9AB74AC201

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xd4f0	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xe000	0x81c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0xc400	0x14c0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x10000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xb544	0xb600	False	0.184495192308	data	5.49483421273	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xe000	0x81c	0xa00	False	0.30546875	data	5.05547520825	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x10000	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	0xe0a0	0x590	data	English	United States
RT_MANIFEST	0xe630	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
LegalCopyright	All Rights Reserved
Assembly Version	1.628.632.750
InternalName	.exe
FileVersion	1.628.632.750
CompanyName	Inc.
LegalTrademarks	
Comments	
ProductName	
ProductVersion	1.628.632.750
FileDescription	
OriginalFilename	.exe
Translation	0x0000 0x0514

Possible Origin

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

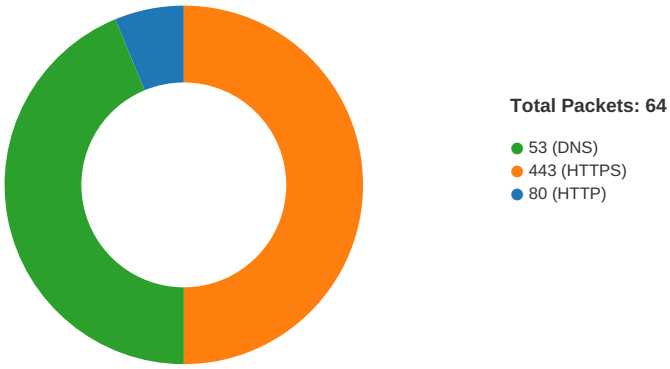
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/07/21-13:02:17.171046	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49700	5353	192.168.2.5	45.15.143.169
04/07/21-13:02:23.616130	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49701	5353	192.168.2.5	45.15.143.169
04/07/21-13:02:29.609043	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49708	5353	192.168.2.5	45.15.143.169
04/07/21-13:02:35.662373	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49711	5353	192.168.2.5	45.15.143.169
04/07/21-13:02:43.025136	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49717	5353	192.168.2.5	45.15.143.169
04/07/21-13:02:48.990683	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49721	5353	192.168.2.5	45.15.143.169
04/07/21-13:02:55.031007	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49724	5353	192.168.2.5	45.15.143.169
04/07/21-13:03:01.040878	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49725	5353	192.168.2.5	45.15.143.169
04/07/21-13:03:06.089379	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49727	5353	192.168.2.5	45.15.143.169
04/07/21-13:03:12.226347	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49728	5353	192.168.2.5	45.15.143.169
04/07/21-13:03:18.456156	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49731	5353	192.168.2.5	45.15.143.169
04/07/21-13:03:25.504170	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49737	5353	192.168.2.5	45.15.143.169
04/07/21-13:03:32.502954	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49738	5353	192.168.2.5	45.15.143.169
04/07/21-13:03:38.477187	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49739	5353	192.168.2.5	45.15.143.169
04/07/21-13:03:44.674403	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49740	5353	192.168.2.5	45.15.143.169
04/07/21-13:03:51.574841	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49741	5353	192.168.2.5	45.15.143.169
04/07/21-13:03:57.560887	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49744	5353	192.168.2.5	45.15.143.169

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/07/21-13:04:03.546218	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49745	5353	192.168.2.5	45.15.143.169
04/07/21-13:04:08.527094	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49746	5353	192.168.2.5	45.15.143.169

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 13:02:06.561278105 CEST	49698	80	192.168.2.5	172.67.150.212
Apr 7, 2021 13:02:06.589848042 CEST	80	49698	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:06.590656042 CEST	49698	80	192.168.2.5	172.67.150.212
Apr 7, 2021 13:02:06.590687990 CEST	49698	80	192.168.2.5	172.67.150.212
Apr 7, 2021 13:02:06.620342016 CEST	80	49698	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:06.633188009 CEST	80	49698	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:06.661340952 CEST	49699	443	192.168.2.5	172.67.150.212
Apr 7, 2021 13:02:06.677747965 CEST	49698	80	192.168.2.5	172.67.150.212
Apr 7, 2021 13:02:06.690354109 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:06.691577911 CEST	49699	443	192.168.2.5	172.67.150.212
Apr 7, 2021 13:02:06.700535059 CEST	49699	443	192.168.2.5	172.67.150.212
Apr 7, 2021 13:02:06.729173899 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:06.740087986 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:06.740125895 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:06.740264893 CEST	49699	443	192.168.2.5	172.67.150.212
Apr 7, 2021 13:02:06.748444080 CEST	49699	443	192.168.2.5	172.67.150.212
Apr 7, 2021 13:02:06.777738094 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:06.778348923 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:06.822460890 CEST	49699	443	192.168.2.5	172.67.150.212
Apr 7, 2021 13:02:06.852838993 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.042640924 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.042685986 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.042733908 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.042764902 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.042777061 CEST	49699	443	192.168.2.5	172.67.150.212
Apr 7, 2021 13:02:07.042802095 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.042823076 CEST	49699	443	192.168.2.5	172.67.150.212
Apr 7, 2021 13:02:07.042829037 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.042866945 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.042891979 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.042902946 CEST	49699	443	192.168.2.5	172.67.150.212
Apr 7, 2021 13:02:07.042927980 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.042954922 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.042977095 CEST	49699	443	192.168.2.5	172.67.150.212
Apr 7, 2021 13:02:07.043055058 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.043085098 CEST	443	49699	172.67.150.212	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 13:02:07.043118954 CEST	49699	443	192.168.2.5	172.67.150.212
Apr 7, 2021 13:02:07.043158054 CEST	49699	443	192.168.2.5	172.67.150.212
Apr 7, 2021 13:02:07.289462090 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.289509058 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.289546967 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.289594889 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.289645910 CEST	49699	443	192.168.2.5	172.67.150.212
Apr 7, 2021 13:02:07.289710999 CEST	49699	443	192.168.2.5	172.67.150.212
Apr 7, 2021 13:02:07.289978981 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.290029049 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.290122032 CEST	49699	443	192.168.2.5	172.67.150.212
Apr 7, 2021 13:02:07.290605068 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.290741920 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.290843010 CEST	49699	443	192.168.2.5	172.67.150.212
Apr 7, 2021 13:02:07.291336060 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.291750908 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.291874886 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.291970015 CEST	49699	443	192.168.2.5	172.67.150.212
Apr 7, 2021 13:02:07.292062998 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.292784929 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.292829037 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.292937994 CEST	49699	443	192.168.2.5	172.67.150.212
Apr 7, 2021 13:02:07.292973995 CEST	49699	443	192.168.2.5	172.67.150.212
Apr 7, 2021 13:02:07.293483019 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.293526888 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.293617010 CEST	49699	443	192.168.2.5	172.67.150.212
Apr 7, 2021 13:02:07.294059992 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.294224977 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.294698954 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.294738054 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.294794083 CEST	49699	443	192.168.2.5	172.67.150.212
Apr 7, 2021 13:02:07.294872046 CEST	49699	443	192.168.2.5	172.67.150.212
Apr 7, 2021 13:02:07.295423985 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.295464039 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.295536041 CEST	49699	443	192.168.2.5	172.67.150.212
Apr 7, 2021 13:02:07.296227932 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.296269894 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.296910048 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.296947956 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.296983004 CEST	49699	443	192.168.2.5	172.67.150.212
Apr 7, 2021 13:02:07.297379971 CEST	49699	443	192.168.2.5	172.67.150.212
Apr 7, 2021 13:02:07.297568083 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.297609091 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.298372984 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.298384905 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.298559904 CEST	49699	443	192.168.2.5	172.67.150.212
Apr 7, 2021 13:02:07.299046040 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.299089909 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.299161911 CEST	49699	443	192.168.2.5	172.67.150.212
Apr 7, 2021 13:02:07.300101042 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.300188065 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.300283909 CEST	49699	443	192.168.2.5	172.67.150.212
Apr 7, 2021 13:02:07.300322056 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.300405025 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.301075935 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.301115036 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.301153898 CEST	49699	443	192.168.2.5	172.67.150.212
Apr 7, 2021 13:02:07.301175117 CEST	49699	443	192.168.2.5	172.67.150.212
Apr 7, 2021 13:02:07.318403959 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.318449974 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.318486929 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.318526983 CEST	443	49699	172.67.150.212	192.168.2.5
Apr 7, 2021 13:02:07.318571091 CEST	49699	443	192.168.2.5	172.67.150.212
Apr 7, 2021 13:02:07.318598986 CEST	49699	443	192.168.2.5	172.67.150.212

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 13:01:57.666064024 CEST	54302	53	192.168.2.5	8.8.8.8
Apr 7, 2021 13:01:57.699048042 CEST	53	54302	8.8.8.8	192.168.2.5
Apr 7, 2021 13:01:57.835232973 CEST	53784	53	192.168.2.5	8.8.8.8
Apr 7, 2021 13:01:57.848604918 CEST	53	53784	8.8.8.8	192.168.2.5
Apr 7, 2021 13:01:57.870088100 CEST	65307	53	192.168.2.5	8.8.8.8
Apr 7, 2021 13:01:57.884546041 CEST	53	65307	8.8.8.8	192.168.2.5
Apr 7, 2021 13:01:58.216387033 CEST	64344	53	192.168.2.5	8.8.8.8
Apr 7, 2021 13:01:58.242887020 CEST	53	64344	8.8.8.8	192.168.2.5
Apr 7, 2021 13:01:59.915389061 CEST	62060	53	192.168.2.5	8.8.8.8
Apr 7, 2021 13:01:59.940996885 CEST	53	62060	8.8.8.8	192.168.2.5
Apr 7, 2021 13:02:05.765697002 CEST	61805	53	192.168.2.5	8.8.8.8
Apr 7, 2021 13:02:05.786441088 CEST	53	61805	8.8.8.8	192.168.2.5
Apr 7, 2021 13:02:06.521837950 CEST	54795	53	192.168.2.5	8.8.8.8
Apr 7, 2021 13:02:06.542304039 CEST	53	54795	8.8.8.8	192.168.2.5
Apr 7, 2021 13:02:06.642534018 CEST	49557	53	192.168.2.5	8.8.8.8
Apr 7, 2021 13:02:06.657759905 CEST	53	49557	8.8.8.8	192.168.2.5
Apr 7, 2021 13:02:26.104932070 CEST	61733	53	192.168.2.5	8.8.8.8
Apr 7, 2021 13:02:26.152183056 CEST	53	61733	8.8.8.8	192.168.2.5
Apr 7, 2021 13:02:28.068749905 CEST	65447	53	192.168.2.5	8.8.8.8
Apr 7, 2021 13:02:28.084856033 CEST	53	65447	8.8.8.8	192.168.2.5
Apr 7, 2021 13:02:28.419487953 CEST	52441	53	192.168.2.5	8.8.8.8
Apr 7, 2021 13:02:28.432147980 CEST	53	52441	8.8.8.8	192.168.2.5
Apr 7, 2021 13:02:29.162633896 CEST	62176	53	192.168.2.5	8.8.8.8
Apr 7, 2021 13:02:29.175187111 CEST	53	62176	8.8.8.8	192.168.2.5
Apr 7, 2021 13:02:30.679785013 CEST	59596	53	192.168.2.5	8.8.8.8
Apr 7, 2021 13:02:30.694525003 CEST	53	59596	8.8.8.8	192.168.2.5
Apr 7, 2021 13:02:33.519079924 CEST	65296	53	192.168.2.5	8.8.8.8
Apr 7, 2021 13:02:33.531760931 CEST	53	65296	8.8.8.8	192.168.2.5
Apr 7, 2021 13:02:35.690540075 CEST	63183	53	192.168.2.5	8.8.8.8
Apr 7, 2021 13:02:35.703210115 CEST	53	63183	8.8.8.8	192.168.2.5
Apr 7, 2021 13:02:39.809226036 CEST	60151	53	192.168.2.5	8.8.8.8
Apr 7, 2021 13:02:39.821969032 CEST	53	60151	8.8.8.8	192.168.2.5
Apr 7, 2021 13:02:40.813354015 CEST	56969	53	192.168.2.5	8.8.8.8
Apr 7, 2021 13:02:40.828380108 CEST	53	56969	8.8.8.8	192.168.2.5
Apr 7, 2021 13:02:41.733205080 CEST	55161	53	192.168.2.5	8.8.8.8
Apr 7, 2021 13:02:41.749515057 CEST	53	55161	8.8.8.8	192.168.2.5
Apr 7, 2021 13:02:43.816843033 CEST	54757	53	192.168.2.5	8.8.8.8
Apr 7, 2021 13:02:43.830353975 CEST	53	54757	8.8.8.8	192.168.2.5
Apr 7, 2021 13:02:44.786832094 CEST	49992	53	192.168.2.5	8.8.8.8
Apr 7, 2021 13:02:44.800668955 CEST	53	49992	8.8.8.8	192.168.2.5
Apr 7, 2021 13:02:46.068089962 CEST	60075	53	192.168.2.5	8.8.8.8
Apr 7, 2021 13:02:46.080852032 CEST	53	60075	8.8.8.8	192.168.2.5
Apr 7, 2021 13:02:51.182168007 CEST	55016	53	192.168.2.5	8.8.8.8
Apr 7, 2021 13:02:51.195074081 CEST	53	55016	8.8.8.8	192.168.2.5
Apr 7, 2021 13:02:52.309345961 CEST	64345	53	192.168.2.5	8.8.8.8
Apr 7, 2021 13:02:52.327894926 CEST	53	64345	8.8.8.8	192.168.2.5
Apr 7, 2021 13:03:05.314524889 CEST	57128	53	192.168.2.5	8.8.8.8
Apr 7, 2021 13:03:05.340697050 CEST	53	57128	8.8.8.8	192.168.2.5
Apr 7, 2021 13:03:18.004636049 CEST	54791	53	192.168.2.5	8.8.8.8
Apr 7, 2021 13:03:18.020281076 CEST	53	54791	8.8.8.8	192.168.2.5
Apr 7, 2021 13:03:21.618623972 CEST	50463	53	192.168.2.5	8.8.8.8
Apr 7, 2021 13:03:21.638210058 CEST	53	50463	8.8.8.8	192.168.2.5
Apr 7, 2021 13:03:52.518874884 CEST	50394	53	192.168.2.5	8.8.8.8
Apr 7, 2021 13:03:52.534435987 CEST	53	50394	8.8.8.8	192.168.2.5
Apr 7, 2021 13:03:54.824187994 CEST	58530	53	192.168.2.5	8.8.8.8
Apr 7, 2021 13:03:54.850320101 CEST	53	58530	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 7, 2021 13:02:06.521837950 CEST	192.168.2.5	8.8.8.8	0xa57f	Standard query (0)	myliverpoolnews.cf	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 7, 2021 13:02:06.642534018 CEST	192.168.2.5	8.8.8.8	0xc83b	Standard query (0)	myliverpoolnews.cf	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 7, 2021 13:02:06.542304039 CEST	8.8.8.8	192.168.2.5	0xa57f	No error (0)	myliverpoolnews.cf		172.67.150.212	A (IP address)	IN (0x0001)
Apr 7, 2021 13:02:06.542304039 CEST	8.8.8.8	192.168.2.5	0xa57f	No error (0)	myliverpoolnews.cf		104.21.56.119	A (IP address)	IN (0x0001)
Apr 7, 2021 13:02:06.657759905 CEST	8.8.8.8	192.168.2.5	0xc83b	No error (0)	myliverpoolnews.cf		172.67.150.212	A (IP address)	IN (0x0001)
Apr 7, 2021 13:02:06.657759905 CEST	8.8.8.8	192.168.2.5	0xc83b	No error (0)	myliverpoolnews.cf		104.21.56.119	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- myliverpoolnews.cf

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49698	172.67.150.212	80	C:\Users\user\Desktop\RFQ #46200058149.exe

Timestamp	kBytes transferred	Direction	Data
Apr 7, 2021 13:02:06.590687990 CEST	1340	OUT	GET /liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-FE6EFB3AED9F05224C930BEF8BE1CC20.html HTTP/1.1 UserAgent: 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: myliverpoolnews.cf Connection: Keep-Alive
Apr 7, 2021 13:02:06.633188009 CEST	1341	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 07 Apr 2021 11:02:06 GMT Transfer-Encoding: chunked Connection: keep-alive Cache-Control: max-age=3600 Expires: Wed, 07 Apr 2021 12:02:06 GMT Location: https://myliverpoolnews.cf/liverpool-fc-news/features/steven-gerrard-liverpool-future-dalglish--goal-FE6EFB3AED9F05224C930BEF8BE1CC20.html cf-request-id: 094d9836110000b7c914187000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=m9eQ%2Bca61StvdHz7yPlbWFTXI1pBp7YQkrNE7je%2FSSf0koz4kSPtrJdseqt2bsqSTUwhZmkNnO%2BGEff%2B6O21ufwbrUCHlDUCH5a17fhuqKxyOlQ%3D"}],"group":"cf-nel","max_age":604800} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 63c2c3034ea8b7c9-CDG alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

HTTPS Packets

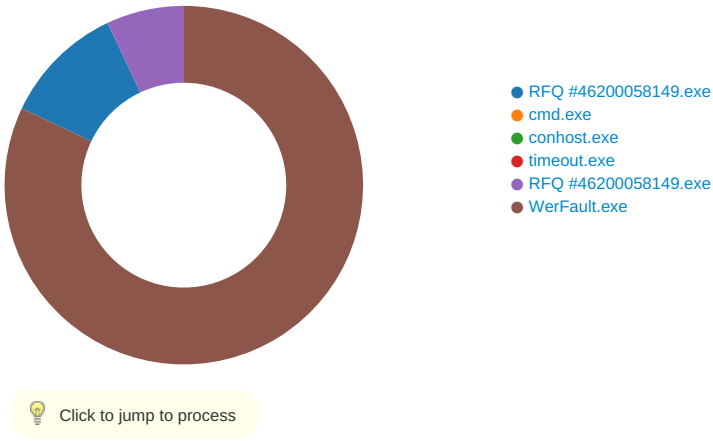
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 7, 2021 13:02:06.740125895 CEST	172.67.150.212	443	192.168.2.5	49699	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Mar 31 02:00:00 CEST 2021 Mon Jan 27 13:48:08 CET 2020	Thu Mar 31 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2025	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: RFQ #46200058149.exe PID: 5340 Parent PID: 5632

