Summary

File Name: Ultimate_Defender_Pro_Shield.exe

File Type: PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows

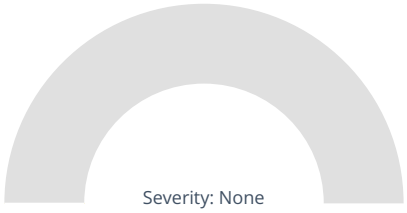
SHA1: f287d570ad26bf3a80479f5ec4301c07fa893f7d

MD5: 66419aebce8e32a65673723580f30a9c

CLEAN

Valkyrie Final Verdict

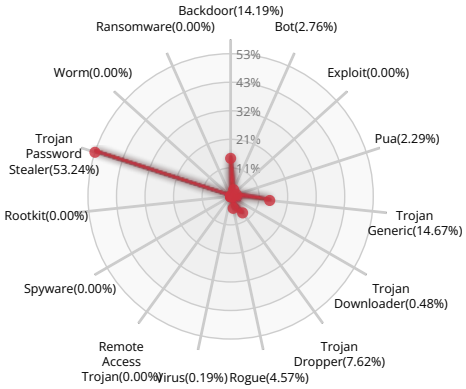
DETECTION SECTION



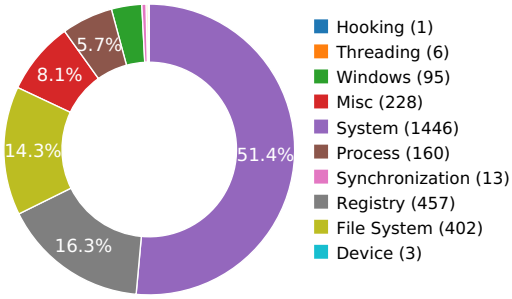
Severity: None

Verdict: Clean

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

VALKYRIE COMODO

Activity Details

INFORMATION DISCOVERY

Reads data out of its own binary image — Show sources

MALWARE ANALYSIS SYSTEM EVASION

Network activity detected but not expressed in API logs

PERSISTENCE AND INSTALLATION BEHAVIOR

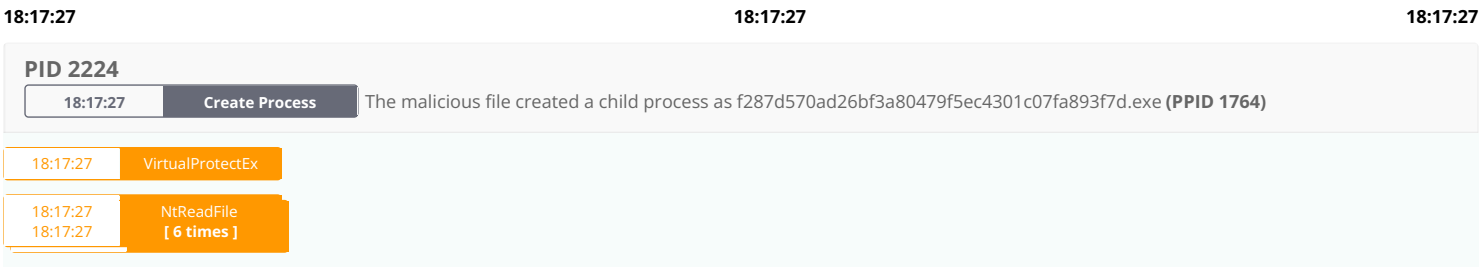
Installs itself for autorun at Windows startup — Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory — Show sources

VALKYRIE COMODO

Behavior Graph



VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Windows\System32\MSCOREE.DLL.local
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscoreei.dll
C:\Windows\Microsoft.NET\Framework*
C:\Windows\Microsoft.NET\Framework\v1.0.3705\clr.dll
C:\Windows\Microsoft.NET\Framework\v1.0.3705\mscorwks.dll
C:\Windows\Microsoft.NET\Framework\v1.1.4322\clr.dll
C:\Windows\Microsoft.NET\Framework\v1.1.4322\mscorwks.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\clr.dll
C:\Windows\System32\tzres.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\clr.dll
C:\Users\user\AppData\Local\Temp\f287d570ad26bf3a80479f5ec4301c07fa893f7d.exe.config
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Users\user\AppData\Local\Temp\f287d570ad26bf3a80479f5ec4301c07fa893f7d.exe
C:\Program Files\Common Files\System\symsrv.dll
C:\Users\user\AppData\Local\Temp\A1D26E2
C:\Users\user\AppData\Local\Temp\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\System32\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\system\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\ProgramData\Oracle\Java\javapath\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\System32\wbem\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\System32\WindowsPowerShell\v1.0\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Program Files\Microsoft Network Monitor 3\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Program Files (x86)\Universal Extractor\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Program Files (x86)\Universal Extractor\bin\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Program Files (x86)\Windows Kits\8.1\Windows Performance Toolkit\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Python27\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Python27\Scripts\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\tools\sysinternals\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\tools\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\tools\IDA_Pro_v6\python\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSVCR120_CLR0400.dll
C:\Windows\System32\MSVCR120_CLR0400.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscoree.dll

C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config
C:\Windows\Microsoft.NET\Framework\v4.0.30319\fusion.localgac
C:\Windows\Microsoft.Net\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib*
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\225759bb87c854c0fff27b1d84858c21\mscorlib.ni.dll
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\225759bb87c854c0fff27b1d84858c21\mscorlib.ni.dll.aux
C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Local
C:\Users\user\AppData\Local\Temp
C:\Windows\Microsoft.NET\Framework\v4.0.30319\ole32.dll
\Device\KsecDD
C:\Windows\assembly\NativeImages_v4.0.30319_32\Ultimate De76facb51#*
C:\Users\user\AppData\Local\Temp\f287d570ad26bf3a80479f5ec4301c07fa893f7d.INI
C:\Windows\Microsoft.NET\Framework\v4.0.30319\clrjit.dll
C:\Windows\assembly\pubpol20.dat
C:\Windows\assembly\GAC\PublisherPolicy.tme
C:\Windows\Microsoft.Net\assembly\GAC_32\System.Windows.Forms\v4.0_4.0.0.0__b77a5c561934e089\System.Windows.Forms.dll
C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Windows.Forms\v4.0_4.0.0.0__b77a5c561934e089\System.Windows.Forms.dll
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms*
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\5aac750b35b27770dccb1a43f83cced7\System.Windows.Forms.ni.dll
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\5aac750b35b27770dccb1a43f83cced7\System.Windows.Forms.ni.dll.aux
C:\Windows\Microsoft.Net\assembly\GAC_32\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll
C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll
C:\Windows\assembly\NativeImages_v4.0.30319_32\System*
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\52cca48930e580e3189eac47158c20be\System.ni.dll
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\52cca48930e580e3189eac47158c20be\System.ni.dll.aux
C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Configuration\v4.0_4.0.0.0__b03f5f7f11d50a3a\System.Configuration.dll
C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Xml\v4.0_4.0.0.0__b77a5c561934e089\System.Xml.dll
C:\Windows\Microsoft.Net\assembly\GAC_32\System.Drawing\v4.0_4.0.0.0__b03f5f7f11d50a3a\System.Drawing.dll
C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Drawing\v4.0_4.0.0.0__b03f5f7f11d50a3a\System.Drawing.dll
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing*
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\646b4b01cb29986f8e076aa65c9e9753\System.Drawing.ni.dll
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\646b4b01cb29986f8e076aa65c9e9753\System.Drawing.ni.dll.aux
C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Security\v4.0_4.0.0.0__b03f5f7f11d50a3a\System.Security.dll
C:\Windows\Microsoft.Net\assembly\GAC_MSIL\Accessibility\v4.0_4.0.0.0__b03f5f7f11d50a3a\Accessibility.dll
C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Core\v4.0_4.0.0.0__b77a5c561934e089\System.Core.dll

C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Deployment\v4.0_4.0.0.0__b03f5f7f11d50a3a\System.Deployment.dll
C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Runtime.Serialization.Formatters.Soap\v4.0_4.0.0.0__b03f5f7f11d50a3a\System.Runtime.Serialization.Formatters.Soap.dll
C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Windows.Forms\v4.0_4.0.0.0__b77a5c561934e089\uxtheme.dll

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\InstallRoot
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\CLRLoadLogDir
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\UseLegacyV2RuntimeActivationPolicyDefaultValue
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\OnlyUseLatestCLR
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Fusion\NoClientChecks
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NET Framework Setup\NDP\v4\Full\Release
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\DisableConfigCache
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\CacheLocation
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\DownloadCacheQuotaInKB
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\EnableLog
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\LoggingLevel
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\ForceLog
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\LogFailures
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\LogResourceBinds
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\FileInUseRetryAttempts
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\FileInUseMillisecondsBetweenRetries
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\UseLegacyIdentityFormat
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\DisableMSIPeek
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DevOverrideEnable
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\NGen\Policy\v4.0\OptimizeUsedBinaries
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\AltJit
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\Latest
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\index20
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\LegacyPolicyTimeStamp
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
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\.NETFramework\DbgJITDebugLaunchSetting
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\DbgManagedDebugger
HKEY_CURRENT_USER\Software\Microsoft\GDIPlus\FontCachePath

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\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en

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\Classes\Wow6432Node\CLSID\{0A29FF9E-7F9C-4437-8B11-F424491E3931}\InprocServer32\(Default)

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{0A29FF9E-7F9C-4437-8B11-F424491E3931}\Server\(Default)

MODIFIED FILES

C:\Users\user\AppData\Local\GDIPFONTCACHEV1.DAT

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Ultimate Defender Pro Shield.exe

RESOLVED APIS

advapi32.dll.RegOpenKeyExW

advapi32.dll.RegQueryInfoKeyW

advapi32.dll.RegEnumKeyExW

advapi32.dll.RegEnumValueW

advapi32.dll.RegCloseKey

advapi32.dll.RegQueryValueExW

kernel32.dll.FlsAlloc

kernel32.dll.FlsFree

kernel32.dll.FlsGetValue
kernel32.dll.FlsSetValue
kernel32.dll.InitializeCriticalSectionEx
kernel32.dll.CreateEventExW
kernel32.dll.CreateSemaphoreExW
kernel32.dll.SetThreadStackGuarantee
kernel32.dll.CreateThreadpoolTimer
kernel32.dll.SetThreadpoolTimer
kernel32.dll.WaitForThreadpoolTimerCallbacks
kernel32.dll.CloseThreadpoolTimer
kernel32.dll.CreateThreadpoolWait
kernel32.dll.SetThreadpoolWait
kernel32.dll.CloseThreadpoolWait
kernel32.dll.FlushProcessWriteBuffers
kernel32.dll.FreeLibraryWhenCallbackReturns
kernel32.dll.GetCurrentProcessorNumber
kernel32.dll.GetLogicalProcessorInformation
kernel32.dll.CreateSymbolicLinkW
kernel32.dll.EnumSystemLocalesEx
kernel32.dll.CompareStringEx
kernel32.dll.GetDateFormatEx
kernel32.dll.GetLocaleInfoEx
kernel32.dll.GetTimeFormatEx
kernel32.dll.GetUserDefaultLocaleName
kernel32.dll.IsValidLocaleName
kernel32.dll.LCMapStringEx
kernel32.dll.GetTickCount64
advapi32.dll.EventRegister
mscoree.dll.#142
mscoreei.dll.RegisterShimImplCallback
mscoreei.dll.OnShimDllMainCalled
mscoreei.dll._CorExeMain
kernel32.dll.OpenProcess
kernel32.dll.TerminateProcess
kernel32.dll.WriteProcessMemory
kernel32.dll.VirtualAllocEx
advapi32.dll.AdjustTokenPrivileges
user32.dll.MessageBoxTimeoutW

wintrust.dll.WinVerifyTrust
kernel32.dll.CreateProcessInternalW
shlwapi.dll.UrlIsW
kernel32.dll.SortGetHandle
kernel32.dll.SortCloseHandle
ws2help.dll.WahReferenceContextByHandle
ntdll.dll.KiUserExceptionDispatcher
version.dll.GetFileVersionInfoSizeW
version.dll.GetFileVersionInfoW
version.dll.VerQueryValueW
clr.dll.SetRuntimeInfo
clr.dll._CorExeMain
mscoree.dll.CreateConfigStream
mscoreei.dll.CreateConfigStream
kernel32.dll.GetNumaHighestNodeNumber
kernel32.dll.GetSystemWindowsDirectoryW
advapi32.dll.AllocateAndInitializeSid
advapi32.dll.OpenProcessToken
advapi32.dll.GetTokenInformation
advapi32.dll.InitializeAcl
advapi32.dll.AddAccessAllowedAce
advapi32.dll.FreeSid
kernel32.dll.AddSIDToBoundaryDescriptor
kernel32.dll.CreateBoundaryDescriptorW
kernel32.dll.CreatePrivateNamespaceW
kernel32.dll.OpenPrivateNamespaceW
kernel32.dll.DeleteBoundaryDescriptor
kernel32.dll.WerRegisterRuntimeExceptionModule
kernel32.dll.RaiseException
mscoree.dll.#24

REGISTRY KEYS

HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\Policy\
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\Policy\v4.0
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\InstallRoot
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\CLRLoadLogDir
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Windows Error Reporting\WMR

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_CURRENT_USER\Software\Microsoft\.NETFramework
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\UseLegacyV2RuntimeActivationPolicyDefaultValue
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\OnlyUseLatestCLR
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
Policy\Standards
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\Policy\Standards
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\Policy\Standards\v4.0.30319
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Fusion\NoClientChecks
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\v4.0.30319\SKUs\
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v4.0.30319\SKUs\default
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NET Framework Setup\NDP\v4\Full
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NET Framework Setup\NDP\v4\Full\Release
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\DisableConfigCache
HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\f287d570ad26bf3a80479f5ec4301c07fa893f7d.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\CacheLocation
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\DownloadCacheQuotaInKB
HKEY_CURRENT_USER\Software\Microsoft\Fusion
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\EnableLog
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\LoggingLevel
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\ForceLog
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\LogFailures
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\LogResourceBinds
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\FileInUseRetryAttempts
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\FileInUseMillisecondsBetweenRetries
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\UseLegacyIdentityFormat
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\DisableMSIPeek
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DevOverrideEnable
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\NGen\Policy\v4.0
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\NGen\Policy\v4.0\OptimizeUsedBinaries
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\Policy\Servicing
HKEY_LOCAL_MACHINE\Software\Microsoft\StrongName

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OLEAUT
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\AltJit
HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion\PublisherPolicy\Default
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\Latest
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\index20
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\LegacyPolicyTimeStamp
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\v4.0_policy.4.0.System.Windows.Forms__b77a5c561934e089
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\policy.4.0.System.Windows.Forms__b77a5c561934e089
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\v4.0_policy.4.0.System__b77a5c561934e089
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\policy.4.0.System__b77a5c561934e089
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\v4.0_policy.4.0.System.Configuration__b03f5f7f11d50a3a
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\policy.4.0.System.Configuration__b03f5f7f11d50a3a
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\v4.0_policy.4.0.System.Xml__b77a5c561934e089
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\policy.4.0.System.Xml__b77a5c561934e089
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\v4.0_policy.4.0.System.Drawing__b03f5f7f11d50a3a
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\policy.4.0.System.Drawing__b03f5f7f11d50a3a
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\v4.0_policy.4.0.System.Security__b03f5f7f11d50a3a
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\policy.4.0.System.Security__b03f5f7f11d50a3a
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\v4.0_policy.4.0.Accessibility__b03f5f7f11d50a3a
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\policy.4.0.Accessibility__b03f5f7f11d50a3a
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\v4.0_policy.4.0.System.Core__b77a5c561934e089
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\policy.4.0.System.Core__b77a5c561934e089
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\v4.0_policy.4.0.System.Deployment__b03f5f7f11d50a3a
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\policy.4.0.System.Deployment__b03f5f7f11d50a3a
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\v4.0_policy.4.0.System.Runtime.Serialization.Formatters.Soap__b03f5f7f11d50a3a
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\policy.4.0.System.Runtime.Serialization.Formatters.Soap__b03f5f7f11d50a3a
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\Policy\APTCA
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
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

READ FILES

C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscoreei.dll
C:\Windows\System32\tzres.dll
C:\Users\user\AppData\Local\Temp\f287d570ad26bf3a80479f5ec4301c07fa893f7d.exe.config
C:\Windows\Globalization\Sorting\sortdefault.nls

C:\Users\user\AppData\Local\Temp\f287d570ad26bf3a80479f5ec4301c07fa893f7d.exe

C:\Program Files\Common Files\System\symsrv.dll

C:\Windows\Microsoft.NET\Framework\v4.0.30319\clr.dll

C:\Windows\System32\MSVCR120_CLR0400.dll

C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config

C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\225759bb87c854c0fff27b1d84858c21\mscorlib.ni.dll.aux

C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\225759bb87c854c0fff27b1d84858c21\mscorlib.ni.dll

\Device\KsecDD

C:\Windows\Microsoft.NET\Framework\v4.0.30319\clrjit.dll

C:\Windows\assembly\pubpol20.dat

C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\5aac750b35b27770dccb1a43f83cced7\System.Windows.Forms.ni.dll.aux

C:\Windows\assembly\NativeImages_v4.0.30319_32\System\52cca48930e580e3189eac47158c20be\System.ni.dll.aux

C:\Windows\assembly\NativeImages_v4.0.30319_32\System\52cca48930e580e3189eac47158c20be\System.ni.dll

C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\646b4b01cb29986f8e076aa65c9e9753\System.Drawing.ni.dll.aux

C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\646b4b01cb29986f8e076aa65c9e9753\System.Drawing.ni.dll

C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\5aac750b35b27770dccb1a43f83cced7\System.Windows.Forms.ni.dll

C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Windows.Forms\v4.0_4.0.0.0__b77a5c561934e089\System.Windows.Forms.dll

C:\Windows\Microsoft.NET\Framework\v4.0.30319\nlssorting.dll

C:\Windows\Microsoft.NET\Framework\v4.0.30319\SortDefault.nlp

C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80\GdiPlus.dll

C:\Users\user\AppData\Local\GDIPFONTCACHEV1.DAT

C:\Windows\Fonts\tahoma.ttf

C:\Windows\Fonts\msjh.ttf

C:\Windows\Fonts\msyh.ttf

C:\Windows\Fonts\malgun.ttf

C:\Windows\Fonts\micross.ttf

C:\Windows\Fonts\segoeui.ttf

C:\Windows\Fonts\staticcache.dat

C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorrc.dll

C:\Users\user\AppData\Local\Temp\Ultimate Defender Pro Shield.exe

C:\Windows\Microsoft.NET\Framework\v4.0.30319\diasymreader.dll

C:\Windows\Microsoft.Net\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll

C:\Windows\Microsoft.Net\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.pdb

C:\Windows\symbols\dll\mscorlib.pdb

C:\Windows\dll\mscorlib.pdb

C:\Windows\mscorlib.pdb

C:\Users\user\AppData\Local\Temp\Ultimate Defender Pro Shield.pdb

C:\Windows\symbols\exe\Ultimate Defender Pro Shield.pdb

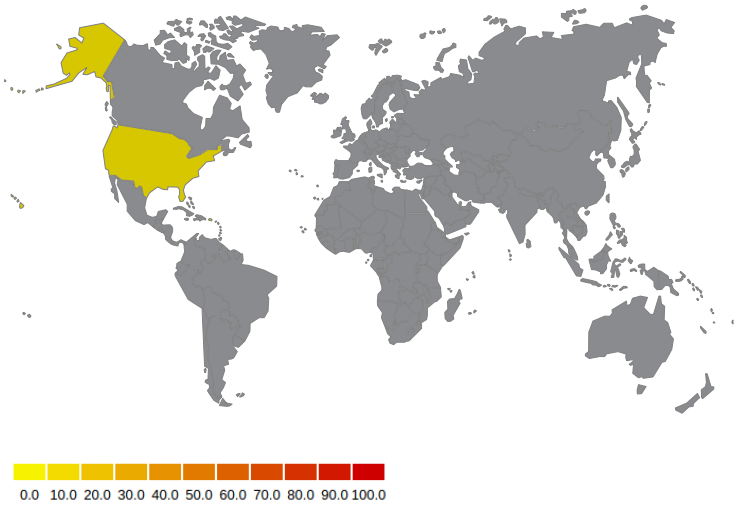
C:\Windows\exe\Ultimate Defender Pro Shield.pdb
C:\Windows\Ultimate Defender Pro Shield.pdb
C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Windows.Forms\v4.0_4.0.0.0__b77a5c561934e089\System.Windows.Forms.pdb
C:\Windows\symbols\dll\System.Windows.Forms.pdb
C:\Windows\dll\System.Windows.Forms.pdb
C:\Windows\System.Windows.Forms.pdb
C:\Windows\SysWOW64\en-US\KERNELBASE.dll.mui
C:\Windows\System32\uxtheme.dll.Config
C:\Windows\System32\uxtheme.dll
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\55560c2014611e9119f99923c9ebdeef\System.Core.ni.dll.aux
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\55560c2014611e9119f99923c9ebdeef\System.Core.ni.dll
C:\Windows\Fonts\msgothic.ttc

MUTEXES

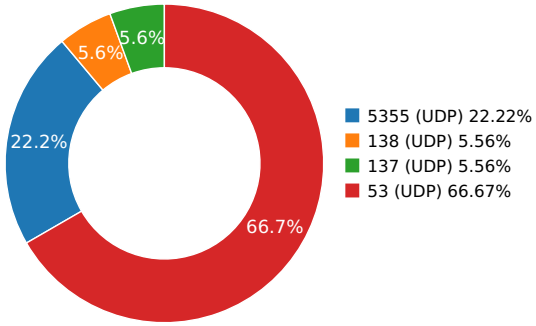
CicLoadWinStaWinSta0
Local\MSCTF.CtfMonitorInstMutexDefault1

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type
	8.8.4.4	United States	15169	Google LLC	Malware Process
	8.8.8.8	United States	15169	Google LLC	Malware Process
					Malware Process
www.aieov.com	45.56.79.23	United States	63949	Akamai Technologies, Inc.	Malware Process

DNS QUERIES

Request	Type
5isohu.com	A
www.aieov.com	A

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.04768395424	Sandbox	224.0.0.252	5355
3.06102395058	Sandbox	224.0.0.252	5355
3.13285684586	Sandbox	192.168.56.255	137
4.05695700645	Sandbox	224.0.0.252	5355
5.61920285225	Sandbox	224.0.0.252	5355
6.63265395164	Sandbox	8.8.4.4	53
7.61719298363	Sandbox	8.8.8.8	53
9.13289403915	Sandbox	192.168.56.255	138
20.9770338535	Sandbox	8.8.8.8	53
21.9761960506	Sandbox	8.8.4.4	53
35.336345911	Sandbox	8.8.8.8	53
36.3359289169	Sandbox	8.8.4.4	53
49.9144330025	Sandbox	8.8.8.8	53
50.9139809608	Sandbox	8.8.4.4	53
64.2735259533	Sandbox	8.8.8.8	53
65.2733690739	Sandbox	8.8.4.4	53
78.6329350471	Sandbox	8.8.8.8	53
79.6331119537	Sandbox	8.8.4.4	53

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\GDIPFONTCACHEV1.DAT	**Type :** data **MD5 :** 696bad2ef23da7f0ccaaa7f76ab9fdf0 **SHA-1 :** 0efe907b47e8331cf56a95c0c06d324257ece202 **SHA-256 :** bd27979561fac15e4043fc980ad62f24f00738cba1f22b **SHA-512 :** fb1a4afdbf5f9e3d7e55eb806f660057927d6c35740c69 **Size :** 84.528 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	Ultimate_Defender_Pro_Shield.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
SHA1:	f287d570ad26bf3a80479f5ec4301c07fa893f7d
MD5:	66419aebce8e32a65673723580f30a9c
First Seen Date:	2024-07-29 14:56:47.665477 (a day ago)
Number Of Clients Seen:	4
Last Analysis Date:	2024-07-29 14:56:47.665477 (a day ago)
Human Expert Analysis Date:	2024-07-30 15:34:14.912528 (about 4 hours ago)
Human Expert Analysis Result:	Clean

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[{u'Path': u'C:\\Users\\lukeo\\source\\repos\\Ultimate Defender Pro Shield\\Ultimate Defender Pro Shield\\obj\\Debug\\Ultimate Defender Pro Shield.pdb\x00', u'GUID': u'{608cd66f-9d23-4dca-8d4e-3de4a4d61583}', u'timestamp': u'2076-06-12 15:54:03'}]
Number Of Sections	3
Trid	[[82.9, u'Generic CIL Executable (.NET, Mono, etc.)'], [7.4, u'Win32 Dynamic Link Library (generic)'], [5.1, u'Win32 Executable (generic)'], [2.2, u'Generic Win/DOS Executable'], [2.2, u'DOS Executable Generic']]
Compilation Time Stamp	0xD1B818B7 [Mon Jun 30 09:58:15 2081 UTC] [SUSPICIOUS]
Translation	0x0000 0x04b0
LegalCopyright	Copyright \xa9 Ultimate Defender Pro Shield 2024
Assembly Version	1.0.0.0
InternalName	Ultimate Defender Pro Shield.exe
FileVersion	1.0.0.0
CompanyName	Ultimate Defender Pro Shield
LegalTrademarks	Ultimate Defender Pro Shield
Comments	Ultimate Defender Pro Shield
ProductName	Ultimate Defender Pro Shield
ProductVersion	1.0.0.0
FileDescription	Ultimate Defender Pro Shield
OriginalFilename	Ultimate Defender Pro Shield.exe
Entry Point	0x4fb64a (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	1191936
Ssdeep	6144:6MtlORkLCsQv0TRXJ3Gv7m1REoIa+Mq9tlORkLCsQv0TRXJ3Gv7m1RECxhBi946P:SRlodla/Rlo7HBlaG
Sha256	a7aae5d2f8175f32d7896b7e8fd11ffe49ce13bc573c785414ccc47adf346399
Exifinfo	[{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/f/2/8/7/f287d570ad26bf3a80479f5ec4301c07fa893f7d', u'EXE:OriginalFileName': u'Ultimate Defender Pro Shield.exe', u'EXE:ProductName': u'Ultimate Defender Pro Shield', u'EXE:InternalName': u'Ultimate Defender Pro Shield.exe', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2024:07:29 14:56:03+00:00', u'EXE:InitializedDataSize': 169472, u'File:FileModifyDate': u'2024:07:29 14:55:49+00:00', u'EXE:AssemblyVersion': u'1.0.0.0', u'EXE:FileVersionNumber': u'1.0.0.0', u'EXE:FileVersion': u'1.0.0.0', u'File:FileSize': u'1164 kB', u'EXE:CharacterSet': u'Unicode', u'EXE:MachineType': u'Intel 386 or later, and compatibles', u'EXE:FileOS': u'Win32', u'EXE:LegalTrademarks': u'Ultimate Defender Pro Shield', u'EXE:ProductVersion': u'1.0.0.0', u'EXE:ObjectFileType': u'Executable application', u'File:FileType': u'Win32 EXE', u'EXE:CompanyName': u'Ultimate Defender Pro Shield', u'File:FileName': u'f287d570ad26bf3a80479f5ec4301c07fa893f7d', u'EXE:ImageVersion': 0.0, u'File:FileTypeExtension': u'exe', u'EXE:OSVersion': 4.0, u'EXE:PEType': u'PE32', u'EXE:TimeStamp': u'2081:06:30 09:58:15+00:00', u'EXE:FileFlagsMask': u'0x003f', u'EXE:LegalCopyright': u'Copyright \xa9 Ultimate Defender Pro Shield 2024', u'EXE:LinkerVersion': 48.0, u'EXE:FileFlags': u'(none)', u'EXE:Subsystem': u'Windows GUI', u'File:Directory': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/f/2/8/7', u'EXE:FileDescription': u'Ultimate Defender Pro Shield', u'EXE:EntryPoint': u'0xfb64a', u'EXE:SubsystemVersion': 6.0, u'EXE:CodeSize': 1021952, u'EXE:Comments': u'Ultimate Defender Pro Shield', u'File:FileInodeChangeDate': u'2024:07:29 14:56:03+00:00', u'EXE:UninitializedDataSize': 0, u'EXE:LanguageCode': u'Neutral', u'ExifTool:ExifToolVersion': 10.1, u'EXE:ProductVersionNumber': u'1.0.0.0'}]
Mime Type	application/x-dosexec
Imphash	f34d5f2d4577ed6d9ceec516c1f5a744

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x2000	0xf9650	0xf9800	4.86335747507	13598cbc914a8ce8fb7ad998a8040778
.rsrc	0xfc000	0x292c4	0x29400	2.59467123862	b739f38ab0fb4fc227624f6d34398c22
.reloc	0x126000	0xc	0x200	0.101910425663	3cdd37b3aa4186cea660adb4b62491c0

PE Imports

- mscoree.dll
  - _CorExeMain

PE Resources

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1032704, u'sha256': u'1ada2fc76d7e96676b1b73e384a68c9856eb8130daff0c35a422fa1da082b624', u'type': u'PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced', u'size': 4417}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1037140, u'sha256': u'480680de136d51732ac2fb4af88b71622d52789d22e4e78d565f2525b92f48ea', u'type': u'dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0', u'size': 67624}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1104780, u'sha256': u'ac906af65da219404188799747f569fb21dd796f9cfcc47a6bc5af4fdc8520c0', u'type': u'data', u'size': 38056}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1142852, u'sha256': u'4e2c2296669ef94f254826fae8ad1f82710fa8c1ed9b8b19fc7b036e5c67d7fa', u'type': u'data', u'size': 21640}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1164508, u'sha256': u'6360f6b44aafb2183aeb5618c907173127beb647b66368f363128dbaffd08997', u'type': u'dBase IV DBT of \\200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 4294967295, next used block 4294967295', u'size': 16936}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1181460, u'sha256': u'3681eca98f24b6c5c27089ddf89a3d3bed39fd5a6d22a37c8c7e2379a9f48a34', u'type': u'data', u'size': 9640}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1191116, u'sha256': u'd07a06971ec31617e1920e07a29c3814bbab33800d3a70d9096685100afaadbb', u'type': u'data', u'size': 4264}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1195396, u'sha256': u'f70bf906c2fc2464b01c5679ee65d8480b03dbdd67aa80ed8779b57a8d02f911', u'type': u'data', u'size': 2440}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1197852, u'sha256': u'6448133392a05eb784bb688f9fb09147cbc81a3a22413be564c46d1ad2cbb62b', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1128}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_ICON', u'offset': 1198996, u'sha256': u'835d1fbce7726bcb950be521a3a7079d81804aa50aa0d8709c96145fafdba59f', u'type': u'MS Windows icon resource - 9 icons, 256x256', u'size': 132}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_VERSION', u'offset': 1199144, u'sha256': u'0575ae8a13182b1925b35f035d72e0bfc2cefd6ed5f224adae0394ebb48ecda7', u'type': u'data', u'size': 1180}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_MANIFEST', u'offset': 1200340, u'sha256': u'539dc26a14b6277e87348594ab7d6e932d16aabb18612d77f29fe421a9f1d46a', u'type': u'XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators', u'size': 490}

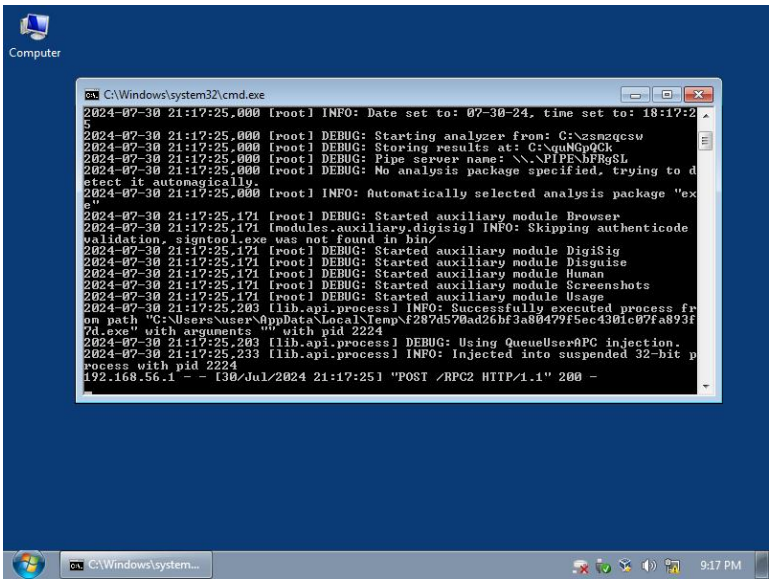
CERTIFICATE VALIDATION

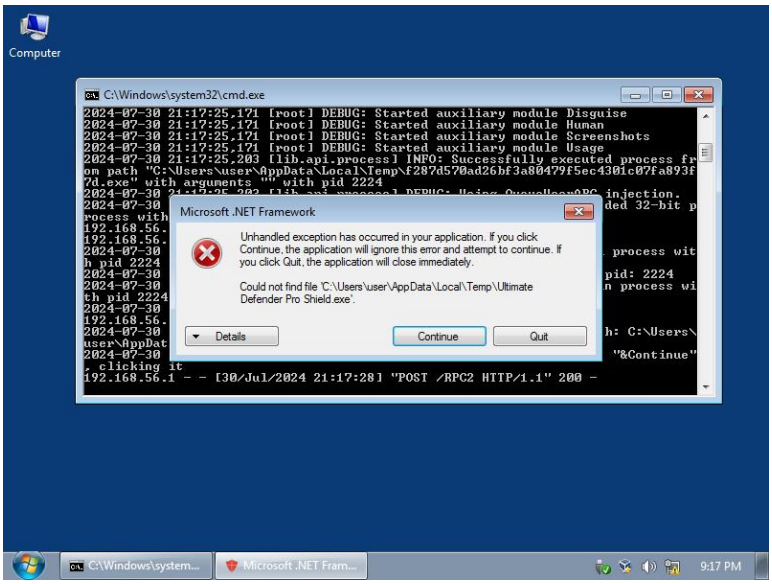
- Certificate Validation is not Applicable ?

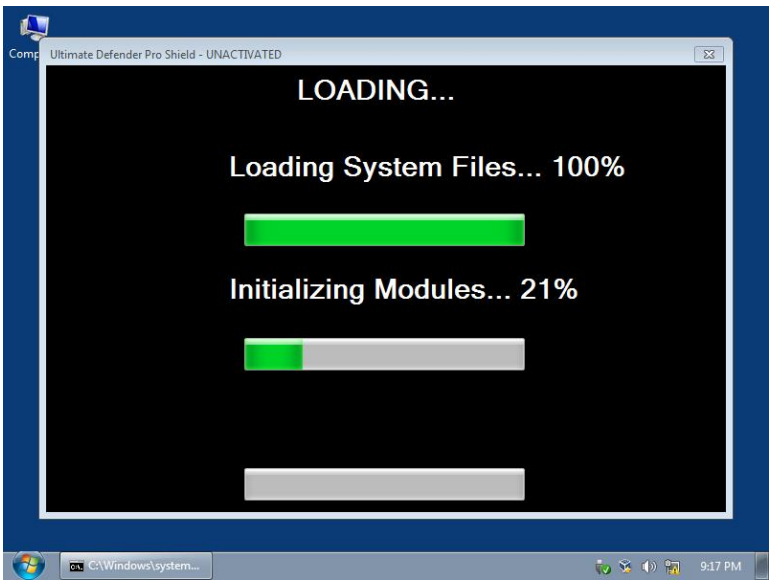
SCREENSHOTS

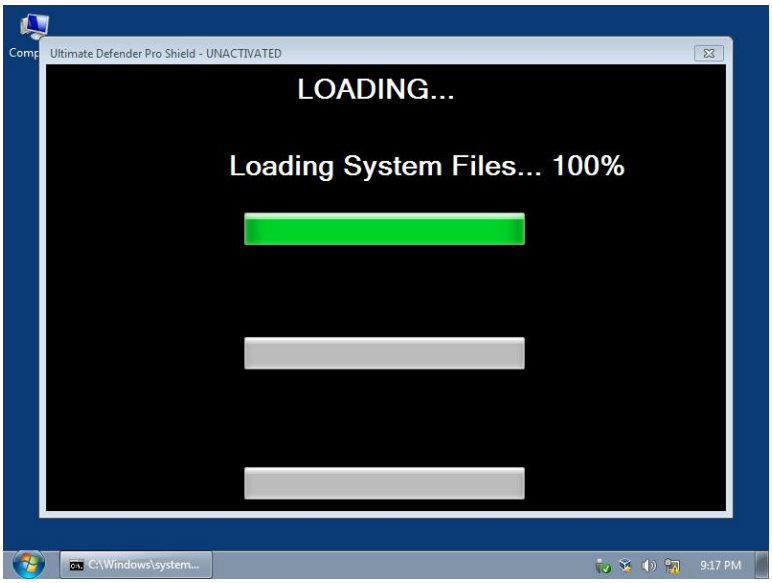

Ultimate Defender Pro Shield
ULTIMATE DEFENDER PRO SHIELD
Protects your computer from malware.
ACTIVAT
VERSI
PROTECTION STATUS
SCAN MY COMPUTER
REAL-TIME PROTECTION
YOUR COMPUTER IS PROTECTED!
PC is threatened! [Trial Licence, Update Failed, Viruses Detected!]
Update And Remove Viruses

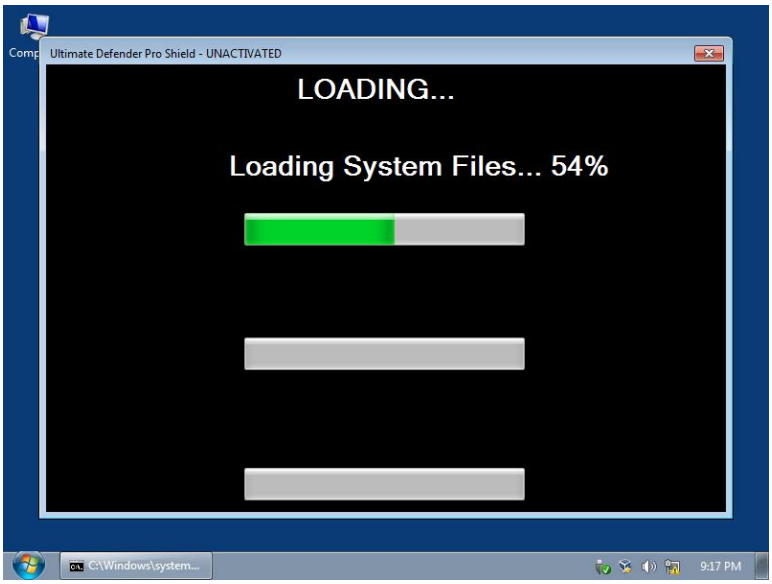

Ultimate Defender Pro Shield
ULTIMATE DEFENDER PRO SHIELD
Protects your computer from malware.
ACTIVAT
VERSI
PROTECTION STATUS
SCAN MY COMPUTER
REAL-TIME PROTECTION
YOUR COMPUTER IS PROTECTED!
PC is threatened! [Trial Licence, Update Failed, Viruses Detected!]
Update And Remove Viruses

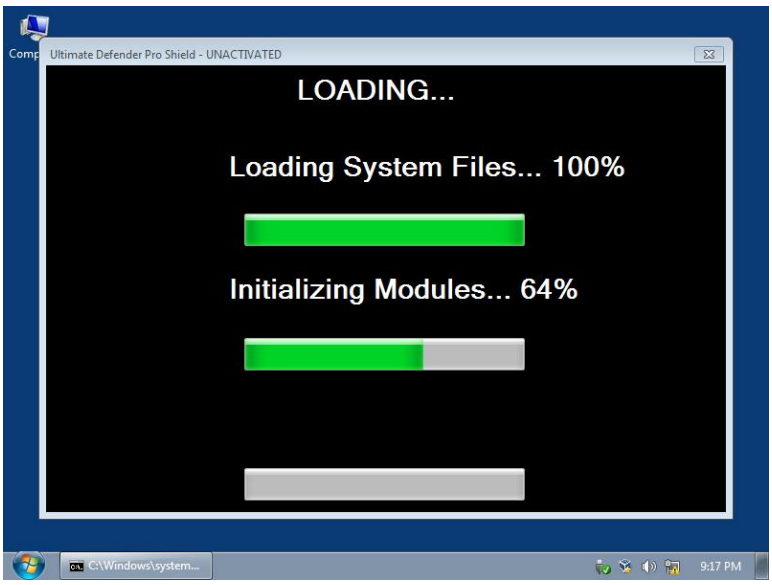

Computer
C:\Windows\system32\cmd.exe
2024-07-30 21:17:25,000 [root] INFO: Date set to: 07-30-24, time set to: 18:17:2
5
2024-07-30 21:17:25,000 [root] DEBUG: Starting analyzer from: C:\zsmzqcsw
2024-07-30 21:17:25,000 [root] DEBUG: Storing results at: C:\quNGpQCk
2024-07-30 21:17:25,000 [root] DEBUG: Pipe server name: \\.\PIPE\bFRgSL
2024-07-30 21:17:25,000 [root] DEBUG: No analysis package specified, trying to d
etect it automagically.
2024-07-30 21:17:25,000 [root] INFO: Automatically selected analysis package "ex
e"
2024-07-30 21:17:25,171 [root] DEBUG: Started auxiliary module Browser
2024-07-30 21:17:25,171 [modules.auxiliary.digisig] INFO: Skipping authenticode
validation, signtool.exe was not found in bin/
2024-07-30 21:17:25,171 [root] DEBUG: Started auxiliary module DigiSig
2024-07-30 21:17:25,171 [root] DEBUG: Started auxiliary module Disguise
2024-07-30 21:17:25,171 [root] DEBUG: Started auxiliary module Human
2024-07-30 21:17:25,171 [root] DEBUG: Started auxiliary module Screenshots
2024-07-30 21:17:25,171 [root] DEBUG: Started auxiliary module Usage
2024-07-30 21:17:25,203 [lib.api.process] INFO: Successfully executed process fr
om path "C:\Users\user\AppData\Local\Temp\f2872570ad26bf3a80479f5ec4301c07fa893f
7d.exe" with arguments "" with pid 2224
2024-07-30 21:17:25,203 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-07-30 21:17:25,233 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2224
192.168.56.1 - - [30/Jul/2024 21:17:25] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
9:17 PM

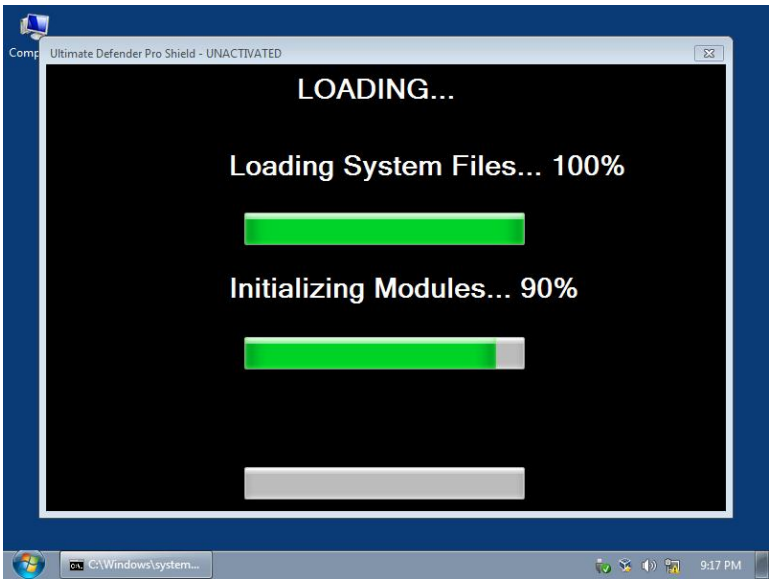

Computer
C:\Windows\system32\cmd.exe
2024-07-30 21:17:25,171 [root] DEBUG: Started auxiliary module Disguise
2024-07-30 21:17:25,171 [root] DEBUG: Started auxiliary module Human
2024-07-30 21:17:25,171 [root] DEBUG: Started auxiliary module Screenshots
2024-07-30 21:17:25,171 [root] DEBUG: Started auxiliary module Usage
2024-07-30 21:17:25,203 [lib.api.process] INFO: Successfully executed process fr
om path "C:\Users\user\AppData\Local\Temp\f287d570ad26bf3a80479f5ec430ic07fa893f
7d.exe" with arguments "" with pid 2224
Microsoft .NET Framework
Unhandled exception has occurred in your application. If you click Continue, the application will ignore this error and attempt to continue. If you click Quit, the application will close immediately.
Could not find file 'C:\Users\user\AppData\Local\Temp\Ultimate Defender Pro Shield.exe'.
Details
Continue
Quit
192.168.56.1 - - [30/Jul/2024 21:17:28] "POST /RPC2 HTTP/1.1" 200 -
9:17 PM

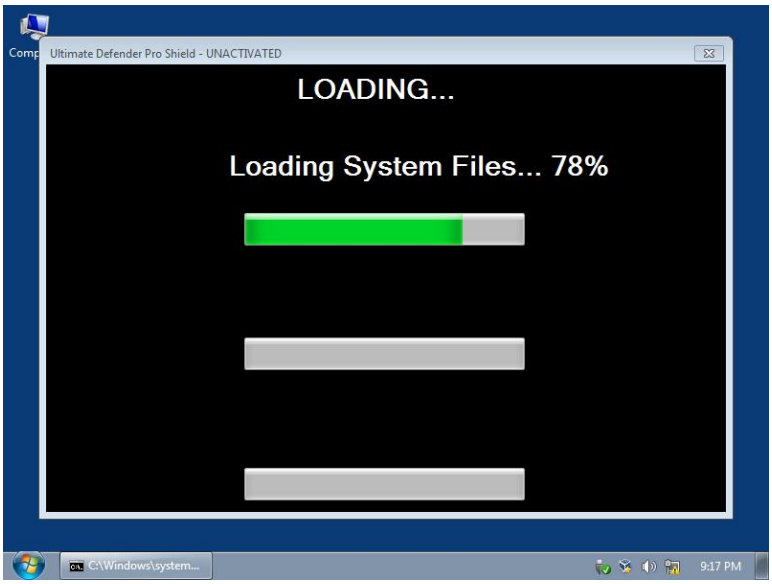

Ultimate Defender Pro Shield - UNACTIVATED
LOADING...
Loading System Files... 100%
Initializing Modules... 21%
9:17 PM


Ultimate Defender Pro Shield - UNACTIVATED
LOADING...
Loading System Files... 100%
9:17 PM

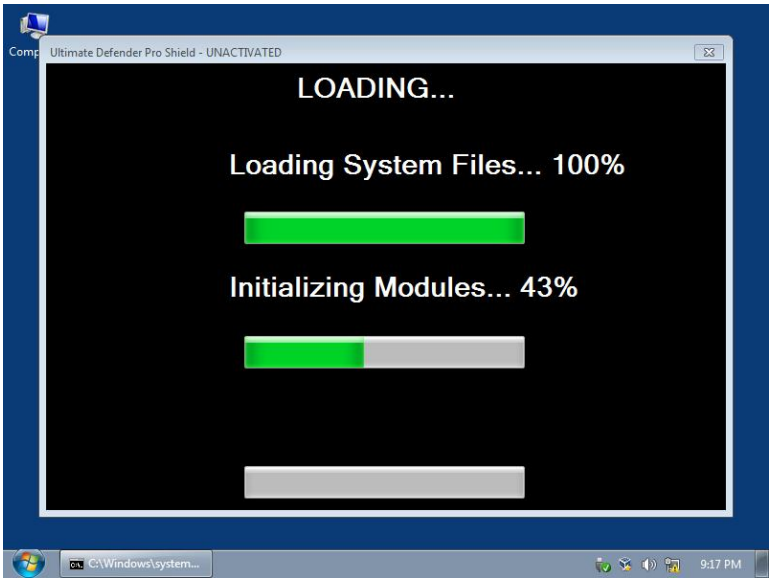

Ultimate Defender Pro Shield - UNACTIVATED
LOADING...
Loading System Files... 54%
C:\Windows\system...
9:17 PM

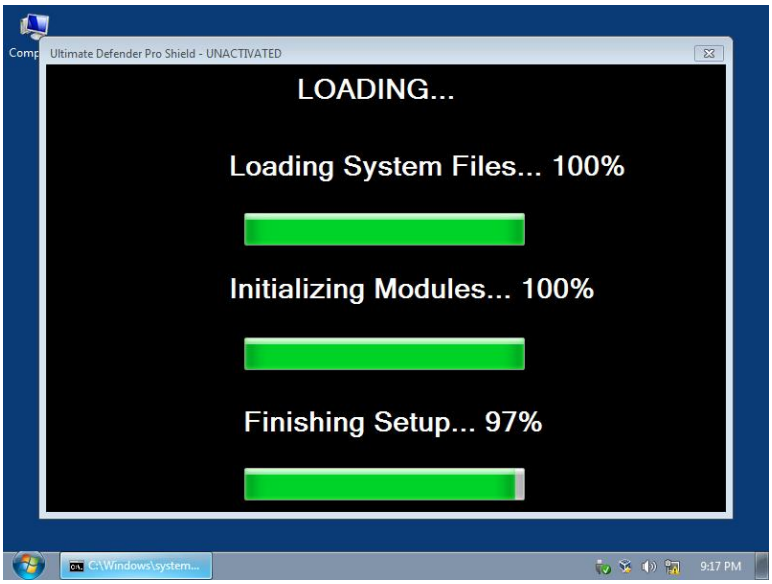

Ultimate Defender Pro Shield - UNACTIVATED
LOADING...
Loading System Files... 100%
Initializing Modules... 64%
C:\Windows\system...
9:17 PM

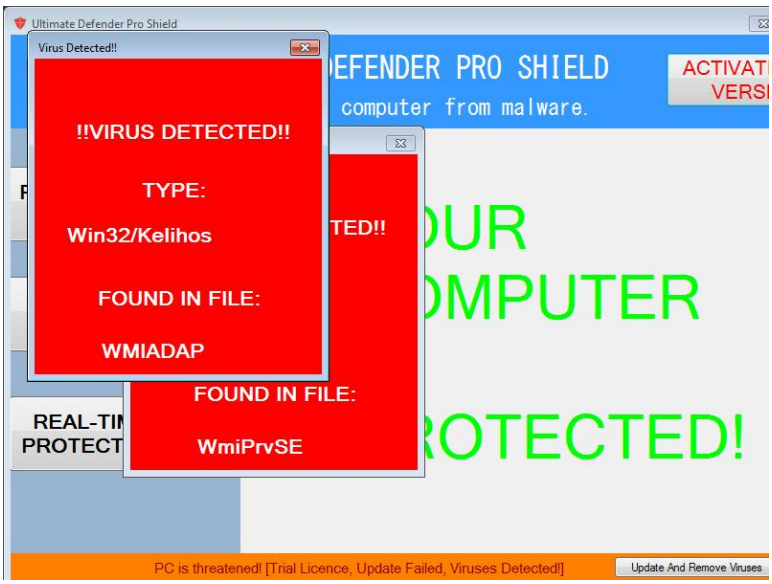

Ultimate Defender Pro Shield - UNACTIVATED
LOADING...
Loading System Files... 100%
Initializing Modules... 90%
C:\Windows\system...
9:17 PM


Ultimate Defender Pro Shield - UNACTIVATED
LOADING...
Loading System Files... 78%
9:17 PM


Ultimate Defender Pro Shield
ULTIMATE DEFENDER PRO SHIELD
Protects your computer from malware.
PROTECTION STATUS
SCAN MY COMPUTER
REAL-TIME PROTECTION
YOUR COMPUTER IS PROTECTED!
9:18 PM


Ultimate Defender Pro Shield - UNACTIVATED
LOADING...
Loading System Files... 100%
Initializing Modules... 43%
9:17 PM

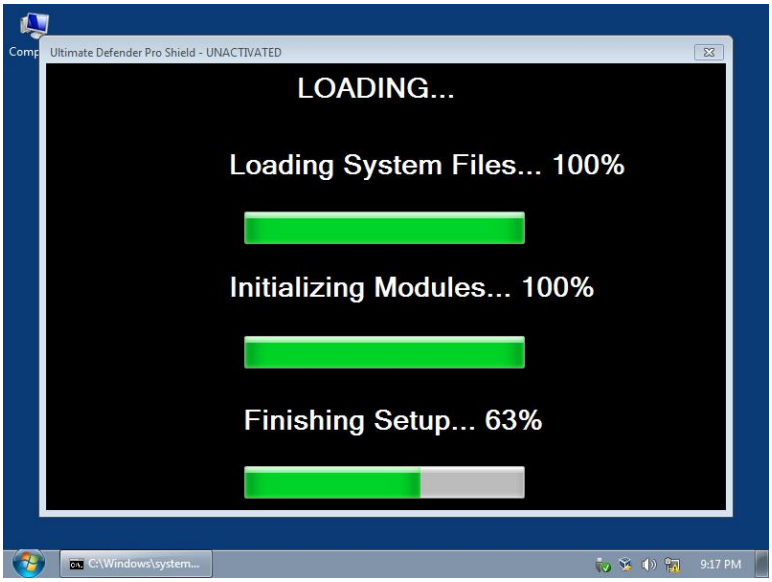

Ultimate Defender Pro Shield - UNACTIVATED
LOADING...
Loading System Files... 100%
Initializing Modules... 100%
Finishing Setup... 97%
9:17 PM

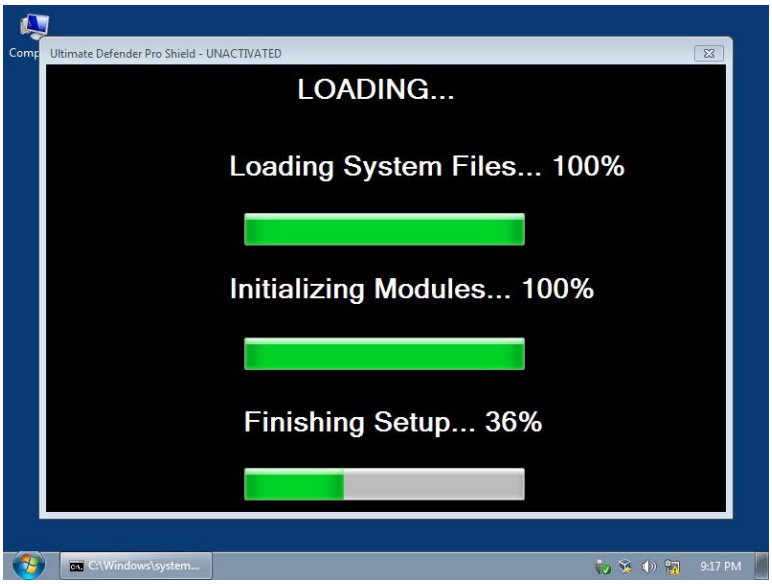

Ultimate Defender Pro Shield
Virus Detected!!
!!VIRUS DETECTED!!
TYPE:
Win32/Kelihos
FOUND IN FILE:
WMIADAP
FOUND IN FILE:
WmiPrvSE
computer from malware.
PC is threatened! [Trial Licence, Update Failed, Viruses Detected!]
Update And Remove Viruses

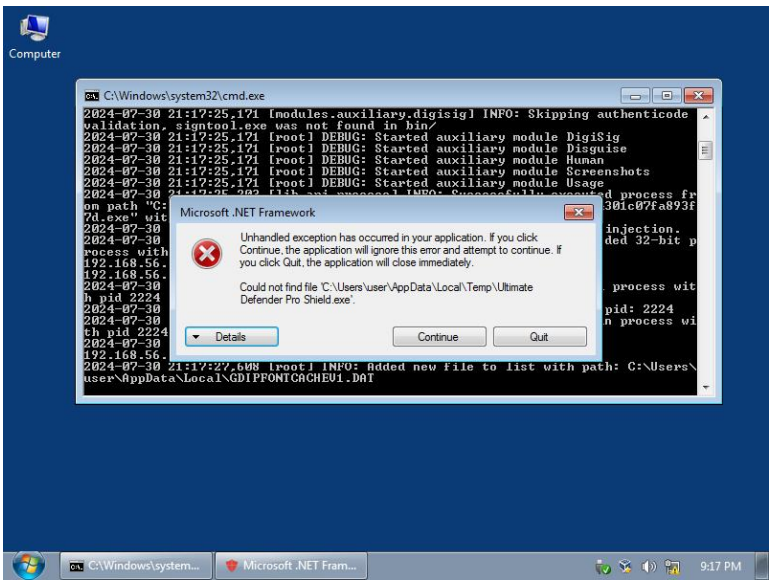

Ultimate Defender Pro Shield
ULTIMATE DEFENDER PRO SHIELD
Protects your computer from malware.
PROTECTION STATUS
SCAN MY COMPUTER
REAL-TIME PROTECTION
YOUR COMPUTER IS PROTECTED!
PC is threatened! [Trial Licence, Update Failed, Viruses Detected!]
Update And Remove Viruses


Ultimate Defender Pro Shield
ULTIMATE DEFENDER PRO SHIELD
Protects your computer from malware.
ACTIVAT
VERSI
PROTECTION STATUS
SCAN MY COMPUTER
REAL-TIME PROTECTION
YOUR COMPUTER IS PROTECTED!
C:\Windows\system...
Ultimate Defender Pr...
9:17 PM


Ultimate Defender Pro Shield
ULTIMATE DEFENDER PRO SHIELD
Protects your computer from malware.
ACTIVAT
VERSI
PROTECTION STATUS
SCAN MY COMPUTER
REAL-TIME PROTECTION
YOUR COMPUTER IS PROTECTED!
PC is threatened! [Trial Licence, Update Failed, Viruses Detected!]
Update And Remove Viruses


Ultimate Defender Pro Shield - UNACTIVATED
LOADING...
Loading System Files... 100%
Initializing Modules... 100%
Finishing Setup... 63%
C:\Windows\system...
9:17 PM

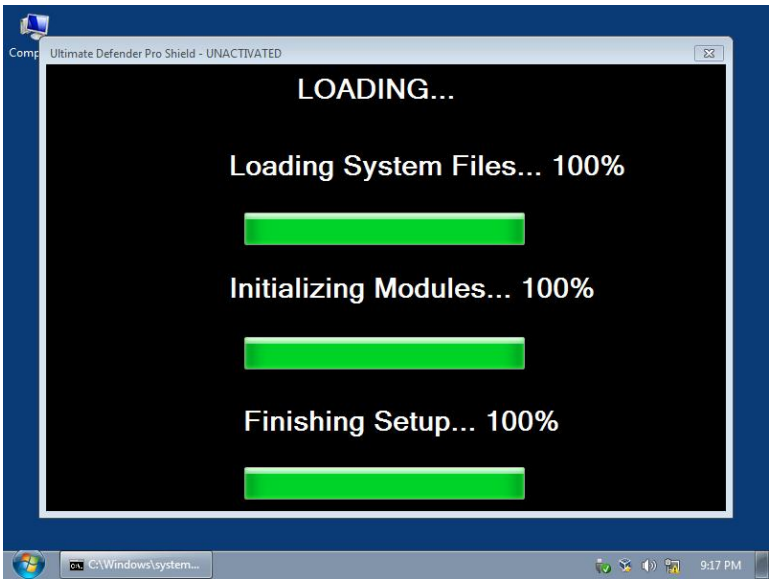

Ultimate Defender Pro Shield - UNACTIVATED
LOADING...
Loading System Files... 100%
Initializing Modules... 100%
Finishing Setup... 36%
9:17 PM

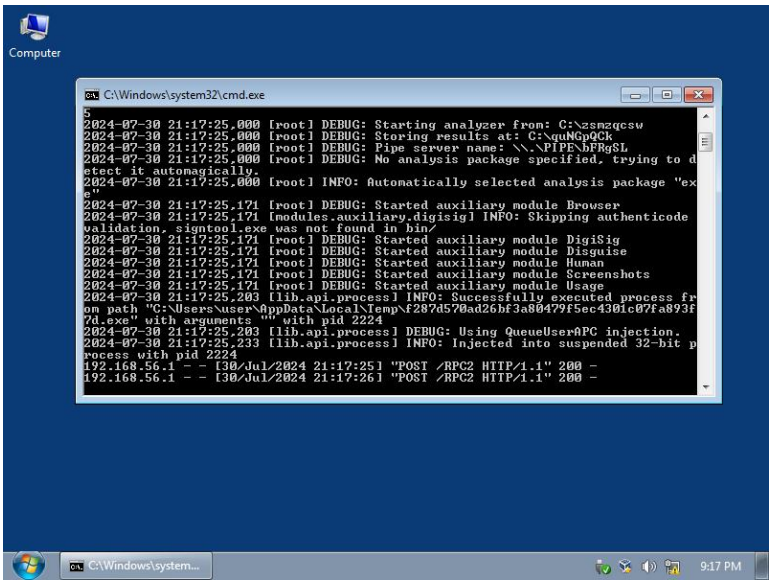

Computer
C:\Windows\system32\cmd.exe
Microsoft .NET Framework
Unhandled exception has occurred in your application. If you click Continue, the application will ignore this error and attempt to continue. If you click Quit, the application will close immediately.
Could not find file 'C:\Users\user\AppData\Local\Temp\Ultimate Defender Pro Shield.exe'.
Details
Continue
Quit
9:17 PM

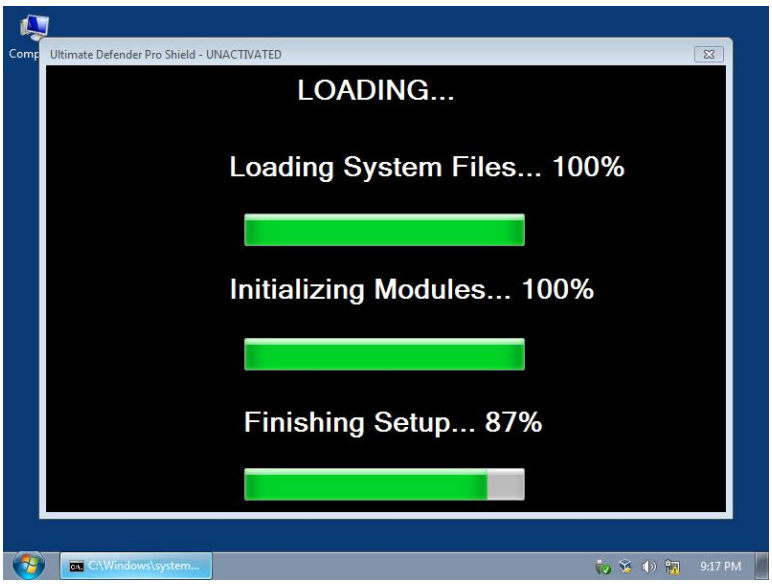

Ultimate Defender Pro Shield
ULTIMATE DEFENDER PRO SHIELD
Protects your computer from malware.
PROTECTION STATUS
SCAN MY COMPUTER
REAL-TIME PROTECTION
YOUR COMPUTER IS PROTECTED!
PC is threatened! [Trial Licence, Update Failed, Viruses Detected!]
Update And Remove Viruses

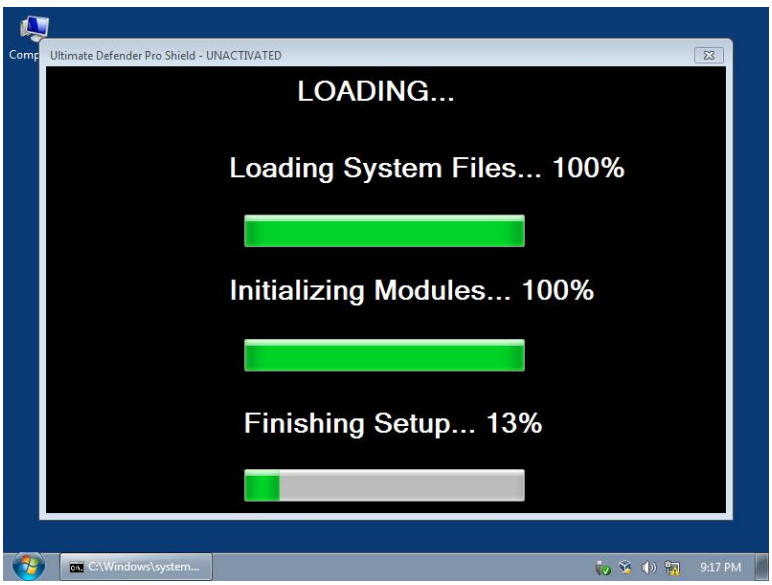

Ultimate Defender Pro Shield
ULTIMATE DEFENDER PRO SHIELD
Protects your computer from malware.
ACTIVAT
VERSI
PROTECTION STATUS
SCAN MY COMPUTER
REAL-TIME PROTECTION
YOUR COMPUTER IS PROTECTED!
PC is threatened! [Trial Licence, Update Failed, Viruses Detected!]
Update And Remove Viruses


Ultimate Defender Pro Shield
ULTIMATE DEFENDER PRO SHIELD
Protects your computer from malware.
ACTIVAT
VERSI
PROTECTION STATUS
SCAN MY COMPUTER
REAL-TIME PROTECTION
YOUR COMPUTER IS PROTECTED!
C:\Windows\system...
Ultimate Defender Pr...
9:18 PM


Ultimate Defender Pro Shield - UNACTIVATED
LOADING...
Loading System Files... 100%
Initializing Modules... 100%
Finishing Setup... 100%
C:\Windows\system...
9:17 PM


Computer
C:\Windows\system32\cmd.exe
2024-07-30 21:17:25,000 [root] DEBUG: Starting analyzer from: C:\zsmzqcsw
2024-07-30 21:17:25,000 [root] DEBUG: Storing results at: C:\quNGpQCk
2024-07-30 21:17:25,000 [root] DEBUG: Pipe server name: \\.\PIPE\bFRgSL
2024-07-30 21:17:25,000 [root] DEBUG: No analysis package specified, trying to d
etect it automagically.
2024-07-30 21:17:25,000 [root] INFO: Automatically selected analysis package "ex
e"
2024-07-30 21:17:25,171 [root] DEBUG: Started auxiliary module Browser
2024-07-30 21:17:25,171 [modules.auxiliary.digisig] INFO: Skipping authenticode
validation, signtool.exe was not found in bin/
2024-07-30 21:17:25,171 [root] DEBUG: Started auxiliary module DigiSig
2024-07-30 21:17:25,171 [root] DEBUG: Started auxiliary module Disguise
2024-07-30 21:17:25,171 [root] DEBUG: Started auxiliary module Human
2024-07-30 21:17:25,171 [root] DEBUG: Started auxiliary module Screenshots
2024-07-30 21:17:25,171 [root] DEBUG: Started auxiliary module Usage
2024-07-30 21:17:25,203 [lib.api.process] INFO: Successfully executed process fr
om path "C:\Users\user\AppData\Local\Temp\f287d570ad26bf3a80479f5ec4301c07fa893f
7d.exe" with arguments "" with pid 2224
2024-07-30 21:17:25,203 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-07-30 21:17:25,233 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2224
192.168.56.1 - - [30/Jul/2024 21:17:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [30/Jul/2024 21:17:26] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
9:17 PM


Ultimate Defender Pro Shield - UNACTIVATED
LOADING...
Loading System Files... 100%
Initializing Modules... 100%
Finishing Setup... 87%
C:\Windows\system...
9:17 PM


Ultimate Defender Pro Shield - UNACTIVATED
LOADING...
Loading System Files... 100%
Initializing Modules... 100%
Finishing Setup... 13%
C:\Windows\system...
9:17 PM