VALKYRIE COMODO

Summary

File Name: ojoh.exe

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

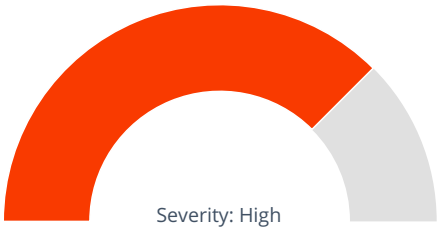
SHA1: 2e2889879b93f72664c66329ea4162de53774477

MD5: a28bf0b304449200b2b461f201a89b59

MALWARE

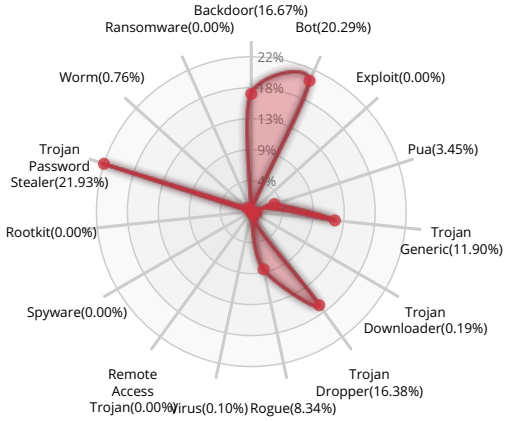
Valkyrie Final Verdict

DETECTION SECTION

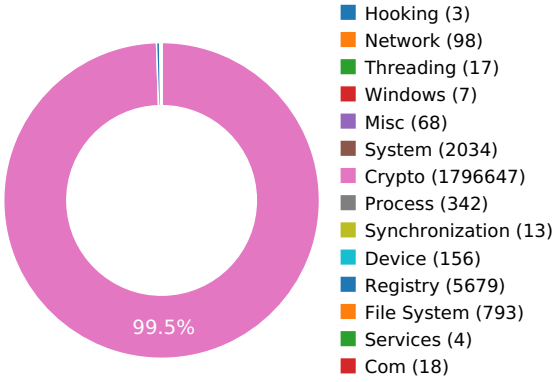


Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

VALKYRIE COMODO

Activity Details

INFORMATION DISCOVERY

Attempts to remove evidence of file being downloaded from the Internet — Show sources

NETWORKING

Attempts to connect to a dead IP:Port (3 unique times) — Show sources

Performs some HTTP requests — Show sources

CRYPTOGRAPHY

At least one IP Address, Domain, or File Name was found in a crypto call — 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

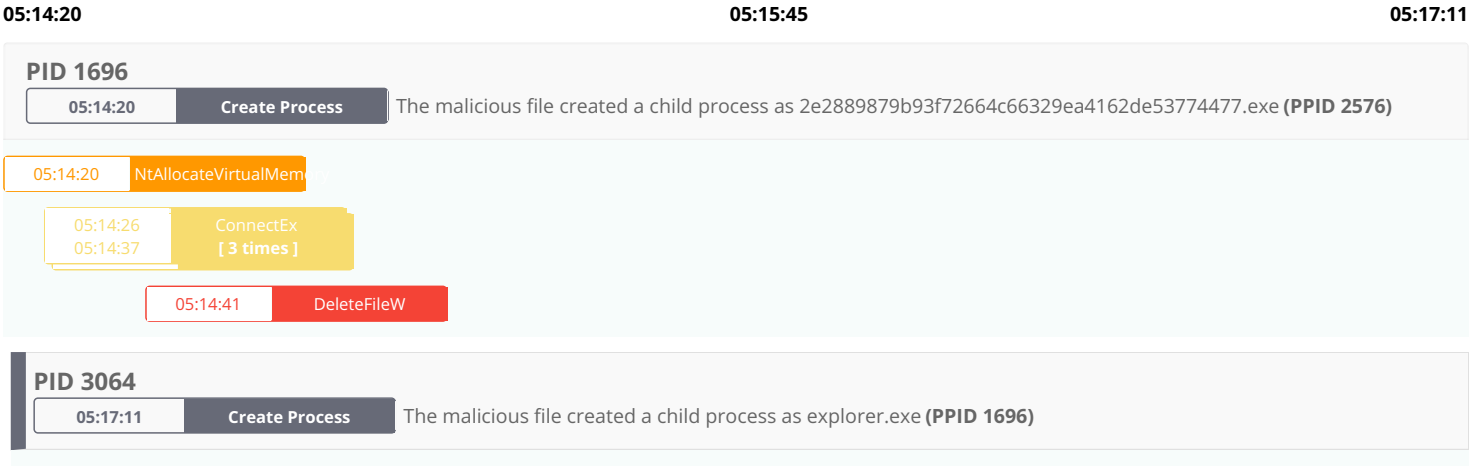
Creates RWX memory — Show sources

PERSISTENCE AND INSTALLATION BEHAVIOR

Creates a copy of itself — 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\2e2889879b93f72664c66329ea4162de53774477.exe.config
C:\Users\user\AppData\Local\Temp\2e2889879b93f72664c66329ea4162de53774477.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:\Users\user\AppData\Local\Temp\2e2889879b93f72664c66329ea4162de53774477.exe.Local\
C:\Windows\winsxs\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc
C:\Windows\winsxs\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc\msvcr80.dll
C:\Windows

C:\Windows\winsxs
C:\Windows\Microsoft.NET\Framework\v4.0.30319
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config
C:\Windows\Microsoft.NET\Framework\v2.0.50727\fusion.localgac
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\security.config
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\security.config.cch
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\enterprisesec.config
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\enterprisesec.config.cch
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch
C:\Windows\assembly\NativeImages_v2.0.50727_32\index126.dat
C:\Windows\assembly\NativeImages_v2.0.50727_32\mscorlib\62a0b3e4b40ec0e8c5cfaa0c8848e64a\mscorlib.ni.dll
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.INI
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\v2.0.50727\mscorsec.dll
C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af
C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll
C:\Windows\System32\p2pcollab.dll
C:\Windows\System32\qagentrt.dll
C:\Windows\System32\dnsapi.dll
C:\Windows\System32\en-US\dnsapi.dll.mui
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates*
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\1233B8D21D2ECB0483D16253D1FF3964BD09EF0C
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\16B1DD478BCE71A0FB1822E8F4F30AB467BBEFD4
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\2064A97B987412930E2994D60AE7EB72D89BC4F7
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\37998502C2CC1852F8774DAF543DD76D10D6FD93
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\418C30DD41197CBAABF21675F8559794F5551115
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\44E5AE16D06F9FBB92D6D9444B5C65C0F331D0EC
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\4FDDCB932603534677ECAE8C7D0FD914FD443E83
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\5D247FE955609769879FB1DD016537EEF650B8EC
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\6A8C669D7D1D5759CE7C1E0C5BE286257C31F366

C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\744CDF45BF43EF285758286CAC89AF786F938342
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\761F091EA5F80A98B0D89734231D300CF9C027E8
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\7A5F1A5DE6AA551C795CC508128C6D894FA2C502
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8291DA84F9266F6D0ED367AF8BE3FA722529EB91
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\871E3CD70B6F8EE3C1E7BE4C7BEF4FFCCE673E32
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8A82FE0617F4170E0BF052CF6BABFC628DA51919
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8B943CF0CAEF7F6F04E98C9405960323B23C516D
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\9317D002FC43BDA932B8397B6E729B83D48EEB8D
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\95EEF9A37407C5B87BCF95D69B01DCFDAFD07635

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\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\GCStressStart
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\GCStressStartAtJit
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\VersioningLog
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\LogResourceBinds
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\UseLegacyIdentityFormat
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\DisableMSIPeek
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NoClientChecks
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DevOverrideEnable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\LatestIndex
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\index126\NIUsageMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\index126\ILUsageMask

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\ConfigMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\ConfigString
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\MVID
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\EvalationData
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\Status
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\ILDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\NIDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\MissingDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83\Status
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83\Modules
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83\SIG
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83\LastModTime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\GACChangeNotification\Default\mscorlib,2.0.0.0,,b77a5c561934e089,x86
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\crypt32\DebugHeapFlags
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\Certificate\{31D1ADC1-D329-11D1-8ED8-0080C76516C6}\$DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\Certificate\{31D1ADC1-D329-11D1-8ED8-0080C76516C6}\$Function
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\FinalPolicy\{31D1ADC1-D329-11D1-8ED8-0080C76516C6}\$DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\FinalPolicy\{31D1ADC1-D329-11D1-8ED8-0080C76516C6}\$Function
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\Initialization\{31D1ADC1-D329-11D1-8ED8-0080C76516C6}\$DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\Initialization\{31D1ADC1-D329-11D1-8ED8-0080C76516C6}\$Function
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\Message\{31D1ADC1-D329-11D1-8ED8-0080C76516C6}\$DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\Message\{31D1ADC1-D329-11D1-8ED8-0080C76516C6}\$Function
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\Signature\{31D1ADC1-D329-11D1-8ED8-0080C76516C6}\$DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\Signature\{31D1ADC1-D329-11D1-8ED8-0080C76516C6}\$Function
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\CertCheck\{31D1ADC1-D329-11D1-8ED8-0080C76516C6}\$DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\CertCheck\{31D1ADC1-D329-11D1-8ED8-0080C76516C6}\$Function
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing\State
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Security\Safety Warning Level
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\crypt32\DiagLevel
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\crypt32\DiagMatchAnyMask

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptDllFindOIDInfo\1.3.6.1.4.1.311.44.3.4!7\Name
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\MUI\StringCacheSettings\StringCacheGeneration
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\p2pcollab.dll,-8042
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptDllFindOIDInfo\1.3.6.1.4.1.311.47.1.1!7\Name
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptDllFindOIDInfo\1.3.6.1.4.1.311.64.1.1!7\Name
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\dnsapi.dll,-103
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\SystemCertificates\AuthRoot\DisableRootAutoUpdate
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\AutoUpdate\DisallowedCertSyncDeltaTime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\DisableMandatoryBasicConstraints
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\DisableCANameConstraints
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\DisableUnsupportedCriticalExtensions
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\MaxAIAUrlCountInCert
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\MaxAIAUrlRetrievalCountPerChain
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\MaxUrlRetrievalByteCount
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\MaxAIAUrlRetrievalByteCount
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\MaxAIAUrlRetrievalCertCount
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\CryptnetPreFetchTriggerPeriodSeconds
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\EnableWeakSignatureFlags
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\MinRsaPubKeyBitLength

MODIFIED FILES

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\378B079587A9184B2E2AB859CB263F40_524AD1B9B08D3C6450727265AE77B7D2
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\378B079587A9184B2E2AB859CB263F40_524AD1B9B08D3C6450727265AE77B7D2
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\8EB35376744F392396307460D546222D_DA4083211FC1CAD4C1215FF8726EF9C8
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\8EB35376744F392396307460D546222D_DA4083211FC1CAD4C1215FF8726EF9C8
C:\Users\user\AppData\Local\GDIPFONTCACHEV1.DAT
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\diagnoseapp.exe
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\security.config.cch.new
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\security.config.cch.1696.26061640
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\security.config.cch

C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch.new
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch.1696.26061640
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\enterprisesec.config.cch.new
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\enterprisesec.config.cch.1696.26061640
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\enterprisesec.config.cch

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
kernel32.dll.InitializeCriticalSectionAndSpinCount
kernel32.dll.IsProcessorFeaturePresent
msvcrt.dll._set_error_mode
msvcrt.dll.?set_terminate@@YAP6AXXZP6AXXZ@Z
kernel32.dll.FindActCtxSectionStringW
kernel32.dll.GetSystemWindowsDirectoryW
mscoree.dll.GetProcessExecutableHeap
mscoreei.dll.GetProcessExecutableHeap
mscorwks.dll._CorExeMain
mscorwks.dll.GetCLRFunction
advapi32.dll.RegisterTraceGuidsW
advapi32.dll.UnregisterTraceGuids
advapi32.dll.GetTraceLoggerHandle
advapi32.dll.GetTraceEnableLevel
advapi32.dll.GetTraceEnableFlags
advapi32.dll.TraceEvent
mscoree.dll.IEE
mscoreei.dll.IEE

mscorwks.dll.IEE
mscoree.dll.GetStartupFlags
mscoreei.dll.GetStartupFlags
mscoree.dll.GetHostConfigurationFile
mscoreei.dll.GetHostConfigurationFile
mscoreei.dll.GetCORVersion
mscoree.dll.GetCORSystemDirectory
mscoreei.dll.GetCORSystemDirectory_RetAddr
mscoreei.dll.CreateConfigStream
ntdll.dll.RtlUnwind
kernel32.dll.IsWow64Process
advapi32.dll.AllocateAndInitializeSid
advapi32.dll.OpenProcessToken
advapi32.dll.GetTokenInformation

DELETED FILES

C:\Users\user\AppData\Local\Temp\2e2889879b93f72664c66329ea4162de53774477.exe:Zone.Identifier
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\diagnoseapp.exe
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\security.config.cch.1696.26061640
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\security.config.cch
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\security.config.cch.new
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch.1696.26061640
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch.new
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\enterprisesec.config.cch.1696.26061640
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\enterprisesec.config.cch
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\enterprisesec.config.cch.new

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\v2.0.50727
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Fusion\NoClientChecks
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide\AssemblyStorageRoots
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\GCStressStart
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\GCStressStartAtJit
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\DisableConfigCache
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\Policy\AppPatch
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\Policy\AppPatch\v4.0.30319.00000
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\Policy\AppPatch\v4.0.30319.00000\mscorwks.dll
HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\2e2889879b93f72664c66329ea4162de53774477.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\VersioningLog
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\LogResourceBinds
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\UseLegacyIdentityFormat
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\DisableMSIPeek
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NoClientChecks
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\Security\Policy\Extensions\NamedPermissionSets
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\Security\Policy\Extensions\NamedPermissionSets\Internet
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\Security\Policy\Extensions\NamedPermissionSets\LocalIntranet

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2298303332-66077612-2598613238-1000
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\v2.0.50727\Security\Policy
HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\LatestIndex
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\index126
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\index126\NIUsageMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\index126\ILUsageMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\ConfigMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\ConfigString
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\MVID
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\EvalationData
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\Status
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\ILDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\NIDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\MissingDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83\Status
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83\Modules
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83\SIG
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83\LastModTime
HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion\GACChangeNotification\Default
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\GACChangeNotification\Default\mscorlib,2.0.0.0,,b77a5c561934e089,x86
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\crypt32
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\crypt32\DebugHeapFlags
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\msasn1
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Providers\Trust\Certificate\{31D1ADC1-D329-11D1-8ED8-0080C76516C6}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\Certificate\{31D1ADC1-D329-11D1-8ED8-0080C76516C6}\$DLL
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\Certificate\{31D1ADC1-D329-11D1-8ED8-0080C76516C6}\$Function
HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Providers\Trust\FinalPolicy\{31D1ADC1-D329-11D1-8ED8-0080C76516C6}

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Providers\Trust\FinalPolicy\{31D1ADC1-D329-11D1-8ED8-0080C76516C6}\$DLL

READ FILES

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

C:\Users\user\AppData\Local\Temp\2e2889879b93f72664c66329ea4162de53774477.exe.config

C:\Users\user\AppData\Local\Temp\2e2889879b93f72664c66329ea4162de53774477.exe

C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll

C:\Windows\winsxs\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc\msvcr80.dll

C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config

C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\security.config

C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\security.config.cch

C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\enterprisesec.config

C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\enterprisesec.config.cch

C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config

C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch

C:\Windows\assembly\NativeImages_v2.0.50727_32\index126.dat

C:\Windows\assembly\NativeImages_v2.0.50727_32\mscorlib\62a0b3e4b40ec0e8c5cfaa0c8848e64a\mscorlib.ni.dll

C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorsec.dll

C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll

C:\Windows\System32\p2pcollab.dll

C:\Windows\System32\dnsapi.dll

C:\Windows\System32\en-US\dnsapi.dll.mui

C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\1233B8D21D2ECB0483D16253D1FF3964BD09EF0C

C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\16B1DD478BCE71A0FB1822E8F4F30AB467BBEFD4

C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\2064A97B987412930E2994D60AE7EB72D89BC4F7

C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\37998502C2CC1852F8774DAF543DD76D10D6FD93

C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\418C30DD41197CBAABF21675F8559794F5551115

C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\44E5AE16D06F9FBB92D6D9444B5C65C0F331D0EC

C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\4FDDCB932603534677ECAE8C7D0FD914FD443E83

C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\5D247FE955609769879FB1DD016537EEF650B8EC

C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\6A8C669D7D1D5759CE7C1E0C5BE286257C31F366

C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\744CDF45BF43EF285758286CAC89AF786F938342

C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\761F091EA5F80A98B0D89734231D300CF9C027E8

C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\7A5F1A5DE6AA551C795CC508128C6D894FA2C502

C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8291DA84F9266F6D0ED367AF8BE3FA722529EB91

C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\871E3CD70B6F8EE3C1E7BE4C7BEF4FFCCE673E32
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8A82FE0617F4170E0BF052CF6BABFC628DA51919
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8B943CF0CAEF7F6F04E98C9405960323B23C516D
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\9317D002FC43BDA932B8397B6E729B83D48EEB8D
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\95EEF9A37407C5B87BCF95D69B01DCFDAFD07635
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\A092A81885DDD5AAD1EC1A803D7183779D81B6F9
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\BAED8A8C5A147CFA78E686BB4A8E5829C2F934F5
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\C8A51E044BF5AF39158BB24E414E8FDCD2891C3A
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\FB45378AB288E369B22C860D123A809F530D5CC1
C:\Windows\System32\en-US\WINHTTP.dll.mui
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\378B079587A9184B2E2AB859CB263F40_524AD1B9B08D3C6450727265AE77B7D2
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\378B079587A9184B2E2AB859CB263F40_524AD1B9B08D3C6450727265AE77B7D2
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\8EB35376744F392396307460D546222D_DA4083211FC1CAD4C1215FF8726EF9C8
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\8EB35376744F392396307460D546222D_DA4083211FC1CAD4C1215FF8726EF9C8
C:\Windows\System32\l_intl.nls
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorjit.dll
C:\Windows\assembly\pubpol20.dat
C:\Windows\assembly\NativeImages_v2.0.50727_32\System\9e0a3b9b9f457233a335d7fba8f95419\System.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\dbfe8642a8ed7b2b103ad28e0c96418a\System.Drawing.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\3afcd5168c7a6cb02eab99d7fd71e102\System.Windows.Forms.ni.dll
C:\Windows\assembly\GAC_MSIL\System.Windows.Forms\2.0.0.0__b77a5c561934e089\System.Windows.Forms.dll
C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80\GdiPlus.dll
C:\Users\user\AppData\Local\GDIPFONTCACHEV1.DAT
C:\Windows\Fonts\pala.ttf
C:\Windows\Fonts\palab.ttf
C:\Windows\Fonts\palai.ttf
C:\Windows\Fonts\palabi.ttf
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

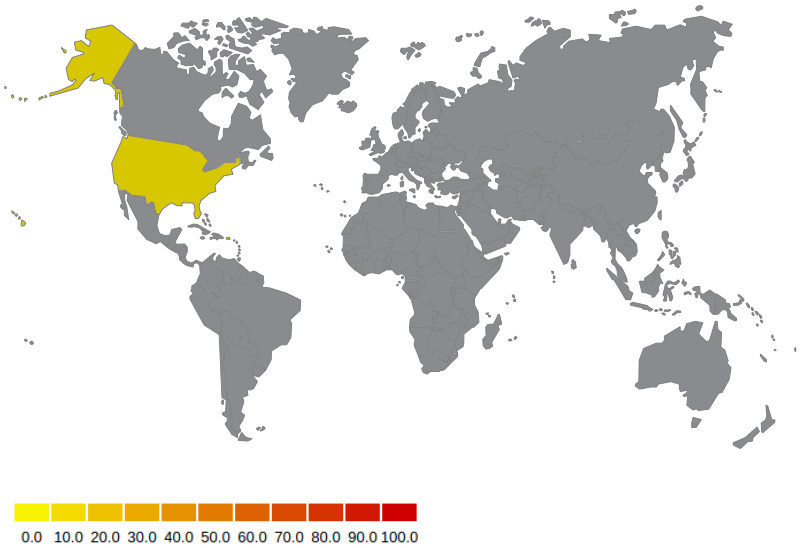
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Core\fbc05b5b05dc6366b02b8e2f77d080f1\System.Core.ni.dll
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\sorttbls.nlp
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\sortkey.nlp
C:\Windows\Microsoft.NET\Framework\v2.0.50727\Culture.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorrc.dll
C:\Windows\SysWOW64\explorer.exe.123.Manifest
\Device\KsecDD
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\SysWOW64\shell32.dll

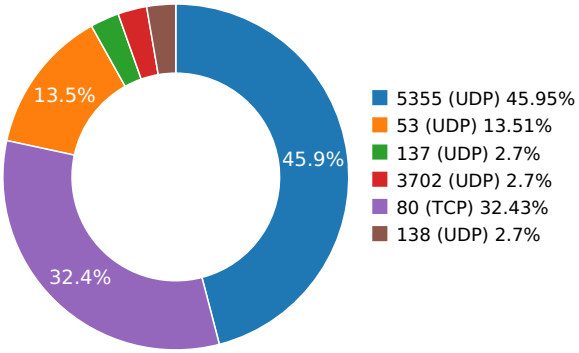
MODIFIED REGISTRY KEYS

HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\LanguageList
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\p2pcollab.dll,-8042
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\dnsapi.dll,-103

Network Behavior

CONTACTED IPS	NETWORK PORT DISTRIBUTION





Name	IP	Country	ASN	ASN Name	Trigger Process Type
	8.8.4.4	United States	15169	Level 3 Parent, LLC	Malware Process
	104.31.74.124	United States	13335	Cloudflare, Inc.	Malware Process
	184.24.97.174	United States	20940	Akamai Technologies, Inc.	OS Process
	23.215.130.42	United States	20940	Akamai Technologies, Inc.	OS Process
t2.symcb.com	23.50.75.27	United States	3257	Akamai Technologies, Inc.	Malware Process
tl.symcd.com	23.35.171.27	United States	20940	Akamai Technologies, Inc.	Malware Process
crl.microsoft.com	63.238.216.18	United States	209	Qwest Communications Com...	OS Process
crl.globalsign.net	104.31.75.124	United States	13335	Cloudflare, Inc.	Malware Process
ctldl.windowsupdate.com	63.238.216.26	United States	209	Qwest Communications Com...	OS Process

HTTP PACKETS

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
ctldl.windowsupdate.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	12.7507491112
Path: /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?5214f422c8e1da2d **URI:** http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?5214f422c8e1da2d						
t2.symcb.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	18.2434639931
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBQwF4prw9S7mCbCEHD%2Fyl6nWPkczAQUe1tFz6%2FOy3r9MZIaarbzRutXSFACEHGgtzaV3bGvwjsrmhjuVMs%3D **URI:** http://t2.symcb.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQwF4prw9S7mCbCEHD%2Fyl6nWPkczAQUe1tFz6%2FOy3r9MZIaarbzRutXSFACEHGgtzaV3bGvwjsrmhjuVMs%3D						
tl.symcd.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	23.519600153
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBSFBjxN%2BWY73bfUnSOp7HDKJ%2Fbx0wQUV4abVLi%2BpimK5PbC4hMYiYXN3LcCEE8%2F60uvN3rqkKRjxd7mOIQ%3D **URI:** http://tl.symcd.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSFBjxN%2BWY73bfUnSOp7HDKJ%2Fbx0wQUV4abVLi%2BpimK5PbC4hMYiYXN3LcCEE8%2F60uvN3rqkKRjxd7mOIQ%3D						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	61.4976251125
Path: /pki/crl/products/tspca.crl **URI:** http://crl.microsoft.com/pki/crl/products/tspca.crl						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	67.2554910183
Path: /pki/crl/products/CodeSignPCA2.crl **URI:** http://crl.microsoft.com/pki/crl/products/CodeSignPCA2.crl						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	72.847618103
Path: /pki/crl/products/WinPCA.crl **URI:** http://crl.microsoft.com/pki/crl/products/WinPCA.crl						
crl.globalsign.net	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	78.0243330002
Path: /primobject.crl **URI:** http://crl.globalsign.net/primobject.crl						

DNS QUERIES

Request	Type
ctldl.windowsupdate.com	A
Answers - ctldl.windowsupdate.nsatc.net (CNAME) - 184.24.97.176 (A) - a1621.g.akamai.net (CNAME) - ctldl.windowsupdate.com.edgesuite.net (CNAME) - 184.24.97.174 (A)	
t2.symcb.com	A
Answers - ocsp-ds.ws.symantec.com.edgekey.net (CNAME) - e8218.dscb1.akamaiedge.net (CNAME) - 23.35.171.27 (A)	
tl.symcd.com	A
Answers - 23.50.75.27 (A)	
crl.microsoft.com	A
Answers - crl.www.ms.akadns.net (CNAME) - 23.215.130.42 (A) - 23.215.130.58 (A) - a1363.dscg.akamai.net (CNAME)	
crl.globalsign.net	A
Answers - 104.31.75.124 (A) - global.prd.cdn.globalsign.com (CNAME) - cdn.globalsigncdn.com.cdn.cloudflare.net (CNAME) - 104.31.74.124 (A)	

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
12.7507491112	Sandbox	184.24.97.174	80
18.2434639931	Sandbox	23.35.171.27	80
23.519600153	Sandbox	23.50.75.27	80
61.4976251125	Sandbox	23.215.130.42	80
78.0243330002	Sandbox	104.31.74.124	80

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.3386721611	Sandbox	192.168.56.255	137
3.33959698677	Sandbox	224.0.0.252	5355
3.34154510498	Sandbox	224.0.0.252	5355
3.34655809402	Sandbox	239.255.255.250	3702
5.89478898048	Sandbox	224.0.0.252	5355
7.4422750473	Sandbox	224.0.0.252	5355
9.33127593994	Sandbox	192.168.56.255	138
10.0410900116	Sandbox	224.0.0.252	5355
12.6023080349	Sandbox	8.8.4.4	53
13.0361559391	Sandbox	224.0.0.252	5355
15.6108880043	Sandbox	224.0.0.252	5355
18.1611709595	Sandbox	8.8.4.4	53
18.3367249966	Sandbox	224.0.0.252	5355
20.9106171131	Sandbox	224.0.0.252	5355
23.4734661579	Sandbox	8.8.4.4	53
56.0682640076	Sandbox	224.0.0.252	5355
58.8197331429	Sandbox	224.0.0.252	5355
61.4429731369	Sandbox	8.8.4.4	53
61.7534580231	Sandbox	224.0.0.252	5355
64.67512393	Sandbox	224.0.0.252	5355
67.3679931164	Sandbox	224.0.0.252	5355
70.2844281197	Sandbox	224.0.0.252	5355
72.8707270622	Sandbox	224.0.0.252	5355
75.4373869896	Sandbox	224.0.0.252	5355
77.9888279438	Sandbox	8.8.4.4	53

