VALKYRIE COMODO

Summary

File Name: Luxuria.exe

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

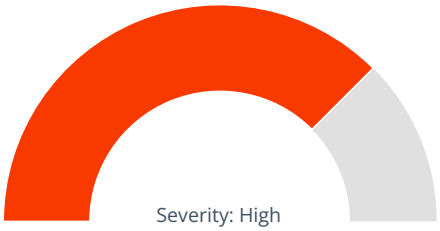
SHA1: 997a45a3707dd6ac76765664503576d3f6a37cb3

MD5: 0ffb5f463f6c63d11a48d2b4ef3be8dd

MALWARE

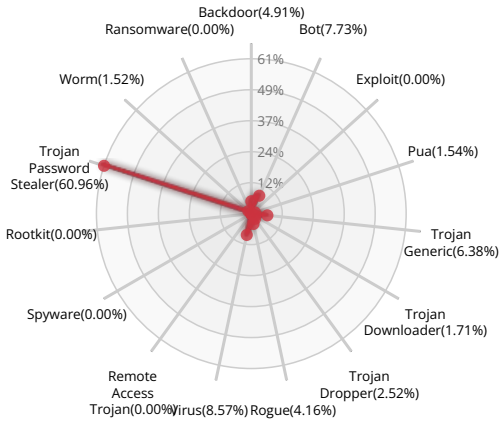
Valkyrie Final Verdict

DETECTION SECTION

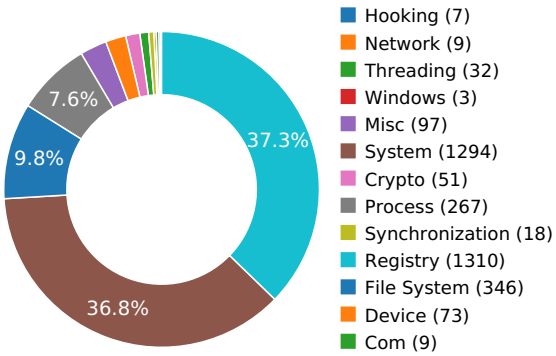


Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

VALKYRIE COMODO

Activity Details

PACKER

The binary likely contains encrypted or compressed data. Show sources

INFORMATION DISCOVERY

Reads data out of its own binary image Show sources

STATIC ANOMALY

Anomalous binary characteristics Show sources

MALWARE ANALYSIS SYSTEM EVASION

Creates a hidden or system file Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory Show sources

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\System32\tzres.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\clr.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\997a45a3707dd6ac76765664503576d3f6a37cb3.exe.config
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Users\user\AppData\Local\Temp\997a45a3707dd6ac76765664503576d3f6a37cb3.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\AutoLauncher*
C:\Users\user\AppData\Local\Temp\997a45a3707dd6ac76765664503576d3f6a37cb3.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\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\Framework\v4.0.30319\nlssorting.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\SortDefault.nlp
C:\Users\user\AppData\Local\Temp\4E07515B.dll
C:\Windows\assembly\NativeImages_v4.0.30319_32\4E07515B*
C:\Users\user\AppData\Local\Temp\4E07515B.INI
C:\Program Files\Common Files\System\symsrv.dll.dat
C:\Windows\Microsoft.Net\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\bcrypt.dll

