VALKYRIE COMODO

Summary

File Name: 36d2a05049b9ad710ff050ae6841d06395916b5efa5bc1316e350f3bb1bca567.ex

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

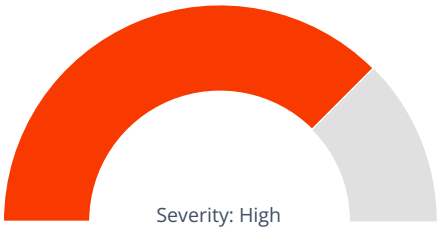
SHA1: 336c36d486b251098dfd6877ea2e4d3cef6482ec

MD5: 243918441cb108423f3561fcd4c1e4d2

MALWARE

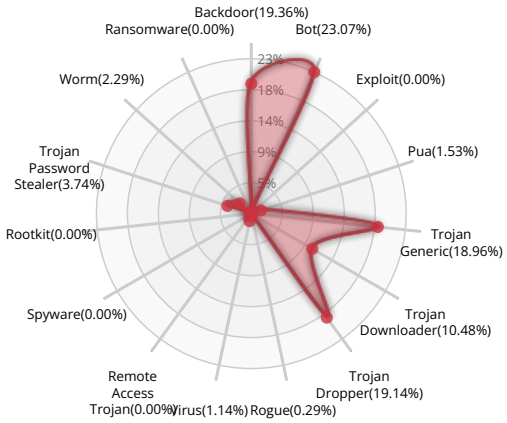
Valkyrie Final Verdict

DETECTION SECTION

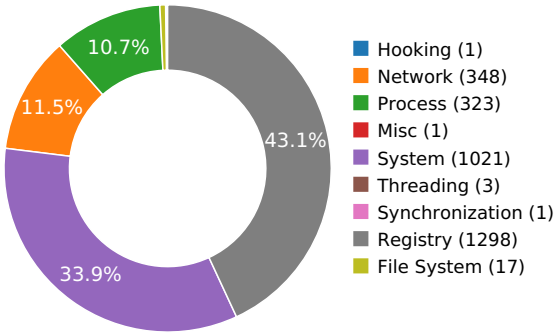


Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

VALKYRIE COMODO

Activity Details

INFORMATION DISCOVERY

Repeatedly searches for a not-found process, may want to run with startbrowser=1 option

NETWORKING

Attempts to connect to a dead IP:Port (1 unique times) Show sources

HIPS/ PFW/ OPERATING SYSTEM PROTECTION EVASION

Detects Avast Antivirus through the presence of a library

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory

Executed a process and injected code into it, probably while unpacking Show sources

PERSISTENCE AND INSTALLATION BEHAVIOR

Deletes its original binary from disk

Installs itself for autorun at Windows startup Show sources

MALWARE ANALYSIS SYSTEM EVASION

A process attempted to delay the analysis task. Show sources

Detects Sandboxie through the presence of a library

Creates a hidden or system file Show sources

Behavior Graph

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Windows\System32\tzres.dll
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\RECYCLER\S-1-5-21-0243556031-888888379-781862338-6985472110112323\systeez.exe
C:\RECYCLER
C:\RECYCLER\S-1-5-21-0243556031-888888379-781862338-6985472110112323\
C:\Users\user\AppData\Local\Temp\336c36d486b251098dfd6877ea2e4d3cef6482ec.exe

READ REGISTRY KEYS

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

kernel32.dll.FlsAlloc
kernel32.dll.FlsGetValue
kernel32.dll.FlsSetValue
kernel32.dll.FlsFree
kernel32.dll.InitializeCriticalSectionAndSpinCount
kernel32.dll.IsProcessorFeaturePresent
kernel32.dll.VirtualAlloc
kernel32.dll.GetLastError
kernel32.dll.LoadLibraryA
kernel32.dll.GetModuleHandleA
kernel32.dll.CloseHandle
kernel32.dll.GetSystemTime
kernel32.dll.GetStartupInfoA
msvcrt.dll._wcslwr
msvcrt.dll._exit
msvcrt.dll._XcptFilter
msvcrt.dll.exit
msvcrt.dll.__getmainargs
msvcrt.dll._initterm

msvcrt.dll.__setusermatherr
msvcrt.dll._adjust_fdiv
msvcrt.dll.__p__commode
msvcrt.dll.__p__fmode
msvcrt.dll.__set_app_type
msvcrt.dll._except_handler3
msvcrt.dll._controlfp
msvcrt.dll._acmdln
winmm.dll.timeKillEvent
winmm.dll.timeGetDevCaps
winmm.dll.timeEndPeriod
winmm.dll.timeSetEvent
ntdll.dll.RtlAdjustPrivilege
kernel32.dll.ExitThread
kernel32.dll.CreateMutexA
kernel32.dll.WaitForSingleObject
kernel32.dll.Sleep
kernel32.dll.LocalAlloc
kernel32.dll.LocalFree
kernel32.dll.DeleteFileA
kernel32.dll.DeleteFileW
kernel32.dll.SetFileAttributesA
kernel32.dll.GetTickCount
kernel32.dll.CreateThread
kernel32.dll.CreateFileA
kernel32.dll.CreateFileW
kernel32.dll.WriteFile
kernel32.dll.GetTempPathA
kernel32.dll.CreateProcessA
kernel32.dll.lstrlenA
kernel32.dll.lstrcatA
kernel32.dll.LoadLibraryW
kernel32.dll.MoveFileExW
kernel32.dll.CreateDirectoryW
kernel32.dll.CopyFileW

kernel32.dll.lstrlenW
kernel32.dll.lstrcpynW
kernel32.dll.GetProcAddress
kernel32.dll.SetFileAttributesW
user32.dll.MessageBoxA
user32.dll.MessageBoxW
user32.dll.MessageBeep
user32.dll.wsprintfA
ws2_32.dll.WSAStartup
ws2_32.dll.socket
ws2_32.dll.send
ws2_32.dll.recv
ws2_32.dll.closesocket
ws2_32.dll.ioctlsocket
ws2_32.dll.connect
ws2_32.dll.inet_addr
ws2_32.dll.gethostbyname
ws2_32.dll.htons
ws2_32.dll.select
ws2_32.dll.setsockopt
ws2_32.dll.WSAGetLastError
kernel32.dll.SortGetHandle

REGISTRY KEYS

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Windows Error Reporting\WMR
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
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
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\syseeeaz
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\syseeeaz

READ FILES

C:\Windows\System32\tzres.dll

C:\Windows\Globalization\Sorting\sortdefault.nls

C:\RECYCLER\S-1-5-21-0243556031-888888379-781862338-6985472110112323\systeez.exe

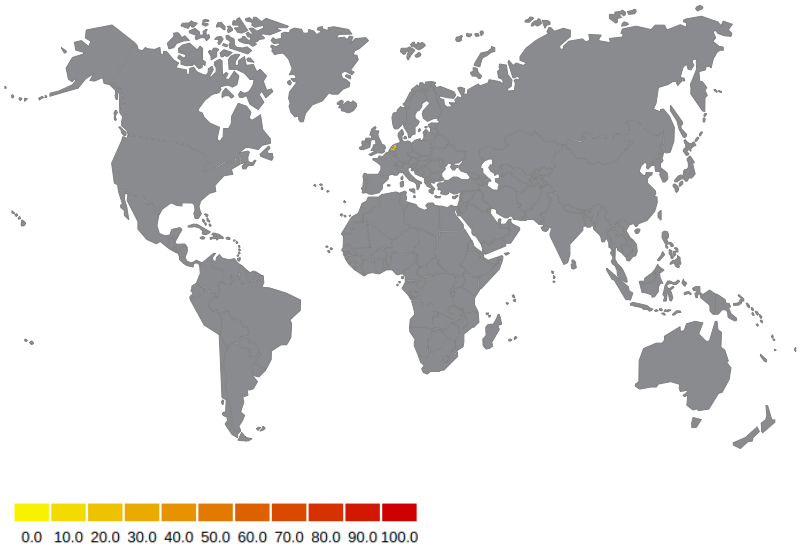
MODIFIED REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\syseeeaz

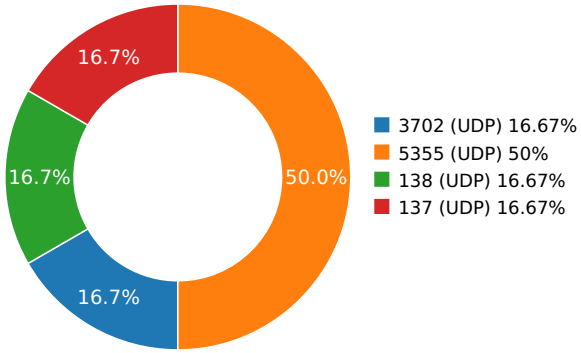
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\syseeeaz

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type
	93.190.139.161	Netherlands	49981	WorldStream IPv4.4	Malware Process

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.09817004204	Sandbox	192.168.56.255	137
3.14103317261	Sandbox	224.0.0.252	5355
3.14478802681	Sandbox	224.0.0.252	5355
3.1514480114	Sandbox	239.255.255.250	3702
5.70482707024	Sandbox	224.0.0.252	5355
9.17253112793	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:	36d2a05049b9ad710ff050ae6841d06395916b5efa5bc1316e350f3bb1bca567.ex
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	336c36d486b251098dfd6877ea2e4d3cef6482ec
MD5:	243918441cb108423f3561fcd4c1e4d2
First Seen Date:	2017-04-22 10:25:33.289332 (9 years ago)
Number Of Clients Seen:	2
Last Analysis Date:	2017-04-22 10:25:33.289332 (9 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	4
Compilation Time Stamp	0x583B275A [Sun Nov 27 18:35:06 2016 UTC]
Entry Point	0x40530e (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	218624
Sha256	36d2a05049b9ad710ff050ae6841d06395916b5efa5bc1316e350f3bb1bca567
Mime Type	application/x-dosexec

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x1543f	0x15600	6.756380	-
.rdata	0x17000	0x1b9e2	0x1ba00	5.728845	-
.data	0x33000	0x96a8	0x1800	3.564231	-
.rsrc	0x3d000	0x28c0	0x2a00	3.960705	-

PE Imports

- KERNEL32.dll
  - lstrlenA
  - lstrcpynA
  - lstrcmpiA
  - lstrcmpA
  - lstrcatA
  - WritePrivateProfileStringA
  - WriteFile
  - WaitForSingleObject
  - Sleep
  - SetFileTime
  - SetFilePointer
  - SetFileAttributesA
  - CopyFileA
  - DeleteFileA
  - FindFirstFileA
  - CloseHandle
  - CompareStringA
  - CreateEventA
  - CreateFileA
  - CreateProcessA
  - CreateThread
  - DeleteCriticalSection
  - EnterCriticalSection
  - EnumCalendarInfoA
  - FindResourceA
  - FormatMessageA
  - FreeLibrary
  - FreeResource
  - GetACP
  - GetCPInfo

- GetCurrentProcessId
- GetCurrentThreadId
- GetDiskFreeSpaceA
- GetLastError
- GetLocaleInfoA
- GetModuleFileNameA
- GetProcAddress
- GetStdHandle
- GetModuleHandleA
- LocalAlloc
- TlsGetValue
- TlsSetValue
- SizeofResource
- LCMapStringW
- LockResource
- LoadResource
- FindResourceW
- GetModuleFileNameW
- SetCurrentDirectoryW
- GetSystemDefaultLangID
- GetUserDefaultLCID
- ReleaseMutex
- CreateMutexW
- FindResourceExW
- SetFilePointerEx
- ReadFile
- EndUpdateResourceW
- UpdateResourceW
- BeginUpdateResourceW
- CreateFileW
- LoadLibraryW
- SetEndOfFile
- MultiByteToWideChar
- GetFileAttributesW
- SetFileAttributesW
- DeleteFileW
- CopyFileW
- GetFullPathNameW
- GetDiskFreeSpaceExW
- GetCurrentDirectoryW
- GetTempPathW
- GetWindowsDirectoryW
- GetSystemDirectoryW
- RemoveDirectoryW
- CreateDirectoryW
- GetCommandLineW
- GetEnvironmentVariableW
- GetSystemDefaultLCID
- GetLocaleInfoW
- GetPrivateProfileStringW
- WritePrivateProfileStringW
- LoadLibraryExW
- GetVersionExW
- GetCurrentProcess
- SetEvent
- CreateEventW
- WideCharToMultiByte
- GetDriveTypeW
- GetExitCodeThread
- SetLastError
- MulDiv
- lstrlenW
- LocalFree
- FormatMessageW
- GlobalUnlock
- GlobalLock
- GlobalAlloc
- GlobalFree
- GetModuleHandleW
- SetErrorMode
- GlobalDeleteAtom
- lstrcmpW
- EnumResourceLanguagesW
- GetVersion
- ConvertDefaultLocale

- GetCurrentThread
- FindClose
- FindNextFileW
- FileTimeToSystemTime
- FileTimeToLocalFileTime
- FindFirstFileW
- LeaveCriticalSection
- GlobalReAlloc
- GlobalHandle
- InitializeCriticalSection
- TlsAlloc
- LocalReAlloc
- TlsFree
- GetThreadLocale
- ResetEvent
- GetLogicalDriveStringsW
- MoveFileA
- GetFileAttributesA
- CreatePipe
- GetExitCodeProcess
- GetDriveTypeA
- GetCurrentDirectoryA
- SetEnvironmentVariableW
- SetEnvironmentVariableA
- WriteConsoleW
- GetConsoleOutputCP
- WriteConsoleA
- IsValidLocale
- EnumSystemLocalesA
- GetStringTypeW
- GetStringTypeA
- GetConsoleMode
- GetConsoleCP
- GetTimeZoneInformation
- GetDateFormatA
- GetTimeFormatA
- QueryPerformanceCounter
- VirtualFree
- HeapCreate
- HeapDestroy
- GetStartupInfoA
- SetHandleCount
- GetCommandLineA
- GetEnvironmentStringsW
- FreeEnvironmentStringsW
- GetEnvironmentStrings
- FreeEnvironmentStringsA
- FlushFileBuffers
- LCMapStringA
- IsValidCodePage
- GetOEMCP
- VirtualQuery
- GetSystemInfo
- VirtualAlloc
- VirtualProtect
- HeapSize
- GetFileType
- SetStdHandle
- HeapReAlloc
- IsDebuggerPresent
- SetUnhandledExceptionFilter
- UnhandledExceptionFilter
- TerminateProcess
- ExitProcess
- GetSystemTimeAsFileTime
- GetStartupInfoW
- GetProcessHeap
- HeapAlloc
- HeapFree
- RtlUnwind
- RaiseException
- GetTickCount
- GlobalFlags
- GlobalAddAtomW
- GlobalFindAtomW

- CompareStringW
- LoadLibraryA
- GetVersionExA
- GetFileTime
- GetVolumeInformationW
- DuplicateHandle
- GetFileSize
- UnlockFile
- LockFile
- InterlockedIncrement
- InterlockedDecrement

PE Resources

RT_ICON
RT_DIALOG
RT_GROUP_ICON
RT_MANIFEST

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS