VALKYRIE COMODO

Summary

File Name: aticfx64.dll

File Type: PE32+ executable (DLL) (console) x86-64, for MS Windows

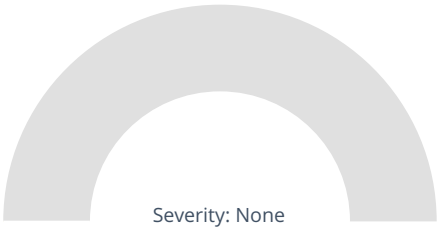
SHA1: 28667d3cd6998c07571cad33ba1dbade6f6ff9a6

MD5: eca1a5b8cb5fd7a969d5dd96c75896e0

CLEAN

Valkyrie Final Verdict

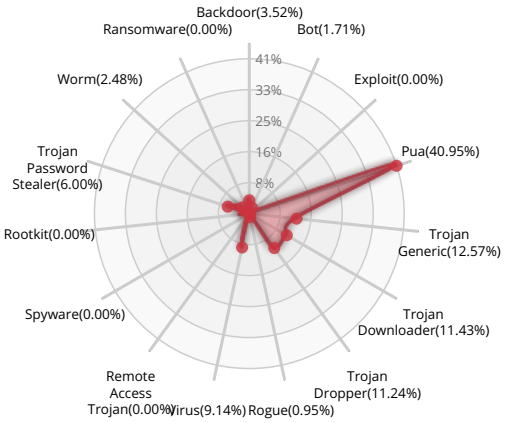
DETECTION SECTION



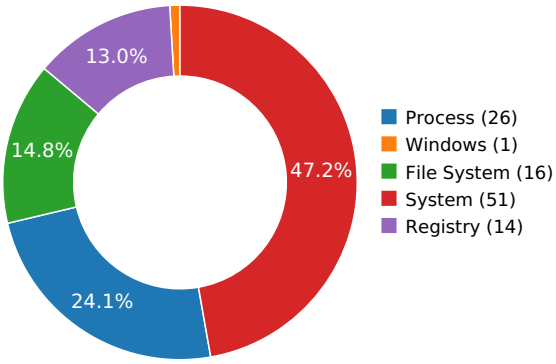
Severity: None

Verdict: Clean

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

Malware Analysis System Evasion 1 (100.00%)

VALKYRIE COMODO

Activity Details

MALWARE ANALYSIS SYSTEM EVASION

Possible date expiration check, exits too soon after checking local time Show sources

VALKYRIE COMODO

Behavior Graph

12:57:49 **12:57:49** **12:57:49**

PID 2560

12:57:49	Create Process	The malicious file created a child process as rundll32.exe **(PPID 1640)**

12:57:49	NtTerminateProcess

Behavior Summary

ACCESSED FILES

C:\Users\user\AppData\Local\Temp\28667d3cd6998c07571cad33ba1dbade6f6ff9a6.dll
C:\Users\user\AppData\Local\Temp\28667d3cd6998c07571cad33ba1dbade6f6ff9a6.dll.123.Manifest
C:\Users\user\AppData\Local\Temp\28667d3cd6998c07571cad33ba1dbade6f6ff9a6.dll.124.Manifest
C:\Users\user\AppData\Local\Temp\28667d3cd6998c07571cad33ba1dbade6f6ff9a6.dll.2.Manifest
C:\Windows\sysnative\rundll32.exe
C:\Users\user\AppData\Local\Temp\VERSION.dll
C:\Windows\sysnative\version.dll
C:\Users\user\AppData\Local\Temp\WINMM.dll
C:\Windows\sysnative\winmm.dll

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles

RESOLVED APIS

28667d3cd6998c07571cad33ba1dbade6f6ff9a6.dll.DllMain
uxtheme.dll.ThemeInitApiHook
user32.dll.IsProcessDPIAware
dwmapi.dll.DwmIsCompositionEnabled

REGISTRY KEYS

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\CustomLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\ExtendedLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\GRE_Initialize
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles

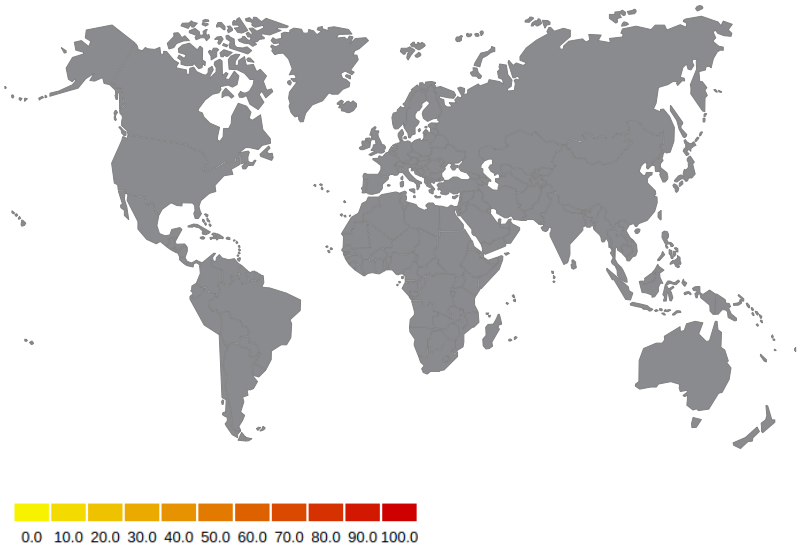
READ FILES

C:\Users\user\AppData\Local\Temp\28667d3cd6998c07571cad33ba1dbade6f6ff9a6.dll

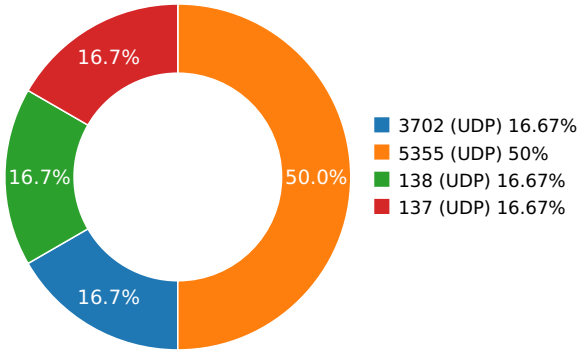
C:\Users\user\AppData\Local\Temp\28667d3cd6998c07571cad33ba1dbade6f6ff9a6.dll.123.Manifest
C:\Users\user\AppData\Local\Temp\28667d3cd6998c07571cad33ba1dbade6f6ff9a6.dll.124.Manifest
C:\Users\user\AppData\Local\Temp\28667d3cd6998c07571cad33ba1dbade6f6ff9a6.dll.2.Manifest
C:\Windows\sysnative\rundll32.exe
C:\Windows\sysnative\version.dll
C:\Windows\sysnative\winmm.dll

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.07235097885	Sandbox	224.0.0.252	5355
3.0977139473	Sandbox	224.0.0.252	5355
3.10285186768	Sandbox	239.255.255.250	3702
3.12872982025	Sandbox	192.168.56.255	137
5.67649579048	Sandbox	224.0.0.252	5355
6.67697095871	Sandbox	192.168.56.255	138

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	aticfx64.dll
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
SHA1:	28667d3cd6998c07571cad33ba1dbade6f6ff9a6
MD5:	eca1a5b8cb5fd7a969d5dd96c75896e0
First Seen Date:	2018-03-06 08:20:59.816225 (12 months ago)
Number Of Clients Seen:	2
Last Analysis Date:	2018-03-06 08:20:59.816225 (12 months ago)
Human Expert Analysis Result:	No human expert analysis verdict given to this sample yet.

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	22
File Type Enum	7
Debug Artifacts	[{u'Path': u'c:\\workarea\\15.301.1901\\drivers\\cfx\\build\\wNow64a\\dll\\B_rel\\aticfx64.pdb\x00', u'GUID': u'{b2ce9313-db63-4ec4-98bc-f24d4b219a96}', u'timestamp': u'2016-02-26 20:13:47'}]
Number Of Sections	6
Trid	[[87.3, u'Win64 Executable (generic)'], [6.3, u'Generic Win/DOS Executable'], [6.3, u'DOS Executable Generic']]
Compilation Time Stamp	0x56D0B1FB [Fri Feb 26 20:13:47 2016 UTC]
LegalCopyright	Copyright (C) 1998-2012 AMD Inc.
InternalName	aticfx64.dll
FileVersion	8.17.10.1433
CompanyName	Advanced Micro Devices, Inc.
Build Version	1433.0
PrivateBuild	Built by swtools on CNABDE05 on 02/26/16 at 15:13
LegalTrademarks	Radeon (TM) is a Trademark of AMD Inc.
ProductName	AMD Inc. Radeon DirectX 11 Driver
Interface Version	UMDKMDIF_VERSION
SpecialBuild	DevStudio Build
ProductVersion	8.17.10.1433
FileDescription	aticfx64.dll
OriginalFilename	aticfx64.dll
Description	Radeon Windows 7 Direct3D 11 Driver
Translation	0x0409 0x04e4
Entry Point	0x1800c78b0 (.text)
Machine Type	AMD64 only, not Itaniums, with 0200 - 64 bit
File Size	1528688
Ssdeep	24576:iayJfImx1kDaXWfnOFi1hgbSh2Zkw0oH:iZJvx+mXWfnOI12bTp0o
Sha256	df86c633e669dc13df61cc3375cee2fd401d46ba838bb6281606e9b1337e1ddd
Exifinfo	[{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'EXE:PrivateBuild': u'Built by swtools on CNABDE05 on 02/26/16 at 15:13', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/2/8/6/6/28667d3cd6998c07571cad33ba1dbade6f6ff9a6', u'EXE:OriginalFileName': u'aticfx64.dll', u'EXE:ProductName': u'AMD Inc. Radeon DirectX 11 Driver', u'EXE:InternalName': u'aticfx64.dll', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2018:03:06 08:20:30+00:00', u'EXE:InitializedDataSize': 605184, u'File:FileModifyDate': u'2018:03:06 08:20:30+00:00', u'EXE:InterfaceVersion': u'UMDKMDIF_VERSION', u'EXE:FileVersionNumber': u'8.17.10.1433', u'EXE:FileVersion': u'8.17.10.1433', u'File:FileSize': u'1493 kB', u'EXE:CharacterSet': u'Windows, Latin1', u'EXE:MachineType': u'AMD AMD64',

PROPERTY	VALUE
	u'EXE:FileOS': u'Windows NT 32-bit', u'EXE:LegalTrademarks': u'Radeon (TM) is a Trademark of AMD Inc.', u'EXE:ProductVersion': u'8.17.10.1433', u'EXE:ObjectFileType': u'Dynamic link library', u'EXE:SpecialBuild': u'DevStudio Build', u'File:FileType': u'Win64 DLL', u'EXE:CompanyName': u'Advanced Micro Devices, Inc. ', u'File:FileName': u'28667d3cd6998c07571cad33ba1dbade6f6ff9a6', u'EXE:Description': u'Radeon Windows 7 Direct3D 11 Driver', u'File:FileTypeExtension': u'dll', u'EXE:OSVersion': 6.0, u'EXE:PEType': u'PE32+', u'EXE:TimeStamp': u'2016:02:26 20:13:47+00:00', u'EXE:FileFlagsMask': u'0x0000', u'EXE:LegalCopyright': u'Copyright (C) 1998-2012 AMD Inc.', u'EXE:LinkerVersion': 11.0, u'EXE:FileFlags': u'Special build', u'EXE:Subsystem': u'Windows command line', u'File:Directory': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/2/8/6/6', u'EXE:FileDescription': u'aticfx64.dll', u'EXE:EntryPoint': u'0xc78b0', u'EXE:SubsystemVersion': 6.0, u'EXE:CodeSize': 895488, u'EXE:BuildVersion': 1433.0, u'File:FileInodeChangeDate': u'2018:03:06 08:20:30+00:00', u'EXE:UninitializedDataSize': 0, u'EXE:LanguageCode': u'English (U.S.)', u'ExifTool:ExifToolVersion': 10.1, u'EXE:ImageVersion': 0.0, u'EXE:ProductVersionNumber': u'8.17.10.1433'}]
Mime Type	application/x-dosexec
Imphash	ef0bd28390e4fd97080fa981fd04aabc

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0xda8c7	0xdaa00	6.16286018051	62bdb429f685b59a6dc2fdb1c9aa0a8e
.rdata	0xdc000	0x6b577	0x6b600	5.05290489504	a1a3481c4d10cda22f2e9d0b6b8d21a2
.data	0x148000	0x9ea8	0x7800	1.45376840731	5a01f54918dfd2b6afece51aee536833
.pdata	0x152000	0xf9d8	0xfa00	6.0698653099	82985e3bb855530c4c1c49d6d32f768a
.rsrc	0x162000	0xba78	0xbc00	3.75724218486	3039f083d6d1758ab337b1a33c3be8c3
.reloc	0x16e000	0x2efe	0x3000	4.07807393046	19675f575ac6420c2c87d3f9d5d2c538

PE Imports

- KERNEL32.dll
  - CreateTimerQueueTimer
  - QueryPerformanceFrequency
  - DeleteCriticalSection
  - LeaveCriticalSection
  - EnterCriticalSection
  - WaitForMultipleObjects
  - HeapAlloc
  - HeapFree
  - HeapDestroy
  - HeapCreate
  - GetEnvironmentVariableW
  - VerSetConditionMask
  - GetCurrentProcess
  - VirtualFree
  - GetModuleFileNameW
  - VerifyVersionInfoW
  - GetLastError
  - GetProcessAffinityMask
  - FreeLibrary
  - LoadLibraryExA
  - Sleep
  - SetEvent
  - CreateEventA
  - GetExitCodeThread
  - GetCurrentThreadId
  - CloseHandle
  - TlsGetValue
  - TlsSetValue
  - TlsAlloc
  - TlsFree
  - Process32FirstW
  - Process32NextW
  - CreateToolhelp32Snapshot
  - GetCurrentProcessId
  - MultiByteToWideChar

    - CreateFileW
    - FlushFileBuffers
    - WriteConsoleW
    - InitializeCriticalSection
    - QueryPerformanceCounter
    - GetModuleHandleA
    - GetProcAddress
    - WideCharToMultiByte
    - WaitForSingleObject
    - GetModuleHandleExA
    - SetStdHandle
    - HeapSize
    - SetFilePointerEx
    - GetConsoleMode
    - GetConsoleCP
    - RaiseException
    - GetCommandLineA
    - EncodePointer
    - DecodePointer
    - CreateThread
    - ExitThread
    - LoadLibraryExW
    - GetSystemTimeAsFileTime
    - SetLastError
    - ExitProcess
    - GetModuleHandleExW
    - GetProcessHeap
    - GetStdHandle
    - GetFileType
    - InitializeCriticalSectionAndSpinCount
    - InitOnceExecuteOnce
    - GetStartupInfoW
    - GetModuleFileNameA
    - GetTickCount64
    - GetEnvironmentStringsW
    - FreeEnvironmentStringsW
    - RtlCaptureContext
    - RtlLookupFunctionEntry
    - RtlVirtualUnwind
    - UnhandledExceptionFilter
    - SetUnhandledExceptionFilter
    - FlsAlloc
    - FlsGetValue
    - FlsSetValue
    - FlsFree
    - TerminateProcess
    - GetModuleHandleW
    - RtlUnwindEx
    - WriteFile
    - IsProcessorFeaturePresent
    - IsDebuggerPresent
    - IsValidCodePage
    - GetACP
    - GetOEMCP
    - GetCPInfo
    - GetStringTypeW
    - HeapReAlloc
    - OutputDebugStringW
    - LoadLibraryW
    - LCMapStringEx
- USER32.dll
    - GetMonitorInfoA
    - EnumDisplayDevicesA
- ADVAPI32.dll
    - RegQueryInfoKeyA
    - RegEnumKeyExA
    - RegCloseKey
    - RegOpenKeyExA
    - RegQueryValueExA
    - RegEnumValueA
- VERSION.dll
    - GetFileVersionInfoSizeW
    - VerQueryValueW
    - GetFileVersionInfoW
- WINMM.dll

- timeBeginPeriod
- timeGetDevCaps
- timeEndPeriod

PE Exports

- AmdExtRequestMgpuAppControl
- AmdQueryPowerXpressDeviceInfo
- AmdQueryPowerXpressDeviceInfoEx
- DllMain
- OpenAdapter
- OpenAdapter10
- OpenAdapter10_2

PE Resources

{u'lang': u'LANG_ENGLISH', u'name': u'WEVT_TEMPLATE', u'offset': 1471552, u'sha256': u'e7c22a95190a236036d577b2b0963ec841cd2bbc490b6233910c3e10a3369cd3', u'type': u'data', u'size': 24770}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_MESSAGETABLE', u'offset': 1450256, u'sha256': u'59663b09fe652d6931504732c19072bd8960456668c9cc5582751c5f05c32f53', u'type': u'Hitachi SH big-endian COFF object, not stripped', u'size': 21296}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_VERSION', u'offset': 1496328, u'sha256': u'9c728bac389dee66eaac9f622fe9a88f7844a8f29e1e98a010b0d87cf63f3a0d', u'type': u'data', u'size': 1388}

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 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
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 Key Identifier	5f 9a f5 6e 5c cc cc 74 9a d4 dd 7d ef 3f db ec 4c 80 2e dd
Issuer Name	Thawte Timestamping CA
Issuer Key Identifier	undefined
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 Key Identifier	undefined
Issuer Name	Thawte Timestamping CA
Issuer Key Identifier	undefined
Crl link	undefined
Key Usage	undefined
Extended Usage	undefined

SCREENSHOTS