VALKYRIE COMODO

# Summary

**File Name:** None

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

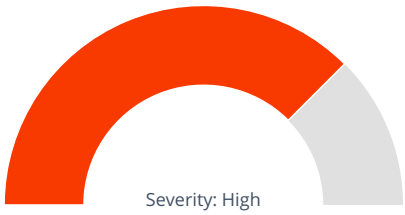
**SHA1:** 920ba11ff3d1a5769530b2be73468d8bd3afbae2

**MD5:** d14c93f4e28206fbe1d35a655eaf7119

MALWARE

Valkyrie Final Verdict

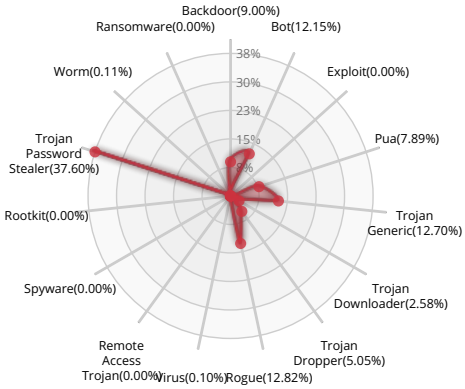
## DETECTION SECTION



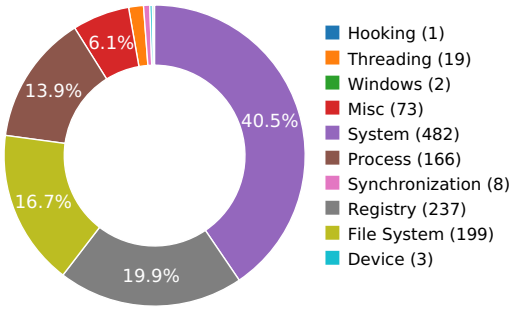
Severity: High

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

### 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\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll |
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\clr.dll |
| C:\Users\user\AppData\Local\Temp\920ba11ff3d1a5769530b2be73468d8bd3afbae2.exe.config |
| C:\Users\user\AppData\Local\Temp\920ba11ff3d1a5769530b2be73468d8bd3afbae2.exe |
| 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\Globalization\Sorting\sortdefault.nls |
| 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\RedBoy V1.4* |
| C:\Users\user\AppData\Local\Temp\920ba11ff3d1a5769530b2be73468d8bd3afbae2.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\Framework\v4.0.30319\en-US\mscorrc.dll |

| |
|---|
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\en-US\mscorrc.dll.DLL |
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\en\mscorrc.dll |
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\en\mscorrc.dll.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\.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\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US |
| HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US |
| 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\Windows Error Reporting\WMR\Disable |
| 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\Windows\CurrentVersion\SideBySide\PreferExternalManifest |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\DbgJITDebugLaunchSetting |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\DbgManagedDebugger |
| 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)

## 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 |
| shlwapi.dll.UrlIsW |
| 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 |
| mscoreei.dll.#24 |
| ntdll.dll.NtSetSystemInformation |
| kernel32.dll.SortGetHandle |
| kernel32.dll.SortCloseHandle |
| kernel32.dll.GetNativeSystemInfo |
| ole32.dll.CoInitializeEx |
| cryptbase.dll.SystemFunction036 |
| uxtheme.dll.ThemeInitApiHook |
| user32.dll.IsProcessDPIAware |

| |
|---|
| ole32.dll.CoGetContextToken |
| clrjit.dll.sxsJitStartup |
| clrjit.dll.getJit |

## 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_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\920ba11ff3d1a5769530b2be73468d8bd3afbae2.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\System\CurrentControlSet\Control\Nls\CustomLocale |
| HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US |
| HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\ExtendedLocale |
| HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US |
| HKEY_LOCAL_MACHINE\Software\Microsoft\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\Windows Error Reporting\WMR |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable |

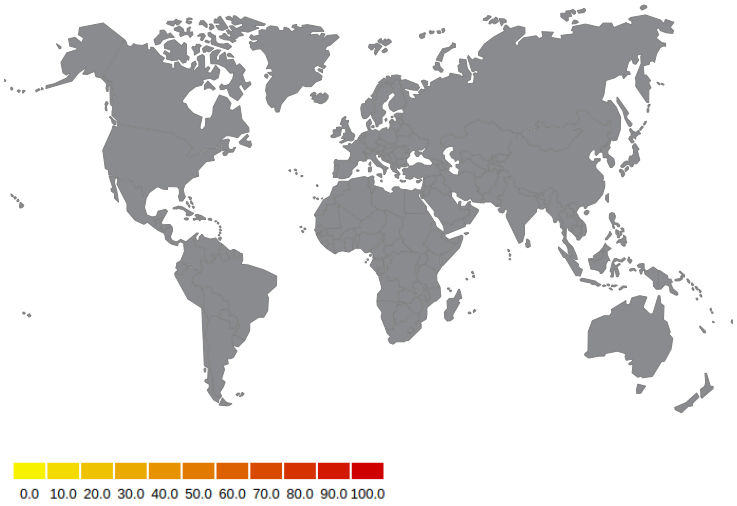
| |
|---|
| HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale |
| HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale\Alternate Sorts |
| HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Language Groups |
| HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409 |
| HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1 |

## READ FILES

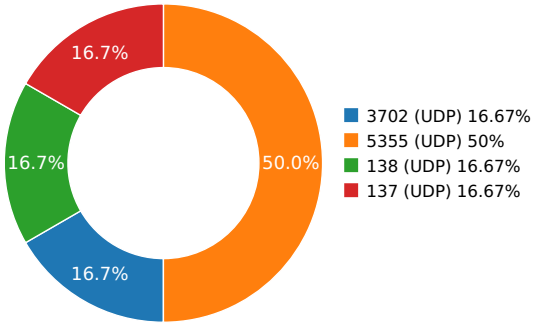
| |
|---|
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscoreei.dll |
| C:\Users\user\AppData\Local\Temp\920ba11ff3d1a5769530b2be73468d8bd3afbae2.exe.config |
| C:\Users\user\AppData\Local\Temp\920ba11ff3d1a5769530b2be73468d8bd3afbae2.exe |
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\clr.dll |
| C:\Windows\System32\MSVCR120_CLR0400.dll |
| C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config |
| C:\Windows\Globalization\Sorting\sortdefault.nls |
| 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\Framework\v4.0.30319\mscorrc.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\SysWOW64\en-US\KERNELBASE.dll.mui |
| 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 |

## Network Behavior

### CONTACTED IPS




### NETWORK PORT DISTRIBUTION




| Name | IP | Country | ASN | ASN Name | Trigger Process Type |
|---|---|---|---|---|---|

### UDP PACKETS

| Call Time During Execution(sec) | Source IP | Dest IP | Dest Port |
|---|---|---|---|
| 3.23597288132 | Sandbox | 224.0.0.252 | 5355 |
| 3.26043391228 | Sandbox | 192.168.56.255 | 137 |
| 3.26399087906 | Sandbox | 224.0.0.252 | 5355 |
| 3.28267288208 | Sandbox | 239.255.255.250 | 3702 |
| 5.82250094414 | Sandbox | 224.0.0.252 | 5355 |
| 6.26731491089 | Sandbox | 192.168.56.255 | 138 |

VALKYRIE COMODO

DETAILED FILE INFO

## CREATED / DROPPED FILES

| FILE PATH | TYPE AND HASHES |
|---|---|

## MATCH YARA RULES

| MATCH RULES |
|---|

## STATIC FILE INFO

| | |
|---|---|
| **File Name:** | None |
| **File Type:** | PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows |
| **SHA1:** | 920ba11ff3d1a5769530b2be73468d8bd3afbae2 |
| **MD5:** | d14c93f4e28206fbe1d35a655eaf7119 |
| **First Seen Date:** | 2018-09-16 07:16:59.007102 ( 3 months ago ) |
| **Number Of Clients Seen:** | 3 |
| **Last Analysis Date:** | 2018-09-16 07:16:59.007102 ( 3 months ago ) |
| **Human Expert Analysis Date:** | 2018-09-16 13:51:00.327058 ( 3 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 | [[38.3, u'Win32 Dynamic Link Library (generic)'], [26.2, u'Win32 Executable (generic)'], [12.0, u'Win16/32 Executable Delphi generic'], [11.6, u'Generic Win/DOS Executable'], [11.6, u'DOS Executable Generic']] |
| Compilation Time Stamp | 0x5B89CFC1 [Fri Aug 31 23:31:13 2018 UTC] |
| Translation | 0x0000 0x04b0 |
| LegalCopyright | Copyright \xa9 HP Inc. 2018 |
| Assembly Version | 1.0.0.0 |
| InternalName | RedBoy V1.4.exe |
| FileVersion | 1.0.0.0 |
| CompanyName | HP Inc. |
| LegalTrademarks | |
| Comments | |
| ProductName | RedBoy V1.4 |
| ProductVersion | 1.0.0.0 |
| FileDescription | RedBoy V1.4 |
| OriginalFilename | RedBoy V1.4.exe |
| Entry Point | 0x46400a () |
| Machine Type | Intel 386 or later - 32Bit |
| File Size | 376832 |
| Ssdeep | 6144:CvnQMO7gAfw3jJfuyXr5yeAkxdaj6RTzKr9TMEAgwqKKfOI81rfaZWVCGqNZG:cug7frbkwf/K5pAHfzrazGq/G |
| Sha256 | 8c530084147696b6a36e37d1622302c5bf48dbb81198dc30db80c0ce79d19d6d |
| Exifinfo | [{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/9/2/0/b/920ba11ff3d1a5769530b2be73468d8bd3afbae2', u'EXE:OriginalFileName': u'RedBoy V1.4.exe', u'EXE:ProductName': u'RedBoy V1.4', u'EXE:InternalName': u'RedBoy V1.4.exe', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2018:09:16 07:10:24+00:00', u'EXE:InitializedDataSize': 325120, u'File:FileModifyDate': u'2018:09:16 07:10:24+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'368 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'', u'EXE:ProductVersion': u'1.0.0.0', u'EXE:ObjectFileType': u'Executable application', u'File:FileType': u'Win32 EXE', u'EXE:CompanyName': u'HP Inc.', u'File:FileName': u'920ba11ff3d1a5769530b2be73468d8bd3afbae2', u'EXE:ImageVersion': 0.0, u'File:FileTypeExtension': u'exe', u'EXE:OSVersion': 4.0, u'EXE:PEType': u'PE32', u'EXE:TimeStamp': u'2018:08:31 23:31:13+00:00', u'EXE:FileFlagsMask': u'0x003f', u'EXE:LegalCopyright': u'Copyright \xa9 HP Inc. 2018', u'EXE:LinkerVersion': 11.0, u'EXE:FileFlags': u'(none)', u'EXE:Subsystem': u'Windows GUI', u'File:Directory': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/9/2/0/b', u'EXE:FileDescription': u'RedBoy V1.4', u'EXE:EntryPoint': u'0x6400a', u'EXE:SubsystemVersion': 4.0, u'EXE:CodeSize': 50688, u'EXE:Comments': u'', u'File:FileInodeChangeDate': u'2018:09:16 07:10:24+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 |
|---|---|---|---|---|---|
| %cJbO | 0x2000 | 0x4ec7c | 0x4ee00 | 7.99942391371 | 2544ff44e7c6b8bf283acc6fab0ebb4a |
| .text | 0x52000 | 0xc2d8 | 0xc400 | 5.87141222068 | 1a6326f27df9cbe8dd784715a3f71e8a |
| .rsrc | 0x60000 | 0x5d8 | 0x600 | 4.1727326009 | 74216610520e479627cbb7a905af31c5 |
| .reloc | 0x62000 | 0xc | 0x200 | 0.0980041756627 | 15ef9779e33bb22c351a0197dcfdd1f1 |
| | 0x64000 | 0x10 | 0x200 | 0.142635768149 | 93884d475f7639bcf7ee6eea271d7bdc |

