

Summary

File Name: setup.exe

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

SHA1: 496594c30db2456816e1acf7de35082c654be99a

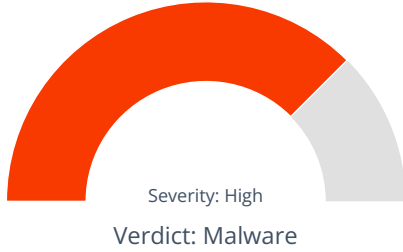
MD5: bbf88bb080208158050247626a5abcb2



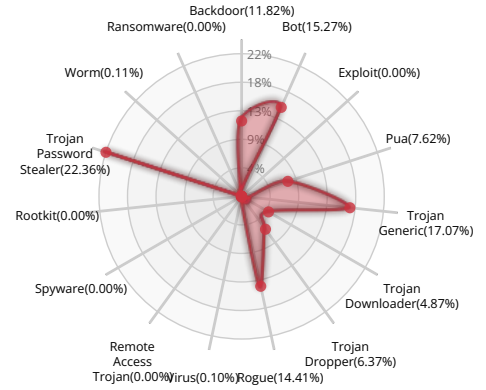
MALWARE

Valkyrie Final Verdict

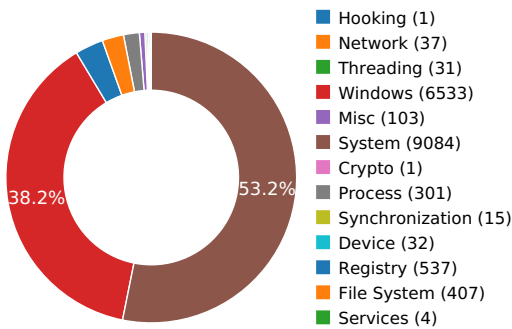
DETECTION SECTION



CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



Activity Details

INFORMATION DISCOVERY



Reads data out of its own binary image

Show sources

NETWORKING



Attempts to connect to a dead IP:Port (2 unique times)

Show sources

PACKER



The binary likely contains encrypted or compressed data.

Show sources

STATIC ANOMALY



Anomalous binary characteristics

Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION



Creates RWX memory

Show sources

MALWARE ANALYSIS SYSTEM EVASION



A process attempted to delay the analysis task.

Show sources



Behavior Graph

Behavior Summary

ACCESSED FILES

C:\Windows\sysnative\MSCOREE.DLL.local
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscoreei.dll
C:\Windows\Microsoft.NET\Framework64*
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\clr.dll
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorwks.dll
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clr.dll
C:\Users\user\AppData\Local\Temp\496594c30db2456816e1acf7de35082c654be99a.exe.config
C:\Users\user\AppData\Local\Temp\496594c30db2456816e1acf7de35082c654be99a.exe
C:\Users\user\AppData\Local\Temp\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\sysnative\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\sysnative\wbem\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\sysnative\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\Framework64\v4.0.30319\MSVCR120_CLR0400.dll
C:\Windows\sysnative\MSVCR120_CLR0400.dll
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscoree.dll
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\fusion.localgac
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\Microsoft.Net\assembly\GAC_64\mscorlib\v4.0.4.0.0__b77a5c561934e089\mscorlib.dll
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib*
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\fa8eef6f6cb67c660d71e15c5cad71b5\mscorlib.ni.dll
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\fa8eef6f6cb67c660d71e15c5cad71b5\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\Framework64\v4.0.30319\ole32.dll
\Device\KsecDD
C:\Windows\assembly\NativeImages_v4.0.30319_64\setup*
C:\Users\user\AppData\Local\Temp\496594c30db2456816e1acf7de35082c654be99a.INI
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clrjit.dll
C:\Windows\assembly\pubpol20.dat
C:\Windows\assembly\GAC\PublisherPolicy.tme
C:\Windows\Microsoft.Net\assembly\GAC_64\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_64\System.Windows.Forms*
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\1a359814ff0333ca2c4ab29f30f55dd20\System.Windows.Forms.ni.dll
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\1a359814ff0333ca2c4ab29f30f55dd20\System.Windows.Forms.ni.dll.aux
C:\Windows\Microsoft.Net\assembly\GAC_64\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_64\System*
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\5f665a4076cb8d9479ca406e7827fb9f\System.ni.dll
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\5f665a4076cb8d9479ca406e7827fb9f\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_64\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_64\System.Drawing*
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\1751687825177cb487c1080d7e37401f\System.Drawing.ni.dll
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\1751687825177cb487c1080d7e37401f\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
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\nlssorting.dll
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SortDefault.nlp
C:\
C:\Windows\

