VALKYRIE

CLEAN
Valkyrie Final Verdict

File Name: aticfx32.dll
File Type: PE32 executable (DLL) (console) Intel 80386, for MS Windows
SHA1: e0c73487574e6ef597ebae9f5efc624e817b3a11
MD5: e40cae13b087b71da3676caf912fe67c
First Seen Date: 2016-11-20 19:53:03 UTC
Number of Clients Seen: 4
Last Analysis Date: 2016-11-20 19:53:03 UTC
Human Expert Analysis Date: 2016-11-21 02:37:39 UTC
Human Expert Analysis Result: Clean
Verdict Source: Valkyrie Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT	
Signature Based Detection	2016-11-20 19:53:03 UTC	Clean	
Static Analysis Overall Verdict	2016-11-20 19:53:03 UTC	No Threat Found	
Dynamic Analysis Overall Verdict	2016-11-20 19:53:03 UTC	No Threat Found	
Human Expert Analysis Overall Verdict	2016-11-21 02:37:39 UTC	Clean	
File Certificate Validation		Certificate and Vendor name are Not Valid	

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	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!	Clean	
Enrty point is outside the 1st(.code) section! Binary is possibly packed	Clean	
Optional Header NumberOfRvaAndSizes field is valued illegal	Clean	
Anti-vm present	Suspicious	
The Size Of Raw data is valued illegal! Binary might crash your disassembler/debugger	Clean	
TLS callback functions array detected	Clean	

Dynamic Analysis

DYNAMIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	

SUSPICIOUS BEHAVIORS
Has no visible windows

Behavioral Information

QueryFilePath

C:\DLL_Loader.exe

Precise Detectors Analysis Results

No Detector Result Received

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Human Expert Analysis Results

Analysis Start Date: 2016-11-21 00:43:39 UTC
Analysis End Date: 2016-11-21 02:37:39 UTC
File Upload Date: 2016-11-20 19:53:03 UTC
Human Expert Analyst Feedback: Safe
Verdict: Clean

Additional File Information

Vendor Validation - Not Verified ✖

[+] AMD PMP-PE CB Code Signer v20150413

Status	Not Valid ✖

Certificate Validation - ChainBuildFailed ✖

[+] AMD PMP-PE CB Code Signer v20150413

Status	NotTimeValid ✖
Start Date	2015-04-13 16:19:24+00:00
End Date	2016-04-13 16:29:24+00:00
Sha256	c06c47ca3425726d6c4ddbae5bed0d3d5f0a61fc113047eaa9f29ec9978aee9e
Serial	611E56D8000500000044
Subject Name	AMD PMP-PE CB Code Signer v20150413
Subject Key Identifier	ef 22 7e 8b 07 4f ae 55 f6 4a d2 18 a0 a6 91 e3 79 74 76 56
Issuer Name	AMD PVP Certificate Authority v1
Issuer Key Identifier	ff b4 87 9f 9a eb 64 12 68 11 1b 00 87 6e ae e7 2f fd ed ad
Issuer Country	amd
Crl link	undefined
Key Usage	Digital Signature,Non-Repudiation (c0)
Extended Usage	Unknown Key Usage (1.3.6.1.4.1.311.10.5.3)

[+] Symantec Time Stamping Services CA - G2

Status	NoError ✔
Start Date	2012-12-21 00:00:00+00:00
End Date	2020-12-30 23:59:59+00:00
Sha256	0b44526ab89f4778858bf831045ec218d0d57734caa10208ea3d8c90c1043266
Serial	7E93EBFB7CC64E59EA4B9A77D406FC3B
Subject Name	Symantec Time Stamping Services CA - G2
Subject Key Identifier	5f 9a f5 6e 5c cc cc 74 9a d4 dd 7d ef 3f db ec 4c 80 2e dd
Subject Organization	Symantec Corporation
Subject Country	US
Issuer Name	Thawte Timestamping CA
Issuer Key Identifier	undefined
Issuer Organization	Thawte
Issuer Locality	Durbanville
Issuer State	Western Cape
Issuer Country	ZA
Issuer Organizational Unit	Thawte Certification
Crl link	http://crl.thawte.com/ThawteTimestampingCA.crl
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	Time Stamping (1.3.6.1.5.5.7.3.8)

[+] Thawte Timestamping CA

Status	NoError ✔
Start Date	1997-01-01 00:00:00+00:00
End Date	2020-12-31 23:59:59+00:00
Sha256	f429a67538b1053ebe3ad5587247d3a6845a82b3e687e079263181f53dbe26d7
Serial	00
Subject Name	Thawte Timestamping CA
Subject Key Identifier	undefined
Subject Organization	Thawte
Subject Locality	Durbanville
Subject State	Western Cape
Subject Country	ZA
Subject Organizational Unit	Thawte Certification
Issuer Name	Thawte Timestamping CA
Issuer Key Identifier	undefined
Issuer Organization	Thawte
Issuer Locality	Durbanville
Issuer State	Western Cape
Issuer Country	ZA
Issuer Organizational Unit	Thawte Certification
Crl link	undefined
Key Usage	undefined
Extended Usage	undefined

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x55D4B4C1 [Wed Aug 19 16:54:25 2015 UTC]
Entry Point	0x1009fc03 (.text)
File Size	1222488
Machine Type	Intel 386 or later - 32Bit
Legal Copyright	Copyright (C) 1998-2012 AMD Inc.
Internal Name	aticfx32.dll
File Version	8.17.10.1404
Company Name	Advanced Micro Devices, Inc.
Build Version	1404.0
Private Build	Built by swtools on CNABDE06 on 08/19/15 at 12:54
Legal Trademarks	Radeon (TM) is a Trademark of AMD Inc.
Product Name	AMD Inc. Radeon DirectX 11 Driver
Interface Version	UMDKMDIF_VERSION
Special Build	DevStudio Build
Product Version	8.17.10.1404
File Description	aticfx32.dll
Original Filename	aticfx32.dll
Description	Radeon Windows 7 Direct3D 11 Driver
Translation	0x0409 0x04e4
Mime Type	application/x-dosexec
Number Of Sections	5
Sha256	259d907fce5db6f8ee7f7acd7ec110bd11aef96c990d6d620870c20f043f18bd

File Paths

FILE PATH ON CLIENT	SEEN COUNT
e0c73487574e6ef597ebae9f5efc624e817b3a11	1

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0xaea46	0xaec00	6.287549	-
.rdata	0xb0000	0x59957	0x59a00	4.987627	-
.data	0x10a000	0x6118	0x4000	3.371871	-
.rsrc	0x111000	0xb8c8	0xba00	3.756329	-
.reloc	0x11d000	0x9ee4	0xa000	5.580914	-

PE Imports

- KERNEL32.dll
  - EnterCriticalSection
  - WaitForMultipleObjects
  - HeapAlloc
  - HeapFree
  - HeapDestroy
  - HeapCreate

- VirtualProtect
- FreeLibrary
- GetProcAddress
- GetModuleHandleA
- LoadLibraryExA
- GetEnvironmentVariableW
- VerSetConditionMask
- GetCurrentProcess
- VirtualFree
- GetModuleFileNameW
- VerifyVersionInfoW
- GetLastError
- GetProcessAffinityMask
- WaitForSingleObject
- LeaveCriticalSection
- CreateEventA
- GetExitCodeThread
- GetCurrentThreadId
- CloseHandle
- TlsGetValue
- TlsSetValue
- TlsAlloc
- TlsFree
- Process32FirstW
- Process32NextW
- CreateToolhelp32Snapshot
- GetCurrentProcessId
- WideCharToMultiByte
- MultiByteToWideChar
- GetModuleHandleExA
- CreateFileW
- FlushFileBuffers
- DeleteCriticalSection
- QueryPerformanceFrequency
- CreateTimerQueueTimer
- Sleep
- InitializeCriticalSection

- SetEvent
- WriteConsoleW
- SetStdHandle
- HeapSize
- RaiseException
- SetFilePointerEx
- GetConsoleMode
- GetConsoleCP
- GetCommandLineA
- EncodePointer
- DecodePointer
- CreateThread
- ExitThread
- LoadLibraryExW
- GetSystemTimeAsFileTime
- SetLastError
- InterlockedIncrement
- InterlockedDecrement
- ExitProcess
- GetModuleHandleExW
- GetProcessHeap
- GetStdHandle
- GetFileType
- InitializeCriticalSectionAndSpinCount
- InitOnceExecuteOnce
- GetStartupInfoW
- GetModuleFileNameA
- GetTickCount64
- GetEnvironmentStringsW
- FreeEnvironmentStringsW
- UnhandledExceptionFilter
- SetUnhandledExceptionFilter
- FlsAlloc
- FlsGetValue
- FlsSetValue
- FlsFree
- TerminateProcess

- GetModuleHandleW
- WriteFile
- IsProcessorFeaturePresent
- IsDebuggerPresent
- IsValidCodePage
- GetACP
- GetOEMCP
- GetCPInfo
- GetStringTypeW
- RtlUnwind
- HeapReAlloc
- OutputDebugStringW
- LoadLibraryW
- LCMapStringEx
- QueryPerformanceCounter

USER32.dll

- GetMonitorInfoA
- EnumDisplayDevicesA

ADVAPI32.dll

- RegQueryValueExA
- RegCloseKey
- RegEnumValueA
- RegQueryInfoKeyA
- RegOpenKeyExA
- RegEnumKeyExA

VERSION.dll

- GetFileVersionInfoSizeW
- VerQueryValueW
- GetFileVersionInfoW

WINMM.dll

- timeBeginPeriod
- timeGetDevCaps
- timeEndPeriod

PE Exports

- AmdExtRequestMgpuAppControl
- AmdQueryPowerXpressDeviceInfo

AmdQueryPowerXpressDeviceInfoEx

DllMain

OpenAdapter

OpenAdapter10

OpenAdapter10_2

PE Resources

RT_MESSAGETABLE
RT_VERSION