VALKYRIE COMODO

Summary

File Name: None

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

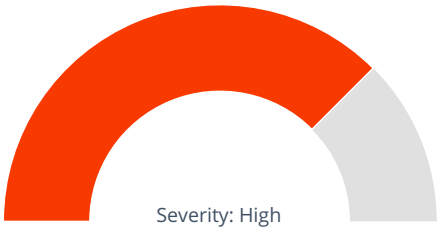
SHA1: 11b7e6fe10e891a7ce79fb97c5b2fb791b05d79e

MD5: b6234d7441ac12355aedf64c746e8f5f

MALWARE

Valkyrie Final Verdict

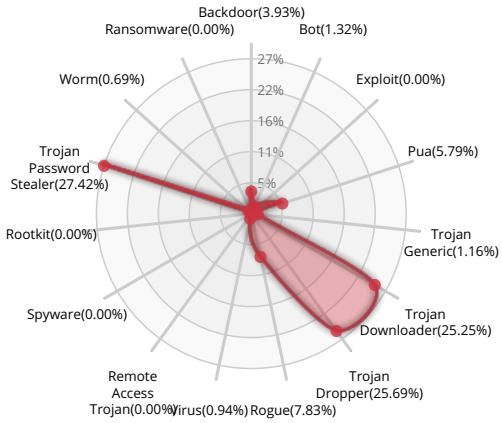
DETECTION SECTION



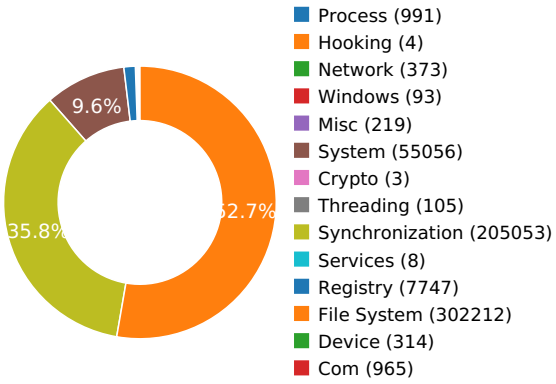
Severity: High

Verdict: Malware

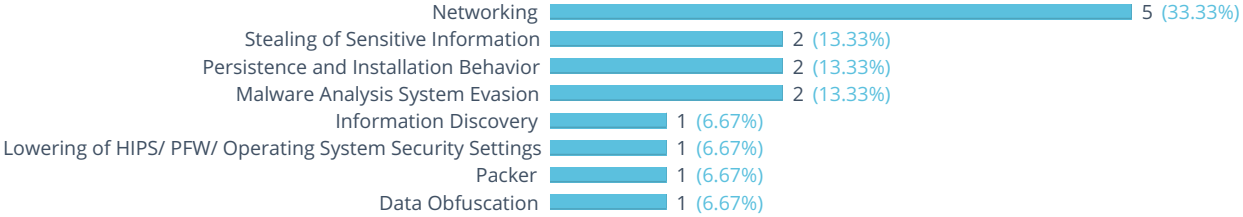
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



VALKYRIE COMODO

Activity Details

INFORMATION DISCOVERY

Reads data out of its own binary image	Show sources

NETWORKING

Attempts to connect to a dead IP:Port (6 unique times)	Show sources
HTTP traffic contains suspicious features which may be indicative of malware related traffic	Show sources
Performs some HTTP requests	Show sources
Network activity contains more than one unique useragent.	Show sources
A wscript.exe process commonly used in script or document file downloaders initiated network activity	Show sources

LOWERING OF HIPS/ PFW/ OPERATING SYSTEM SECURITY SETTINGS

Attempts to block SafeBoot use by removing registry keys	Show sources

PACKER

The binary likely contains encrypted or compressed data.	Show sources

STEALING OF SENSITIVE INFORMATION

Sniffs keystrokes	Show sources
Collects information to fingerprint the system	Show sources

DATA OBFUSCATION

Drops a binary and executes it	Show sources

PERSISTENCE AND INSTALLATION BEHAVIOR

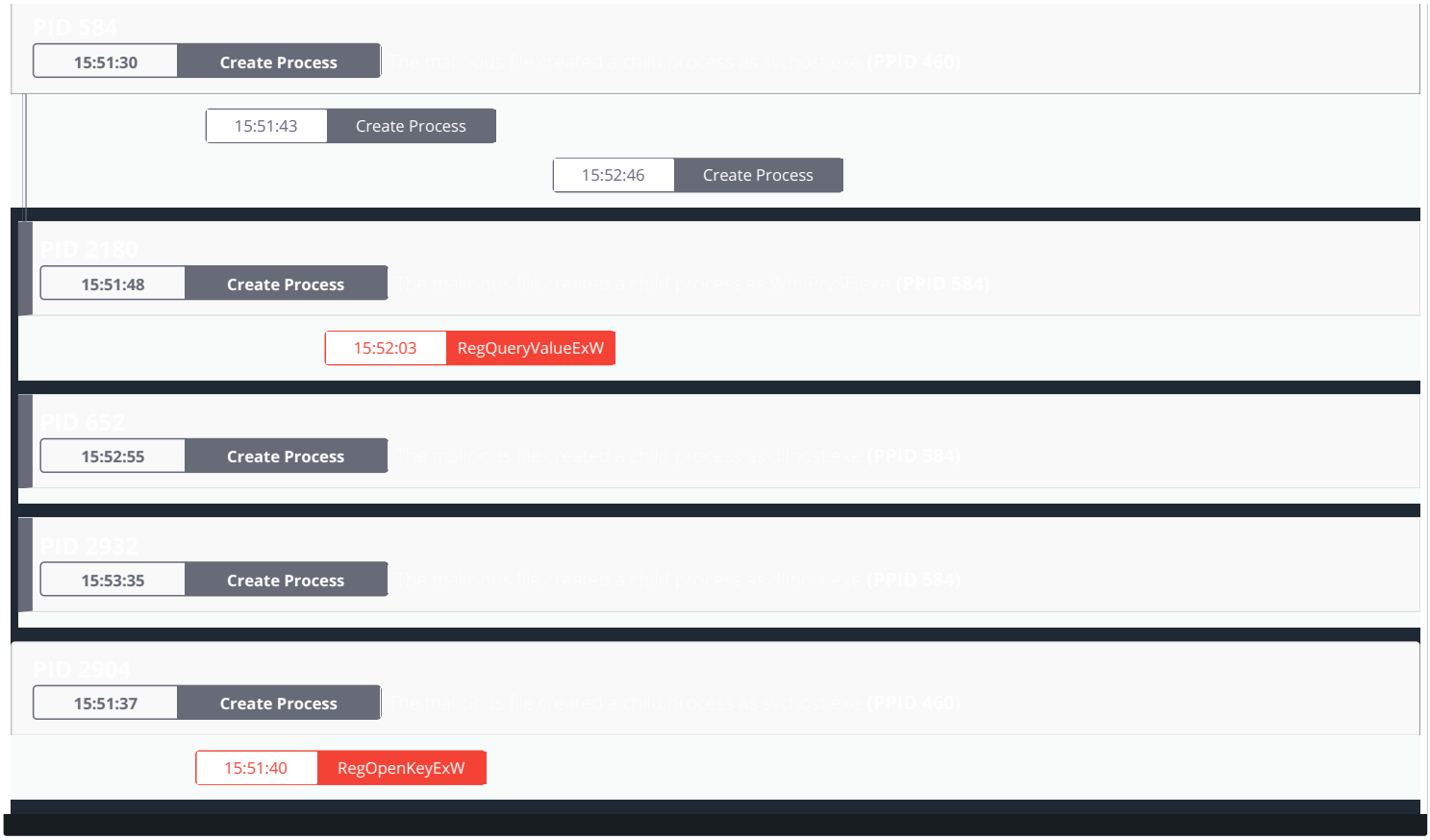
Installs itself for autorun at Windows startup	Show sources
Attempts to interact with an Alternate Data Stream (ADS)	Show sources

MALWARE ANALYSIS SYSTEM EVASION

Possible date expiration check, exits too soon after checking local time	Show sources
A process attempted to delay the analysis task.	Show sources

VALKYRIE COMODO

Behavior Graph


PID 584
15:51:30
Create Process
The malicious file created a child process as svchost.exe (PPID 460)
15:51:43
Create Process
15:52:46
Create Process
PID 2180
15:51:48
Create Process
The malicious file created a child process as WmiPrvSE.exe (PPID 584)
15:52:03
RegQueryValueExW
PID 652
15:52:55
Create Process
The malicious file created a child process as dllhost.exe (PPID 584)
PID 2932
15:53:35
Create Process
The malicious file created a child process as dllhost.exe (PPID 584)
PID 2904
15:51:37
Create Process
The malicious file created a child process as svchost.exe (PPID 460)
15:51:40
RegOpenKeyExW

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

\Device\KsecDD
\??\MountPointManager
C:\Users\user\AppData\Local\Temp\
C:\Users\user\AppData\Local\Temp
C:\Users\user\AppData\Local\Temp\nso5034.tmp
C:\Users\user\AppData\Local\Temp\11b7e6fe10e891a7ce79fb97c5b2fb791b05d79e.exe
C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Roaming
C:\Users\user\AppData\Roaming\FV2-XSONICX-11.0_Windows64b-32b-NewUpdate.exe
C:\Users\user\AppData\Roaming\Patch.vbs
C:\Users\user\AppData\Roaming\Patch.vbs:Zone.Identifier
C:\Windows\System32\wscript.exe
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Users\user\AppData\Roaming\Fv2XsonicXTrainer
C:\Users\user\AppData\Roaming\Fv2XsonicXTrainer\FV2-XSONICX.XSONICX
C:\Users\user\AppData\Roaming\Fv2XsonicXTrainer\FV2-XSONICX(Windows 32Bits).exe
C:\Users\user\AppData\Roaming\Fv2XsonicXTrainer\FV2-XSONICX(Windows 64Bits).exe
C:\Users\user\AppData\Roaming\Fv2XsonicXTrainer\lua53-32.dll
C:\Users\user\AppData\Roaming\Fv2XsonicXTrainer\lua53-64.dll
C:\Users\Public\Desktop
C:\
C:\Users\desktop.ini
\??\PIPE\srvsvc
C:\DosDevices\pipe\
C:\Users\user\AppData\Roaming\Fv2XsonicXTrainer\
C:\Users\Public\Desktop\Fv2XsonicX Trainer 32bits.lnk
C:\Users\Public\Desktop\Fv2XsonicX Trainer 64bits.lnk
C:\Users\user\Desktop
C:\Users\user\Desktop\Fv2XsonicX Trainer 32bits.lnk
C:\Users\user\Desktop\Fv2XsonicX Trainer 64bits.lnk

C:\ProgramData\Microsoft\Windows\Start Menu\Programs
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Fv2XsonicX Trainer 64bits.lnk
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Fv2XsonicX Trainer 32bits.lnk
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Fv2XsonicX Trainer 32bits .lnk
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Fv2XsonicX Trainer 64bits.lnk
C:\ProgramData\Microsoft\Windows\Start Menu
C:\ProgramData\Microsoft\Windows\Start Menu\Fv2XsonicX Trainer 32bits.lnk
C:\ProgramData\Microsoft\Windows\Start Menu\Fv2XsonicX Trainer 64bits.lnk
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Fv2XsonicX Trainer 32bits.lnk
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Fv2XsonicX Trainer 64bits.lnk
C:\Users\user\AppData\Local\Temp\7ZSfx000.cmd
C:\Windows\SysWOW64\wscript.exe
C:\Windows\SysWOW64\wshom.ocx
C:\Windows\SysWOW64\shell32.dll
C:\Users\user\AppData\Local\Microsoft\Windows\Caches
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x000000000000004a.db
C:\Users\Public
C:\Users\Public\desktop.ini
C:\Users\Public\Desktop\desktop.ini
C:\ProgramData
C:\ProgramData\Microsoft
C:\ProgramData\Microsoft\desktop.ini
C:\ProgramData\Microsoft\Windows
C:\ProgramData\Microsoft\Windows\Start Menu\desktop.ini
C:\Users\user\Desktop\desktop.ini
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\desktop.ini
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\Printer Shortcuts
C:\Users\user\AppData\Roaming\Microsoft
C:\Users\user\AppData\Roaming\Microsoft\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates
C:\Windows\Fonts
C:\Windows
C:\Windows\Fonts\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\Network Shortcuts
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\SendTo
C:\Users\user\AppData\Roaming\Microsoft\Windows\SendTo\Desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent

READ REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.vbs\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.vbs\PerceivedType
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\VBSFile\DocObject
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\VBSFile\BrowseInPlace
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.vbs\Content Type
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\VBSFile\IsShortcut
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\VBSFile\AlwaysShowExt
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\VBSFile\NeverShowExt
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\UsersFiles\NameSpace\DelegateFolders\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\UsersFiles\NameSpace\DelegateFolders\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\UsersFiles\NameSpace\DelegateFolders\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\InProcServer32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\InProcServer32\LoadWithoutCOM
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\KindMap\.vbs

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\VBSFile\NoStaticDefaultVerb
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\VBSFile\Shell\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\VBSFile\Shell\Open\NeverDefault
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\VBSFile\Shell\Open\Command\DelegateExecute
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.asp\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.bas\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.bat\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.cer\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.chm\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.cmd\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.com\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.cpl\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.crt\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.exe\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.gadget\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.grp\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.hlp\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.hta\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.inf\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.js\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.JSE\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.lnk\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.msc\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.msi\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.msp\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.pif\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.pl\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.prf\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.pst\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.reg\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.scf\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.scr\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.sct\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.URL\(Default)

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.VBE\(Default)
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Security\DisableSecuritySettingsCheck
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Security\DisableSecuritySettingsCheck
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers\TransparentEnabled
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\VBSFile\Shell\Open\Command\command
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\VBSFile\Shell\Open\Command\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\VBSFile\Shell\Open\SetWorkingDirectoryFromTarget
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\VBSFile\Shell\Open\NoWorkingDirectory
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Drive\shellex\FolderExtensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}\DriveMask
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\{DE92C1C7-837F-4F69-A3BB-86E631204A23}
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\My Music
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\User Shell Folders\{3D644C9B-1FB8-4F30-9B45-F670235F79C0}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\ProfilesDirectory
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\Public
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\{52A4F021-7B75-48A9-9F6B-4B87A210BC8F}
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\AppData
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows Script Host\Settings\IgnoreUserSettings

MODIFIED FILES

C:\Users\user\AppData\Roaming\FV2-XSONICX-11.0_Windows64b-32b-NewUpdate.exe
C:\Users\user\AppData\Roaming\Patch.vbs
C:\Users\user\AppData\Roaming\Fv2XsonicXTrainer\FV2-XSONICX.XSONICX
C:\Users\user\AppData\Roaming\Fv2XsonicXTrainer\FV2-XSONICX(Windows 32Bits).exe
C:\Users\user\AppData\Roaming\Fv2XsonicXTrainer\FV2-XSONICX(Windows 64Bits).exe
C:\Users\user\AppData\Roaming\Fv2XsonicXTrainer\lua53-32.dll
C:\Users\user\AppData\Roaming\Fv2XsonicXTrainer\lua53-64.dll
\??\PIPE\srvsvc
C:\Users\Public\Desktop\Fv2XsonicX Trainer 32bits.lnk
C:\Users\Public\Desktop\Fv2XsonicX Trainer 64bits.lnk
C:\Users\user\Desktop\Fv2XsonicX Trainer 32bits.lnk
C:\Users\user\Desktop\Fv2XsonicX Trainer 64bits.lnk
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Fv2XsonicX Trainer 64bits.lnk

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Fv2XsonicX Trainer 32bits.lnk
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Fv2XsonicX Trainer 32bits .lnk
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Fv2XsonicX Trainer 64bits.lnk
C:\ProgramData\Microsoft\Windows\Start Menu\Fv2XsonicX Trainer 32bits.lnk
C:\ProgramData\Microsoft\Windows\Start Menu\Fv2XsonicX Trainer 64bits.lnk
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Fv2XsonicX Trainer 32bits.lnk
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Fv2XsonicX Trainer 64bits.lnk
C:\Users\user\AppData\Local\Temp\7ZSfx000.cmd
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Patch.vbs
C:\Windows\sysnative\ntdll.dll
C:\Windows\sysnative\kernel32.dll
C:\Windows\sysnative\KERNELBASE.dll
C:\Windows\sysnative\advapi32.dll
C:\Windows\sysnative\msvcrt.dll
C:\Windows\sysnative\sechost.dll
C:\Windows\sysnative\rpcrt4.dll
C:\Windows\winsxs\amd64_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_a4d6a923711520a9\comctl32.dll
C:\Windows\sysnative\gdi32.dll
C:\Windows\sysnative\user32.dll
C:\Windows\sysnative\lpk.dll
C:\Windows\sysnative\usp10.dll
C:\Windows\sysnative\comdlg32.dll
C:\Windows\sysnative\shlwapi.dll
C:\Windows\sysnative\shell32.dll
C:\Windows\sysnative\hhctrl.ocx
C:\Windows\sysnative\ole32.dll
C:\Windows\sysnative\oleaut32.dll
C:\Windows\sysnative\imagehlp.dll
C:\Windows\sysnative\imm32.dll
C:\Windows\sysnative\msctf.dll
C:\Windows\sysnative\opengl32.dll
C:\Windows\sysnative\glu32.dll
C:\Windows\sysnative\ddraw.dll
C:\Windows\sysnative\dciman32.dll

C:\Windows\sysnative\setupapi.dll

C:\Windows\sysnative\cfgmgr32.dll

C:\Windows\sysnative\devobj.dll

C:\Windows\sysnative\dwmapi.dll

C:\Windows\sysnative\psapi.dll

C:\Windows\sysnative\version.dll

C:\Windows\sysnative\wininet.dll

C:\Windows\sysnative\urlmon.dll

C:\Windows\sysnative\crypt32.dll

C:\Windows\sysnative\msasn1.dll

C:\Windows\sysnative\iertutil.dll

C:\Windows\sysnative\ws2_32.dll

C:\Windows\sysnative\nsi.dll

C:\Windows\sysnative\wsock32.dll

C:\Windows\sysnative\api-ms-win-core-synch-l1-2-0.DLL

C:\Windows\sysnative\sspicli.dll

C:\Windows\sysnative\uxtheme.dll

C:\Windows\sysnative\msimg32.dll

C:\Windows\sysnative\CRYPTBASE.dll

C:\Windows\sysnative\clbcatq.dll

C:\Windows\sysnative\explorerframe.dll

C:\Windows\sysnative\duser.dll

C:\Windows\sysnative\dui70.dll

C:\Windows\sysnative\shfolder.dll

C:\Windows\sysnative\profapi.dll

C:\Windows\winsxs\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9ac\comctl32.dll

C:\Windows\sysnative\propsys.dll

C:\Windows\sysnative\ntmarta.dll

C:\Windows\sysnative\Wldap32.dll

RESOLVED APIS

version.dll.GetFileVersionInfoA

shfolder.dll.SHGetFolderPathA

cryptbase.dll.SystemFunction036

uxtheme.dll.ThemeInitApiHook

user32.dll.IsProcessDPIAware
setupapi.dll.CM_Get_Device_Interface_List_Size_ExW
setupapi.dll.CM_Get_Device_Interface_List_ExW
kernel32.dll.GetUserDefaultUILanguage
ole32.dll.OleInitialize
ole32.dll.OleUninitialize
ole32.dll.CoRevokeInitializeSpy
comctl32.dll.#388
oleaut32.dll.#500
advapi32.dll.UnregisterTraceGuids
comctl32.dll.#321
kernel32.dll.GetFileSize
kernel32.dll.SetFilePointer
kernel32.dll.ReadFile
kernel32.dll.WaitForMultipleObjects
kernel32.dll.GetModuleHandleA
kernel32.dll.SetFileTime
kernel32.dll.SetEndOfFile
kernel32.dll.LeaveCriticalSection
kernel32.dll.EnterCriticalSection
kernel32.dll.DeleteCriticalSection
kernel32.dll.FormatMessageW
kernel32.dll.lstrcpyW
kernel32.dll.LocalFree
kernel32.dll.IsBadReadPtr
kernel32.dll.GetSystemDirectoryW
kernel32.dll.GetCurrentThreadId
kernel32.dll.SuspendThread
kernel32.dll.TerminateThread
kernel32.dll.InitializeCriticalSection
kernel32.dll.ResetEvent
kernel32.dll.SetEvent
kernel32.dll.CreateEventW
kernel32.dll.GetVersionExW
kernel32.dll.GetModuleFileNameW

kernel32.dll.GetCurrentProcess
kernel32.dll.SetProcessWorkingSetSize
kernel32.dll.SetCurrentDirectoryW
kernel32.dll.GetDriveTypeW
kernel32.dll.CreateFileW
kernel32.dll.GetCommandLineW
kernel32.dll.GetStartupInfoW
kernel32.dll.CreateProcessW
kernel32.dll.CreateJobObjectW
kernel32.dll.ResumeThread
kernel32.dll.AssignProcessToJobObject
kernel32.dll.CreateIoCompletionPort
kernel32.dll.SetInformationJobObject
kernel32.dll.GetQueuedCompletionStatus
kernel32.dll.GetExitCodeProcess
kernel32.dll.CloseHandle
kernel32.dll.SetEnvironmentVariableW
kernel32.dll.GetTempPathW
kernel32.dll.GetSystemTimeAsFileTime
kernel32.dll.lstrlenW
kernel32.dll.CompareFileTime
kernel32.dll.SetThreadLocale
kernel32.dll.FindFirstFileW
kernel32.dll.DeleteFileW
kernel32.dll.FindNextFileW
kernel32.dll.FindClose
kernel32.dll.RemoveDirectoryW
kernel32.dll.ExpandEnvironmentStringsW
kernel32.dll.WideCharToMultiByte
kernel32.dll.VirtualAlloc
kernel32.dll.GlobalMemoryStatusEx
kernel32.dll.lstrcmpW
kernel32.dll.GetEnvironmentVariableW
kernel32.dll.lstrcmpiW

kernel32.dll.lstrlenA
kernel32.dll.GetLocaleInfoW
kernel32.dll.MultiByteToWideChar

DELETED FILES

C:\Users\user\AppData\Local\Temp\nso5034.tmp
C:\Users\user\AppData\Roaming\Fv2XsonicXTrainer\Memory.TMP
C:\Users\user\AppData\Roaming\Fv2XsonicXTrainer\Addresses.TMP
C:\Users\user\AppData\Roaming\Fv2XsonicXTrainer\Memory.UNDO
C:\Users\user\AppData\Roaming\Fv2XsonicXTrainer\Addresses.UNDO
C:\Users\user\AppData\Roaming\FV2-XSONICX-11.0_Windows64b-32b-NewUpdate.exe
C:\Users\user\AppData\Local\Temp\7ZSfx000.cmd

DELETED REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName

REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CLASSES_ROOT\.vbs

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.vbs\(Default)
HKEY_CLASSES_ROOT\.vbs\OpenWithProgids
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.vbs\OpenWithProgids
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.vbs
HKEY_CLASSES_ROOT\VBSFile
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\VBSFile\CurVer
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\VBSFile\
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\VBSFile\ShellEx\IconHandler
HKEY_CLASSES_ROOT\SystemFileAssociations\.vbs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.vbs\PerceivedType
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\VBSFile\DocObject
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\VBSFile\BrowseInPlace
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.vbs\Content Type
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\VBSFile\Clsid
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\VBSFile\IsShortcut
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\VBSFile\AlwaysShowExt
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\VBSFile\NeverShowExt
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\UsersFiles\NameSpace
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\UsersFiles\NameSpace\DelegateFolders
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\UsersFiles\NameSpace\DelegateFolders\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\UsersFiles\NameSpace\DelegateFolders\(Default)
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UsersFiles\NameSpace
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\UsersFiles\NameSpace\DelegateFolders
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\UsersFiles\NameSpace\DelegateFolders\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\UsersFiles\NameSpace\DelegateFolders\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\SuppressionPolicy
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UsersFiles\NameSpace\DelegateFolders
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\UsersFiles\NameSpace
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\UsersFiles\NameSpace\DelegateFolders
HKEY_CLASSES_ROOT\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\InProcServer32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\InProcServer32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}\InProcServer32\LoadWithoutCOM
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Objects\{DFFACDC5-679F-4156-8947-C5C76BC0B67F}
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\KindMap

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\KindMap\.vbs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\VBSFile\NoStaticDefaultVerb
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\VBSFile\shell
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\VBSFile\Shell\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\VBSFile\Shell\Open
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\VBSFile\Shell\Open\NeverDefault
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\VBSFile\Shell\Open\
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\VBSFile\Shell\Open\command
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\VBSFile\Shell\Open\Command\DelegateExecute
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\VBSFile\Shell\Open\DropTarget
HKEY_CLASSES_ROOT\.ade
HKEY_CLASSES_ROOT\.adp
HKEY_CLASSES_ROOT\.app
HKEY_CLASSES_ROOT\.asp
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.asp\(Default)
HKEY_CLASSES_ROOT\.bas
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.bas\(Default)
HKEY_CLASSES_ROOT\.bat
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.bat\(Default)
HKEY_CLASSES_ROOT\.cer
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.cer\(Default)
HKEY_CLASSES_ROOT\.chm
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.chm\(Default)
HKEY_CLASSES_ROOT\.cmd
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.cmd\(Default)
HKEY_CLASSES_ROOT\.com
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.com\(Default)
HKEY_CLASSES_ROOT\.cpl

EXECUTED COMMANDS

C:\Users\user\AppData\Roaming\FV2-XSONICX-11.0_Windows64b-32b-NewUpdate.exe
"C:\Windows\System32\WScript.exe" "C:\Users\user\AppData\Roaming\Patch.vbs"
C:\Users\user\AppData\Roaming\Patch.vbs
C:\Users\user\AppData\Roaming\Fv2XsonicXTrainer\FV2-XSONICX(Windows 64Bits).exe
C:\Users\user\AppData\Local\Temp\7ZSfx000.cmd

C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding

C:\Windows\system32\DllHost.exe /Processid:{AB8902B4-09CA-4BB6-B78D-A8F59079A8D5}

READ FILES

\Device\KsecDD

C:\Users\user\AppData\Local\Temp\nso5034.tmp

C:\Users\user\AppData\Local\Temp\11b7e6fe10e891a7ce79fb97c5b2fb791b05d79e.exe

C:\Users\user\AppData\Roaming\Patch.vbs

C:\Windows\System32\wscript.exe

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

C:\Users\user\AppData\Roaming\FV2-XSONICX-11.0_Windows64b-32b-NewUpdate.exe

C:\

C:\Users\desktop.ini

C:\Users

C:\Users\user

C:\Users\user\AppData

C:\Users\user\AppData\Roaming

C:\Users\user\AppData\Roaming\Fv2XsonicXTrainer

\??\PIPE\srvsvc

C:\Users\user\AppData\Roaming\Fv2XsonicXTrainer\FV2-XSONICX(Windows 32Bits).exe

C:\Users\Public\Desktop\Fv2XsonicX Trainer 32bits.lnk

C:\Users\user\AppData\Roaming\Fv2XsonicXTrainer\FV2-XSONICX(Windows 64Bits).exe

C:\Users\Public\Desktop\Fv2XsonicX Trainer 64bits.lnk

C:\Users\user\Desktop\Fv2XsonicX Trainer 32bits.lnk

C:\Users\user\Desktop\Fv2XsonicX Trainer 64bits.lnk

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Fv2XsonicX Trainer 64bits.lnk

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Fv2XsonicX Trainer 32bits.lnk

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Fv2XsonicX Trainer 32bits .lnk

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Fv2XsonicX Trainer 64bits.lnk

C:\ProgramData\Microsoft\Windows\Start Menu\Fv2XsonicX Trainer 32bits.lnk

C:\ProgramData\Microsoft\Windows\Start Menu\Fv2XsonicX Trainer 64bits.lnk

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Fv2XsonicX Trainer 32bits.lnk

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Fv2XsonicX Trainer 64bits.lnk

C:\Windows\SysWOW64\wscript.exe

C:\Windows\SysWOW64\wshom.ocx

C:\Windows\SysWOW64\shell32.dll
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x000000000000004a.db
C:\Users\Public\desktop.ini
C:\Users\Public
C:\Users\Public\Desktop\desktop.ini
C:\ProgramData
C:\ProgramData\Microsoft\desktop.ini
C:\ProgramData\Microsoft
C:\ProgramData\Microsoft\Windows
C:\ProgramData\Microsoft\Windows\Start Menu\desktop.ini
C:\Users\user\Desktop\desktop.ini
C:\ProgramData\Microsoft\Windows\Start Menu
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\desktop.ini
C:\ProgramData\Microsoft\Windows\Start Menu\Programs
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft
C:\Users\user\AppData\Roaming\Microsoft\Windows
C:\Windows
C:\Windows\Fonts\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\SendTo\Desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini
C:\Users\user\Favorites\desktop.ini
C:\Users\user\Documents\desktop.ini
C:\Windows\System32\msxml3.dll\1
C:\Windows\System32\msxml3.dll
C:\Windows\System32\wbem\wbemdisp.tlb
C:\Windows\SysWOW64\stdole2.tlb
C:\Windows\winsxs\amd64_microsoft.windows.c..-controls.resources_6595b64144ccf1df_5.82.7600.16385_en-us_ba5641d1849f93bc\comctl32.dll.mui

C:\Windows\sysnative\shell32.dll
C:\Windows\sysnative\ntdll.dll
C:\Windows\sysnative\kernel32.dll
C:\Windows\sysnative\KERNELBASE.dll
C:\Windows\sysnative\advapi32.dll
C:\Windows\sysnative\msvcrt.dll
C:\Windows\sysnative\sechost.dll
C:\Windows\sysnative\rpcrt4.dll
C:\Windows\winsxs\amd64_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_a4d6a923711520a9\comctl32.dll
C:\Windows\sysnative\gdi32.dll

MUTEXES

Local\!IETld!Mutex
Local\ZonesCounterMutex
Local\ZoneAttributeCacheCounterMutex
Local\ZonesCacheCounterMutex
Local\ZonesLockedCacheCounterMutex
IESQMMUTEX_0_208
DBWinMutex
CicLoadWinStaWinSta0
Local\MSCTF.CtfMonitorInstMutexDefault1

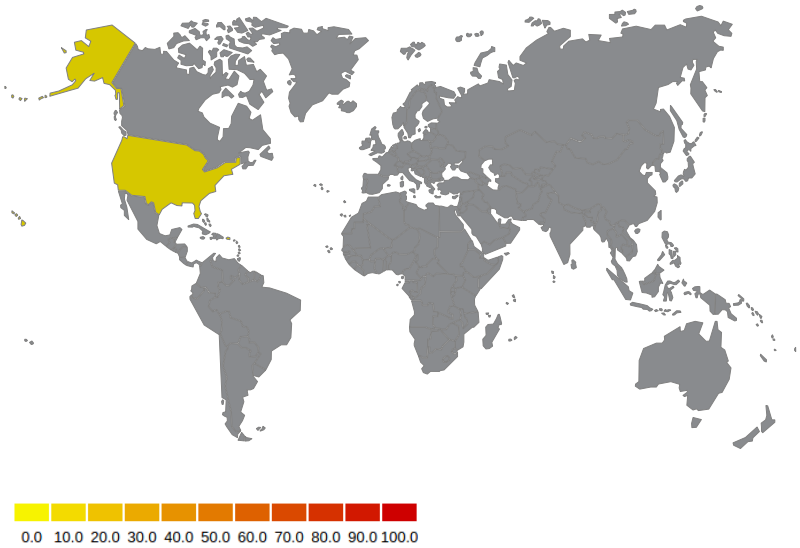
MODIFIED REGISTRY KEYS

HKEY_LOCAL_MACHINE\software\Patch
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Patch\(Default)
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Patch
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\Patch
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect
HKEY_CURRENT_USER\Software\Cheat Engine
HKEY_CURRENT_USER\Software\Cheat Engine\DPI Aware
HKEY_CURRENT_USER\Software\Cheat Engine\Window Positions 96
HKEY_CURRENT_USER\Software\Cheat Engine\Window Positions 96\AdvancedOptions Position
HKEY_CURRENT_USER\Software\Cheat Engine\Window Positions 96\frmAutoInject Position
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecisionReason

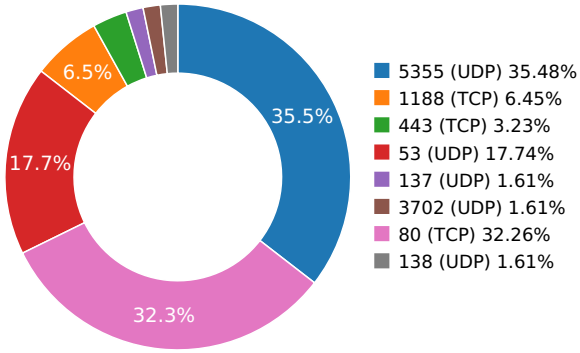
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecisionTime
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecision
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadNetworkName
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecisionReason
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecisionTime
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecision
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\WpadLastNetwork
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\LastServiceStart
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Transports\Decoupled\Server
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Server\CreationTime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Server\MarshaledProxy
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Server\ProcessIdentifier
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\ConfigValueEssNeedsLoading
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\List of event-active namespaces
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\ESS\//./root/CIMV2\SCM Event Provider

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type
	8.8.4.4	United States	15169	Level 3 Parent, LLC	Malware Process
	104.20.209.21	United States	13335	Cloudflare, Inc.	Malware Process
	184.24.97.184	United States	20940	Akamai Technologies, Inc.	OS Process
	23.67.251.10	United States	20940	Akamai Technologies, Inc.	Malware Process
ocsp.comodoca4.com	184.84.243.43	Canada	20940	Akamai Technologies, Inc.	Malware Process
crl.globalsign.net	104.31.74.124	United States	13335	Cloudflare, Inc.	Malware Process
ctldl.windowsupdate.com	184.26.44.105	United States	20940	Akamai Technologies, Inc.	OS Process
s.dropcanvas.com	69.55.50.17	United States	14061	ServerStack, Inc.	Malware Process
crl.microsoft.com	23.72.137.121	United States	20940	Akamai Technologies, Inc.	OS Process
crl.comodoca.com	104.16.91.188	United States	13335	Cloudflare, Inc.	Malware Process
raw.githubusercontent.com	151.101.0.133	United States	54113	Fastly	Malware Process
ocsp.usertrust.com	178.255.83.1	United States	35838		OS Process
ocsp.digicert.com	72.21.91.29	United States	15133	MCI Communications Service...	Malware Process
pastebin.com	104.20.208.21	United States	13335	Cloudflare, Inc.	Malware Process
musigiallifuck.ddns.net	95.248.69.185	Italy	3269		Malware Process

HTTP PACKETS

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
ctldl.windowsupdate.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	46.5231328011
Path: /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?e1c0d2221d06bcfd **URI:** http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?e1c0d2221d06bcfd						
ocsp.usertrust.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	53.6929779053

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBR8sWZUnKvbRO5iJhat9GV793rVlAQUrb2YejS0Jvf6xCZU7wO94CTLVBoCECdm7lbrSfOOq9dwovyE3iI%3D **URI:** http://ocsp.usertrust.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBR8sWZUnKvbRO5iJhat9GV793rVlAQUrb2YejS0Jvf6xCZU7wO94CTLVBoCECdm7lbrSfOOq9dwovyE3iI%3D						
ocsp.comodoca4.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	61.640996933
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBReAhtobFzTvhaRmVeJ38QUchY9AwQUu69%2BAj36pvE8hI6t7jiY7NkyMtQCEAui0B3Ly3d26KxlCXrBJUE%3D **URI:** http://ocsp.comodoca4.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBReAhtobFzTvhaRmVeJ38QUchY9AwQUu69%2BAj36pvE8hI6t7jiY7NkyMtQCEAui0B3Ly3d26KxlCXrBJUE%3D						
crl.comodoca.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	65.7525908947
Path: /COMODORSACertificationAuthority.crl **URI:** http://crl.comodoca.com/COMODORSACertificationAuthority.crl						
ocsp.digicert.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	66.331900835
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTfqhLjKLEJQZPin0KCzkdAQpVYowQUsT7DaQP4v0cB1JgmGggC72NkK8MCEATh56TcXPLzbcArQrhdFZ8%3D **URI:** http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTfqhLjKLEJQZPin0KCzkdAQpVYowQUsT7DaQP4v0cB1JgmGggC72NkK8MCEATh56TcXPLzbcArQrhdFZ8%3D						
s.dropcanvas.com	80	GET	1.1	Cheat Engine 6.6 : luascript	1	67.093364954
Path: /1000000/965000/964641/FV2-XSONICX.XSONICX **URI:** http://s.dropcanvas.com/1000000/965000/964641/FV2-XSONICX.XSONICX						
s.dropcanvas.com	80	GET	1.1	Cheat Engine 6.6 : luascript	1	67.286482811
Path: /1000000/930000/929710/updates.txt **URI:** http://s.dropcanvas.com/1000000/930000/929710/updates.txt						
musigiallifuck.ddns.net:1188	1188	POST	1.1	20503A4E<|>V-PC<|>user<..	3	91.0382080078
Path: /is-ready **URI:** http://musigiallifuck.ddns.net:1188/is-ready						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	97.0456748009
Path: /pki/crl/products/tspca.crl **URI:** http://crl.microsoft.com/pki/crl/products/tspca.crl						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	103.468065023
Path: /pki/crl/products/CodeSignPCA2.crl **URI:** http://crl.microsoft.com/pki/crl/products/CodeSignPCA2.crl						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	109.719549894
Path: /pki/crl/products/WinPCA.crl **URI:** http://crl.microsoft.com/pki/crl/products/WinPCA.crl						
crl.globalsign.net	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	116.183516979
Path: /primobject.crl **URI:** http://crl.globalsign.net/primobject.crl						

DNS QUERIES

Request	Type
pastebin.com	A

Request	Type
Answers - 104.20.209.21 (A) - 104.20.208.21 (A)	
ctldl.windowsupdate.com	A
Answers - ctldl.windowsupdate.nsatc.net (CNAME) - 184.26.44.105 (A) - a1621.g.akamai.net (CNAME) - 184.26.44.97 (A) - ctldl.windowsupdate.com.edgesuite.net (CNAME)	
ocsp.usertrust.com	A
Answers - 178.255.83.1 (A)	
raw.githubusercontent.com	A
Answers - github.map.fastly.net (CNAME) - 151.101.128.133 (A) - 151.101.0.133 (A) - 151.101.64.133 (A) - 151.101.192.133 (A)	
ocsp.comodoca4.com	A
Answers - ocsp.comodoca4.com.edgesuite.net (CNAME) - 23.67.251.10 (A) - a875.dscb.akamai.net (CNAME) - 23.67.251.18 (A)	
crl.comodoca.com	A
Answers - crl.comodoca.com.cdn.cloudflare.net (CNAME) - 104.16.92.188 (A) - 104.16.93.188 (A) - 104.16.90.188 (A) - 104.16.91.188 (A) - 104.16.89.188 (A)	
ocsp.digicert.com	A
Answers - cs9.wac.phicdn.net (CNAME) - 72.21.91.29 (A)	
s.dropcanvas.com	A
Answers - www.dropcanvas.com (CNAME) - 69.55.50.17 (A)	
musigiallifuck.ddns.net	A
Answers - 95.248.69.185 (A)	
crl.microsoft.com	A

Request	Type
Answers - 184.24.97.184 (A) - crl.www.ms.akadns.net (CNAME) - 184.24.97.182 (A) - a1363.dscg.akamai.net (CNAME)	
crl.globalsign.net	A
Answers - 104.31.75.124 (A) - global.prd.cdn.globalsign.com (CNAME) - cdn.globalsigncdn.com.cdn.cloudflare.net (CNAME) - 104.31.74.124 (A)	

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
38.7308828831	Sandbox	104.20.209.21	443
46.5231328011	Sandbox	184.26.44.105	80
53.6929779053	Sandbox	178.255.83.1	80
59.4904308319	Sandbox	151.101.0.133	443
61.640996933	Sandbox	23.67.251.10	80
65.7525908947	Sandbox	104.16.91.188	80
66.331900835	Sandbox	72.21.91.29	80
67.093364954	Sandbox	69.55.50.17	80
67.286482811	Sandbox	69.55.50.17	80
91.0382080078	Sandbox	95.248.69.185	1188
97.0456748009	Sandbox	184.24.97.184	80
116.183516979	Sandbox	104.31.74.124	80
155.096805811	Sandbox	95.248.69.185	1188
220.604798794	Sandbox	95.248.69.185	1188

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.17365193367	Sandbox	224.0.0.252	5355
3.27274799347	Sandbox	192.168.56.255	137
3.34808301926	Sandbox	224.0.0.252	5355
3.73211288452	Sandbox	239.255.255.250	3702
5.92567801476	Sandbox	224.0.0.252	5355
9.31417798996	Sandbox	192.168.56.255	138
34.7830469608	Sandbox	224.0.0.252	5355
38.675360918	Sandbox	8.8.4.4	53

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
40.7516458035	Sandbox	224.0.0.252	5355
43.6286668777	Sandbox	224.0.0.252	5355
46.3764498234	Sandbox	8.8.4.4	53
47.5323758125	Sandbox	224.0.0.252	5355
50.7057919502	Sandbox	224.0.0.252	5355
53.6736409664	Sandbox	8.8.4.4	53
55.4238770008	Sandbox	224.0.0.252	5355
58.7356908321	Sandbox	224.0.0.252	5355
59.4415400028	Sandbox	8.8.4.4	53
59.5854058266	Sandbox	224.0.0.252	5355
60.1270890236	Sandbox	224.0.0.252	5355
61.5953509808	Sandbox	8.8.4.4	53
62.7766568661	Sandbox	224.0.0.252	5355
63.5413689613	Sandbox	224.0.0.252	5355
65.7055039406	Sandbox	8.8.4.4	53
66.28510499	Sandbox	8.8.4.4	53
66.9551999569	Sandbox	8.8.4.4	53
90.8717639446	Sandbox	8.8.4.4	53
90.9701178074	Sandbox	224.0.0.252	5355
94.207005024	Sandbox	224.0.0.252	5355
96.9701759815	Sandbox	8.8.4.4	53
98.0075478554	Sandbox	224.0.0.252	5355
100.876696825	Sandbox	224.0.0.252	5355
103.612162828	Sandbox	224.0.0.252	5355
107.111351013	Sandbox	224.0.0.252	5355
110.026763916	Sandbox	224.0.0.252	5355
113.473032951	Sandbox	224.0.0.252	5355
116.12714386	Sandbox	8.8.4.4	53

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Roaming\FV2-XSONICX-11.0_Windows64b-32b-NewUpdate.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed **MD5 :** 81af0599f74639b1e23e01a6777ff897 **SHA-1 :** c83942992611f215c93d3c6d9c5508683258f935 **SHA-256 :** f2b387e6a1c43177cc5f03898b50abc2c551866a(**SHA-512 :** 59b63baa08824aa07b195b80427f495c2c11750f **Size :** 5726.955 Kilobytes.
C:\Users\User\AppData\Local\Temp\7ZSfx000.Cmd	**Type :** ASCII text, with CRLF line terminators **MD5 :** 5b5c89fad0c121babbc61fa910ebdc7e **SHA-1 :** d3d945561dbdd43ad66454be40ed56142b9ff076 **SHA-256 :** 33a563c4cfd07878b0cde60d973e01b4ec1f58d1 **SHA-512 :** ac7adace825b2f18389fb470affa7061be87f470e **Size :** 0.245 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	None
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	11b7e6fe10e891a7ce79fb97c5b2fb791b05d79e
MD5:	b6234d7441ac12355aedf64c746e8f5f
First Seen Date:	2018-05-15 12:48:48.197400 (about a year ago)
Number Of Clients Seen:	2
Last Analysis Date:	2018-05-15 12:48:48.197400 (about a year ago)
Human Expert Analysis Date:	2019-01-20 16:52:19.705085 (10 months ago)
Human Expert Analysis Result:	Malware

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	[]
Compilation Time Stamp	0x567F796F [Sun Dec 27 05:38:55 2015 UTC]
Entry Point	0x40310d (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	5707548
Ssdeep	
Sha256	d4f90dc46dd8387121719e4d731b8941e06b7eb63ef9b624f93fe288490f174f
Exifinfo	[]
Mime Type	application/x-dosexec
Imphash	

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x5e3c	0x6000	6.43229528851	1a13b408c917b27c9106545148d3b8d3
.rdata	0x7000	0x126a	0x1400	5.00588726545	921acf8cb0aea87c0603fa899765fcc2
.data	0x9000	0x25d38	0x600	4.29175604973	797517c6ef57aa95d53df2cf07568953
.ndata	0x2f000	0x8000	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.rsrc	0x37000	0x3928	0x3a00	7.46089774173	f56cde0bb2ac18bfabb860fa4a7a98ce

PE Resources

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 225680, u'sha256': u'6e5b099c83fc58147be4744c8b808de616ef5bd92282f9fff54f7f5dccf1191e', u'type': u'dBase IV DBT of \\200.DBF, blocks size 0, block length 12288, next free block index 40, next free block 2899965097, next used block 4002992881', u'size': 12840}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_DIALOG', u'offset': 238520, u'sha256': u'fecdb955f8d7f1c219ff8167f90b64f3cb52e53337494577ff73c0ac1dafcd96', u'type': u'data', u'size': 256}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_DIALOG', u'offset': 238776, u'sha256': u'69897c784f1491eb3024b0d52c2897196a2e245974497fda1915db5fefcf8729', u'type': u'data', u'size': 284}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_DIALOG', u'offset': 239064, u'sha256': u'85025c8556952f6a651c2468c8a0d58853b0ba482be9ad5cd3060f216540dfc0', u'type': u'data', u'size': 96}

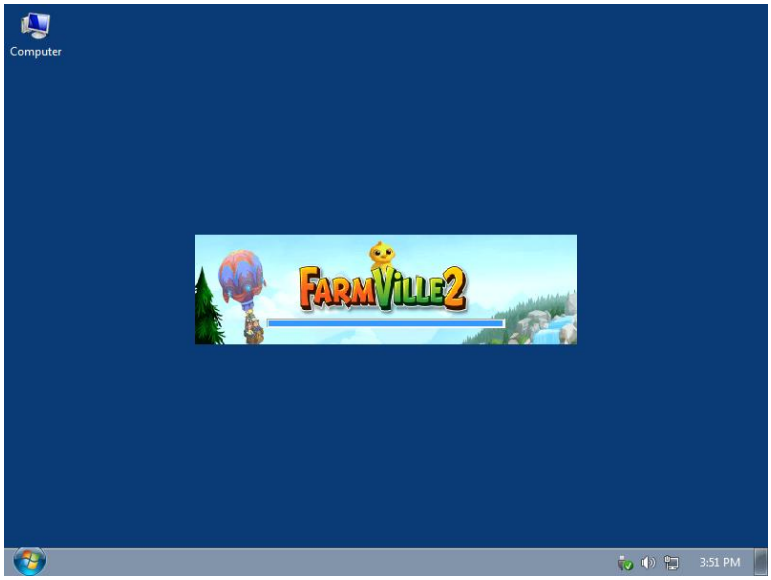
{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_ICON', u'offset': 239160, u'sha256': u'4e80c0b99ba6b3d510c73c163d7ae04afe361f76d022ef8c81ef3926df7cfee3', u'type': u'MS Windows icon resource - 1 icon, 64x128', u'size': 20}

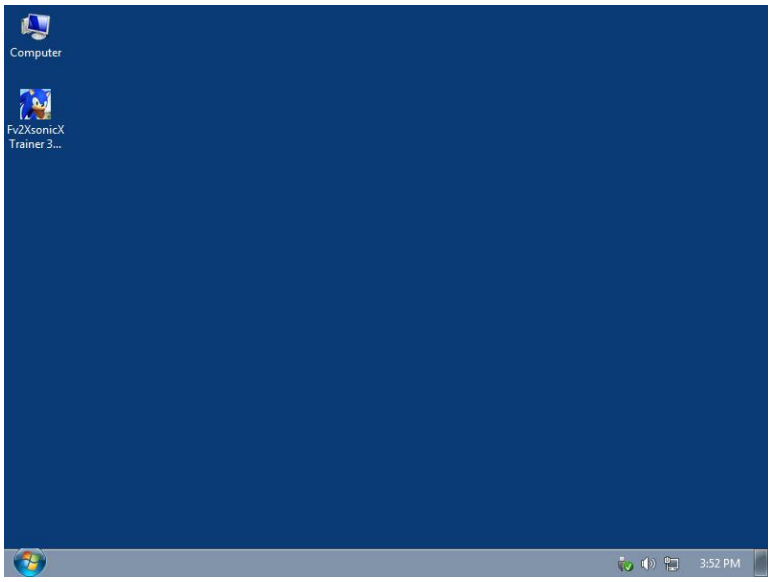
{u'lang': u'LANG_ENGLISH', u'name': u'RT_MANIFEST', u'offset': 239184, u'sha256': u'bbed26dc3b9eca44c2dccffc1c644a5fc9cd50e828ccc2db366cb389beb35b50', u'type': u'XML 1.0 document, ASCII text, with very long lines, with no line terminators', u'size': 727}

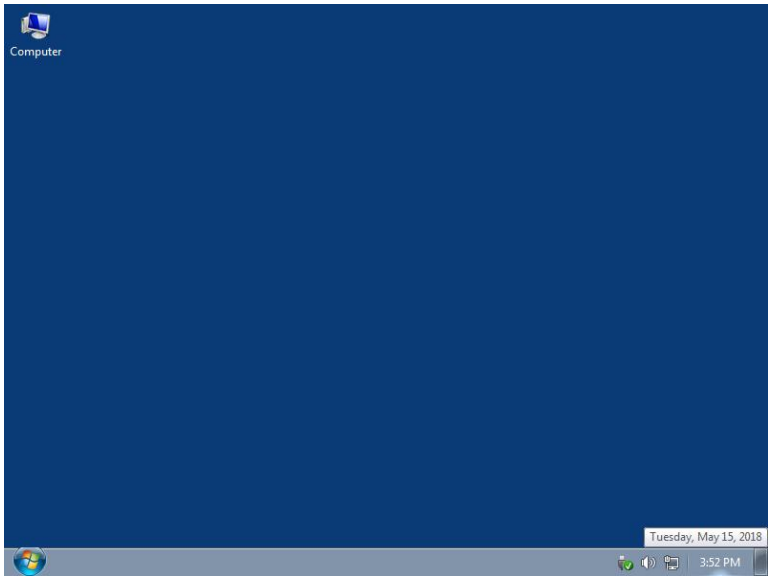
CERTIFICATE VALIDATION

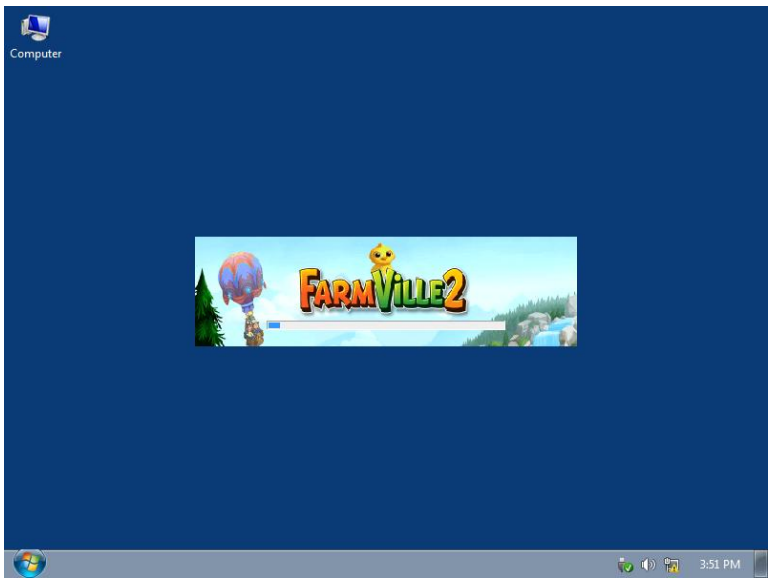
- Certificate Validation is not Applicable ?

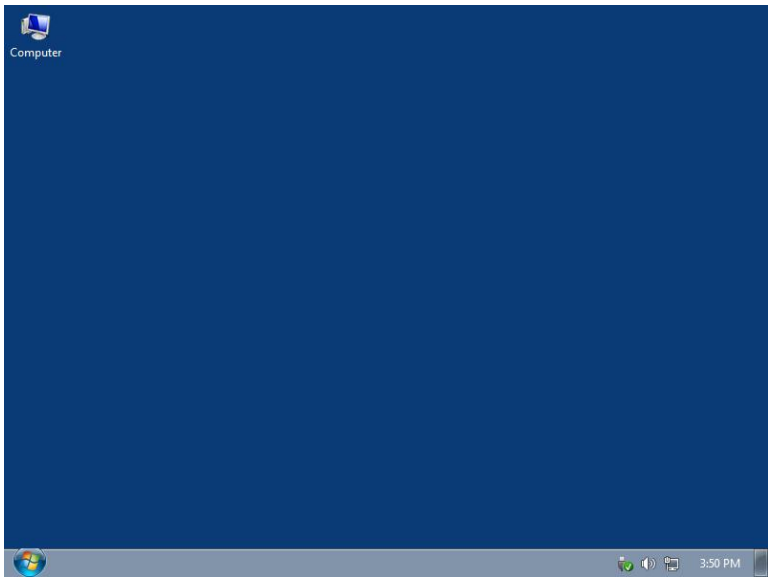
SCREENSHOTS

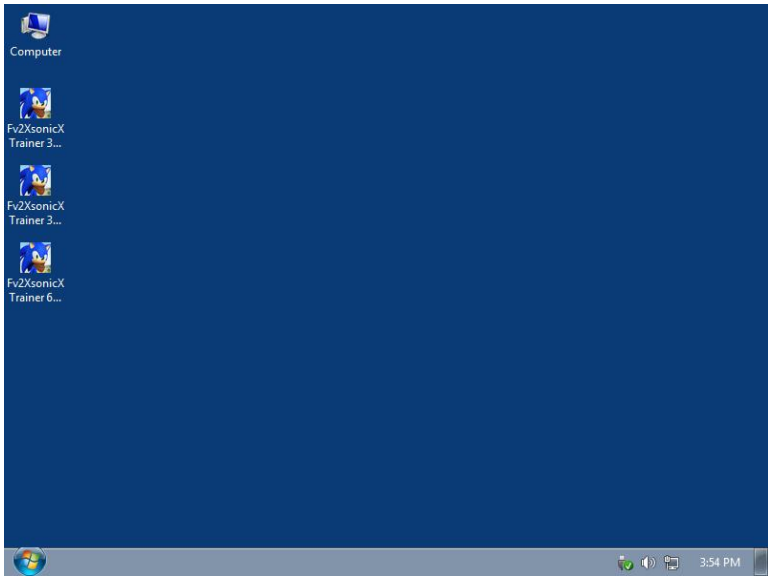


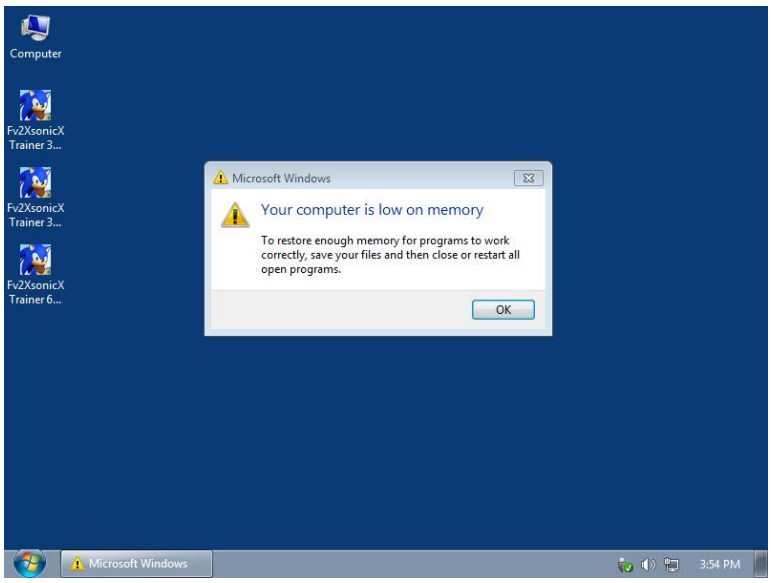

Computer
Fv2XsonicX Trainer 3...
3:52 PM

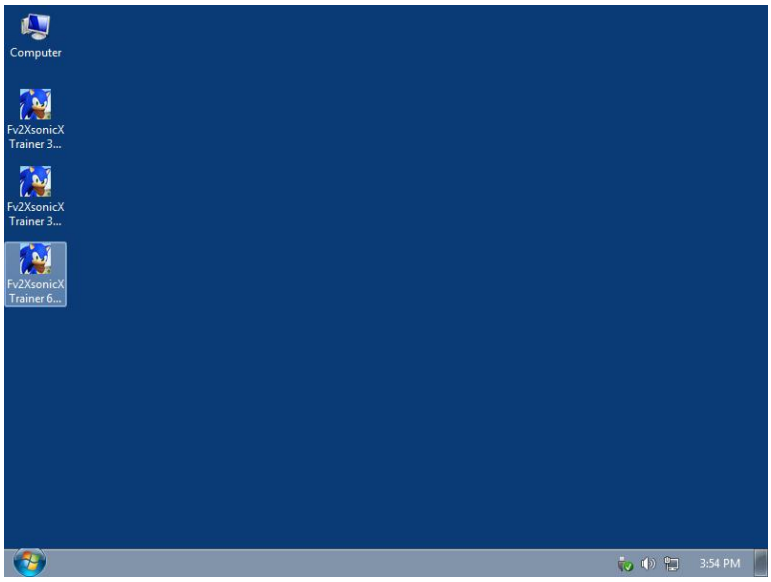

Computer
Tuesday, May 15, 2018
3:52 PM


Computer
FARMVILLE2
3:51 PM

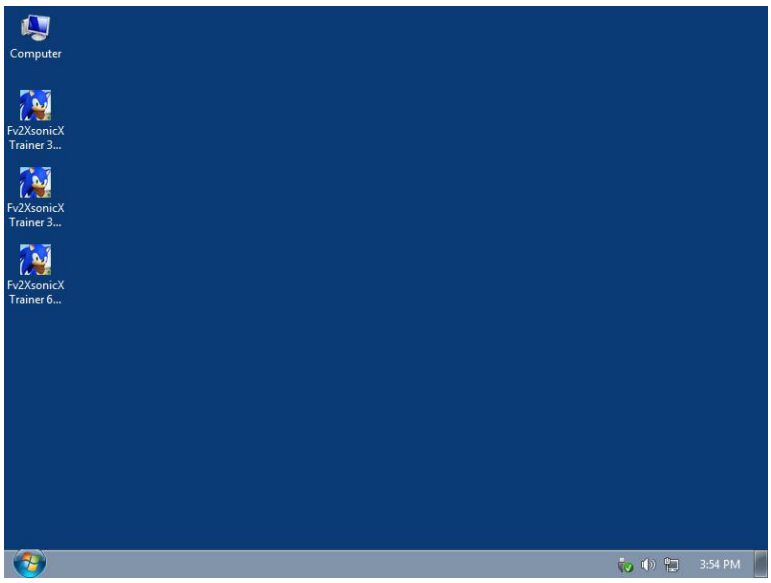

Computer
3:50 PM


Computer
Fv2XsonicX Trainer 3...
Fv2XsonicX Trainer 3...
Fv2XsonicX Trainer 6...
3:54 PM


Computer
Fv2XsonicX Trainer 3...
Fv2XsonicX Trainer 3...
Fv2XsonicX Trainer 6...
Microsoft Windows
Your computer is low on memory
To restore enough memory for programs to work correctly, save your files and then close or restart all open programs.
OK
Microsoft Windows
3:54 PM


Computer
Fv2XsonicX Trainer 3...
Fv2XsonicX Trainer 3...
Fv2XsonicX Trainer 6...
3:54 PM


Computer
3:52 PM


Computer
Fv2XsonicX Trainer 3...
Fv2XsonicX Trainer 3...
Fv2XsonicX Trainer 6...
3:54 PM


Computer
3:51 PM