General

Start time:	13:02:04
Start date:	07/04/2021
Path:	C:\Users\user\Desktop\RFQ #46200058149.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\RFQ #46200058149.exe'
Imagebase:	0xea0000
File size:	55488 bytes
MD5 hash:	67B96DC502B0C7A496092D7E6D1DA6C5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.301376960.000000000505E000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.301376960.000000000505E000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.301376960.000000000505E000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000003.240375757.000000000507F000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000003.240375757.000000000507F000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.240375757.000000000507F000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.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	6D92CF06	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	6D92CF06	unknown
C:\Users\user\AppData\Local\????????????????????????????	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C77BEFF	CreateDirectoryW
C:\Users\user\AppData\Local\????????????????????????????\RFQ_#46200058149.exe_Url_ctkhc4ktipcqngjefh42yihypvjrfm5z	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C77BEFF	CreateDirectoryW
C:\Users\user\AppData\Local\????????????????????????????\RFQ_#46200058149.exe_Url_ctkhc4ktipcqngjefh42yihypvjrfm5z\3.371.288.95	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C77BEFF	CreateDirectoryW
C:\Users\user\AppData\Local\????????????????????????????\RFQ_#46200058149.exe_Url_ctkhc4ktipcqngjefh42yihypvjrfm5z\3.371.288.95\a3kbdic0.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C771E60	CreateFileW
C:\Users\user\AppData\Local\????????????????????????????\RFQ_#46200058149.exe_Url_ctkhc4ktipcqngjefh42yihypvjrfm5z\3.371.288.95\a3kbdic0.newcfg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C771E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\????????????????????????????\RFQ_#46200058149.exe_Url_ctkhc4ktipcqngjefh42yihypvjrfm5z\3.371.288.95\a3kbdic0.tmp	success or wait	1	6C776A95	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\????????????????????????????\RFQ_#46200058149.exe_Url_ctkhc4ktipcqngjefh42yihypvjrfm5z\3.371.288.95\a3kbdic0.newcfg	C:\Users\user\AppData\Local\LORz[JQM]oup|Q~\`xh.^.xtU\RFQ_#46200058149.exe_Url_ctkhc4ktipcqngjefh42yihypvjrfm5z\3.371.288.95\user.config	success or wait	1	6B032684	MoveFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\??????????????????????????\RFQ_#46200058149.exe_Url_ctkhc4ktipc qngjefh42yihypvjrfm5z\3.371.288.95\a3kbdic0.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	6C771B4F	WriteFile
C:\Users\user\AppData\Local\??????????????????????????\RFQ_#46200058149.exe_Url_ctkhc4ktipc qngjefh42yihypvjrfm5z\3.371.288.95\a3kbdic0.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	6C771B4F	WriteFile
C:\Users\user\AppData\Local\??????????????????????????\RFQ_#46200058149.exe_Url_ctkhc4ktipc qngjefh42yihypvjrfm5z\3.371.288.95\a3kbdic0.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	6C771B4F	WriteFile
C:\Users\user\AppData\Local\??????????????????????????\RFQ_#46200058149.exe_Url_ctkhc4ktipc qngjefh42yihypvjrfm5z\3.371.288.95\a3kbdic0.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	6C771B4F	WriteFile
C:\Users\user\AppData\Local\??????????????????????????\RFQ_#46200058149.exe_Url_ctkhc4ktipc qngjefh42yihypvjrfm5z\3.371.288.95\a3kbdic0.newcfg	unknown	622	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 eb bb eb bb af eb bc 95 eb bb bc eb bc 8a eb bc 9a eb bc 87 eb bc 9d eb bc 9f eb bc 8d eb bb b8 eb bc 9e eb bb a7 eb bb a9 eb bc 99 eb bb b3 eb bc 8d eb bb a8 eb bc 94 eb bc 9b eb bb ab eb bb ba eb bc 90 eb bb bb eb bb aa 2e 5f 78 31 34 38 41 5f 5f 78 31 34 38 34 5f 5f 78 31 34 37 35 5f 5f 78 31 34 37 46 5f 5f 78 31 34 38 41 5f 5f 78 31 34 38 37 5f 5f 78 31 34 38 33 5f 5f 78 31 34 36 39 5f 5f 78 31 34 36 32 5f 5f 78 31 34 35 35 5f 5f 78 31 34 35 34 5f 5f 78 31 34 35 33 5f 5f 78 31 34 35 36 5f 5f 78 31 34 35 46 5f 5f 78 31 34 36 31 5f 5f 78 31 34 36 39 5f 5f 78 31 34 38 34 5f 5f 78 31 34 36 42 5f 5f 78 31 34 35 33 5f 5f 78 31 34 36 32 5f 5f 78 31 34 38 38 5f 5f 78 31 34 35	<section name="... ...._x148A__x1484__x1 475__x147F__x148A__x1487__x1483__x1469__x1462__x1455__x1454_ _x1453__x1456__x145F__x1461__x1469__x1484__x146B__x1453__x1462__x1488__x145	success or wait	1	6C771B4F	WriteFile
C:\Users\user\AppData\Local\??????????????????????????\RFQ_#46200058149.exe_Url_ctkhc4ktipc qngjefh42yihypvjrfm5z\3.371.288.95\a3kbdic0.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	6C771B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\?????????????????????????? \RFQ_#46200058149.exe_Url_ctkhc4ktipc qngjefh42yihypvjrfm5z\3.371.288.95\a3kbdic0.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	6C771B4F	WriteFile
C:\Users\user\AppData\Local\?????????????????????????? \RFQ_#46200058149.exe_Url_ctkhc4ktipc qngjefh42yihypvjrfm5z\3.371.288.95\a3kbdic0.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	6C771B4F	WriteFile
C:\Users\user\AppData\Local\?????????????????????????? \RFQ_#46200058149.exe_Url_ctkhc4ktipc qngjefh42yihypvjrfm5z\3.371.288.95\a3kbdic0.newcfg	unknown	410	20 20 20 20 20 20 20 20 3c eb bb bb eb bb af eb bc 95 eb bb bc eb bc 8a eb bc 9a eb bc 87 eb bc 9d eb bc 9f eb bc 8d eb bb b8 eb bc 9e eb bb a7 eb bb a9 eb bc 99 eb bb b3 eb bc 8d eb bb a8 eb bc 94 eb bc 9b eb bb ab eb bb ba eb bc 90 eb bb bb eb bb aa 2e 5f 78 31 34 38 41 5f 5f 78 31 34 38 34 5f 5f 78 31 34 37 35 5f 5f 78 31 34 37 46 5f 5f 78 31 34 38 41 5f 5f 78 31 34 38 37 5f 5f 78 31 34 38 33 5f 5f 78 31 34 36 39 5f 5f 78 31 34 36 32 5f 5f 78 31 34 35 35 5f 5f 78 31 34 35 34 5f 5f 78 31 34 35 33 5f 5f 78 31 34 35 36 5f 5f 78 31 34 35 46 5f 5f 78 31 34 36 31 5f 5f 78 31 34 36 39 5f 5f 78 31 34 38 34 5f 5f 78 31 34 36 42 5f 5f 78 31 34 35 33 5f 5f 78 31 34 36 32 5f 5f 78 31 34 38 38 5f 5f 78 31 34 35 44 5f 5f 78 31 34 35 36 5f 5f 78 31 34 38 37 5f 5f 78	<..................... ...._x148 A__x1484__x1475__x147 F__x148A_ _x1487__x1483__x1469__ x1462__x 1455__x1454__x1453__x1 456__x14 5F__x1461__x1469__x148 4__x146B __x1453__x1462__x1488_ _x145D__ x1456__x1487__x	success or wait	5	6C771B4F	WriteFile
C:\Users\user\AppData\Local\?????????????????????????? \RFQ_#46200058149.exe_Url_ctkhc4ktipc qngjefh42yihypvjrfm5z\3.371.288.95\a3kbdic0.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 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 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	230	6C771B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\??????????????????????????\RFQ_#46200058149.exe_Url_ctkhc4ktipc qngjefh42yihypvjrfm5z\3.371.288.95\a3kbdic0.newcfg	unknown	411	20 20 20 20 20 20 20 3c 2f eb bb bb eb bb af eb bc 95 eb bb bc eb bc 8a eb bc 9a eb bc 87 eb bc 9d eb bc 9f eb bc 8d eb bb b8 eb bc 9e eb bb a7 eb bb a9 eb bc 99 eb bb b3 eb bc 8d eb bb a8 eb bc 94 eb bc 9b eb bb ab eb bb ba eb bc 90 eb bb bb eb bb aa 2e 5f 78 31 34 38 41 5f 5f 78 31 34 38 34 5f 5f 78 31 34 37 35 5f 5f 78 31 34 37 46 5f 5f 78 31 34 38 41 5f 5f 78 31 34 38 37 5f 5f 78 31 34 38 33 5f 5f 78 31 34 36 39 5f 5f 78 31 34 36 32 5f 5f 78 31 34 35 35 5f 5f 78 31 34 35 34 5f 5f 78 31 34 35 33 5f 5f 78 31 34 35 36 5f 5f 78 31 34 35 46 5f 5f 78 31 34 36 31 5f 5f 78 31 34 36 39 5f 5f 78 31 34 38 34 5f 5f 78 31 34 36 42 5f 5f 78 31 34 35 33 5f 5f 78 31 34 36 32 5f 5f 78 31 34 38 38 5f 5f 78 31 34 35 44 5f 5f 78 31 34 35 36 5f 5f 78 31 34 38 37 5f 5f 5f	</..... ...._x14 8A__x1484__x1475__x147 F__x148A __x1487__x1483__x1469_ _x1462__ x1455__x1454__x1453__x 1456__x1 45F__x1461__x1469__x14 84__x146 B__x1453__x1462__x1488 __x145D_ _x1456__x1487__	success or wait	1	6C771B4F	WriteFile
C:\Users\user\AppData\Local\??????????????????????????\RFQ_#46200058149.exe_Url_ctkhc4ktipc qngjefh42yihypvjrfm5z\3.371.288.95\a3kbdic0.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	6C771B4F	WriteFile
C:\Users\user\AppData\Local\??????????????????????????\RFQ_#46200058149.exe_Url_ctkhc4ktipc qngjefh42yihypvjrfm5z\3.371.288.95\a3kbdic0.newcfg	unknown	16	3c 2f 63 6f 6e 66 69 67 75 72 61 74 69 6f 6e 3e	</configuration>	success or wait	1	6C771B4F	WriteFile

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	6D905705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D905705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D8603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D90CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D8603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D8603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D8603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D8603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D905705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D905705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C771B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C771B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C771B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C771B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C771B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C771B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6D8ED72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6D8ED72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11d50a3a\Microsoft.VisualBasic.dll	unknown	4096	success or wait	1	6D8ED72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11d50a3a\Microsoft.VisualBasic.dll	unknown	512	success or wait	1	6D8ED72F	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\RFQ #46200058149.exe	unknown	4096	success or wait	1	6D8ED72F	unknown
C:\Users\user\Desktop\RFQ #46200058149.exe	unknown	512	success or wait	1	6D8ED72F	unknown

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 5912 Parent PID: 5340

General

Start time:	13:02:10
Start date:	07/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c timeout 1
Imagebase:	0x150000
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: 5964 Parent PID: 5912

General

Start time:	13:02:10
Start date:	07/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: 5504 Parent PID: 5912

General

Start time:	13:02:11
Start date:	07/04/2021
Path:	C:\Windows\SysWOW64\timeout.exe

Wow64 process (32bit):	true
Commandline:	timeout 1
Imagebase:	0x160000
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: RFQ #46200058149.exe PID: 5972 Parent PID: 5340

General

Start time:	13:02:12
Start date:	07/04/2021
Path:	C:\Users\user\Desktop\RFQ #46200058149.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\RFQ #46200058149.exe
Imagebase:	0x640000
File size:	55488 bytes
MD5 hash:	67B96DC502B0C7A496092D7E6D1DA6C5
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	6D92CF06	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	6D92CF06	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C77BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C771E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C77BEFF	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C77BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	17	6C771E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C771E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C771E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\RFQ #46200058149.exe:Zone.Identifier	success or wait	1	6C6F2935	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	unknown	8	33 e7 73 0a 00 fa d8 48	3.s....H	success or wait	1	6C771B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	232	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 c6 e5 50 83 63 4c 54 a1 9f c5 82 41 c5 62 c9 e2 1b 95 b8 f0 f0 e7 34 68 a6 12 b5 74 bc 2b f0 07 5a 5c b0 bf 20 9f 69 cc d5 c2 a4 ed f2 80 40 dc 33 8c a4 7b 0c cc 1c 67 72 76 2b 56 81 e7 f3 bf b9 42 19 0e 82 0d c5 eb 15 5d f3 50 8b f6 16 57 df 34 43 7d 75 4c 1e b2 93 0b a6 73 7e 82 c7 46 04 b7 fb 7d 99 ad 83 81 ed 81 00 45 f9 c7 db f0 db f0 45 f9 14 f3 b4 36 45 8f 94 b5 81 a3 7b d9 9f 05 18 7b ed a9 79 53 82 bd bf 37 fa c4 22 16 68 4b d7 21 03 78 86 32 be 99 69 df a3 8f 7a 4a d5 da bb fa 20 fc b4 c0 c0 66 d0 dd a7 3f c0 5f 0b e4 fb a3 30 ca 3a 65 5b 37 77 7b 31 81 21 de 34 a9 bb 99 d3 ca 26 b9	Gj.h\.3..A...5.x..&...i+...c(1 .P..P.cLT....A.b.....4h...t .+..Z\.. .i.....@.3..{...grv +V.....B.....].P...W.4C}uL.. ...s~..F...}.....E.....E... .6E.....{....{..yS...7..".hK.! .x.2..i...zJ.... ....f...?._.. ..0.:e[7w{1.!.4.....&.	success or wait	8	6C771B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	unknown	327432	70 54 c7 ab ad 21 b0 08 57 f6 fa 47 14 4a ba aa 61 dd a0 29 17 40 c6 8b 69 8b df 77 70 4b 98 73 6f 40 e2 06 e5 35 e7 b7 3d e9 b8 90 5e ab 1d 51 82 6f 79 f9 3d 65 40 39 c3 42 8d f7 95 46 bc cb 30 39 75 22 33 8b f5 20 30 74 c0 19 52 44 6e 5f 34 64 fb b8 17 02 df 45 c0 90 06 69 f4 08 9f ae bb 8a 7e 0c 89 85 7c 87 eb 66 58 5f 0e c2 ed 58 66 88 70 5e e2 f5 ff 94 03 e5 3e 61 db 8b 91 24 8d 8a 8f 65 05 36 3a 37 64 b6 28 61 05 41 e4 fe e0 3d be 29 2a 0d 96 a8 90 8e 7b 42 1c 5b ab 87 cb 79 25 b3 2a e4 b8 b1 9f 69 a7 51 84 3c f3 94 a2 90 78 74 c4 a9 58 13 11 48 09 d7 20 ad cc a4 48 46 37 67 0f e0 c5 49 96 2a 33 03 7b 0c 6e 92 bf 90 be 4c d1 9b 79 3b 69 87 bc 73 2d 1e b6 f9 b8 28 35 69 c2 8b 92 d6 10 ac a7 02 93 ee 89 08 17 4a 09 35 62 37 7d fe 86 66 4b af ab 48 56	pT...!..W..G.J..a..).@..i..wpK .so@...5..=...^..Q.oy.=e@9 .B...F..09u"3.. 0t..RDn_4d.....E.. .i.....~...|..fX_....Xf.p^.... ..>a...$...e.6:7d.(a.A...=.)*. ....{B.[...y%.*....i.Q.<....xt ..X..H.. ...HF7g...I.*3.{.n... .L..y;i..s-....(5i..... .J.5b7}..fK..HV	success or wait	1	6C771B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	unknown	40	39 69 48 cc 1a df 85 7d 5a d7 8d 34 00 a8 66 0d 85 16 f4 a5 20 38 a2 6a 80 a4 a3 f3 7c 88 26 58 b6 ca 65 a6 46 b8 2a 80	9iH....}Z..4..f..... 8.j....|. &X..e.F.*.	success or wait	1	6C771B4F	WriteFile