C:\Windows\SysWOW64\
 C:\Windows\SysWOW64\kr\
 C:\Windows\SysWOW64\kr

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\InstallRoot
 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\CLRLoadLogDir
 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\UseLegacyV2RuntimeActivationPolicyDefaultValue
 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\OnlyUseLatestCLR
 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NoClientChecks
 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NET Framework Setup\NDP\v4\Full\Release
 HKEY_LOCAL_MACHINE\SOFTWARE\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\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\Microsoft\.NETFramework\UseRyuJIT
 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\FeatureSIMD
 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\JitTimeLogCsv
 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\JitFuncInfoLogFile
 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AltJit
 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\JitELTHookEnabled
 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\TailCallOpt
 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\JitVnMapSelBudget
 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\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\Microsoft\NETFramework\DbgJITDebugLaunchSetting
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NETFramework\DbgManagedDebugger
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\InstallationType
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\EnableConsoleTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\496594c30db2456816e1acf7de35082c654be99a_RASAPI32\EnableFileTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\496594c30db2456816e1acf7de35082c654be99a_RASAPI32\FileTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\496594c30db2456816e1acf7de35082c654be99a_RASAPI32\EnableConsoleTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\496594c30db2456816e1acf7de35082c654be99a_RASAPI32\ConsoleTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\496594c30db2456816e1acf7de35082c654be99a_RASAPI32\MaxFileSize
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\496594c30db2456816e1acf7de35082c654be99a_RASAPI32\FileDirectory
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NETFramework\LegacyWPADSupport
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OLE\MaximumAllowedAllocationSize
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecision
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecisionTime
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\WpadExpirationDays
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OLE\AppCompat\RaiseDefaultAuthnLevel
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OLE\DefaultAccessPermission
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\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\ABDDCF67
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledSessions\MachineThrottling
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\DisabledSessions\GlobalSession
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\GTB Standard Time\TZI
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\GTB Standard Time\MUI_Display
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\GTB Standard Time\MUI_Std
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\GTB Standard Time\MUI_Dlt
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NETFramework\v4.0.30319\HWRPortReuseOnSocketBind
HKEY_CURRENT_USER\Software\Microsoft\GDIPlus\FontCachePath
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{0A29FF9E-7F9C-4437-8B11-F424491E3931}\InprocServer32(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{0A29FF9E-7F9C-4437-8B11-F424491E3931}\Server(Default)
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

MODIFIED FILES

C:\Windows\SysWOW64\kr\winlogon.exe
C:\Users\user\AppData\Local\GDIPFONTCACHEV1.DAT

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

ntdll.dll.RtlVirtualUnwind

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
kernel32.dll.SortGetHandle
kernel32.dll.SortCloseHandle
ole32.dll.CoInitializeEx
cryptbase.dll.SystemFunction036
uxtheme.dll.ThemeInitApiHook
user32.dll.IsProcessDPIAware
ole32.dll.CoGetContextToken
clrjit.dll.sxsjitStartup
clrjit.dll.getjit
kernel32.dll.GetFullPathNameW

REGISTRY KEYS

HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\Policy\
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\Policy\v4.0
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\InstallRoot
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\CLRLoadLogDir
HKEY_CURRENT_USER\Software\Microsoft\.NETFramework
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\UseLegacyV2RuntimeActivationPolicyDefaultValue
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\OnlyUseLatestCLR
Policy\Standards
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\Policy\Standards
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\Policy\standards\v4.0.30319
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NoClientChecks
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\v4.0.30319\SKUs\
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SKUs\default
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NET Framework Setup\NDP\v4\Full
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NET Framework Setup\NDP\v4\Full\Release
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\DisableConfigCache
HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\496594c30db2456816e1acf7de35082c654be99a.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\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\ .NETFramework\UseRyuJIT
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ .NETFramework\FeatureSIMD
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OLEAUT
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ .NETFramework\JitTimeLogCsv
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ .NETFramework\JitFuncInfoLogFile
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ .NETFramework\AltJit
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ .NETFramework\JitELTHookEnabled
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ .NETFramework\TailCallOpt
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ .NETFramework\JitVNMapSelBudget
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.Formatteratters.Soap__b03f5f7f11d50a3a
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\policy.4.0.System.Runtime.Serialization.Formatteratters.Soap__b03f5f7f11d50a3a
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NETFramework\Policy\APTCA

READ FILES

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorlib.dll
C:\Users\user\AppData\Local\Temp\496594c30db2456816e1acf7de35082c654be99a.exe.config
C:\Users\user\AppData\Local\Temp\496594c30db2456816e1acf7de35082c654be99a.exe
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clr.dll
C:\Windows\sysnative\MSVCR120_CLR0400.dll
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\fa8eef6f6cb67c660d71e15c5cad71b5\mscorlib.ni.dll.aux
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\fa8eef6f6cb67c660d71e15c5cad71b5\mscorlib.ni.dll
\Device\KsecDD
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clrjit.dll
C:\Windows\assembly\pubpol20.dat
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\fa359814ff0333ca2c4ab29f30f55dd20\System.Windows.Forms.ni.dll.aux
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\5f665a4076cb8d9479ca406e7827fb9f\System.ni.dll.aux
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\5f665a4076cb8d9479ca406e7827fb9f\System.ni.dll
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\1751687825177cb487c1080d7e37401f\System.Drawing.ni.dll.aux
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\1751687825177cb487c1080d7e37401f\System.Drawing.ni.dll
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\fa359814ff0333ca2c4ab29f30f55dd20\System.Windows.Forms.ni.dll
C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Windows.Forms\v4.0.4.0.0__b77a5c561934e089\System.Windows.Forms.dll
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\nls\sorting.dll
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SortDefault.nlp
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\46ec60579b59cedcc8c39cabca6d1153\System.Configuration.ni.dll.aux
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\5034a88e58f966dd7d69fe9b9875832c\System.Core.ni.dll.aux

C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\5034a88e58f966dd7d69fe9b9875832c\System.Core.ni.dll
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\46ec60579b59cedcc8c39cabca6d1153\System.Configuration.ni.dll
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\c9576235d85a3db71a0bee45aa4155ba\System.Xml.ni.dll.aux
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\c9576235d85a3db71a0bee45aa4155ba\System.Xml.ni.dll
C:\Windows\sysnative\en-US\KERNELBASE.dll.mui
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorrc.dll
C:\Windows\sysnative\tzres.dll
C:\Windows\sysnative\en-US\tzres.dll.mui
C:\Windows\winsxs\amd64_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_2b24536c71ed437a\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\Microsoft.NET\Framework64\v4.0.30319\diasymreader.dll
C:\Windows\Microsoft.Net\assembly\GAC_MSIL\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.pdb
C:\Windows\symbols\dll\System.pdb
C:\Windows\dll\System.pdb
C:\Windows\System.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\Fonts\staticcache.dat
C:\Windows\sysnative\luxtheme.dll.Config
C:\Windows\sysnative\luxtheme.dll

