VALKYRIE COMODO

Summary

File Name: filedata

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

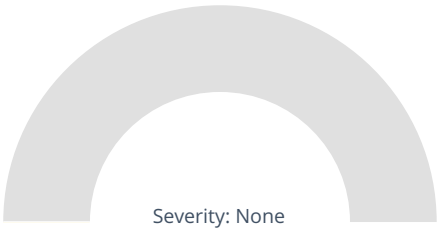
SHA1: c596d3996b782414fa812a12d91ac6a23e393efd

MD5: 615ca56d988022b8a0d46a6865467413

MALWARE

Valkyrie Final Verdict

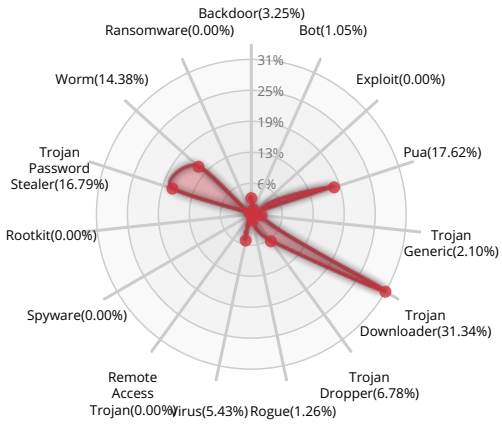
DETECTION SECTION



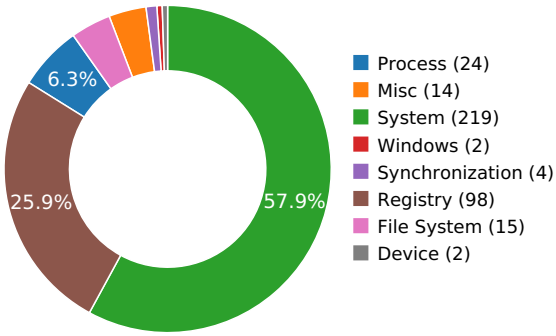
Severity: None

Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

VALKYRIE COMODO

Activity Details

INFORMATION DISCOVERY

Reads data out of its own binary image — Show sources

STATIC ANOMALY

Anomalous binary characteristics — Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory

VALKYRIE COMODO

Behaviour Graph

11:51:28 **11:51:28** **11:51:28**

PID 2724

11:51:28	Create Process	The malicious file created a child process as c596d3996b782414fa812a12d91ac6a23e393efd.exe **(PPID 2576)**

11:51:28	VirtualProtectEx

11:51:28	NtReadFile

VALKYRIE COMODO

Behaviour Summary

ACCESSED FILES

C:\Windows\SysWOW64\en-US\KERNELBASE.dll.mui
C:\Users\user\AppData\Local\Temp\netmsg.dll
C:\Windows\System32\netmsg.dll
C:\Users\user\AppData\Local\Temp\c596d3996b782414fa812a12d91ac6a23e393efd.exe
C:\Windows\Fonts\staticcache.dat
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Users\user\AppData\Local\Temp\imageres.dll
C:\Windows\System32\imageres.dll
\Device\KsecDD

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\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFilePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane7
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane8
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane9
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane10
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane11
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane12
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane13
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane14
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane15

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane16
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}\Enable
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\CTF\EnableAnchorContext
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles

RESOLVED APIS

kernel32.dll.SetDllDirectoryW
kernel32.dll.SetSearchPathMode
kernel32.dll.SetProcessDEPPolicy
kernel32.dll.Wow64DisableWow64FsRedirection
kernel32.dll.Wow64RevertWow64FsRedirection
kernel32.dll.GetCommandLineW
kernel32.dll.AreFileApisANSI
kernel32.dll.GetModuleFileNameW
kernel32.dll.CreateFileW
kernel32.dll.VirtualAlloc
kernel32.dll.LoadLibraryA
kernel32.dll.VirtualProtect
kernel32.dll.VirtualFree
kernel32.dll.FreeLibrary
kernel32.dll.DeleteCriticalSection
kernel32.dll.LeaveCriticalSection
kernel32.dll.EnterCriticalSection
kernel32.dll.InitializeCriticalSection
kernel32.dll.LocalFree
kernel32.dll.LocalAlloc
kernel32.dll.GetCurrentThreadId
kernel32.dll.WideCharToMultiByte
kernel32.dll.lstrlenA
kernel32.dll.lstrcpynA
kernel32.dll.LoadLibraryExA
kernel32.dll.GetThreadLocale
kernel32.dll.GetStartupInfoA
kernel32.dll.GetProcAddress
kernel32.dll.GetModuleHandleA

kernel32.dll.GetModuleFileNameA
kernel32.dll.GetLocaleInfoA
kernel32.dll.GetCommandLineA
kernel32.dll.FindFirstFileA
kernel32.dll.FindClose
kernel32.dll.ExitProcess
kernel32.dll.WriteFile
kernel32.dll.UnhandledExceptionFilter
kernel32.dll.RtlUnwind
kernel32.dll.RaiseException
kernel32.dll.GetStdHandle
user32.dll.GetKeyboardType
user32.dll.LoadStringA
user32.dll.MessageBoxA
user32.dll.CharNextA
advapi32.dll.RegQueryValueExA
advapi32.dll.RegOpenKeyExA
advapi32.dll.RegCloseKey
oleaut32.dll.SysFreeString
oleaut32.dll.SysReAllocStringLen
kernel32.dll.TlsSetValue
kernel32.dll.TlsGetValue
kernel32.dll.TlsFree
kernel32.dll.TlsAlloc
kernel32.dll.VirtualQueryEx
kernel32.dll.VirtualQuery
kernel32.dll.ReadProcessMemory
kernel32.dll.OpenProcess
kernel32.dll.MoveFileExA
kernel32.dll.GetVersionExW
kernel32.dll.GetVersionExA
kernel32.dll.GetTickCount
kernel32.dll.GetSystemInfo
kernel32.dll.GetStringTypeExA
kernel32.dll.GetDiskFreeSpaceA

kernel32.dll.GetCurrentProcessId
kernel32.dll.GetCPInfo
kernel32.dll.GetACP
kernel32.dll.EnumCalendarInfoA
kernel32.dll.CreateSemaphoreW
kernel32.dll.CloseHandle
kernel32.dll.BuildCommDCBAndTimeoutsA
user32.dll.RegisterClipboardFormatA
user32.dll.GetSystemMetrics
user32.dll.GetLastInputInfo
user32.dll.DlgDirListComboBoxA
kernel32.dll.GetDiskFreeSpaceExA

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_CURRENT_USER\Software\Borland\Locales
HKEY_LOCAL_MACHINE\Software\Borland\Locales
HKEY_CURRENT_USER\Software\Borland\Delphi\Locales
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\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontLink\SystemLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFilePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane2

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane7
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane8
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane9
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane10
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane11
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane12
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane13
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane14
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane15
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane16
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Segoe UI
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\Compatibility\c596d3996b782414fa812a12d91ac6a23e393efd.exe
HKEY_LOCAL_MACHINE\Software\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}\Enable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\CTF\EnableAnchorContext
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\KnownClasses
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\GRE_Initialize
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles

READ FILES

C:\Windows\SysWOW64\en-US\KERNELBASE.dll.mui
C:\Windows\System32\netmsg.dll
C:\Users\user\AppData\Local\Temp\c596d3996b782414fa812a12d91ac6a23e393efd.exe
C:\Windows\Fonts\staticcache.dat
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\System32\imageres.dll
\Device\KsecDD