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	6D905705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D905705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D8603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D90CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D8603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D8603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D8603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D8603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D905705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D905705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C771B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C771B4F	ReadFile
C:\Users\user\Desktop\RFQ #46200058149.exe	unknown	4096	success or wait	1	6D8ED72F	unknown
C:\Users\user\Desktop\RFQ #46200058149.exe	unknown	512	success or wait	1	6D8ED72F	unknown

Analysis Process: WerFault.exe PID: 5416 Parent PID: 5340

General

Start time:	13:02:15
Start date:	07/04/2021

Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5340 -s 2672
Imagebase:	0xf10000
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
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	69DD1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5FCE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5FCE.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER758B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER758B.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_RFQ#46200058149_b4d3e1611dc98a70f1fcdf76f5b66818af29bc_427b5a83_156ea880	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_RFQ#46200058149_b4d3e1611dc98a70f1fcdf76f5b66818af29bc_427b5a83_156ea880\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	69DC497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5FCE.tmp	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER758B.tmp	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5FCE.tmp.dmp	success or wait	1	69DC4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	success or wait	1	69DC4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER758B.tmp.xml	success or wait	1	69DC4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7589.tmp.csv	success or wait	1	69DC4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78A7.tmp.txt	success or wait	1	69DC4BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5FCE.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0f 00 00 00 20 00 00 00 00 00 00 00 cd 0f 6e 60 a4 05 12 00 00 00 00 00	MDMP........ ....n`........	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5FCE.tmp.dmp	unknown	6	00 00 00 00 00 00	......	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5FCE.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 74 32 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 dc 14 00 00 bc 0f 6e 60 00 00 00 00 02 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 02 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......t2.... ..GenuineIntelW...........T... ....n`.................. ....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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5FCE.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 68 ea 2f 01 05 00 00 00 00 00 00 00 05 00 00 00 a8 e9 2f 01 00 ea 2f 01 22 d7 32 77 23 00 00 00 12 02 00 00 a8 e9 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	....+...S...+. ..+.......h./.............../. ../.".2w#........./.+.........	success or wait	1	69DC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5FCE.tmp.dmp	unknown	168	f0 14 00 00 00 00 00 00 52 43 43 e0 01 00 00 00 00 00 00 00 00 00 00 00 22 d7 32 77 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 79 6d 00 00 00 00 10 1c 45 01 00 00 00 00 e8 ea 2f 01 00 00 00 00 01 00 00 00 00 00 00 00 70 ea 2f 01 00 00 00 00 68 ea 2f 01 00 00 00 00 f4 76 7a 6d 00 00 00 00 e0 4d aa 03 00 00 00 00 10 1c 45 01 00 00 00 00 7a 77 7a 6d 00 00 00 00 c8 e9 2f 01 00 00 00 00 cc 02 00 00 ce 3d 00 00	........RCC............".2w.. ....ym......E....... /............p./.....h./..... .vzm.....M........E.....zwzm.. ..../..........=..	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5FCE.tmp.dmp	unknown	20	d1 02 00 00 78 f1 9b 05 00 00 00 00 1c 00 00 00 3a 9d 00 00	....x...........:...	success or wait	721	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5FCE.tmp.dmp	unknown	28	00 00 6b 6a 00 e0 de 6a 68 df 43 01 88 51 4d 01 00 00 00 00 00 00 00 00 00 10 6b 6a	..kj...jh.C..QM...........kj	success or wait	720	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5FCE.tmp.dmp	unknown	1344	94 9b 8b 6d 20 b2 02 02 00 00 00 00 f4 f1 4c 06 00 00 00 00 e0 bf 44 01 01 00 00 00 03 00 00 00 cc ea 9b 05 cc ea 9b 05 cc ea 9b 05 00 00 00 00 00 00 00 00 00 00 00 00 68 3f 43 01 00 30 10 01 00 00 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e4 87 4a 01 84 d4 7a 6c 18 e5 9b 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 11 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 2c 80 3b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 68 84 4a 01 00 00 00 00 00 00 00 00 0c 0a a3 05 00 00 00 00 00 00 4d 06 00 00 3d 06 00 00 45 06 cc cc cc cc cc cc cc	...m .........L.......D....... ....h?C. .0........... ....J...zl............ .... ,.;................ ....h.J...................M. ..=...E........	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5FCE.tmp.dmp	unknown	4	11 00 00 00	....	success or wait	17	69DC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5FCE.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 aa 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 40 db 2f 01 bc 9a a2 77 23 00 00 00 12 02 00 00 b0 d9 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...+. ..+.......................... @./....w#........./.+.........	success or wait	17	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5FCE.tmp.dmp	unknown	48	40 17 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 f0 10 01 00 00 00 00 00 f7 da 08 00 00 00 00 00 09 00 00 be 5e 04 00 cc 02 00 00 5a 6d 00 00	@....... ....^......Zm..	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5FCE.tmp.dmp	unknown	4	58 00 00 00	X...	success or wait	88	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5FCE.tmp.dmp	unknown	46	28 00 00 00 52 00 46 00 51 00 20 00 23 00 34 00 36 00 32 00 30 00 30 00 30 00 35 00 38 00 31 00 34 00 39 00 2e 00 65 00 78 00 65 00 00 00	(...R.F.Q. .#.4.6.2.0.0.0.5.8. 1.4.9...e.x.e...	success or wait	88	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5FCE.tmp.dmp	unknown	120	00 00 05 6a 00 00 00 00 00 80 0e 00 00 08 0f 00 d5 60 8e 5a e0 3c 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 00 29 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 0c 00 00 00 18 00 00 00 05 00 00 00	...j............`.Z.<....... ....?........... ....)............ ..@A.........................	success or wait	5	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5FCE.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	69DC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5FCE.tmp.dmp	unknown	668	00 00 59 6a 00 00 00 00 00 10 01 00 03 ab 01 00 c4 1f 6d 8d 92 3d 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 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 c0 38 02 00 00 00 00 00 b0 c5 02 00 00 00 00 30 46 01 00 00 01 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 db dc 00 00 00 00 00 00 f2 3a 03 00 00 00 00 00 0d 6e 02 00 00 00 00 00 b1 77 02 00 00 00 00 00 8f 87 1d 00 00 00 00 00 40 ff 1f 00 00 00 00 00 61 b6 1d 00 00 00 00 00 66 19 90 4f 00 00 00 00 d4 df 7f 15 00 00 00 00 46 bd 9e 0c 00 00 00 00 cb 24 df 00 00 00 00 00 63 95 00 00 85 87 00 00 41 6b 04 00 bb cc 00 00 8f 87 1d 00 10 62 23 00 61 b6 1d 00 be 22 35 00 38 14 01 00 00 fb 0d 00 00 00 00 00 d3 c3 26 00 c2 56 04	..Yj.....m..=.....Zb ....8..... .....0F..... .....:.....n.....w..... .....@.....a.....f..O.... .....F.....$.....c..... ..Ak.....b#.a....”5.8... .....&..V.	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5FCE.tmp.dmp	unknown	43658	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 00 74 00 43 00 6f 00 6d 00 70 00 6c	....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.....l.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.t.C.o.m.p.l	success or wait	1	69DC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5FCE.tmp.dmp	unknown	120	03 00 00 00 34 03 00 00 08 07 00 00 04 00 00 00 24 25 00 00 48 0a 00 00 0e 00 00 00 84 00 00 00 6c 2f 00 00 05 00 00 00 14 2d 00 00 26 70 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 a8 67 00 00 8f cb 04 00 15 00 00 00 ec 01 00 00 f0 2f 00 00 16 00 00 00 98 00 00 00 dc 31 00 00	....4.....$%..H..... ..l/.....-..&p.....`... ....8.....T.....g ...../.....1..	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69DC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69DC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 35 00 33 00 34 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.5.3.4.0.<./.P.i.d.>.	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	86	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 52 00 46 00 51 00 20 00 23 00 34 00 36 00 32 00 30 00 30 00 30 00 30 00 35 00 38 00 31 00 34 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.>.R.F.Q. . #.4.6.2.0.0.0.5.8.1.4.9...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69DC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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 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.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 38 00 38 00 36 00 32 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.>.1.8.8.6.2.<./.U.p.t.i.m.e.>.	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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 36 00 36 00 39 00 38 00 31 00 33 00 37 00 36 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.>.2.6.6.9.8.1.3.7.6.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	69DC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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 35 00 30 00 31 00 32 00 36 00 33 00 33 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.>.2.5.0.1.2.6.3.3.6.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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 32 00 36 00 31 00 36 00 30 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.>.2.6.1.6.0.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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 36 00 38 00 38 00 37 00 34 00 32 00 34 00 30 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.>.6.8.8.7.4.2.4.0.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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 36 00 38 00 37 00 35 00 31 00 33 00 36 00 30 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.>.6.8.7.5.1.3.6.0.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	69DC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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 37 00 31 00 30 00 38 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.>.3.7.1.0.8.8.<./.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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 33 00 35 00 31 00 32 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.>.3.6.3.5.1.2.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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 33 00 32 00 39 00 31 00 33 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 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.>.3.2.9.1.3.6.<./.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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 33 00 32 00 38 00 38 00 36 00 34 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.>.3.2.8.8.6.4.<./.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	69DC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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 35 00 30 00 32 00 38 00 32 00 34 00 39 00 36 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.>.5.0.2.8.2.4.9.6.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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 35 00 35 00 30 00 38 00 37 00 31 00 30 00 34 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.>.5.5.0.8.7.1.0.4.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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 35 00 30 00 32 00 38 00 32 00 34 00 39 00 36 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.>.5.0.2.8.2.4.9.6.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	69DC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 34 00 37 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.4.7.2.<./.P.i.d.>.	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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 34 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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	48	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 36 00 31 00 35 00 33 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.>.4.6.1.5.3.6.6.<./.U.p.t.i.m.e.>.	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	69DC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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 38 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.>.4.8.8.3.3.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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 33 00 35 00 37 00 39 00 36 00 34 00 38 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.>.1.0.3.5.7.9.6.4.8.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	69DC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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 39 00 37 00 38 00 36 00 35 00 37 00 32 00 38 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.>.9.7.8.6.5.7.2.8.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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 39 00 36 00 39 00 30 00 38 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.>.9.6.9.0.8.8.<./.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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 39 00 32 00 33 00 39 00 35 00 32 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.>.9.2.3.9.5.2.<./.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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 30 00 38 00 34 00 30 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.>.7.0.8.4.0.<./.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	69DC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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 36 00 38 00 32 00 34 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.>.6.8.2.4.0.<./.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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 32 00 39 00 34 00 39 00 31 00 32 00 30 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.>.2.9.4.9.1.2.0.0.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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 31 00 32 00 32 00 30 00 34 00 38 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.>.3.7.1.2.2.0.4.8.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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 32 00 39 00 34 00 39 00 31 00 32 00 30 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.>.2.9.4.9.1.2.0.0.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	69DC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	9	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	18	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	90	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 52 00 46 00 51 00 20 00 23 00 34 00 36 00 32 00 30 00 30 00 30 00 30 00 35 00 38 00 31 00 34 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.>.R.F.Q. .#.4.6.2.0.0.0.5.8.1.4.9...e.x.e.<./.P.a.r.a.m.e.t.e.r.0.>.	success or wait	9	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	69DC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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 70 00 70 00 61 00 70 00 69 00 77 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.>.p.p.a.p.i.w.,. .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	69DC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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 70 00 70 00 61 00 70 00 69 00 77 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.>.p.p.a.p.i.w.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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 37 00 31 00 35 00 39 00 30 00 33 00 36 00 36 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.>.1.5.7.1.5.9.0.3.6.6.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69DC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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 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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	69DC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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 34 00 2d 00 30 00 37 00 54 00 32 00 30 00 3a 00 30 00 32 00 3a 00 32 00 33 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.-.0.4.-.0.7.T.2.0.:.0.2.:.2.3.Z.".>.	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	262	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 32 00 34 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 33 00 34 00 30 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 39 00 39 00 33 00 37 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 39 00 39 00 33 00 37 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 00 3d 00 22	<.P.r.o.c.e.s.s. .A.s.I.d.=.".3.2.4.". .P.I.D.=.".5.3.4.0.". .U.p.t.i.m.e.M.S.=.".9.9.3.7.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".9.9.3.7.". .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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 64 00 37 00 37 00 64 00 32 00 34 00 38 00 32 00 2d 00 63 00 36 00 62 00 65 00 2d 00 34 00 32 00 66 00 66 00 2d 00 61 00 66 00 62 00 34 00 2d 00 66 00 37 00 64 00 35 00 35 00 38 00 34 00 34 00 37 00 36 00 36 00 66 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.d.7.7.d.2.4.8.2.-.c.6.b.e.-.4.2.f.f.-.a.f.b.4.-.f.7.d.5.5.8.4.4.7.6.6.f.<./.G.u.i.d.>.	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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 34 00 2d 00 30 00 37 00 54 00 32 00 30 00 3a 00 30 00 32 00 3a 00 32 00 33 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.-.0.4.-.0.7.T.2.0.:.0.2.:.2.3.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7357.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	69DC497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER758B.tmp.xml	unknown	4731	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	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_RFQ #46200058149_b4d3e1611dc98 a70f1fcdf76f5b66818af29bc_427b5a83_156ea880\Report.wer	unknown	2	ff fe	..	success or wait	1	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_RFQ #46200058149_b4d3e1611dc98 a70f1fcdf76f5b66818af29bc_427b5a83_156ea880\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	220	69DC497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_RFQ #46200058149_b4d3e1611dc98 a70f1fcdf76f5b66818af29bc_427b5a83_156ea880\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 31 00 33 00 37 00 38 00 32 00 35 00 31 00 37 00 32 00 30 00	M.e.t.a.d.a.t.a.H.a.s.h.=.1.3.7.8.2.5.1.7.2.0.	success or wait	1	69DC497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{757902f7-27c2-8541-16d8-369f8276edbd}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	69DE36BF	unknown
\REGISTRY\A\{757902f7-27c2-8541-16d8-369f8276edbd}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	69DE36BF	unknown
\REGISTRY\A\{757902f7-27c2-8541-16d8-369f8276edbd}\Root\InventoryApplicationFile\rfq #46200058149|99025e7e	success or wait	1	69DE36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	69DE1FB2	RegCreateKeyExW
\REGISTRY\A\{757902f7-27c2-8541-16d8-369f8276edbd}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	69DC43D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{757902f7-27c2-8541-16d8-369f8276edbd}\Root\InventoryApplicationFile\rfq #46200058149|99025e7e	ProgramId	unicode	000650f9261fe093f0967f4035d3c4ed3daf00000000	success or wait	1	69DE36BF	unknown
\REGISTRY\A\{757902f7-27c2-8541-16d8-369f8276edbd}\Root\InventoryApplicationFile\rfq #46200058149|99025e7e	FileId	unicode	0000a7c79eeaaafb23e8e40457cd5d44c61148cd1f5f	success or wait	1	69DE36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{757902f7-27c2-8541-16d8-369f8276edbd}\Root\InventoryApplicationFile\rfq #46200058149|99025e7e	LowerCaseLongPath	unicode	c:\users\user\desktop\rfq #462 00058149.exe	success or wait	1	69DE36BF	unknown
\REGISTRY\A\{757902f7-27c2-8541-16d8-369f8276edbd}\Root\InventoryApplicationFile\rfq #46200058149|99025e7e	LongPathHash	unicode	rfq #46200058149|99025e7e	success or wait	1	69DE36BF	unknown
\REGISTRY\A\{757902f7-27c2-8541-16d8-369f8276edbd}\Root\InventoryApplicationFile\rfq #46200058149|99025e7e	Name	unicode	rfq #46200058149.exe	success or wait	1	69DE36BF	unknown
\REGISTRY\A\{757902f7-27c2-8541-16d8-369f8276edbd}\Root\InventoryApplicationFile\rfq #46200058149|99025e7e	Publisher	unicode	LORz[JQM]oup|Q~\`xh.^.xtUzhys` ^mrP`VLHwtvN^h\P inc.	success or wait	1	69DE36BF	unknown
\REGISTRY\A\{757902f7-27c2-8541-16d8-369f8276edbd}\Root\InventoryApplicationFile\rfq #46200058149|99025e7e	Version	unicode	1.628.632.750	success or wait	1	69DE36BF	unknown
\REGISTRY\A\{757902f7-27c2-8541-16d8-369f8276edbd}\Root\InventoryApplicationFile\rfq #46200058149|99025e7e	BinFileVersion	unicode	1.628.632.750	success or wait	1	69DE36BF	unknown
\REGISTRY\A\{757902f7-27c2-8541-16d8-369f8276edbd}\Root\InventoryApplicationFile\rfq #46200058149|99025e7e	BinaryType	unicode	pe32_clr_32	success or wait	1	69DE36BF	unknown
\REGISTRY\A\{757902f7-27c2-8541-16d8-369f8276edbd}\Root\InventoryApplicationFile\rfq #46200058149|99025e7e	ProductName	unicode	LORz[JQM]oup|Q~\`xh.^.xtUzhys` ^mrP`VLHwtvN^h\P	success or wait	1	69DE36BF	unknown
\REGISTRY\A\{757902f7-27c2-8541-16d8-369f8276edbd}\Root\InventoryApplicationFile\rfq #46200058149|99025e7e	ProductVersion	unicode	1.628.632.750	success or wait	1	69DE36BF	unknown
\REGISTRY\A\{757902f7-27c2-8541-16d8-369f8276edbd}\Root\InventoryApplicationFile\rfq #46200058149|99025e7e	LinkDate	unicode	04/05/2066 21:20:36	success or wait	1	69DE36BF	unknown
\REGISTRY\A\{757902f7-27c2-8541-16d8-369f8276edbd}\Root\InventoryApplicationFile\rfq #46200058149|99025e7e	BinProductVersion	unicode	1.628.632.750	success or wait	1	69DE36BF	unknown
\REGISTRY\A\{757902f7-27c2-8541-16d8-369f8276edbd}\Root\InventoryApplicationFile\rfq #46200058149|99025e7e	Size	B	C0 D8 00 00 00 00 00 00	success or wait	1	69DE36BF	unknown
\REGISTRY\A\{757902f7-27c2-8541-16d8-369f8276edbd}\Root\InventoryApplicationFile\rfq #46200058149|99025e7e	Language	dword	0	success or wait	1	69DE36BF	unknown
\REGISTRY\A\{757902f7-27c2-8541-16d8-369f8276edbd}\Root\InventoryApplicationFile\rfq #46200058149|99025e7e	IsPeFile	dword	1	success or wait	1	69DE36BF	unknown
\REGISTRY\A\{757902f7-27c2-8541-16d8-369f8276edbd}\Root\InventoryApplicationFile\rfq #46200058149|99025e7e	IsOsComponent	dword	0	success or wait	1	69DE36BF	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	52 43 43 E0 01 00 00 00 00 00 00 00 22 D7 32 77 05 00 00 00 04 16 13 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 79 6D 10 1C 45 01 E8 EA 2F 01 01 00 00 00 70 EA 2F 01 68 EA 2F 01 F4 76 7A 6D E0 4D AA 03 10 1C 45 01 7A 77 7A 6D C8 E9 2F 01	success or wait	1	69DE1FE8	RegSetValueExW

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis