VALKYRIE COMODO

Summary

File Name: Nds.exe

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

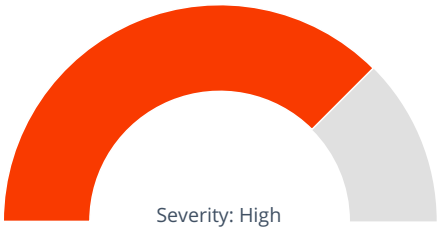
SHA1: 1c70d198f89ecc6aca0b30d6494995175e29d26b

MD5: 1e12a7676dd6c56db832b801aa8a1063

MALWARE

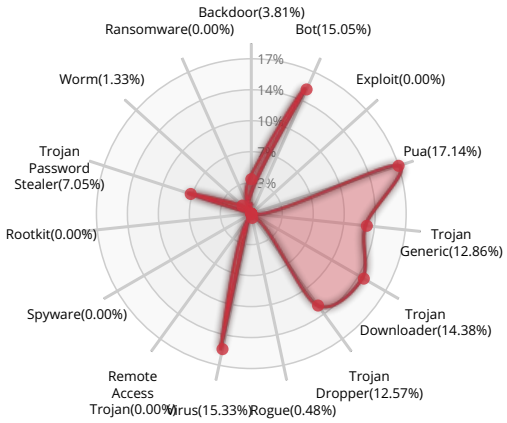
Valkyrie Final Verdict

DETECTION SECTION

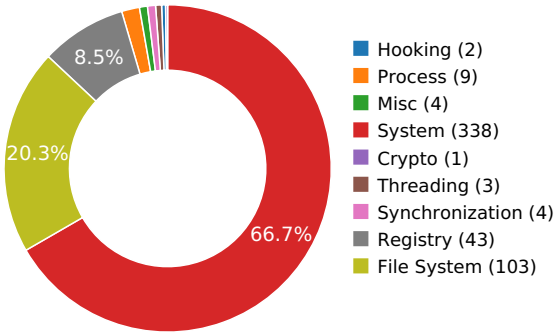


Verdict: Malware

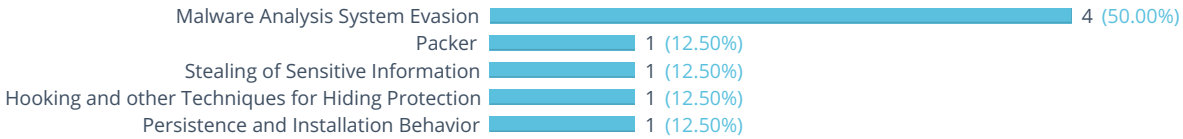
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



VALKYRIE COMODO

Activity Details

PACKER

The binary likely contains encrypted or compressed data. Show sources

STEALING OF SENSITIVE INFORMATION

Collects information to fingerprint the system Show sources

MALWARE ANALYSIS SYSTEM EVASION

Detects Sandboxie through the presence of a library Show sources

Detects Sandboxie using a known mutex Show sources

Checks for a known DeepFreeze Frozen State Mutex Show sources

Attempts to identify installed analysis tools by a known file location Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

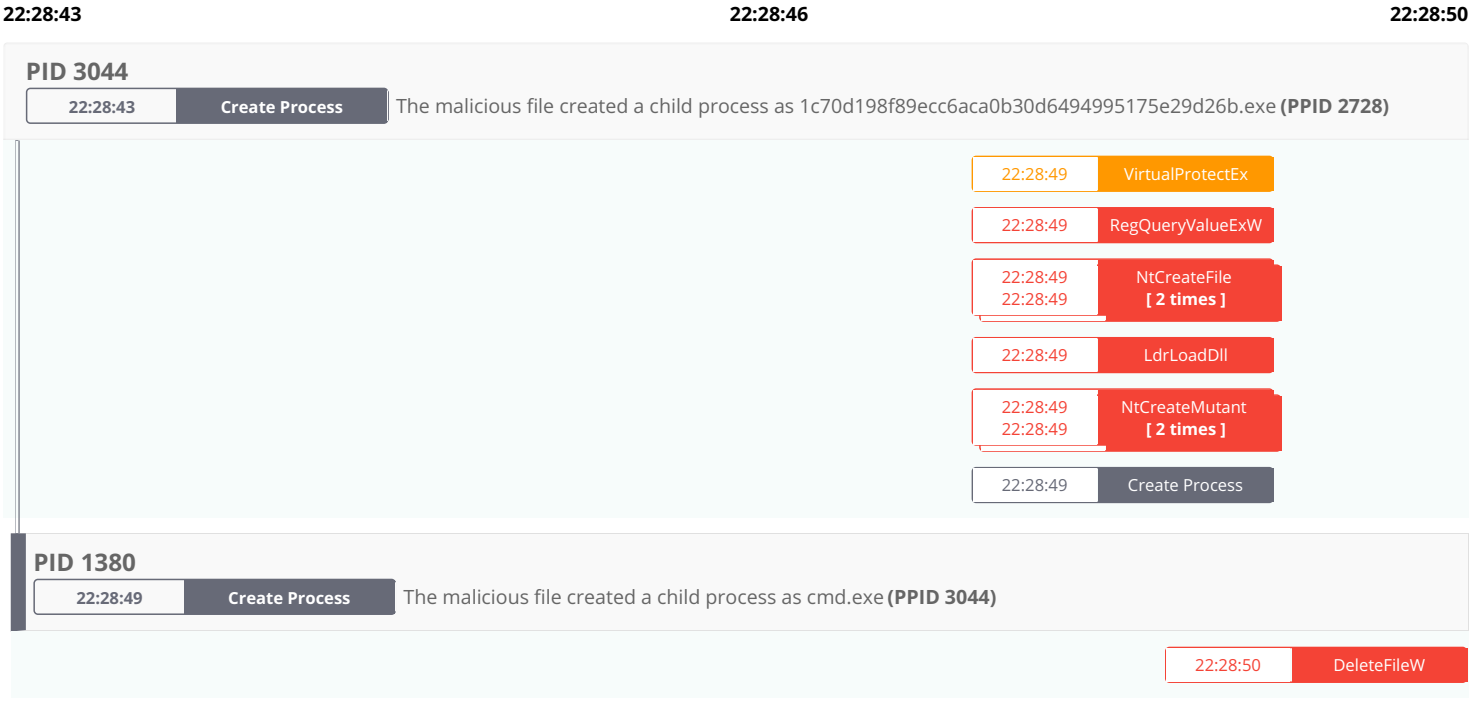
Creates RWX memory Show sources

PERSISTENCE AND INSTALLATION BEHAVIOR

Deletes its original binary from disk Show sources

VALKYRIE COMODO

Behavior Graph



VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Users\user\AppData\Local\Temp\msvcr100.dll
C:\Windows\System32\msvcr100.dll
C:\Windows\system\msvcr100.dll
C:\Windows\msvcr100.dll
C:\ProgramData\Oracle\Java\javapath\msvcr100.dll
C:\Windows\System32\wbem\msvcr100.dll
C:\Windows\System32\WindowsPowerShell\v1.0\msvcr100.dll
C:\Program Files\Microsoft Network Monitor 3\msvcr100.dll
C:\Program Files (x86)\Universal Extractor\msvcr100.dll
C:\Program Files (x86)\Universal Extractor\bin\msvcr100.dll
C:\Program Files (x86)\Windows Kits\8.1\Windows Performance Toolkit\msvcr100.dll
C:\Python27\msvcr100.dll
C:\Python27\Scripts\msvcr100.dll
C:\tools\sysinternals\msvcr100.dll
C:\tools\msvcr100.dll
C:\tools\IDA_Pro_v6\python\msvcr100.dll
C:\
C:\Users\user\AppData\Local\Temp\1c70d198f89ecc6aca0b30d6494995175e29d26b.exe
C:\Users\user\AppData\Local\Temp\1c70d198f89ecc6aca0b30d6494995175e29d26b.dbg
C:\popupkiller.exe
C:\stimulator.exe
C:\tools\execute.exe
C:\Users\user\AppData\Local\Temp\SbieDll.dll
C:\Windows\System32\SbieDll.dll
C:\Windows\system\SbieDll.dll
C:\Windows\SbieDll.dll
C:\ProgramData\Oracle\Java\javapath\SbieDll.dll
C:\Windows\System32\wbem\SbieDll.dll
C:\Windows\System32\WindowsPowerShell\v1.0\SbieDll.dll
C:\Program Files\Microsoft Network Monitor 3\SbieDll.dll
C:\Program Files (x86)\Universal Extractor\SbieDll.dll
C:\Program Files (x86)\Universal Extractor\bin\SbieDll.dll

C:\Program Files (x86)\Windows Kits\8.1\Windows Performance Toolkit\SbieDll.dll
C:\Python27\SbieDll.dll
C:\Python27\Scripts\SbieDll.dll
C:\tools\sysinternals\SbieDll.dll
C:\tools\SbieDll.dll
C:\tools\IDA_Pro_v6\python\SbieDll.dll
\??\NPF_NdisWanIp
C:\Users\user\AppData\Local\Temp\upd4bf58516.bat
C:\Users\user\AppData\Local\Temp
C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Local

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\InstallDate
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DigitalProductId
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\DisableUNCCheck
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\EnableExtensions
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\DelayedExpansion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\DefaultColor
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\CompletionChar
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\PathCompletionChar
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\AutoRun
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DisableUNCCheck
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\EnableExtensions
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DelayedExpansion
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DefaultColor
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\CompletionChar
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\PathCompletionChar
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\AutoRun
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable

RESOLVED APIS

kernel32.dll.FlsAlloc

kernel32.dll.FlsGetValue

kernel32.dll.FlsSetValue

kernel32.dll.FlsFree

kernel32.dll.IsProcessorFeaturePresent

kernel32.dll.VirtualProtect

kernel32.dll.LoadLibraryA

kernel32.dll.VirtualAlloc

kernel32.dll.VirtualFree

kernel32.dll.GetVersionExA

kernel32.dll.TerminateProcess

kernel32.dll.TerminateThread

kernel32.dll.DeleteFileW

kernel32.dll.HeapReAlloc

kernel32.dll.GetNativeSystemInfo

kernel32.dll.CreateThread

kernel32.dll.HeapAlloc

kernel32.dll.HeapDestroy

kernel32.dll.VirtualAllocEx

kernel32.dll.LocalFree

kernel32.dll.DeleteCriticalSection

kernel32.dll.GetComputerNameW

kernel32.dll.GetProcessHeap

kernel32.dll.SystemTimeToFileTime

kernel32.dll.GlobalMemoryStatusEx

kernel32.dll.CreateProcessW

kernel32.dll.WideCharToMultiByte

kernel32.dll.InterlockedIncrement

kernel32.dll.GetSystemTime

kernel32.dll.VirtualFreeEx

kernel32.dll.IsBadReadPtr

kernel32.dll.lstrcmpiW
kernel32.dll.OpenMutexW
kernel32.dll.SetEndOfFile
kernel32.dll.GetCurrentThread
kernel32.dll.FlushFileBuffers
kernel32.dll.RemoveVectoredExceptionHandler
kernel32.dll.GetCurrentProcess
kernel32.dll.SetErrorMode
kernel32.dll.GetVersionExW
kernel32.dll.DuplicateHandle
kernel32.dll.GetModuleHandleA
kernel32.dll.AddVectoredExceptionHandler
kernel32.dll.ExitProcess
kernel32.dll.GetCurrentProcessId
kernel32.dll.CopyFileW
kernel32.dll.lstrcmpiA
kernel32.dll.IsWow64Process
kernel32.dll.FindFirstChangeNotificationW
kernel32.dll.FindNextChangeNotification
kernel32.dll.IsProcessInJob
kernel32.dll.CreateRemoteThread
kernel32.dll.CreateNamedPipeW
kernel32.dll.DisconnectNamedPipe
kernel32.dll.ConnectNamedPipe
kernel32.dll.GetLogicalDrives
kernel32.dll.GetDriveTypeW
kernel32.dll.GetUserDefaultUILanguage
kernel32.dll.CopyFileExW
kernel32.dll.GetEnvironmentVariableW
kernel32.dll.SetFilePointer
kernel32.dll.InitializeCriticalSection
kernel32.dll.GetTimeZoneInformation
kernel32.dll.MultiByteToWideChar
kernel32.dll.SetFileAttributesW
kernel32.dll.GetVolumeNameForVolumeMountPointW

kernel32.dll.OpenProcess
kernel32.dll.GetFileTime
kernel32.dll.ReleaseMutex
kernel32.dll.LeaveCriticalSection
kernel32.dll.GetModuleFileNameW
kernel32.dll.SetFileTime
kernel32.dll.RemoveDirectoryW
kernel32.dll.ExpandEnvironmentStringsW
kernel32.dll.WriteFile
kernel32.dll.FindNextFileW

DELETED FILES

C:\Users\user\AppData\Local\Temp\1c70d198f89ecc6aca0b30d6494995175e29d26b.exe
C:\Users\user\AppData\Local\Temp\upd4bf58516.bat

REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\InstallDate
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\DigitalProductId
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\GRE_Initialize
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\DisableUNCCheck
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\EnableExtensions
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\DelayedExpansion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\DefaultColor
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\CompletionChar
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\PathCompletionChar
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Command Processor\AutoRun
HKEY_CURRENT_USER\Software\Microsoft\Command Processor
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DisableUNCCheck
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\EnableExtensions
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DelayedExpansion
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DefaultColor

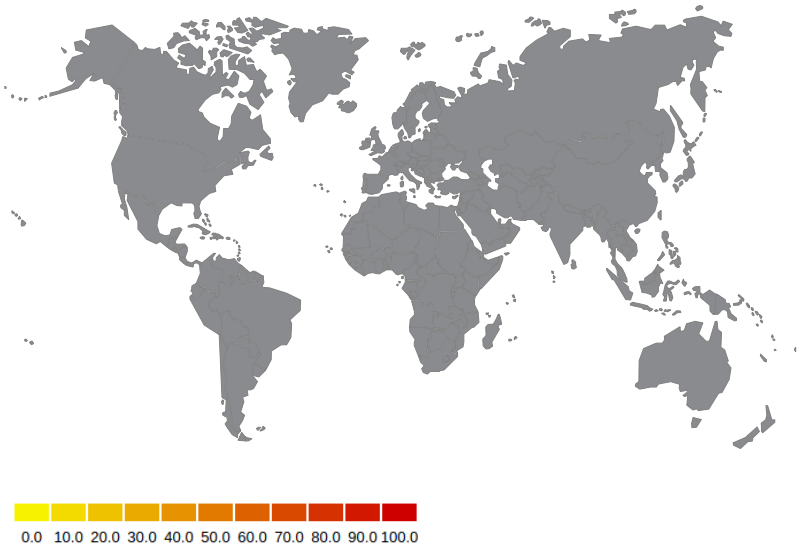
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\CompletionChar
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\PathCompletionChar
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\AutoRun
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\CustomLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\ExtendedLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale\Alternate Sorts
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Language Groups
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SafeBoot\Option
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Windows Error Reporting\WMR
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable

MUTEXES

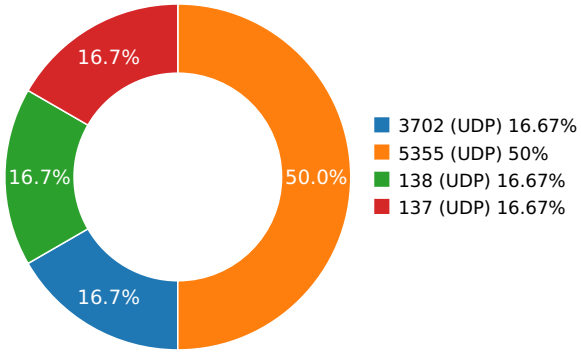
B7FF73F88E807F713F6A2E141FBE1459
37C47B02C4CFCFAA08145C16F9800F8C
Sandboxie_SingleInstanceMutex_Control
Frz_State

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
3.02633595467	Sandbox	224.0.0.252	5355
3.02745199203	Sandbox	224.0.0.252	5355
3.03393507004	Sandbox	239.255.255.250	3702
3.0891520977	Sandbox	192.168.56.255	137
5.58121013641	Sandbox	224.0.0.252	5355
9.07950210571	Sandbox	192.168.56.255	138

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\Upd4bf58516.Bat	**Type :** DOS batch file, ASCII text, with CRLF line terminators **MD5 :** 341472a44c0053085f71b23f4c90cad5 **SHA-1 :** 5180424cc89a2eb9be45375616d4b93fcbe97993 **SHA-256 :** f9a869073ad59d76815f9517ebfe153d06f83578 **SHA-512 :** 79e6bbd5496529c5f10259114a16125e39a40f79 **Size :** 0.262 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	Nds.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	1c70d198f89ecc6aca0b30d6494995175e29d26b
MD5:	1e12a7676dd6c56db832b801aa8a1063
First Seen Date:	2018-01-08 15:57:23.356490 (12 months ago)
Number Of Clients Seen:	2
Last Analysis Date:	2018-01-08 15:57:23.356490 (12 months ago)
Human Expert Analysis Date:	2018-01-08 19:12:39.355199 (12 months ago)
Human Expert Analysis Result:	Malware

VALKYRIE COMODO

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[]
Number Of Sections	5
Trid	[[42.2, u'Win32 Executable MS Visual C++ (generic)'], [37.3, u'Win64 Executable (generic)'], [8.8, u'Win32 Dynamic Link Library (generic)'], [6.0, u'Win32 Executable (generic)'], [2.7, u'Generic Win/DOS Executable']]
Compilation Time Stamp	0x5A533662 [Mon Jan 8 09:14:10 2018 UTC]
LegalCopyright	Copyright (C) 2017, fdjgndfkglte
FileVersion	10.1.10.11
ProductVersion	10.1.10.11
Translation	0x0809 0x04b0
Entry Point	0x40ea83 (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	283136
Ssdeep	6144:IHETEE0XxrLB5dWR3zW0vDRY4DMyl4Fmnrh:IHETEEGpb8RlvDRY4Qycm
Sha256	7a056a448afeb1e48f1e8d9753e4b225b1b079439d210d2a03bb5b55f107a0fd
Exifinfo	[{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/1/c/7/0/1c70d198f89ecc6aca0b30d6494995175e29d26b', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2018:01:08 15:56:43+00:00', u'EXE:InitializedDataSize': 919040, u'File:FileModifyDate': u'2018:01:08 15:56:42+00:00', u'EXE:FileVersionNumber': u'1.0.0.1', u'EXE:FileVersion': u'10.1.10.11', u'File:FileSize': u'276 kB', u'EXE:CharacterSet': u'Unicode', u'EXE:MachineType': u'Intel 386 or later, and compatibles', u'EXE:FileOS': u'Windows NT 32-bit', u'EXE:ProductVersion': u'10.1.10.11', u'EXE:ObjectFileType': u'Executable application', u'File:FileType': u'Win32 EXE', u'EXE:UninitializedDataSize': 0, u'File:FileName': u'1c70d198f89ecc6aca0b30d6494995175e29d26b', u'EXE:ImageVersion': 0.0, u'File:FileTypeExtension': u'exe', u'EXE:OSVersion': 5.0, u'EXE:PEType': u'PE32', u'EXE:TimeStamp': u'2018:01:08 09:14:10+00:00', u'EXE:FileFlagsMask': u'0x003f', u'EXE:LegalCopyright': u'Copyright (C) 2017, fdjgndfkglte', u'EXE:LinkerVersion': 9.0, u'EXE:FileFlags': u'(none)', u'EXE:Subsystem': u'Windows GUI', u'File:Directory': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/1/c/7/0', u'EXE:EntryPoint': u'0xea83', u'EXE:SubsystemVersion': 5.0, u'EXE:CodeSize': 142336, u'File:FileInodeChangeDate': u'2018:01:08 15:56:42+00:00', u'EXE:LanguageCode': u'English (British)', u'ExifTool:ExifToolVersion': 10.1, u'EXE:ProductVersionNumber': u'1.0.0.1'}]
Mime Type	application/x-dosexec
Imphash	f63950f0f912acb3c007a9db7d9c636c

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x22a91	0x22c00	6.56523792449	3c31a619d94a08f877154dffa43cc66a
.rdata	0x24000	0x83ba	0x8400	6.0208670345	b86de7fb91dc783e322ccf65946d856b
.data	0x2d000	0xc0fdc	0x1e00	3.84016084253	1edd6c0af84a17629a53c503c7304b23
.rsrc	0xee000	0x1548c	0x15600	7.84670700534	2fd0611349bad539834013db890d8f7d
.reloc	0x104000	0x29f8	0x2a00	4.52804958485	af50ac717b2c2d44647765cc90fbba81

PE Imports

- KERNEL32.dll
  - GetProcAddress
  - GetExitCodeThread
  - AddAtomA
  - GetFileInformationByHandle
  - lstrcpyA
  - CreateFileA
  - GetLocaleInfoW
  - GetModuleHandleA
  - SetStdHandle
  - WriteConsoleW
  - GetConsoleOutputCP
  - GetLastError
  - IsValidLocale
  - EnumSystemLocalesA
  - GetLocaleInfoA
  - GetUserDefaultLCID
  - IsValidCodePage
  - GetOEMCP
  - GetACP
  - HeapSize
  - GetStringTypeA
  - GetSystemTimeAsFileTime
  - GetCurrentProcessId
  - QueryPerformanceCounter
  - GetEnvironmentStringsW
  - TerminateProcess
  - GetThreadSelectorEntry
  - TerminateThread
  - GlobalAlloc
  - LoadLibraryW
  - GetTickCount
  - GetCPInfo
  - WriteConsoleA
  - ExitProcess
  - FreeEnvironmentStringsW
  - GetEnvironmentStrings
  - FreeEnvironmentStringsA
  - InitializeCriticalSectionAndSpinCount
  - LoadLibraryA
  - GetModuleFileNameA
  - WideCharToMultiByte
  - InterlockedIncrement
  - InterlockedDecrement
  - InterlockedCompareExchange
  - InterlockedExchange
  - MultiByteToWideChar
  - Sleep
  - InitializeCriticalSection
  - DeleteCriticalSection
  - EnterCriticalSection
  - LeaveCriticalSection
  - HeapFree
  - GetCurrentProcess
  - UnhandledExceptionFilter
  - SetUnhandledExceptionFilter
  - IsDebuggerPresent
  - HeapReAlloc
  - HeapAlloc

    - GetModuleHandleW
    - GetCommandLineA
    - GetStartupInfoA
    - RtlUnwind
    - RaiseException
    - LCMapStringA
    - LCMapStringW
    - GetStringTypeW
    - SetHandleCount
    - GetStdHandle
    - GetFileType
    - HeapCreate
    - VirtualFree
    - VirtualAlloc
    - ReadFile
    - WriteFile
    - GetConsoleCP
    - GetConsoleMode
    - FlushFileBuffers
    - TlsGetValue
    - TlsAlloc
    - TlsSetValue
    - TlsFree
    - SetLastError
    - GetCurrentThreadId
    - SetFilePointer
    - CloseHandle
- USER32.dll
    - DispatchMessageW
    - EndPaint
    - CloseClipboard
    - LoadMenuIndirectA
    - GetMessageExtraInfo
    - LoadImageW
    - LoadStringA
    - LoadMenuA
    - LoadCursorW
    - UserHandleGrantAccess
    - BeginPaint
    - GetUpdateRect
    - TranslateMessage
    - LoadAcceleratorsW
    - LoadIconW
    - GetAltTabInfoA
    - PeekMessageA
    - TranslateAcceleratorA
    - GetCaretPos
    - LoadBitmapW
    - DefDlgProcA
    - GetDlgCtrlID
    - LookupIconIdFromDirectory
    - LoadCursorFromFileA
- GDI32.dll
    - CombineRgn
    - ColorMatchToTarget
    - FillPath
    - CopyEnhMetaFileA
- ADVAPI32.dll
    - AdjustTokenGroups
    - AddAccessAllowedAceEx
    - AddAccessAllowedAce
- SHELL32.dll
    - DragFinish
    - ShellAboutW
    - FindExecutableA
- MSIMG32.dll
    - TransparentBlt
- WINHTTP.dll
    - WinHttpConnect

PE Resources

{u'lang': u'LANG_NEUTRAL', u'name': u'LPPOHPQGS', u'offset': 975292, u'sha256': u'3ec069377826d614e9247c7be17d74c23466676d69cbe2da0a8cd7f4d37799a0', u'type': u'data', u'size': 65001}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1040296, u'sha256':

u'bcd14209e1c0e299165f889c1d7a8833e195f1e563fb1da7b4728c0ae47baa60', u'type': u'data', u'size': 4264}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1044560, u'sha256': u'af507ec35b4c49e078cc637b7586bfe155c35b93ef4c4831e583c1a154582ad9', u'type': u'data', u'size': 16936}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ACCELERATOR', u'offset': 1061496, u'sha256': u'80ed7d54b9d8fc82382f79c92b7f77525b55043ca5c3370aa174fba83488e028', u'type': u'data', u'size': 56}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_ICON', u'offset': 1061552, u'sha256': u'1fd4367fd02dbea6b41889b17d691be481dae6d172a081ed9b5ab7555a02ff9f', u'type': u'MS Windows icon resource - 2 icons, 32x32', u'size': 34}

{u'lang': u'LANG_ITALIAN', u'name': u'RT_VERSION', u'offset': 1061588, u'sha256': u'02ecb8fa76c5d6175cfea7aca8f671c451c62fccdd3cd8d0a76c7458da02e366', u'type': u'COM executable for DOS', u'size': 440}

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS