VALKYRIE COMODO

Summary

File Name: KHYnZx4nz.zk

File Type: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows

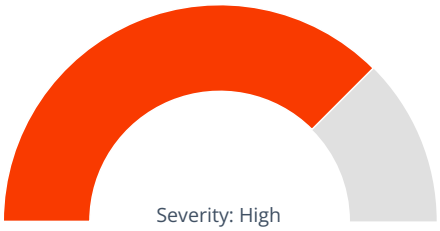
SHA1: f8b5c98e21b2a05fd83ba772091a2ed8bbf1bc12

MD5: a88491a1e76fd8e433adad53bd330d31

MALWARE

Valkyrie Final Verdict

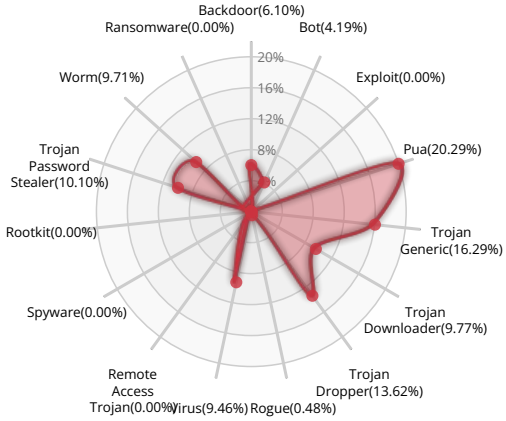
DETECTION SECTION



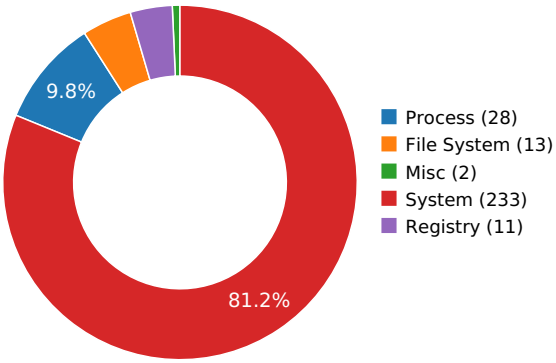
Severity: High

Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

VALKYRIE COMODO

Activity Details

PACKER

The binary likely contains encrypted or compressed data. Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory Show sources

Behavior Graph

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Users\user\AppData\Local\Temp\f8b5c98e21b2a05fd83ba772091a2ed8bbf1bc12.dll
C:\Users\user\AppData\Local\Temp\f8b5c98e21b2a05fd83ba772091a2ed8bbf1bc12.dll.123.Manifest
C:\Users\user\AppData\Local\Temp\f8b5c98e21b2a05fd83ba772091a2ed8bbf1bc12.dll.124.Manifest
C:\Users\user\AppData\Local\Temp\f8b5c98e21b2a05fd83ba772091a2ed8bbf1bc12.dll.2.Manifest
C:\Windows\SysWOW64\rundll32.exe
C:\Users\user\AppData\Local\Temp\msi.dll
C:\Windows\System32\msi.dll

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\FileSystem\Win31FileSystem

RESOLVED APIS

kernel32.dll.GetNativeSystemInfo
kernel32.dll.VirtualAlloc
kernel32.dll.VirtualFree
kernel32.dll.VirtualProtect
kernel32.dll.UnmapViewOfFile
ntdll.dll.RtlCompressBuffer
ntdll.dll.RtlDecompressBuffer
ntdll.dll.RtlZeroMemory
kernel32.dll.FlsFree
kernel32.dll.GetEnvironmentVariableA
kernel32.dll.GetVolumeNameForVolumeMountPointA
kernel32.dll.GetCurrentProcess
kernel32.dll.CreateProcessW
kernel32.dll.InitializeCriticalSection
kernel32.dll.DeleteCriticalSection
kernel32.dll.EnterCriticalSection
kernel32.dll.LeaveCriticalSection
kernel32.dll.GetCurrentThread
kernel32.dll.FindNextFileW
kernel32.dll.GetDiskFreeSpaceExW

kernel32.dll.GetVolumeInformationW
kernel32.dll.GetLogicalDrives
kernel32.dll.GetWindowsDirectoryA
kernel32.dll.InterlockedDecrement
kernel32.dll.GetTickCount
kernel32.dll.LoadLibraryA
kernel32.dll.FreeLibrary
kernel32.dll.GetSystemDirectoryW
kernel32.dll.lstrlenA
kernel32.dll.LoadLibraryW
kernel32.dll.GetLocaleInfoA
kernel32.dll.SetUnhandledExceptionFilter
kernel32.dll.FindClose
kernel32.dll.FindFirstFileW
kernel32.dll.MultiByteToWideChar
kernel32.dll.WideCharToMultiByte
kernel32.dll.DisableThreadLibraryCalls
kernel32.dll.WaitForSingleObject
kernel32.dll.CreateThread
kernel32.dll.Sleep
kernel32.dll.GetUserDefaultLangID
kernel32.dll.GetSystemDefaultLangID
kernel32.dll.SetErrorMode
kernel32.dll.GlobalAddAtomA
kernel32.dll.AddAtomA
kernel32.dll.FindAtomA
kernel32.dll.GlobalFindAtomA
kernel32.dll.OpenMutexA
kernel32.dll.LocalFree
kernel32.dll.CreateEventA
kernel32.dll.MulDiv
kernel32.dll.GetUserDefaultUILanguage
kernel32.dll.GetVersionExA
kernel32.dll.ExitProcess
kernel32.dll.GetModuleFileNameW

kernel32.dll.FlushFileBuffers
kernel32.dll.SetFileTime
kernel32.dll.GetSystemTimeAsFileTime
kernel32.dll.SetFilePointer
kernel32.dll.ReadFile
kernel32.dll.SetFileAttributesW
kernel32.dll.GetLastError
kernel32.dll.GetFileAttributesExW
kernel32.dll.DeleteFileW
kernel32.dll.MoveFileExW
kernel32.dll.WriteFile
kernel32.dll.GetFileSizeEx
kernel32.dll.CreateFileW
kernel32.dll.CloseHandle
kernel32.dll.GetModuleHandleA
kernel32.dll.GetProcAddress
kernel32.dll.GetDriveTypeW
kernel32.dll.RtlUnwind
kernel32.dll.GetCurrentProcessId
kernel32.dll.QueryPerformanceCounter
kernel32.dll.GetEnvironmentStringsW

REGISTRY KEYS

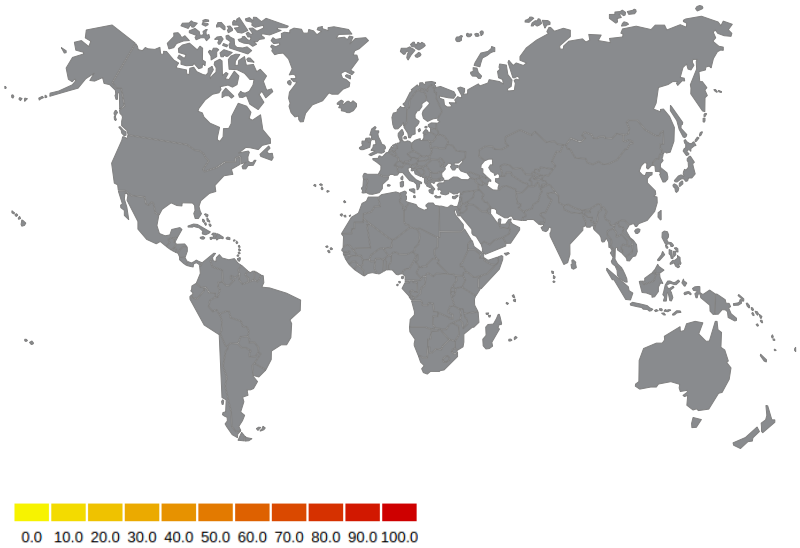
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\FileSystem\Win31FileSystem

READ FILES

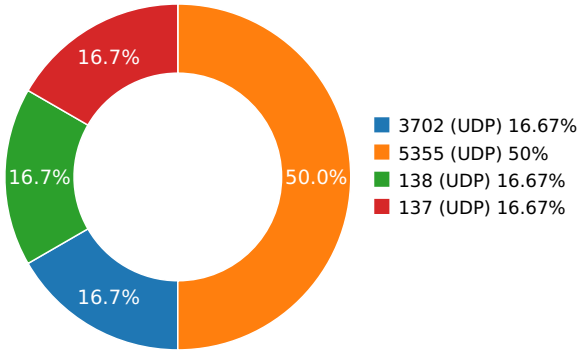
C:\Users\user\AppData\Local\Temp\f8b5c98e21b2a05fd83ba772091a2ed8bbf1bc12.dll
C:\Users\user\AppData\Local\Temp\f8b5c98e21b2a05fd83ba772091a2ed8bbf1bc12.dll.123.Manifest
C:\Users\user\AppData\Local\Temp\f8b5c98e21b2a05fd83ba772091a2ed8bbf1bc12.dll.124.Manifest
C:\Users\user\AppData\Local\Temp\f8b5c98e21b2a05fd83ba772091a2ed8bbf1bc12.dll.2.Manifest
C:\Windows\SysWOW64\rundll32.exe
C:\Windows\System32\msi.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
3.01803588867	Sandbox	224.0.0.252	5355
3.04926609993	Sandbox	224.0.0.252	5355
3.05260205269	Sandbox	239.255.255.250	3702
3.07947707176	Sandbox	192.168.56.255	137
5.61338305473	Sandbox	224.0.0.252	5355
9.07860589027	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:	KHYnZx4nz.zk
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
SHA1:	f8b5c98e21b2a05fd83ba772091a2ed8bbf1bc12
MD5:	a88491a1e76fd8e433adad53bd330d31
First Seen Date:	2016-12-24 09:46:58.745892 (7 years ago)
Number Of Clients Seen:	4
Last Analysis Date:	2016-12-24 09:46:58.745892 (7 years ago)
Human Expert Analysis Date:	2019-12-24 16:58:56.356909 (4 years ago)
Human Expert Analysis Result:	Malware

VALKYRIE COMODO

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Number Of Sections	5
Compilation Time Stamp	0x5848354C [Wed Dec 7 16:14:04 2016 UTC]
LegalCopyright	Copyright \xa9 1999-2013
FileDescription	BASS
FileVersion	2.4.10
CompanyName	Un4seen Developments
Translation	0x0000 0x04b0
Entry Point	0x415d96 (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	187110
Sha256	e407a9b7adba2587150d66ec638a4a9b64d57ac23b320c0f7df02668479c61da
Mime Type	application/x-dosexec

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x22070	0x22200	7.168980[SUSPICIOUS]	-
.rdata	0x24000	0x216d	0x2200	7.009640[SUSPICIOUS]	-
.data	0x27000	0xa240	0x400	4.992754	-
.rsrc	0x32000	0x3570	0x3600	4.109366	-
.reloc	0x36000	0x2dd2	0x2e00	5.884982	-

PE Imports

- KERNEL32.dll
  - CloseHandle
  - GetOEMCP
  - TlsFree
  - GetACP
  - InterlockedDecrement
  - GetEnvironmentStringsW
  - TlsAlloc
  - GetFileSize
  - FlushFileBuffers
  - GetConsoleMode
  - DeleteFileW
  - LCMapStringW
  - IsProcessorFeaturePresent
  - WriteFile
  - LoadLibraryW
  - RaiseException
  - GetModuleFileNameW
  - ExitProcess

    - IsValidCodePage
    - InitializeCriticalSectionAndSpinCount
    - GetCurrentThreadId
    - UnhandledExceptionFilter
    - GetLastError
    - IsDebuggerPresent
    - GetModuleHandleW
    - GetConsoleCP
    - GetLocalTime
    - HeapReAlloc
    - GetCurrentProcessId
    - DeleteCriticalSection
    - RtlUnwind
    - LoadLibraryExW
    - GetModuleFileNameA
    - SetLastError
    - SetUnhandledExceptionFilter
    - EnterCriticalSection
    - LocalFree
    - SetFilePointerEx
    - InterlockedIncrement
    - FreeEnvironmentStringsW
    - GetCPInfo
    - HeapDestroy
    - GetCommandLineA
    - TlsSetValue
    - HeapAlloc
    - GetFileType
    - WriteConsoleW
    - TlsGetValue
    - GetStdHandle
    - GetSystemTimeAsFileTime
    - lstrlenA
    - SetStdHandle
    - OutputDebugStringW
    - WideCharToMultiByte
    - Sleep
    - GetStartupInfoW
    - GetCurrentProcess
    - HeapFree
    - GetStringTypeW
    - MultiByteToWideChar
    - GetProcessHeap
    - QueryPerformanceCounter
    - VirtualQuery
    - FreeLibrary
    - TerminateProcess
    - LeaveCriticalSection
    - GetProcAddress
    - CreateFileW
    - HeapSize
    - GetCommandLineW
- USER32.dll
    - SendMessageA
    - wvsprintfW
    - wsprintfW
    - CharLowerA
- GDI32.dll
    - AbortPath
    - AnimatePalette
    - BeginPath
    - AngleArc
- ole32.dll
    - CoInitializeSecurity
    - CoInitialize
    - CoSetProxyBlanket
    - CoUninitialize
    - CoCreateInstance
- OLEAUT32.dll
    - SysFreeString
    - VariantInit
    - SysAllocString
    - VariantClear
- msvcrt.dll
    - __set_app_type

    - _exit
- msi.dll
    - None

PE Resources

RT_BITMAP
RT_VERSION

CERTIFICATE VALIDATION

- FileNotSigned ✖

SCREENSHOTS