VALKYRIE

CLEAN
Valkyrie Final Verdict

File Name: vk_swiftshader.dll
File Type: PE32+ executable (DLL) (console) x86-64, for MS Windows
SHA1: 6b646517dcb24d81dcde87ea5223737422095431
MD5: b024ac9c54480fc0aad669acf6b95cb4
First Seen Date: 2022-01-31 13:29:38 UTC
Number of Clients Seen: 2
Last Analysis Date: 2022-01-31 13:29:38 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 02:31:19 UTC	Clean	
Static Analysis Overall Verdict	2022-01-31 13:29:38 UTC	No Threat Found	
Precise Detectors Overall Verdict	2022-01-31 13:29:38 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 13:29:31 UTC	No Match		NotDetected
Static Precise PUA Detector 4	2022-01-31 13:29:31 UTC	No Match		NotDetected
Static Precise NI Detector 3	2022-01-31 13:29:31 UTC	No Match		NotDetected
Static Precise PUA Detector 5	2022-01-31 13:29:31 UTC	No Match		NotDetected
Static Precise Trojan Detector 1	2022-01-31 13:29:31 UTC	No Match		NotDetected
Static Precise Trojan Detector 3	2022-01-31 13:29:31 UTC	No Match		NotDetected
Static Precise PUA Detector 6	2022-01-31 13:29:31 UTC	No Match		NotDetected
Static Precise Trojan Detector 12	2022-01-31 13:29:31 UTC	No Match		NotDetected
Static Precise Virus Detector 1	2022-01-31 13:29:31 UTC	No Match		NotDetected
Static Precise Virus Detector 2	2022-01-31 13:29:31 UTC	No Match		NotDetected
Static Precise Trojan Detector 13	2022-01-31 13:29:31 UTC	No Match		NotDetected
Static Precise PUA Detector 2	2022-01-31 13:29:31 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	0x1802ec480 (.text)
Exifinfo	[object Object]
File Size	4487680
File Type Enum	7
Imphash	9a4b90b161eb746862cd987fb9ff69c9
Machine Type	AMD64 only, not Itaniums, with 0200 - 64 bit
Magic Literal Enum	22
Legal Copyright	Copyright (C) 2018 Google Inc.
Internal Name	Vulkan
File Version	5.0.0
File Description	SwiftShader Vulkan 32-bit Dynamic Link Library
Product Name	SwiftShader Vulkan Dynamic Link Library
Product Version	5.0.0
Private Build	5.0.0
Original Filename	vk_swiftshader.dll
Translation	0x0409 0x04b0
Mime Type	application/x-dosexec
Number Of Sections	8
Sha256	40f0ef9e4b1fa3bcc2edcccf318109d6c97c724324dc3b11ce79e5e47e1d0fdf
Ssdeep	49152:vyVVFWS+38pwsSoz+JY7x+kmo+j5sMvp7higLrIR1be5XO1NDNQfLcpXXJeBQ1QS:k/sTDSWeR40iopgN
Trid	50,Generic Win/DOS Executable,49.9,DOS Executable Generic

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x382e46	0x383000	6.32802571885	f8420cfb624dba4eb2f1263a1449f424
.rdata	0x384000	0xaa38c	0xaa400	4.44528259342	27014900f970bc2364eaa27b58c631e5
.data	0x42f000	0x58964	0x2600	3.83873403477	8396227833b407d4d8d68b8fbb521511
.pdata	0x488000	0x11658	0x11800	6.00222506727	fcf5b48fd38384248c5574f2863adf85
.00cfg	0x49a000	0x10	0x200	0.195869406087	97ca51b21043dd52f3560b11bacdd3c6
.tls	0x49b000	0x41	0x200	0.0203931352361	1f354d76203061bfdd5a53dae48d5435
.rsrc	0x49c000	0x4d8	0x600	2.8172003938	d247656c631ec84c94d4d7389eaf9116
.reloc	0x49d000	0x58f0	0x5a00	5.43587996641	73df05e7bb04965dfc4f5c3784ecf76f

PE Imports

- KERNEL32.dll
  - AcquireSRWLockExclusive
  - CloseHandle
  - CompareStringW
  - ConvertFiberToThread
  - ConvertThreadToFiberEx
  - CreateEventW

- CreateFiberEx
- CreateFileW
- CreateRemoteThreadEx
- CreateThread
- DeleteCriticalSection
- DeleteFiber
- DeleteFileW
- DeleteProcThreadAttributeList
- EncodePointer
- EnterCriticalSection
- EnumSystemLocalesW
- ExitProcess
- ExitThread
- FindClose
- FindFirstFileExW
- FindNextFileW
- FlsAlloc
- FlsSetValue
- FlushFileBuffers
- FlushInstructionCache
- FreeEnvironmentStringsW
- FreeLibrary
- FreeLibraryAndExitThread
- GetACP
- GetCPInfo
- GetCommandLineA
- GetCommandLineW
- GetConsoleMode
- GetConsoleOutputCP
- GetConsoleScreenBufferInfo
- GetCurrentDirectoryW
- GetCurrentProcess
- GetCurrentProcessId
- GetCurrentThread
- GetCurrentThreadId
- GetDateFormatW
- GetEnvironmentStringsW

