VALKYRIE

CLEAN
Valkyrie Final Verdict

File Name: vulkan-1.dll
File Type: PE32+ executable (DLL) (console) x86-64, for MS Windows
SHA1: c5a460bf882d091019b62b5ae712a62fdfbf23a0
MD5: 139004a617fae98ec7c474db45a577e6
First Seen Date: 2022-01-31 13:29:29 UTC
Number of Clients Seen: 2
Last Analysis Date: 2022-01-31 13:29:29 UTC
Human Expert Analysis Result: No human expert analysis verdict given to this sample yet.
Verdict Source: Signature Based Detection

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT	
Signature Based Detection	2022-02-01 03:14:43 UTC	Clean	
Static Analysis Overall Verdict	2022-01-31 13:29:29 UTC	No Threat Found	
Precise Detectors Overall Verdict	2022-01-31 13:29:29 UTC	No Match	
File Certificate Validation		Not Applicable	

Static Analysis

STATIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	

DETECTOR	RESULT	
Optional Header LoaderFlags field is valued illegal	Clean	
Non-ascii or empty section names detected	Suspicious	
Illegal size of optional Header	Suspicious	
Packer detection on signature database	Unknown	
Based on the sections entropy check! file is possibly packed	Clean	
Timestamp value suspicious	Suspicious	
Header Checksum is zero!	Suspicious	
Enrty 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

DETECTOR NAME	DATE	VERDICT	REASON
Static Precise PUA Detector 1	2022-01-31 13:29:25 UTC	No Match	NotDetected
Static Precise PUA Detector 4	2022-01-31 13:29:25 UTC	No Match	NotDetected
Static Precise NI Detector 3	2022-01-31 13:29:25 UTC	No Match	NotDetected
Static Precise PUA Detector 5	2022-01-31 13:29:25 UTC	No Match	NotDetected
Static Precise Trojan Detector 1	2022-01-31 13:29:25 UTC	No Match	NotDetected
Static Precise Trojan Detector 3	2022-01-31 13:29:25 UTC	No Match	NotDetected
Static Precise PUA Detector 6	2022-01-31 13:29:25 UTC	No Match	NotDetected
Static Precise Trojan Detector 12	2022-01-31 13:29:25 UTC	No Match	NotDetected
Static Precise Virus Detector 1	2022-01-31 13:29:25 UTC	No Match	NotDetected
Static Precise Virus Detector 2	2022-01-31 13:29:25 UTC	No Match	NotDetected
Static Precise Trojan Detector 13	2022-01-31 13:29:25 UTC	No Match	NotDetected
Static Precise PUA Detector 2	2022-01-31 13:29:25 UTC	No Match	NotDetected

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Additional File Information

Vendor Validation - Vendor Validation is not Applicable ?

Certificate Validation - Certificate Validation is not Applicable ?

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x0 [Thu Jan 1 00:00:00 1970 UTC] [SUSPICIOUS]
Debug Artifacts	[object Object]
Entry Point	0x180043670 (.text)
Exifinfo	[object Object]
File Size	733696
File Type Enum	7
Imphash	00a11204bd7ac096090b7bdfc42df6d6
Machine Type	AMD64 only, not Itaniums, with 0200 - 64 bit
Magic Literal Enum	22
Legal Copyright	Copyright (C) 2015-2021
Product Version	1.0.1111.2222.Dev Build
Product Name	Vulkan Runtime
File Version	1.0.1111.2222.Dev Build
File Description	Vulkan Loader - Dev Build
Translation	0x0409 0x0000
Mime Type	application/x-dosexec
Number Of Sections	8
Sha256	1c34bf2e786a62efd1c0e9700c343c09a93995b9513c03346e61a442e78dbd6f
Ssdeep	12288:k/4iJIMwx1R59xBt8/MRTAC6jYJpf8o1pWo:E4ir0R5z80RTQjeV8
Trid	50,Generic Win/DOS Executable,49.9,DOS Executable Generic

