VALKYRIE COMODO

Summary

File Name: peparser.dll

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

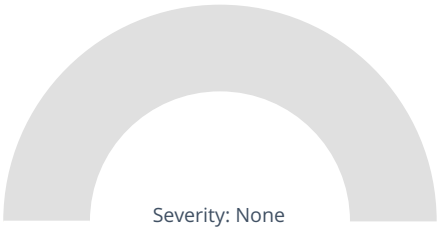
SHA1: 0d25a6b7d964f262355186b0dbd6609fccb1117c

MD5: 6d02aad36a0b84c5fc7d943fe7737f44

CLEAN

Valkyrie Final Verdict

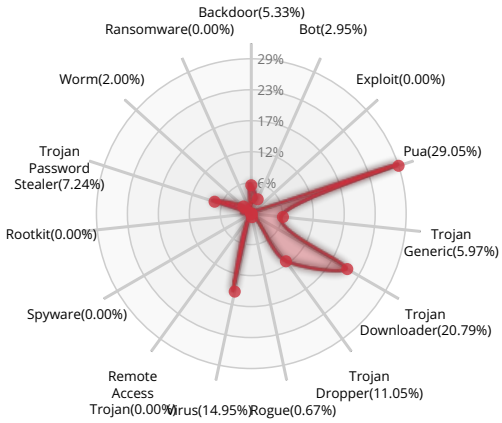
DETECTION SECTION



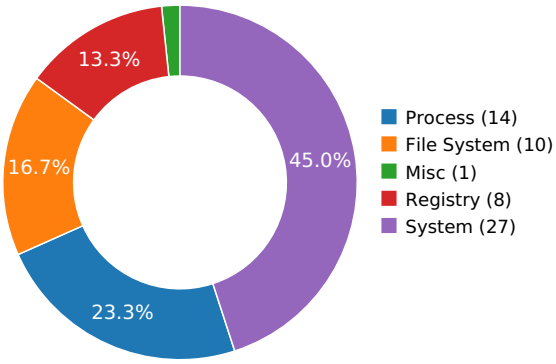
Severity: None

Verdict: Clean

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

VALKYRIE COMODO

Activity Details

STATIC ANOMALY

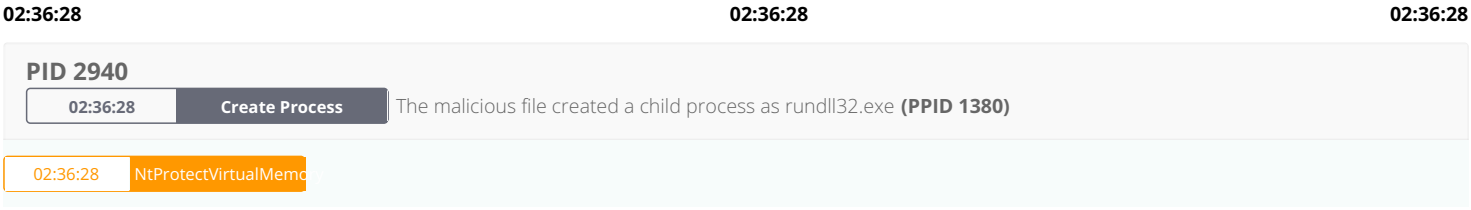
Anomalous binary characteristics Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory Show sources

VALKYRIE COMODO

Behavior Graph



Behavior Summary

ACCESSED FILES

C:\Users\user\AppData\Local\Temp\0d25a6b7d964f262355186b0dbd6609fccb1117c.dll
C:\Users\user\AppData\Local\Temp\0d25a6b7d964f262355186b0dbd6609fccb1117c.dll.123.Manifest
C:\Users\user\AppData\Local\Temp\0d25a6b7d964f262355186b0dbd6609fccb1117c.dll.124.Manifest

RESOLVED APIS

kernel32.dll.FlsAlloc
kernel32.dll.FlsGetValue
kernel32.dll.FlsSetValue
kernel32.dll.FlsFree
kernel32.dll.IsProcessorFeaturePresent