C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\ws2_32.dll
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration*
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\469570308309641656 44b52b0696c5d9\System.Configuration.ni.dll
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\469570308309641656 44b52b0696c5d9\System.Configuration.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_32\System.Core\v4.0_4.0.0.0__b77a5c561934e089\System.Core.dll
C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Core\v4.0_4.0.0.0__b77a5c561934e089\System.Core.dll
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core*
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\55560c2014611e9119f99923c9ebdeef\System.Core.ni.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\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\UseLegacyV2RuntimeActivationPolicyDefaultValue
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\OnlyUseLatestCLR
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\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Defaults\Provider Types\Type 024\Name
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OLE\AppCompat\RaiseDefaultAuthnLevel
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OLE\DefaultAccessPermission
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{00000134-0000-0000-C000-000000000046}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc\Extensions\NdrOleExtDLL
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc\Extensions\RemoteRpcDll
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledProcesses\2EE2A5A8
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledSessions\MachineThrottling
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledSessions\GlobalSession
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\FipsAlgorithmPolicy\Enabled
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\FipsAlgorithmPolicy
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Dnscache\Parameters\QueryAdapterName
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\DisableAdapterDomainName
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Dnscache\Parameters\UseDomainNameDevolution
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\UseDomainNameDevolution
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Dnscache\Parameters\DomainNameDevolutionLevel
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Dnscache\Parameters\PrioritizeRecordData
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\PrioritizeRecordData
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Dnscache\Parameters\AllowUnqualifiedQuery
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\AllowUnqualifiedQuery
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Dnscache\Parameters\AppendToMultiLabelName
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Dnscache\Parameters\ScreenBadTlds
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Dnscache\Parameters\ScreenUnreachableServers
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Dnscache\Parameters\ScreenDefaultServers
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Dnscache\Parameters\DynamicServerQueryOrder
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Dnscache\Parameters\FilterClusterIp
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Dnscache\Parameters\WaitForNameErrorOnAll
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Dnscache\Parameters\UseEdns
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Dnscache\Parameters\DnsSecureNameQueryFallback
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Dnscache\Parameters\EnableDAForAllNetworks

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Dnscache\Parameters\DirectAccessQueryOrder
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Dnscache\Parameters\QueryIpMatching
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Dnscache\Parameters\UseHostsFile
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Dnscache\Parameters\AddrConfigControl
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Dnscache\Parameters\RegistrationEnabled
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\DisableDynamicUpdate
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Dnscache\Parameters\RegisterPrimaryName
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Dnscache\Parameters\RegisterAdapterName
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\EnableAdapterDomainNameRegistration
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Dnscache\Parameters\RegisterReverseLookup
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\DisableReverseAddressRegistrations
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Dnscache\Parameters\RegisterWanAdapters
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\DisableWanDynamicUpdate
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Dnscache\Parameters\RegistrationTtl
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\DefaultRegistrationTTL
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Dnscache\Parameters\RegistrationRefreshInterval
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\DefaultRegistrationRefreshInterval

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
kernel32.dll.SortGetHandle
kernel32.dll.SortCloseHandle
shlwapi.dll.UrlIsW

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_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\CustomLocale

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\ExtendedLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_CURRENT_USER\Software\Microsoft\.NETFramework
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\UseLegacyV2RuntimeActivationPolicyDefaultValue
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\OnlyUseLatestCLR
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\997a45a3707dd6ac76765664503576d3f6a37cb3.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__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\.NETFramework\Policy\APTCA
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale\Alternate Sorts
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Language Groups
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2298303332-66077612-2598613238-1000
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Defaults\Provider Types\Type 024
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Defaults\Provider Types\Type 024\Name
HKEY_CURRENT_USER\Software\Classes
HKEY_CURRENT_USER\Software\Classes\AppID\997a45a3707dd6ac76765664503576d3f6a37cb3.exe
HKEY_LOCAL_MACHINE\Software\Microsoft\OLE\AppCompat
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OLE\AppCompat\RaiseDefaultAuthnLevel
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OLE
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OLE\DefaultAccessPermission
HKEY_CURRENT_USER\Software\Classes\Interface\{00000134-0000-0000-C000-000000000046}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{00000134-0000-0000-C000-000000000046}\ProxyStubClsid32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{00000134-0000-0000-C000-000000000046}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\Software\Microsoft\Rpc\Extensions
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc\Extensions\NdrOleExtDLL

EXECUTED COMMANDS

cmd.exe /C choice /C Y /N /D Y /T 3 & Del "C:\Users\user\AppData\Local\Temp\4E07515B.dll" /A:H

choice /C Y /N /D Y /T 3

READ FILES

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

C:\Windows\System32\tzres.dll

C:\Users\user\AppData\Local\Temp\997a45a3707dd6ac76765664503576d3f6a37cb3.exe.config

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

C:\Users\user\AppData\Local\Temp\997a45a3707dd6ac76765664503576d3f6a37cb3.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\52cca48930e580e3189eac47158c20be\System.ni.dll.aux

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

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

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

C:\Users\user\AppData\Local\Temp\4E07515B.dll

C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\46957030830964165644b52b0696c5d9\System.Configuration.ni.dll.aux

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\assembly\NativeImages_v4.0.30319_32\System.Configuration\46957030830964165644b52b0696c5d9\System.Configuration.ni.dll

C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\d86b080a37c60a872c82b912a2a63dac\System.Xml.ni.dll.aux

C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\d86b080a37c60a872c82b912a2a63dac\System.Xml.ni.dll

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

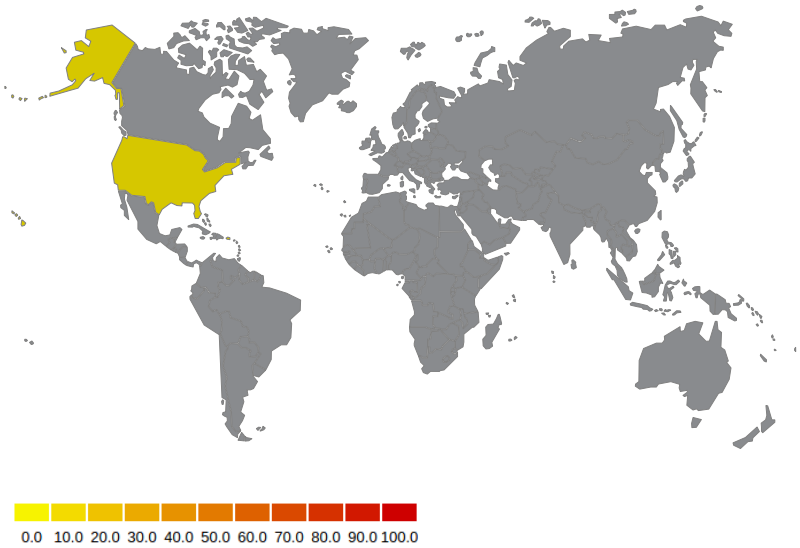
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorrc.dll
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\5aac750b35b27770dccb1a43f83cced7\System.Windows.Forms.ni.dll.aux
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\646b4b01cb29986f8e076aa65c9e9753\System.Drawing.ni.dll.aux
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\Fonts\staticcache.dat

MUTEXES

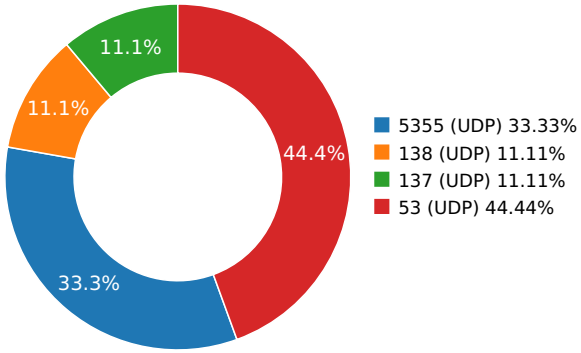
DBWinMutex
Global\{924b889b-59b7-43ff-93dc-08b94c0b7681}
CicLoadWinStaWinSta0
Local\MSCTF.CtfMonitorInstMutexDefault1

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
7.22744393349	Sandbox	224.0.0.252	5355
7.24340891838	Sandbox	224.0.0.252	5355
7.24491882324	Sandbox	8.8.4.4	53
7.30160498619	Sandbox	192.168.56.255	137
8.23886084557	Sandbox	8.8.8.8	53
9.80473089218	Sandbox	224.0.0.252	5355
13.3043358326	Sandbox	192.168.56.255	138
21.6490929127	Sandbox	8.8.4.4	53
22.6450719833	Sandbox	8.8.8.8	53

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\4E07515B.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** 0e7d38086b978ce94f32e916b216ff29 **SHA-1 :** 462108a73d1ec0d9a5b76f08a9af3c4241c5dae8 **SHA-256 :** 012d051f54d282075c3d147761a5b303ab74cefb **SHA-512 :** 6ef0b27b16fa9c66817df09bdb99cf37dd451720 **Size :** 564.736 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	Luxuria.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
SHA1:	997a45a3707dd6ac76765664503576d3f6a37cb3
MD5:	0ffb5f463f6c63d11a48d2b4ef3be8dd
First Seen Date:	2024-05-05 13:52:00.764095 (2 months ago)
Number Of Clients Seen:	3
Last Analysis Date:	2024-05-05 13:54:43.206724 (2 months ago)
Human Expert Analysis Date:	2024-05-06 16:19:27.849548 (2 months ago)
Human Expert Analysis Result:	Malware

VALKYRIE COMODO

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[]
Number Of Sections	5
Trid	[[61.9, u'Win32 Executable MS Visual C++ (generic)'], [13.0, u'Win32 Dynamic Link Library (generic)'], [8.9, u'Win32 Executable (generic)'], [4.1, u'Win16/32 Executable Delphi generic'], [4.0, u'OS/2 Executable (generic)']]
Compilation Time Stamp	0xAE8C39C6 [Wed Oct 18 19:30:14 2062 UTC] [SUSPICIOUS]
Translation	0x0000 0x04b0
LegalCopyright	Copyright \xa9 2024
Assembly Version	1.0.0.0
InternalName	AutoLauncher.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	Luxuria
ProductVersion	1.0.0.0
FileDescription	Luxuria
OriginalFilename	AutoLauncher.exe
Entry Point	0x5fc00a ()
Machine Type	Intel 386 or later - 32Bit
File Size	2059280
Ssdeep	49152:ZWFxPJFPcZYQKes8mugsPngHr79/Hx8vkXhWF+DDxaUKY:ZoxPyw8mRPmvRF4DQ4
Sha256	ae3da52225038e4f4ad470079fa2c2c08a3481456e1734e3953e539bdedc1ea3
Exifinfo	[{u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs-aws/fvs/valkyrie_shared/core/valkyrie_files/9/9/7/a/997a45a3707dd6ac76765664503576d3f6a37cb3', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2024:05:05 09:51:23-04:00', u'EXE:InitializedDataSize': 22016, u'File:FileModifyDate': u'2024:05:05 09:51:21-04:00', u'File:FileSize': u'2011 kB', u'EXE:MachineType': u'Intel 386 or later, and compatibles', u'File:FileType': u'Win32 EXE', u'EXE:UninitializedDataSize': 0, u'File:FileName': u'997a45a3707dd6ac76765664503576d3f6a37cb3', u'EXE:ImageVersion': 0.0, u'File:FileTypeExtension': u'exe', u'EXE:OSVersion': 4.0, u'EXE:PEType': u'PE32', u'EXE:TimeStamp': u'2062:10:18 15:30:14-04:00', u'EXE:LinkerVersion': 48.0, u'ExifTool:ExifToolVersion': 10.1, u'File:Directory': u'/nfs-aws/fvs/valkyrie_shared/core/valkyrie_files/9/9/7/a', u'EXE:EntryPoint': u'0x1fc00a', u'EXE:SubsystemVersion': 6.0, u'EXE:CodeSize': 2036224, u'File:FileInodeChangeDate': u'2024:05:05 09:51:22-04:00', u'EXE:Subsystem': u'Windows GUI'}]
Mime Type	application/x-dosexec
Imphash	f34d5f2d4577ed6d9ceec516c1f5a744

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
"`j+"t\	0x2000	0x74	0x200	7.66655983521	1195df2a2080004d970ea835d65f7626
.text	0x4000	0x1f0fbc	0x1f1000	7.98582700111	a9fc25c6e0288f6f4f04449b296d78ac
.UN]M6	0x1f6000	0x5172	0x5200	7.82232696925	faf8fc9418aae050a8b6f79e8e2a4d96
	0x1fc000	0x10	0x200	0.118369631259	d1fe83af3b534a501051bc91a03c10cd
.reloc	0x1fe000	0xc	0x200	0.0980041756627	a4fe72978ba527f1ceb38d4fe8ad726f

PE Imports

- mscoree.dll
  - _CorExeMain

PE Resources

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 2056496, u'sha256': u'cbeee9fb5b0477f3a4f74db325509a8fe0e85e5c5145cd5d670ecda657bc0fa8', u'type': u'PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced', u'size': 19229}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_ICON', u'offset': 2075728, u'sha256': u'c309187de1a82ec9bae4dd4568472f49af4b1c9c5a52f21f424b2b45ed22bc4f', u'type': u'MS Windows icon resource - 1 icon, 256x256', u'size': 20}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_VERSION', u'offset': 2075748, u'sha256': u'cca30bd640c48925d4c761d47562972c39abc7d7501cb42e4c2e1cdb596ca4e8', u'type': u'data', u'size': 804}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_MANIFEST', u'offset': 2076552, 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