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x7fa56	0x7fc00	6.38097858391	ce389d91fd3bcf1bd595824182d2efcd
.rdata	0x81000	0x2aa04	0x2ac00	5.68834753256	c1323d29c586cae21851437165442104
.data	0xac000	0x4cb8	0x2000	3.5388902771	7e7b225bc0e80a8cd5b2cbe895da746b
.pdata	0xb1000	0x4f14	0x5000	5.73753925167	7c6f3437b052e93ce12c0efd342d7a70
.00cfg	0xb6000	0x10	0x200	0.195869406087	a8a52f8714bd6a20945094aeaea2fa8e
.tls	0xb7000	0x9	0x200	0.0203931352361	1f354d76203061bfdd5a53dae48d5435
.rsrc	0xb8000	0x2d0	0x400	2.48106979684	b9d91be53ac7a55584c4b3c0c08aee06
.reloc	0xb9000	0xd88	0xe00	5.35597156178	20a23c83b068f1a26484dc98cc102f07

PE Imports

KERNEL32.dll

- AcquireSRWLockExclusive
- CloseHandle
- CompareStringW
- CreateEventW
- CreateFileW
- DeleteCriticalSection
- EncodePointer
- EnterCriticalSection
- EnumSystemLocalesW

- ExitProcess
- FileTimeToSystemTime
- FindClose
- FindFirstFileExW
- FindNextFileW
- FlushFileBuffers
- FreeEnvironmentStringsW
- FreeLibrary
- GetACP
- GetCPInfo
- GetCommandLineA
- GetCommandLineW
- GetConsoleMode
- GetConsoleOutputCP
- GetCurrentProcess
- GetCurrentProcessId
- GetCurrentThreadId
- GetDateFormatW
- GetEnvironmentStringsW
- GetEnvironmentVariableA
- GetFileAttributesExW
- GetFileSizeEx
- GetFileType
- GetLastError
- GetLocaleInfoW
- GetModuleFileNameA
- GetModuleFileNameW
- GetModuleHandleA
- GetModuleHandleExA
- GetModuleHandleExW
- GetModuleHandleW
- GetOEMCP
- GetProcAddress
- GetProcessHeap
- GetStartupInfoW
- GetStdHandle
- GetStringTypeW

- GetSystemDirectoryA
- GetSystemTimeAsFileTime
- GetTimeFormatW
- GetTimeZoneInformation
- GetUserDefaultLCID
- HeapAlloc
- HeapFree
- HeapReAlloc
- HeapSize
- InitializeCriticalSection
- InitializeCriticalSectionAndSpinCount
- InitializeSListHead
- InterlockedFlushSList
- IsDebuggerPresent
- IsProcessorFeaturePresent
- IsValidCodePage
- IsValidLocale
- IsWow64Process
- LCMapStringW
- LeaveCriticalSection
- LoadLibraryA
- LoadLibraryExA
- LoadLibraryExW
- MultiByteToWideChar
- OutputDebugStringA
- QueryPerformanceCounter
- RaiseException
- ReadConsoleW
- ReadFile
- ReleaseSRWLockExclusive
- ResetEvent
- RtlCaptureContext
- RtlLookupFunctionEntry
- RtlPcToFileHeader
- RtlUnwind
- RtlUnwindEx
- RtlVirtualUnwind

- SetEndOfFile
- SetEnvironmentVariableW
- SetEvent
- SetFilePointerEx
- SetLastError
- SetStdHandle
- SetUnhandledExceptionFilter
- SleepConditionVariableSRW
- SystemTimeToTzSpecificLocalTime
- TerminateProcess
- TlsAlloc
- TlsFree
- TlsGetValue
- TlsSetValue
- UnhandledExceptionFilter
- WaitForSingleObjectEx
- WakeAllConditionVariable
- WideCharToMultiByte
- WriteConsoleW
- WriteFile

ADVAPI32.dll

- GetSidSubAuthority
- GetSidSubAuthorityCount
- GetTokenInformation
- OpenProcessToken
- RegCloseKey
- RegEnumValueA
- RegOpenKeyExA
- RegQueryValueExA

CFGMGR32.dll

- CM_Get_Child
- CM_Get_DevNode_Registry_PropertyW
- CM_Get_DevNode_Status
- CM_Get_Device_IDW
- CM_Get_Device_ID_ListW
- CM_Get_Device_ID_List_SizeW
- CM_Get_Sibling

CM_Locate_DevNodeW

CM_Open_DevNode_Key

PE Exports

vkAcquireNextImage2KHR

vkAcquireNextImageKHR

vkAllocateCommandBuffers

vkAllocateDescriptorSets

vkAllocateMemory

vkBeginCommandBuffer

vkBindBufferMemory

vkBindBufferMemory2

vkBindImageMemory

vkBindImageMemory2

vkCmdBeginQuery

vkCmdBeginRenderPass

vkCmdBeginRenderPass2

vkCmdBindDescriptorSets

vkCmdBindIndexBuffer

vkCmdBindPipeline

vkCmdBindVertexBuffers

vkCmdBlitImage

vkCmdClearAttachments

vkCmdClearColorImage

vkCmdClearDepthStencilImage

vkCmdCopyBuffer

vkCmdCopyBufferToImage

vkCmdCopyImage

vkCmdCopyImageToBuffer

vkCmdCopyQueryPoolResults

vkCmdDispatch

vkCmdDispatchBase

vkCmdDispatchIndirect

vkCmdDraw

vkCmdDrawIndexed

vkCmdDrawIndexedIndirect

vkCmdDrawIndexedIndirectCount

vkCmdDrawIndirect

vkCmdDrawIndirectCount

vkCmdEndQuery

vkCmdEndRenderPass

vkCmdEndRenderPass2

vkCmdExecuteCommands

vkCmdFillBuffer

vkCmdNextSubpass

- vkCmdNextSubpass2
- vkCmdPipelineBarrier
- vkCmdPushConstants
- vkCmdResetEvent
- vkCmdResetQueryPool
- vkCmdResolveImage
- vkCmdSetBlendConstants
- vkCmdSetDepthBias
- vkCmdSetDepthBounds
- vkCmdSetDeviceMask
- vkCmdSetEvent
- vkCmdSetLineWidth
- vkCmdSetScissor
- vkCmdSetStencilCompareMask
- vkCmdSetStencilReference
- vkCmdSetStencilWriteMask
- vkCmdSetViewport
- vkCmdUpdateBuffer
- vkCmdWaitEvents
- vkCmdWriteTimestamp
- vkCreateBuffer
- vkCreateBufferView
- vkCreateCommandPool
- vkCreateComputePipelines
- vkCreateDescriptorPool
- vkCreateDescriptorSetLayout
- vkCreateDescriptorUpdateTemplate
- vkCreateDevice
- vkCreateDisplayModeKHR
- vkCreateDisplayPlaneSurfaceKHR
- vkCreateEvent
- vkCreateFence
- vkCreateFramebuffer
- vkCreateGraphicsPipelines
- vkCreateImage
- vkCreateImageView
- vkCreateInstance
- vkCreatePipelineCache
- vkCreatePipelineLayout
- vkCreateQueryPool
- vkCreateRenderPass
- vkCreateRenderPass2
- vkCreateSampler
- vkCreateSamplerYcbcrConversion
- vkCreateSemaphore

- vkCreateShaderModule
- vkCreateSharedSwapchainsKHR
- vkCreateSwapchainKHR
- vkCreateWin32SurfaceKHR
- vkDestroyBuffer
- vkDestroyBufferView
- vkDestroyCommandPool
- vkDestroyDescriptorPool
- vkDestroyDescriptorSetLayout
- vkDestroyDescriptorUpdateTemplate
- vkDestroyDevice
- vkDestroyEvent
- vkDestroyFence
- vkDestroyFramebuffer
- vkDestroyImage
- vkDestroyImageView
- vkDestroyInstance
- vkDestroyPipeline
- vkDestroyPipelineCache
- vkDestroyPipelineLayout
- vkDestroyQueryPool
- vkDestroyRenderPass
- vkDestroySampler
- vkDestroySamplerYcbcrConversion
- vkDestroySemaphore
- vkDestroyShaderModule
- vkDestroySurfaceKHR
- vkDestroySwapchainKHR
- vkDeviceWaitIdle
- vkEndCommandBuffer
- vkEnumerateDeviceExtensionProperties
- vkEnumerateDeviceLayerProperties
- vkEnumerateInstanceExtensionProperties
- vkEnumerateInstanceLayerProperties
- vkEnumerateInstanceVersion
- vkEnumeratePhysicalDeviceGroups
- vkEnumeratePhysicalDevices
- vkFlushMappedMemoryRanges
- vkFreeCommandBuffers
- vkFreeDescriptorSets
- vkFreeMemory
- vkGetBufferDeviceAddress
- vkGetBufferMemoryRequirements
- vkGetBufferMemoryRequirements2
- vkGetBufferOpaqueCaptureAddress
- vkGetDescriptorSetLayoutSupport

- vkGetDeviceGroupPeerMemoryFeatures
- vkGetDeviceGroupPresentCapabilitiesKHR
- vkGetDeviceGroupSurfacePresentModesKHR
- vkGetDeviceMemoryCommitment
- vkGetDeviceMemoryOpaqueCaptureAddress
- vkGetDeviceProcAddr
- vkGetDeviceQueue
- vkGetDeviceQueue2
- vkGetDisplayModeProperties2KHR
- vkGetDisplayModePropertiesKHR
- vkGetDisplayPlaneCapabilities2KHR
- vkGetDisplayPlaneCapabilitiesKHR
- vkGetDisplayPlaneSupportedDisplaysKHR
- vkGetEventStatus
- vkGetFenceStatus
- vkGetImageMemoryRequirements
- vkGetImageMemoryRequirements2
- vkGetImageSparseMemoryRequirements
- vkGetImageSparseMemoryRequirements2
- vkGetImageSubresourceLayout
- vkGetInstanceProcAddr
- vkGetPhysicalDeviceDisplayPlaneProperties2KHR
- vkGetPhysicalDeviceDisplayPlanePropertiesKHR
- vkGetPhysicalDeviceDisplayProperties2KHR
- vkGetPhysicalDeviceDisplayPropertiesKHR
- vkGetPhysicalDeviceExternalBufferProperties
- vkGetPhysicalDeviceExternalFenceProperties
- vkGetPhysicalDeviceExternalSemaphoreProperties
- vkGetPhysicalDeviceFeatures
- vkGetPhysicalDeviceFeatures2
- vkGetPhysicalDeviceFormatProperties
- vkGetPhysicalDeviceFormatProperties2
- vkGetPhysicalDeviceImageFormatProperties
- vkGetPhysicalDeviceImageFormatProperties2
- vkGetPhysicalDeviceMemoryProperties
- vkGetPhysicalDeviceMemoryProperties2
- vkGetPhysicalDevicePresentRectanglesKHR
- vkGetPhysicalDeviceProperties
- vkGetPhysicalDeviceProperties2
- vkGetPhysicalDeviceQueueFamilyProperties
- vkGetPhysicalDeviceQueueFamilyProperties2
- vkGetPhysicalDeviceSparseImageFormatProperties
- vkGetPhysicalDeviceSparseImageFormatProperties2
- vkGetPhysicalDeviceSurfaceCapabilities2KHR
- vkGetPhysicalDeviceSurfaceCapabilitiesKHR

- vkGetPhysicalDeviceSurfaceFormats2KHR
- vkGetPhysicalDeviceSurfaceFormatsKHR
- vkGetPhysicalDeviceSurfacePresentModesKHR
- vkGetPhysicalDeviceSurfaceSupportKHR
- vkGetPhysicalDeviceWin32PresentationSupportKHR
- vkGetPipelineCacheData
- vkGetQueryPoolResults
- vkGetRenderAreaGranularity
- vkGetSemaphoreCounterValue
- vkGetSwapchainImagesKHR
- vkInvalidateMappedMemoryRanges
- vkMapMemory
- vkMergePipelineCaches
- vkQueueBindSparse
- vkQueuePresentKHR
- vkQueueSubmit
- vkQueueWaitIdle
- vkResetCommandBuffer
- vkResetCommandPool
- vkResetDescriptorPool
- vkResetEvent
- vkResetFences
- vkResetQueryPool
- vkSetEvent
- vkSignalSemaphore
- vkTrimCommandPool
- vkUnmapMemory
- vkUpdateDescriptorSetWithTemplate
- vkUpdateDescriptorSets
- vkWaitForFences
- vkWaitSemaphores

PE Resources

[object Object]