GetFileAttributesW

GetFileInformationByHandle

GetFileSizeEx

GetFileType

GetLastError

GetLocaleInfoW

GetLogicalProcessorInformationEx

GetModuleFileNameW

GetModuleHandleA

GetModuleHandleExW

GetModuleHandleW

GetOEMCP

GetProcAddress

GetProcessHeap

GetStartupInfoW

GetStdHandle

GetStringTypeW

GetSystemInfo

GetSystemTimeAsFileTime

GetTimeFormatW

GetTimeZoneInformation

GetUserDefaultLCID

HeapAlloc

HeapFree

HeapReAlloc

HeapSize

InitializeCriticalSection

InitializeCriticalSectionAndSpinCount

InitializeProcThreadAttributeList

InitializeSListHead

InterlockedFlushSList

IsDebuggerPresent

IsProcessorFeaturePresent

IsValidCodePage

IsValidLocale

LCMapStringW

LeaveCriticalSection

- LoadLibraryExW
- MultiByteToWideChar
- OutputDebugStringA
- QueryPerformanceCounter
- QueryPerformanceFrequency
- RaiseException
- ReadConsoleW
- ReadFile
- ReleaseSRWLockExclusive
- RemoveDirectoryW
- ResetEvent
- RtlCaptureContext
- RtlLookupFunctionEntry
- RtlPcToFileHeader
- RtlUnwind
- RtlUnwindEx
- RtlVirtualUnwind
- SetConsoleTextAttribute
- SetEnvironmentVariableW
- SetEvent
- SetFilePointerEx
- SetLastError
- SetStdHandle
- SetUnhandledExceptionFilter
- SleepConditionVariableSRW
- SwitchToFiber
- SwitchToThread
- TerminateProcess
- TlsAlloc
- TlsFree
- TlsGetValue
- TlsSetValue
- TryAcquireSRWLockExclusive
- UnhandledExceptionFilter
- UpdateProcThreadAttribute
- VerSetConditionMask
- VerifyVersionInfoW

- VirtualAlloc
- VirtualFree
- VirtualProtect
- WaitForSingleObject
- WaitForSingleObjectEx
- WakeAllConditionVariable
- WakeConditionVariable
- WideCharToMultiByte
- WriteConsoleW
- WriteFile

USER32.dll

- GetClientRect
- GetDC
- IsWindow
- ReleaseDC

GDI32.dll

- CreateCompatibleDC
- CreateDIBSection
- DeleteDC
- DeleteObject
- GetObjectA
- SelectObject
- StretchBlt

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
- vkCreateEvent
- vkCreateFence
- vkCreateFramebuffer
- vkCreateGraphicsPipelines
- vkCreateImage
- vkCreateImageView
- vkCreateInstance
- vkCreatePipelineCache
- vkCreatePipelineLayout
- vkCreateQueryPool
- vkCreateRenderPass
- vkCreateRenderPass2
- vkCreateSampler
- vkCreateSamplerYcbcrConversion
- vkCreateSemaphore
- vkCreateShaderModule
- 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
- vkGetEventStatus
- vkGetFenceStatus
- vkGetImageMemoryRequirements
- vkGetImageMemoryRequirements2
- vkGetImageSparseMemoryRequirements
- vkGetImageSparseMemoryRequirements2
- vkGetImageSubresourceLayout
- vkGetInstanceProcAddr
- vkGetPhysicalDeviceExternalBufferProperties
- vkGetPhysicalDeviceExternalFenceProperties
- vkGetPhysicalDeviceExternalSemaphoreProperties
- vkGetPhysicalDeviceFeatures
- vkGetPhysicalDeviceFeatures2
- vkGetPhysicalDeviceFormatProperties

- vkGetPhysicalDeviceFormatProperties2
- vkGetPhysicalDeviceImageFormatProperties
- vkGetPhysicalDeviceImageFormatProperties2
- vkGetPhysicalDeviceMemoryProperties
- vkGetPhysicalDeviceMemoryProperties2
- vkGetPhysicalDevicePresentRectanglesKHR
- vkGetPhysicalDeviceProperties
- vkGetPhysicalDeviceProperties2
- vkGetPhysicalDeviceQueueFamilyProperties
- vkGetPhysicalDeviceQueueFamilyProperties2
- vkGetPhysicalDeviceSparseImageFormatProperties
- vkGetPhysicalDeviceSparseImageFormatProperties2
- vkGetPhysicalDeviceSurfaceCapabilitiesKHR
- 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
- vk_icdGetInstanceProcAddr
- vk_icdNegotiateLoaderICDInterfaceVersion

PE Resources

[object Object]
[object Object]