REGISTRY KEYS

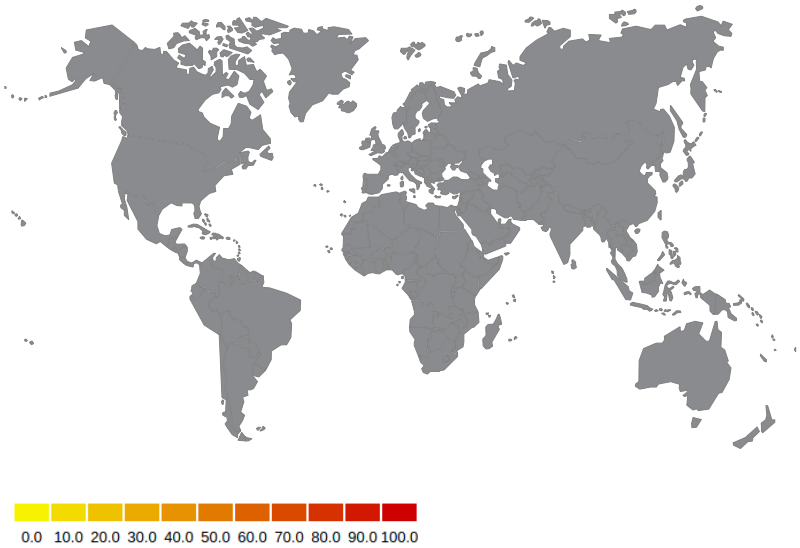
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest

READ FILES

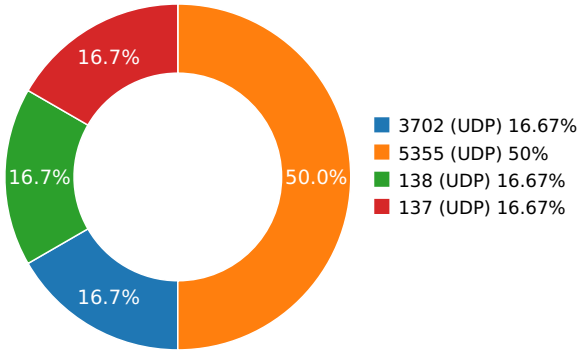
C:\Users\user\AppData\Local\Temp\0d25a6b7d964f262355186b0dbd6609fccb1117c.dll
C:\Users\user\AppData\Local\Temp\0d25a6b7d964f262355186b0dbd6609fccb1117c.dll.123.Manifest
C:\Users\user\AppData\Local\Temp\0d25a6b7d964f262355186b0dbd6609fccb1117c.dll.124.Manifest

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
3.08581185341	Sandbox	224.0.0.252	5355
3.10919880867	Sandbox	224.0.0.252	5355
3.1145298481	Sandbox	239.255.255.250	3702
3.14003181458	Sandbox	192.168.56.255	137
5.67215394974	Sandbox	224.0.0.252	5355
6.15265202522	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:	peparser.dll
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
SHA1:	0d25a6b7d964f262355186b0dbd6609fccb1117c
MD5:	6d02aad36a0b84c5fc7d943fe7737f44
First Seen Date:	2017-05-22 21:12:39.208612 (4 years ago)
Number Of Clients Seen:	2
Last Analysis Date:	2017-05-22 21:12:39.208612 (4 years ago)
Human Expert Analysis Result:	No human expert analysis verdict given to this sample yet.

VALKYRIE COMODO

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Number Of Sections	6
Compilation Time Stamp	0x592042EE [Sat May 20 13:21:50 2017 UTC]
LegalCopyright	Copyright \xa9 2009-2017 Marc Ochsenmeier
InternalName	peparser
FileVersion	8, 60, 0, 0
CompanyName	www.winitor.com
LegalTrademarks	www.winitor.com
Comments	Malware Initial Assessment
ProductName	peparser
ProductVersion	8, 60, 0, 0
FileDescription	Malware Initial Assessment
OriginalFilename	peparser.dll
Translation	0x0000 0x04b0
Entry Point	0x30094740 (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	801792
Sha256	86db6ae7f3a86a5e8e3dba46523e82d55fa1138b811660e5c9c1babc5035013b
Mime Type	application/x-dosexec

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0xa8970	0xa8a00	6.576794	-
.rdata	0xaa000	0xd0b6	0xd200	5.526284	-
.data	0xb8000	0x3cfc	0x1e00	3.816384	-
.bss	0xbc000	0xe95	0x1000	7.954666[SUSPICIOUS]	-
.rsrc	0xbd000	0x5a4	0x600	4.265865	-
.reloc	0xbe000	0xa6de	0xa800	5.405006	-

PE Imports

- KERNEL32.dll
  - OpenProcess
  - DosDateTimeToFileTime
  - FileTimeToSystemTime
  - FreeLibrary

- DeactivateActCtx
- ReleaseActCtx
- CreateActCtxW
- ActivateActCtx
- LoadLibraryExW
- SetUnhandledExceptionFilter
- SetErrorMode
- GetSystemDirectoryW
- GetWindowsDirectoryA
- GetCurrentDirectoryW
- MultiByteToWideChar
- InitializeCriticalSection
- TryEnterCriticalSection
- LeaveCriticalSection
- GetProcAddress
- GetNativeSystemInfo
- TerminateThread
- CreateThread
- Sleep
- FormatMessageW
- CreateFileMappingW
- MapViewOfFile
- WideCharToMultiByte
- InterlockedDecrement
- InterlockedIncrement
- GetSystemTime
- SystemTimeToFileTime
- CompareFileTime
- VerLanguageNameW
- GetConsoleMode
- GetConsoleCP
- SetEnvironmentVariableA
- LoadLibraryA
- GetModuleHandleW
- ReadFile
- CloseHandle
- UnmapViewOfFile
- GetFileSize
- CreateFileW
- GetModuleFileNameW
- GetLastError
- IsBadReadPtr
- DeleteCriticalSection
- ExpandEnvironmentStringsA
- CompareStringW
- CompareStringA
- FlushFileBuffers
- CreateFileA
- WriteConsoleW
- GetConsoleOutputCP
- WriteConsoleA
- SetFilePointer
- InitializeCriticalSectionAndSpinCount
- SetStdHandle
- GetLocaleInfoA
- lstrlenA
- HeapFree
- GetProcessHeap
- TerminateProcess
- GetCurrentProcess
- UnhandledExceptionFilter
- IsDebuggerPresent
- GetCurrentThreadId
- GetCommandLineA
- RaiseException
- RtlUnwind
- HeapAlloc
- GetCPInfo
- GetACP
- GetOEMCP
- IsValidCodePage
- TlsGetValue
- TlsAlloc
- TlsSetValue
- TlsFree

- SetLastError
- LCMapStringA
- LCMapStringW
- WriteFile
- GetStdHandle
- GetModuleFileNameA
- HeapSize
- ExitProcess
- GetTimeZoneInformation
- SetHandleCount
- GetFileType
- GetStartupInfoA
- FreeEnvironmentStringsA
- GetEnvironmentStrings
- FreeEnvironmentStringsW
- GetEnvironmentStringsW
- HeapCreate
- HeapDestroy
- VirtualFree
- QueryPerformanceCounter
- GetTickCount
- GetCurrentProcessId
- GetSystemTimeAsFileTime
- EnterCriticalSection
- VirtualAlloc
- HeapReAlloc
- GetModuleHandleA
- GetStringTypeA
- GetStringTypeW

- USER32.dll
  - PostMessageW
  - SendMessageW
- ADVAPI32.dll
  - CryptDestroyHash
  - CryptGetHashParam
  - CryptAcquireContextW
  - CryptHashData
  - CryptCreateHash
  - RegCloseKey
  - RegQueryValueExA
  - RegOpenKeyExA
  - RegEnumKeyExA
  - RegEnumValueA
- SHELL32.dll
  - ShellExecuteW
- ole32.dll
  - CoUninitialize
  - OleRun
  - CoInitializeEx
  - CoCreateInstance
- OLEAUT32.dll
  - VariantInit
  - VariantCopy
  - VariantClear
  - SysAllocString
  - SysFreeString
  - GetErrorInfo

PE Exports

create

PE Resources

RT_VERSION
RT_MANIFEST

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS