



MALWARE
Valkyrie Final Verdict

File Name: d3dx9_28.dll
File Type: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
SHA1: 0309e43c514e9ec964e090f3001b13f1384f10fc
MD5: 261996f3ab4b02cbbbe1e72c1641a018
First Seen Date: 2016-11-08 10:58:17 UTC
Number of Clients Seen: 3
Last Analysis Date: 2016-11-08 10:58:17 UTC
Human Expert Analysis Date: 2016-12-10 19:21:57 UTC
Human Expert Analysis Result: Malware
Verdict Source: Valkyrie Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT	
Signature Based Detection	2016-11-08 10:58:17 UTC	Malware	!
Human Expert Analysis Overall Verdict	2016-12-10 19:21:57 UTC	Malware	!
File Certificate Validation		Not Applicable	?

Static Analysis

No Static Analysis Result Received

DETECTOR	RESULT	
Optional Header LoaderFlags field is valued illegal	Clean	✓
Non-ascii or empty section names detected	Clean	✓
Illegal size of optional Header	Clean	✓
Packer detection on signature database	Unknown	?
Based on the sections entropy check! file is possibly packed	Clean	✓
Timestamp value suspicious	Clean	✓
Header Checksum is zero!	Suspicious	!
Entry point is outside the 1st(.code) section! Binary is possibly packed	Clean	✓
Optional Header NumberOfRvaAndSizes field is valued illegal	Clean	✓
Anti-vm present	Clean	✓
The Size Of Raw data is valued illegal! Binary might crash your disassembler/debugger	Clean	✓
TLS callback functions array detected	Clean	✓

Dynamic Analysis

No Dynamic Analysis Result Received

Behavioral Information is not Available

Precise Detectors Analysis Results

No Detector Result Received

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Human Expert Analysis Results

Analysis Start Date: 2016-12-10 18:12:41 UTC
Analysis End Date: 2016-12-10 19:21:57 UTC
File Upload Date: 2016-11-08 10:58:17 UTC
Human Expert Analyst Feedback:
Verdict: Malware

Additional File Information

Vendor Validation - Vendor Validation is not Applicable ?

Certificate Validation - Certificate Validation is not Applicable ?

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x5776401D [Fri Jul 1 10:04:13 2016 UTC]
Entry Point	0x10022efb (.text)
File Size	218624
Machine Type	Intel 386 or later - 32Bit
Mime Type	application/x-dosexec
Number Of Sections	4
Sha256	9203b693009a99a7524d6cfd184ace2272387107943fae14b4f21e27a61dbfa3

File Paths

FILE PATH ON CLIENT	SEEN COUNT
0309e43c514e9ec964e090f3001b13f1384f10fc	1

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x25ee4	0x26000	5.173467	-
.rdata	0x27000	0x828e	0x8400	5.728782	-
.data	0x30000	0x1b60	0xe00	3.088960	-
.reloc	0x32000	0x5f7e	0x6000	6.463364	-

PE Imports

KERNEL32.dll

HeapAlloc

GetProcessHeap

VirtualAlloc

GetFileType

 FindClose

 IstrlenA

 VirtualProtect

 VirtualFree

 GetProcAddress

 LoadLibraryA

 IsBadReadPtr

 HeapFree

 FreeLibrary

 Sleep

 CloseHandle

 ReadFile

 GetFileSize

 CreateFileA

 IstrcpyA

 IstrcatA

 GetModuleFileNameA

 GlobalAlloc

 GetCommandLineA

 GetModuleHandleA

 GetLastError

 HeapReAlloc

 GetCurrentThreadId

 DecodePointer

 IsProcessorFeaturePresent

 EncodePointer

 HeapCreate

 HeapDestroy

 TlsAlloc

 TlsGetValue

 TlsSetValue

 TlsFree

 InterlockedIncrement

 GetModuleHandleW

 SetLastError

 InterlockedDecrement

 ExitProcess

 SetHandleCount

 GetStdHandle

 InitializeCriticalSectionAndSpinCount

 GetStartupInfoW

 DeleteCriticalSection

 FreeEnvironmentStringsW

 WideCharToMultiByte

 GetEnvironmentStringsW

 QueryPerformanceCounter

 GetTickCount

 GetCurrentProcessId

 GetSystemTimeAsFileTime

 UnhandledExceptionFilter

 SetUnhandledExceptionFilter

 IsDebuggerPresent

 TerminateProcess

 GetCurrentProcess

 LeaveCriticalSection

 EnterCriticalSection

 WriteFile

 GetModuleFileNameW

 GetCPInfo

 GetACP

 GetOEMCP

 IsValidCodePage

 LoadLibraryW

 RtlUnwind

 LCMultiByteToWideChar

 MultiByteToWideChar

 GetStringTypeW

 HeapSize

—

 USER32.dll

 DrawTextA

 PE Exports

 D3DXAssembleShader

 D3DXAssembleShaderFromFileA

-  D3DXAssembleShaderFromFileW
-  D3DXAssembleShaderFromResourceA
-  D3DXAssembleShaderFromResourceW
-  D3DXBoxBoundProbe
-  D3DXCheckCubeTextureRequirements
-  D3DXCheckTextureRequirements
-  D3DXCheckVersion
-  D3DXCheckVolumeTextureRequirements
-  D3DXCleanMesh
-  D3DXColorAdjustContrast
-  D3DXColorAdjustSaturation
-  D3DXCompileShader
-  D3DXCompileShaderFromFileA
-  D3DXCompileShaderFromFileW
-  D3DXCompileShaderFromResourceA
-  D3DXCompileShaderFromResourceW
-  D3DXComputeBoundingBox
-  D3DXComputeBoundingSphere
-  D3DXComputeIMTFFromPerTexelSignal
-  D3DXComputeIMTFFromPerVertexSignal
-  D3DXComputeIMTFFromSignal
-  D3DXComputeIMTFFromTexture
-  D3DXComputeNormalMap
-  D3DXComputeNormals
-  D3DXComputeTangent
-  D3DXComputeTangentFrame
-  D3DXComputeTangentFrameEx
-  D3DXConcatenateMeshes
-  D3DXConvertMeshSubsetToSingleStrip
-  D3DXConvertMeshSubsetToStrips
-  D3DXCpuOptimizations
-  D3DXCreateAnimationController
-  D3DXCreateBox
-  D3DXCreateBuffer
-  D3DXCreateCompressedAnimationSet
-  D3DXCreateCubeTexture
-  D3DXCreateCubeTextureFromFileA
-  D3DXCreateCubeTextureFromFileExA
-  D3DXCreateCubeTextureFromFileExW
-  D3DXCreateCubeTextureFromFileInMemory
-  D3DXCreateCubeTextureFromFileInMemoryEx
-  D3DXCreateCubeTextureFromFileW
-  D3DXCreateCubeTextureFromResourceA
-  D3DXCreateCubeTextureFromResourceExA
-  D3DXCreateCubeTextureFromResourceExW
-  D3DXCreateCubeTextureFromResourceW

 D3DXCreateCylinder

 D3DXCreateEffect

 D3DXCreateEffectCompiler

 D3DXCreateEffectCompilerFromFileA

 D3DXCreateEffectCompilerFromFileW

 D3DXCreateEffectCompilerFromResourceA

 D3DXCreateEffectCompilerFromResourceW

 D3DXCreateEffectEx

 D3DXCreateEffectFromFileA

 D3DXCreateEffectFromFileExA

 D3DXCreateEffectFromFileExW

 D3DXCreateEffectFromFileW

 D3DXCreateEffectFromResourceA

 D3DXCreateEffectFromResourceExA

 D3DXCreateEffectFromResourceExW

 D3DXCreateEffectFromResourceW

 D3DXCreateEffectPool

 D3DXCreateFontA

 D3DXCreateFontIndirectA

 D3DXCreateFontIndirectW

 D3DXCreateFontW

 D3DXCreateFragmentLinker

 D3DXCreateKeyframedAnimationSet

 D3DXCreateLine

 D3DXCreateMatrixStack

 D3DXCreateMesh

 D3DXCreateMeshFVF

 D3DXCreateNPatchMesh

 D3DXCreatePMeshFromStream

 D3DXCreatePRTBuffer

 D3DXCreatePRTBufferTex

 D3DXCreatePRTCompBuffer

 D3DXCreatePRTEngine

 D3DXCreatePatchMesh

 D3DXCreatePolygon

 D3DXCreateRenderToEnvMap

 D3DXCreateRenderToSurface

 D3DXCreateSPMesh

 D3DXCreateSkinInfo

 D3DXCreateSkinInfoFVF

 D3DXCreateSkinInfoFromBlendedMesh

 D3DXCreateSphere

 D3DXCreateSprite

 D3DXCreateTeapot

 D3DXCreateTextA

 D3DXCreateTextW

 D3DXCreateTexture

 D3DXCreateTextureFromFileA

 D3DXCreateTextureFromFileExA

 D3DXCreateTextureFromFileExW

 D3DXCreateTextureFromFileInMemory

 D3DXCreateTextureFromFileInMemoryEx

 D3DXCreateTextureFromFileW

 D3DXCreateTextureFromResourceA

 D3DXCreateTextureFromResourceExA

 D3DXCreateTextureFromResourceExW

 D3DXCreateTextureFromResourceW

 D3DXCreateTextureGutterHelper

 D3DXCreateTextureShader

 D3DXCreateTorus

 D3DXCreateVolumeTexture

 D3DXCreateVolumeTextureFromFileA

 D3DXCreateVolumeTextureFromFileExA

 D3DXCreateVolumeTextureFromFileExW

 D3DXCreateVolumeTextureFromFileInMemory

 D3DXCreateVolumeTextureFromFileInMemoryEx

 D3DXCreateVolumeTextureFromFileW

 D3DXCreateVolumeTextureFromResourceA

 D3DXCreateVolumeTextureFromResourceExA

 D3DXCreateVolumeTextureFromResourceExW

 D3DXCreateVolumeTextureFromResourceW

 D3DXDebugMute

 D3DXDeclaratorFromFVF

 D3DXDisassembleEffect

 D3DXDisassembleShader

 D3DXFVFFromDeclarator

 D3DXFileCreate

 D3DXFillCubeTexture

 D3DXFillCubeTextureTX

 D3DXFillTexture

 D3DXFillTextureTX

 D3DXFillVolumeTexture

 D3DXFillVolumeTextureTX

 D3DXFilterTexture

 D3DXFindShaderComment

 D3DXFloat16To32Array

 D3DXFloat32To16Array

 D3DXFrameAppendChild

 D3DXFrameCalculateBoundingSphere

 D3DXFrameDestroy

 D3DXFrameFind

 D3DXFrameNumNamedMatrices

 D3DXFrameRegisterNamedMatrices

 D3DXFresnelTerm

 D3DXGatherFragments

 D3DXGatherFragmentsFromFileA

 D3DXGatherFragmentsFromFileW

 D3DXGatherFragmentsFromResourceA

 D3DXGatherFragmentsFromResourceW

 D3DXGenerateOutputDecl

 D3DXGeneratePMesh

 D3DXGetDeclLength

 D3DXGetDeclVertexSize

 D3DXGetDriverLevel

 D3DXGetFVFVertexSize

 D3DXGetImageInfoFromFileA

 D3DXGetImageInfoFromFileInMemory

 D3DXGetImageInfoFromFileW

 D3DXGetImageInfoFromResourceA

 D3DXGetImageInfoFromResourceW

 D3DXGetPixelShaderProfile

 D3DXGetShaderConstantTable

 D3DXGetShaderInputSemantics

 D3DXGetShaderOutputSemantics

 D3DXGetShaderSamplers

 D3DXGetShaderSize

 D3DXGetShaderVersion

 D3DXGetTargetDescByName

 D3DXGetTargetDescByVersion

 D3DXGetVertexShaderProfile

 D3DXIntersect

 D3DXIntersectSubset

 D3DXIntersectTri

 D3DXLoadMeshFromXA

 D3DXLoadMeshFromXInMemory

 D3DXLoadMeshFromXResource

 D3DXLoadMeshFromXW

 D3DXLoadMeshFromXof

 D3DXLoadMeshHierarchyFromXA

 D3DXLoadMeshHierarchyFromXInMemory

 D3DXLoadMeshHierarchyFromXW

 D3DXLoadPRTBufferFromFileA

 D3DXLoadPRTBufferFromFileW

 D3DXLoadPRTCompBufferFromFileA

 D3DXLoadPRTCompBufferFromFileW

 D3DXLoadPatchMeshFromXof

 D3DXLoadSkinMeshFromXof

 D3DXLoadSurfaceFromFileA

 D3DXLoadSurfaceFromFileInMemory

 D3DXLoadSurfaceFromFileW

 D3DXLoadSurfaceFromMemory

 D3DXLoadSurfaceFromResourceA

 D3DXLoadSurfaceFromResourceW

 D3DXLoadSurfaceFromSurface

 D3DXLoadVolumeFromFileA

 D3DXLoadVolumeFromFileInMemory

 D3DXLoadVolumeFromFileW

 D3DXLoadVolumeFromMemory

 D3DXLoadVolumeFromResourceA

 D3DXLoadVolumeFromResourceW

 D3DXLoadVolumeFromVolume

 D3DXMatrixAffineTransformation

 D3DXMatrixAffineTransformation2D

 D3DXMatrixDecompose

 D3DXMatrixDeterminant

 D3DXMatrixInverse

 D3DXMatrixLookAtLH

 D3DXMatrixLookAtRH

 D3DXMatrixMultiply

 D3DXMatrixMultiplyTranspose

 D3DXMatrixOrthoLH

 D3DXMatrixOrthoOffCenterLH

 D3DXMatrixOrthoOffCenterRH

 D3DXMatrixOrthoRH

 D3DXMatrixPerspectiveFovLH

 D3DXMatrixPerspectiveFovRH

 D3DXMatrixPerspectiveLH

 D3DXMatrixPerspectiveOffCenterLH

 D3DXMatrixPerspectiveOffCenterRH

 D3DXMatrixPerspectiveRH

 D3DXMatrixReflect

 D3DXMatrixRotationAxis

 D3DXMatrixRotationQuaternion

 D3DXMatrixRotationX

 D3DXMatrixRotationY

 D3DXMatrixRotationYawPitchRoll

 D3DXMatrixRotationZ

 D3DXMatrixScaling

 D3DXMatrixShadow

 D3DXMatrixTransformation

 D3DXMatrixTransformation2D

 D3DXMatrixTranslation

 D3DXMatrixTranspose

 D3DXOptimizeFaces

 D3DXOptimizeVertices

 D3DXPlaneFromPointNormal

 D3DXPlaneFromPoints

 D3DXPlaneIntersectLine

 D3DXPlaneNormalize

 D3DXPlaneTransform

 D3DXPlaneTransformArray

 D3DXPreprocessShader

 D3DXPreprocessShaderFromFileA

 D3DXPreprocessShaderFromFileW

 D3DXPreprocessShaderFromResourceA

 D3DXPreprocessShaderFromResourceW

 D3DXQuaternionBaryCentric

 D3DXQuaternionExp

 D3DXQuaternionInverse

 D3DXQuaternionLn

 D3DXQuaternionMultiply

 D3DXQuaternionNormalize

 D3DXQuaternionRotationAxis

 D3DXQuaternionRotationMatrix

 D3DXQuaternionRotationYawPitchRoll

 D3DXQuaternionSlerp

 D3DXQuaternionSquad

 D3DXQuaternionSquadSetup

 D3DXQuaternionToAxisAngle

 D3DXRectPatchSize

 D3DXSHAdd

 D3DXSHDot

 D3DXSHEvalConeLight

 D3DXSHEvalDirection

 D3DXSHEvalDirectionalLight

 D3DXSHEvalHemisphereLight

 D3DXSHEvalSphericalLight

 D3DXSHPRTCompSplitMeshSC

 D3DXSHPRTCompSuperCluster

 D3DXSHProjectCubeMap

 D3DXSHRotate

 D3DXSHRotateZ

 D3DXSHScale

 D3DXSaveMeshHierarchyToFileA

 D3DXSaveMeshHierarchyToFileW

 D3DXSaveMeshToXA

 D3DXSaveMeshToXW

 D3DXSavePRTBufferToFileA

 D3DXSavePRTBufferToFileW

 D3DXSavePRTCompBufferToFileA

 D3DXSavePRTCompBufferToFileW

 D3DXSaveSurfaceToFileA

 D3DXSaveSurfaceToFileInMemory

 D3DXSaveSurfaceToFileW

 D3DXSaveTextureToFileA

 D3DXSaveTextureToFileInMemory

 D3DXSaveTextureToFileW

 D3DXSaveVolumeToFileA

 D3DXSaveVolumeToFileInMemory

 D3DXSaveVolumeToFileW

 D3DXSimplifyMesh

 D3DXSphereBoundProbe

 D3DXSplitMesh

 D3DXTessellateNPatches

 D3DXTessellateRectPatch

 D3DXTessellateTriPatch

 D3DXTriPatchSize

 D3DXUVAtlasCreate

 D3DXUVAtlasPack

 D3DXUVAtlasPartition

 D3DXValidMesh

 D3DXValidPatchMesh

 D3DXVec2BaryCentric

 D3DXVec2CatmullRom

 D3DXVec2Hermite

 D3DXVec2Normalize

 D3DXVec2Transform

 D3DXVec2TransformArray

 D3DXVec2TransformCoord

 D3DXVec2TransformCoordArray

 D3DXVec2TransformNormal

 D3DXVec2TransformNormalArray

 D3DXVec3BaryCentric

 D3DXVec3CatmullRom

 D3DXVec3Hermite

 D3DXVec3Normalize

 D3DXVec3Project

 D3DXVec3ProjectArray

 D3DXVec3Transform

 D3DXVec3TransformArray

 D3DXVec3TransformCoord

 D3DXVec3TransformCoordArray

-  D3DXVec3TransformNormal
-  D3DXVec3TransformNormalArray
-  D3DXVec3Unproject
-  D3DXVec3UnprojectArray
-  D3DXVec4BaryCentric
-  D3DXVec4CatmullRom
-  D3DXVec4Cross
-  D3DXVec4Hermite
-  D3DXVec4Normalize
-  D3DXVec4Transform
-  D3DXVec4TransformArray
-  D3DXWeldVertices
-  DSshenme

 PE Resources