### PE Imports

- mscoree.dll
  - _CorExeMain

### PE Resources

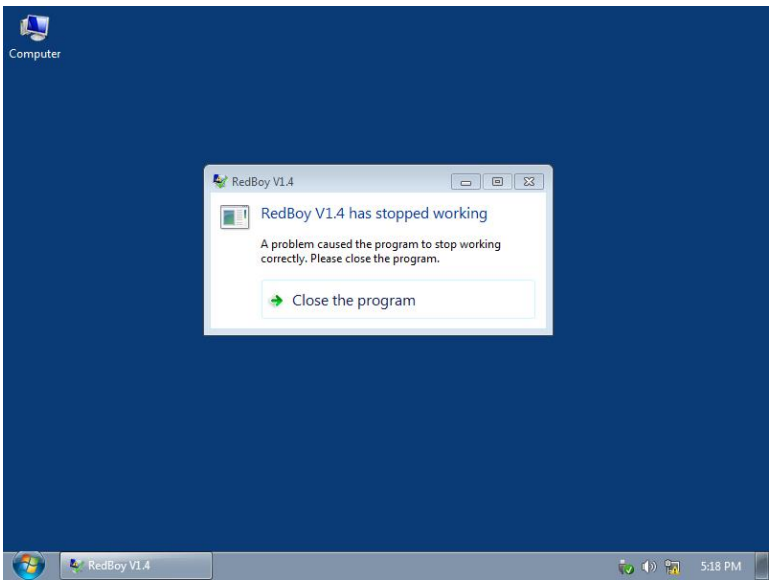
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_VERSION', u'offset': 393376, u'sha256': u'a8f6e2bbfc18655df5bbf6efa0bab714f8697dc6d9175adc03682b7f48a25dc7', u'type': u'data', u'size': 840}

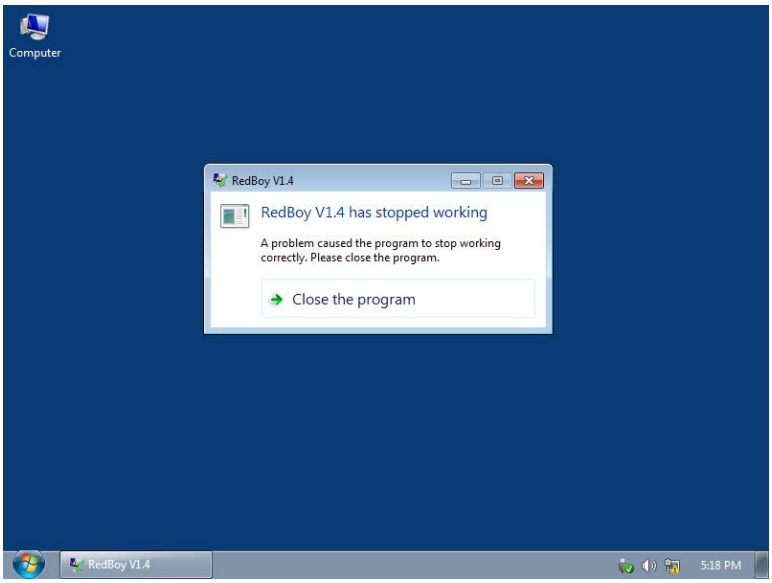
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_MANIFEST', u'offset': 394216, u'sha256': u'539dc26a14b6277e87348594ab7d6e932d16aabb18612d77f29fe421a9f1d46a', u'type': u'XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators', u'size': 490}

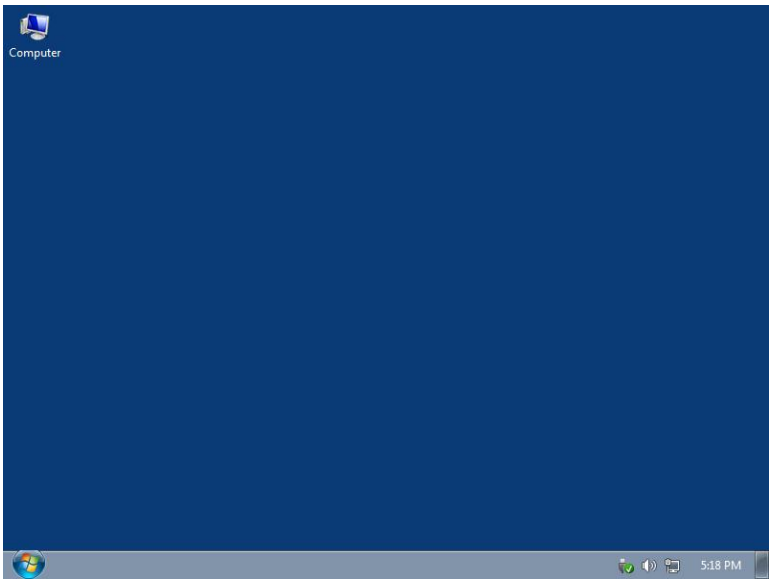
## CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

## SCREENSHOTS




Computer
RedBoy V1.4
RedBoy V1.4 has stopped working
A problem caused the program to stop working correctly. Please close the program.
Close the program
RedBoy V1.4
5:18 PM


Computer
5:18 PM


Computer
5:18 PM