MUTEXES

CicLoadWinStaWinSta0
Local\MSCTF.CtfMonitorInstMutexDefault1

MODIFIED REGISTRY KEYS

HKEY_LOCAL_MACHINE\Software\Microsoft\Tracing\496594c30db2456816e1acf7de35082c654be99a_RASAPI32
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\496594c30db2456816e1acf7de35082c654be99a_RASAPI32\EnableFileTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\496594c30db2456816e1acf7de35082c654be99a_RASAPI32\EnableConsoleTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\496594c30db2456816e1acf7de35082c654be99a_RASAPI32\FileTracingMask

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\496594c30db2456816e1acf7de35082c654be99a_RASAPI32\ConsoleTracingMask

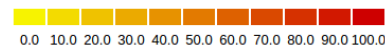
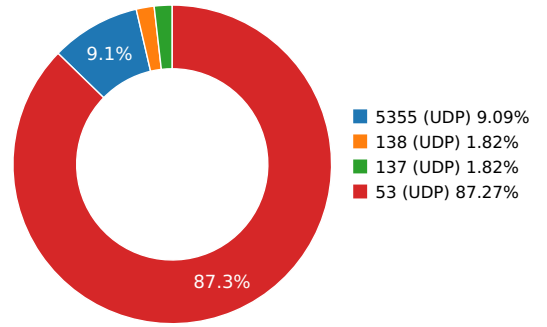
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\496594c30db2456816e1acf7de35082c654be99a_RASAPI32\MaxFileSize

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\496594c30db2456816e1acf7de35082c654be99a_RASAPI32\FileDirectory

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
	185.254.240.73	Japan	34985	AIComputing	Malware Process
www.aieov.com	96.126.123.244	United States	63949	Akamai Technologies, Inc.	Malware Process
					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
3.01062583923	Sandbox	224.0.0.252	5355
3.02439689636	Sandbox	224.0.0.252	5355
3.07862377167	Sandbox	192.168.56.255	137
5.57940578461	Sandbox	224.0.0.252	5355
7.00850200653	Sandbox	224.0.0.252	5355
9.08284878731	Sandbox	192.168.56.255	138
9.64139389992	Sandbox	8.8.4.4	53
10.641204834	Sandbox	8.8.8.8	53
14.2336568832	Sandbox	224.0.0.252	5355
24.0011548996	Sandbox	8.8.8.8	53
25.0005447865	Sandbox	8.8.4.4	53

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
38.3601257801	Sandbox	8.8.8.8	53
39.3596408367	Sandbox	8.8.4.4	53
52.9386839867	Sandbox	8.8.8.8	53
53.9377889633	Sandbox	8.8.4.4	53
67.2972848415	Sandbox	8.8.8.8	53
68.2973799706	Sandbox	8.8.4.4	53
81.6568639278	Sandbox	8.8.8.8	53
82.6564838886	Sandbox	8.8.4.4	53
99.9072508812	Sandbox	8.8.8.8	53
100.906241894	Sandbox	8.8.4.4	53
114.266594887	Sandbox	8.8.8.8	53
115.265775919	Sandbox	8.8.4.4	53
128.626236916	Sandbox	8.8.8.8	53
129.625152826	Sandbox	8.8.4.4	53
146.875850916	Sandbox	8.8.8.8	53
147.875472784	Sandbox	8.8.4.4	53
161.235022783	Sandbox	8.8.8.8	53
162.234387875	Sandbox	8.8.4.4	53
175.594506979	Sandbox	8.8.8.8	53
176.593833923	Sandbox	8.8.4.4	53
193.845269918	Sandbox	8.8.8.8	53
194.843961	Sandbox	8.8.4.4	53
208.204236984	Sandbox	8.8.8.8	53
209.203066826	Sandbox	8.8.4.4	53
222.563264847	Sandbox	8.8.8.8	53
223.562915802	Sandbox	8.8.4.4	53
240.813315868	Sandbox	8.8.8.8	53
241.812543869	Sandbox	8.8.4.4	53
255.172679901	Sandbox	8.8.8.8	53
256.172607899	Sandbox	8.8.4.4	53
269.531823874	Sandbox	8.8.8.8	53
270.531711817	Sandbox	8.8.4.4	53
287.782284975	Sandbox	8.8.8.8	53
288.781178951	Sandbox	8.8.4.4	53
302.14109683	Sandbox	8.8.8.8	53
303.141133785	Sandbox	8.8.4.4	53
316.500568867	Sandbox	8.8.8.8	53
317.500205994	Sandbox	8.8.4.4	53
330.751271963	Sandbox	8.8.8.8	53
331.75007081	Sandbox	8.8.4.4	53
345.109918833	Sandbox	8.8.8.8	53

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
346.109255791	Sandbox	8.8.4.4	53
359.469680786	Sandbox	8.8.8.8	53
360.468745947	Sandbox	8.8.4.4	53

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:	setup.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
SHA1:	496594c30db2456816e1acf7de35082c654be99a
MD5:	bbfd8bb080208158050247626a5abcb2
First Seen Date:	2024-07-23 12:20:35.656974 (2 years ago)
Number Of Clients Seen:	2
Last Analysis Date:	2024-07-23 12:20:35.656974 (2 years ago)
Human Expert Analysis Date:	2024-07-23 20:01:50.782724 (2 years ago)
Human Expert Analysis Result:	Malware

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[]
Number Of Sections	5
Trid	[[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	0x95297733 [Tue Apr 20 09:11:15 2049 UTC] [SUSPICIOUS]
Translation	0x0000 0x04b0
LegalCopyright	Copyright \xa9 2022
Assembly Version	1.0.0.0
InternalName	setup.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	setup
ProductVersion	1.0.0.0
FileDescription	setup
OriginalFilename	setup.exe
Entry Point	0x41a00a ()
Machine Type	Intel 386 or later - 32Bit
File Size	79872
Ssdeep	1536:7qUB3dAvrxeZ/H+tiuUO/hl74sGkAlZKWLZ:7jdAjKetjUOO74sGkAlZKW1
Sha256	6b2f1fac20a3dc679fbfc685f47868e56566724c529e5337f37488ced42ff08e
Exifinfo	[[{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r-', u'SourceFile': u'\\nfs\\fvs\\valkyrie_shared\\core\\valkyrie_files\\4\\9\\6\\5\\496594c30db2456816e1acf7de35082c654be99a', u'EXE:OriginalFileName': u'setup.exe', u'EXE:ProductName': u'setup', u'EXE:InternalName': u'setup.exe', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2024:07:23 12:19:54+00:00', u'EXE:InitializedDataSize': 34816, u'File:FileModifyDate': u'2024:07:23 12:19:42+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'78 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'', u'File:FileName': u'496594c30db2456816e1acf7de35082c654be99a', u'EXE:ImageVersion': 0.0, u'File:FileTypeExtension': u'.exe', u'EXE:OSVersion': 4.0, u'EXE:PEType': u'PE32', u'EXE:TimeStamp': u'2049:04:20 09:11:15+00:00', u'EXE:FileFlagsMask': u'0x003f', u'EXE:LegalCopyright': u'Copyright \xa9 2022', 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\\4\\9\\6\\5', u'EXE:FileDescription': u'setup', u'EXE:EntryPoint': u'0x1a00a', u'EXE:SubsystemVersion': 6.0, u'EXE:CodeSize': 44032, u'EXE:Comments': u'', u'File:FileInodeChangeDate': u'2024:07:23 12:19:54+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

A series of horizontal lines for writing, consisting of 30 pairs of parallel lines spaced evenly down the page.



A series of horizontal lines for writing, consisting of 30 pairs of parallel lines spaced evenly down the page.

A series of horizontal lines for writing, consisting of 40 pairs of parallel lines spaced evenly down the page.

A series of horizontal lines for writing, consisting of 30 pairs of parallel lines spaced evenly down the page.