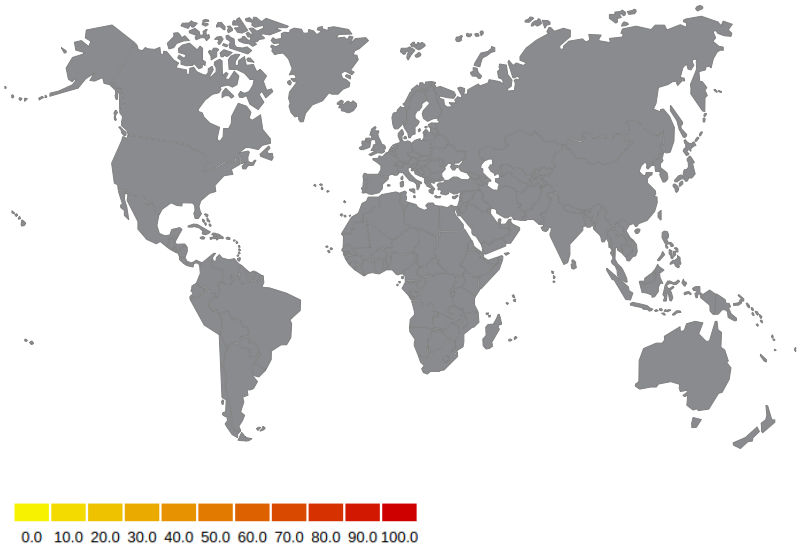
MUTEXES

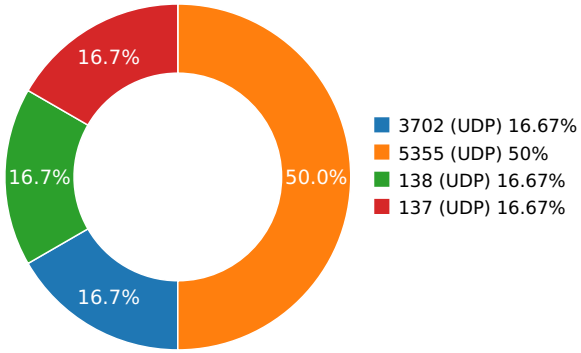
CicLoadWinStaWinSta0

Local\MSCTF.CtfMonitorInstMutexDefault1

Network Behaviour

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
7.14129090309	Sandbox	224.0.0.252	5355
7.16240787506	Sandbox	224.0.0.252	5355
7.16820287704	Sandbox	239.255.255.250	3702
7.20000600815	Sandbox	192.168.56.255	137
9.71636605263	Sandbox	224.0.0.252	5355
13.198734045	Sandbox	192.168.56.255	138

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES

STATIC FILE INFO

File Name:	filedata
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	c596d3996b782414fa812a12d91ac6a23e393efd
MD5:	615ca56d988022b8a0d46a6865467413
First Seen Date:	2017-06-17 22:12:21.604456 (a day ago)
Number Of Clients Seen:	2
Last Analysis Date:	2017-06-17 22:12:21.604456 (a day 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
File Type Enum	6
Number Of Sections	8
Compilation Time Stamp	0x2A425E19 [Fri Jun 19 22:22:17 1992 UTC] [SUSPICIOUS]
LegalCopyright	Internet
FileVersion	5.1.4.2
CompanyName	
Comments	This installation was built with Inno Setup.
ProductName	Redod
ProductVersion	4.5.6
FileDescription	Redod Setup
Translation	0x0000 0x04b0
Entry Point	0x40a5f8 (CODE)
Machine Type	Intel 386 or later - 32Bit
File Size	1527256
Sha256	5cc49fbb472571ef216aa81fcb0f63e09d533ba11fcf9b0badfc64de6d210635
Mime Type	application/x-dosexec

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
CODE	0x1000	0x9d30	0x9e00	6.62607332099	09134bbfe2b42c53497d3fac1d71f439
DATA	0xb000	0x250	0x400	2.75182066229	1ee71d84f1c77af85f1f5c278f880572
BSS	0xc000	0xe8c	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.idata	0xd000	0x950	0xa00	4.4307330698	bb5485bf968b970e5ea81292af2acdba
.tls	0xe000	0x8	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.rdata	0xf000	0x18	0x200	0.20448815744	9ba824905bf9c7922b6fc87a38b74366
.reloc	0x10000	0x8c4	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.rsrc	0x11000	0x2c00	0x2c00	4.53719595799	ff2e3741e6477431947ad5f16a3056b9

PE Imports

- kernel32.dll
  - DeleteCriticalSection
  - LeaveCriticalSection
  - EnterCriticalSection
  - InitializeCriticalSection

        - VirtualFree
        - VirtualAlloc
        - LocalFree
        - LocalAlloc
        - WideCharToMultiByte
        - TlsSetValue
        - TlsGetValue
        - MultiByteToWideChar
        - GetModuleHandleA
        - GetLastError
        - GetCommandLineA
        - WriteFile
        - SetFilePointer
        - SetEndOfFile
        - RtlUnwind
        - ReadFile
        - RaiseException
        - GetStdHandle
        - GetFileSize
        - GetSystemTime
        - GetFileType
        - ExitProcess
        - CreateFileA
        - CloseHandle
    - user32.dll
        - MessageBoxA
    - oleaut32.dll
        - VariantChangeTypeEx
        - VariantCopyInd
        - VariantClear
        - SysStringLen
        - SysAllocStringLen
    - advapi32.dll
        - RegQueryValueExA
        - RegOpenKeyExA
        - RegCloseKey
        - OpenProcessToken
        - LookupPrivilegeValueA
    - kernel32.dll
        - WriteFile
        - VirtualQuery
        - VirtualProtect
        - VirtualFree
        - VirtualAlloc
        - Sleep
        - SizeofResource
        - SetLastError
        - SetFilePointer
        - SetErrorMode
        - SetEndOfFile
        - RemoveDirectoryA
        - ReadFile
        - LockResource
        - LoadResource
        - LoadLibraryA
        - IsDBCSLeadByte
        - GetWindowsDirectoryA
        - GetVersionExA
        - GetUserDefaultLangID
        - GetSystemInfo
        - GetSystemDefaultLCID
        - GetProcAddress
        - GetModuleHandleA
        - GetModuleFileNameA
        - GetLocaleInfoA
        - GetLastError
        - GetFullPathNameA
        - GetFileSize
        - GetFileAttributesA
        - GetExitCodeProcess
        - GetEnvironmentVariableA
        - GetCurrentProcess
        - GetCommandLineA
        - GetACP
        - InterlockedExchange

- FormatMessageA
- FindResourceA
- DeleteFileA
- CreateProcessA
- CreateFileA
- CreateDirectoryA
- CloseHandle

- user32.dll
  - TranslateMessage
  - SetWindowLongA
  - PeekMessageA
  - MsgWaitForMultipleObjects
  - MessageBoxA
  - LoadStringA
  - ExitWindowsEx
  - DispatchMessageA
  - DestroyWindow
  - CreateWindowExA
  - CallWindowProcA
  - CharPrevA
- comctl32.dll
  - InitCommonControls
- advapi32.dll
  - AdjustTokenPrivileges

PE Resources

RT_ICON
RT_STRING
RT_RCDATA
RT_GROUP_ICON
RT_VERSION
RT_MANIFEST

CERTIFICATE VALIDATION

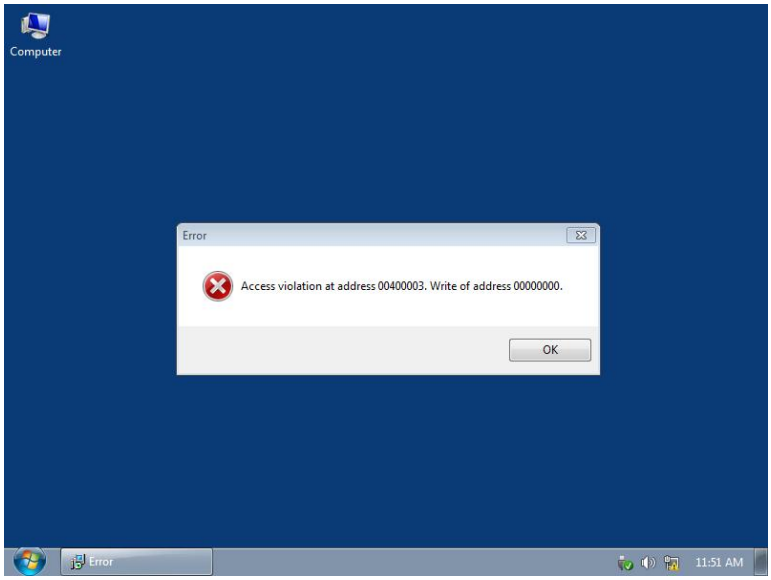
- Success ✔

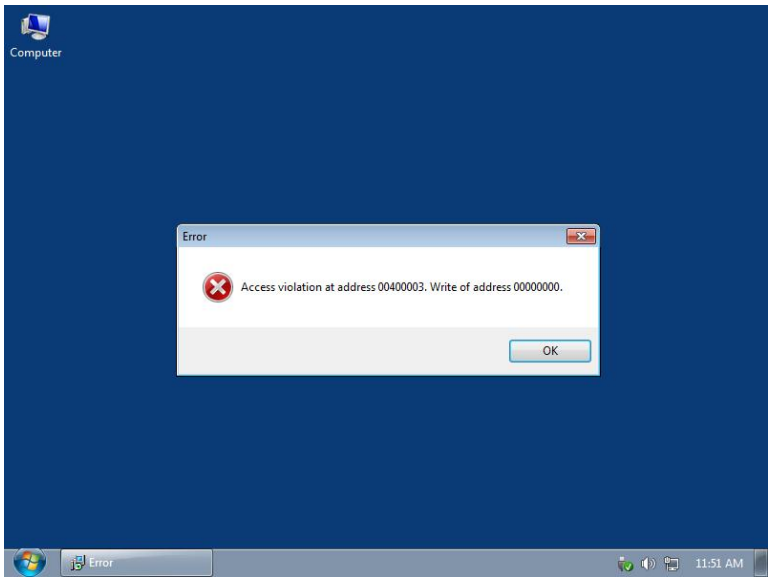
[+] VIZARD-TORG, TOV	
Status	NoError ✔
Start Date	2017-03-01 00:00:00+00:00
End Date	2018-03-01 23:59:59+00:00
Sha256	32094389aca8cf52bf4d3dd9ec88000f8875a2e82aa3b97b172e0f76c685fad4
Serial	00B3389E614CF0C2D06A9AEBBACB8443D3
Subject Key Identifier	07 5b e6 45 a3 f8 ea 71 2b a7 c2 89 97 b5 3d 6d 85 3a 98 4e
Issuer Name	COMODO RSA Code Signing CA
Issuer Key Identifier	29 91 60 ff 8a 4d fa eb f9 a6 6a b8 cf f9 e6 4b bd 49 ce 12
Crl link	http://crl.comodoca.com/COMODORSACodeSigningCA.crl
Key Usage	Digital Signature (80)
Extended Usage	Code Signing (1.3.6.1.5.5.7.3.3)

[+] COMODO RSA Code Signing CA	
Status	NoError ✔
Start Date	2013-05-09 00:00:00+00:00
End Date	2028-05-08 23:59:59+00:00
Sha256	be4b37864cefc39611d4b6a1de110074e5f282de90016aa5d36849ab452eab2c
Serial	2E7C87CC0E934A52FE94FD1CB7CD34AF
Subject Key Identifier	29 91 60 ff 8a 4d fa eb f9 a6 6a b8 cf f9 e6 4b bd 49 ce 12
Issuer Name	COMODO RSA Certification Authority
Issuer Key Identifier	bb af 7e 02 3d fa a6 f1 3c 84 8e ad ee 38 98 ec d9 32 32 d4
Crl link	http://crl.comodoca.com/COMODORSACertificationAuthority.crl
Key Usage	Digital Signature,Certificate Signing,Off-line CRL Signing,CRL Signing (86)
Extended Usage	Code Signing (1.3.6.1.5.5.7.3.3)

[+] COMODO RSA Certification Authority	
Status	NoError ✔
Start Date	2010-01-19 00:00:00+00:00
End Date	2038-01-18 23:59:59+00:00
Sha256	f1bc8293a80c7d1bb2fd1d6e9b714b06e6b66686ca9b26a76d91e06e2934fa83
Serial	4CAAF9CADB636FE01FF74ED85B03869D
Subject Key Identifier	bb af 7e 02 3d fa a6 f1 3c 84 8e ad ee 38 98 ec d9 32 32 d4
Issuer Name	COMODO RSA Certification Authority
Issuer Key Identifier	undefined
Crl link	undefined
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	undefined

SCREENSHOTS


Computer
Error
Access violation at address 00400003. Write of address 00000000.
OK
Error
11:51 AM


Computer
Error
Access violation at address 00400003. Write of address 00000000.
OK
Error
11:51 AM


Computer
11:51 AM


Computer
11:51 AM