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\378B079587A9184B2E2AB859CB263F40_524AD1B9B08D3C6450727265AE77B7D2	**Type :** data **MD5 :** bb2658875e9b6b8e4c2322938ccd08ea **SHA-1 :** 166e3027bf70687070df7a6069fb402e955482e9 **SHA-256 :** 0ed42266c312031700a04bb0827d17162ed5a96 **SHA-512 :** 5b6c0500f182f82902616d4a8dc78c8ba19e94d8 **Size :** 1.561 Kilobytes.
C:\Windows\Microsoft.NET\Framework\V2.0.50727\CONFIG\Security.Config.Cch **C:\Users\User\AppData\Roaming\Microsoft\CLR Security Config\V2.0.50727.312\Security.Config.Cch** **C:\Windows\Microsoft.NET\Framework\V2.0.50727\CONFIG\Enterprisesec.Config.Cch**	**Type :** data **MD5 :** d9f8e8f4945d2e545fbedec724bd5539 **SHA-1 :** 78b05853e9ef5c61b39520304cef1d485569e88b **SHA-256 :** 6998a98c2fcb5377e76b1474de77a8f89b6c6a1c **SHA-512 :** 9462f7498064b4e70edc87ffcfee8b9f39a4e9fefb **Size :** 1.634 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157	**Type :** Microsoft Cabinet archive data, 6509 bytes, 1 file **MD5 :** 33b39e2a516ef730a8fa922894f0fbd5 **SHA-1 :** 03d455583dda59215d945af76af6293b202f586f **SHA-256 :** 9446e8f2056fea3ac1365a809ada04602606242c **SHA-512 :** 75763aa13b43eb96294b0f84e13106611198872 **Size :** 6.509 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Diagnoseapp.Exe	**Type :** PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** a28bf0b304449200b2b461f201a89b59 **SHA-1 :** 2e2889879b93f72664c66329ea4162de53774477 **SHA-256 :** 17afcbb091442bb609220b6470baa5fe772f4fd4 **SHA-512 :** fcc8ef7ac23bf072642937f0f512a7793bd7c55f93 **Size :** 1899.768 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\8EB35376744F392396307460D546222D_DA4083211FC1CAD4C1215FF8726EF9C8	**Type :** data **MD5 :** 164b6fc9ccb102b3542fab71d042adc9 **SHA-1 :** c4022f6c4831202ee7b6a4027d18919dde45727c **SHA-256 :** 6851e17e3f7f57f0eaf1bcc270a780c0d4f68546c8 **SHA-512 :** 315bf334e91cd4d5467e826211030134d213cb9a **Size :** 1.436 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\8EB35376744F392396307460D546222D_DA4083211FC1CAD4C1215FF8726EF9C8	**Type :** data **MD5 :** 9e0fcc637569e2fda4659be800221492 **SHA-1 :** b28419f68606b7b01be7d1f94e9ed6576728a637 **SHA-256 :** deb95cd3c651ab50d3d93e291d615f218a7fc54b **SHA-512 :** 929e5b74be46b4aa39601799254995dcc40a005 **Size :** 0.402 Kilobytes.
C:\Users\User\AppData\Local\GDIPFONTCACHEV1.DAT	**Type :** data **MD5 :** 696bad2ef23da7f0ccaaa7f76ab9fdf0 **SHA-1 :** 0efe907b47e8331cf56a95c0c06d324257ece202 **SHA-256 :** bd27979561fac15e4043fc980ad62f24f00738cba **SHA-512 :** fb1a4afdbf5f9e3d7e55eb806f660057927d6c357 **Size :** 84.528 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157	**Type :** data **MD5 :** 9f848f9104e30e1910a75c38c7507034 **SHA-1 :** 36c3698bcae96df830d417255a6934a1039a8704 **SHA-256 :** 13bffebca39ecc6008ad90305238caa6115807bd **SHA-512 :** fe8116525fbc10dd0bbadf4b08ae29d0bd5cd685 **Size :** 0.342 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\378B079587A9184B2E2AB859CB263F40_524AD1B9B08D3C6450727265AE77B7D2	**Type :** data **MD5 :** c57a1425741e8d4d6fa4a0a40c1404f9 **SHA-1 :** d1f5536b7440170a4b3d47dd8e9e31957d84b9d0 **SHA-256 :** f04bca59e9e6ce09d8db96c55e9040b7cd731fd9 **SHA-512 :** e50e79fbccdad3eb2b59b20f4f45167a4a1d90c2 **Size :** 0.394 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	ojoh.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
SHA1:	2e2889879b93f72664c66329ea4162de53774477
MD5:	a28bf0b304449200b2b461f201a89b59
First Seen Date:	2018-05-18 21:36:27.774906 (7 months ago)
Number Of Clients Seen:	1
Last Analysis Date:	2018-05-18 21:36:27.774906 (7 months ago)
Human Expert Analysis Result:	No human expert analysis verdict given to this sample yet.

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	[[61.6, u'Win64 Executable (generic)'], [14.6, u'Win32 Dynamic Link Library (generic)'], [10.0, u'Win32 Executable (generic)'], [4.6, u'Win16/32 Executable Delphi generic'], [4.4, u'Generic Win/DOS Executable']]
Compilation Time Stamp	0x598A211C [Tue Aug 8 20:37:48 2017 UTC]
LegalCopyright	\xa9 2015 Advanced Micro Devices, Inc.
InternalName	CLIStart
FileVersion	3.5.0.0
CompanyName	Advanced Micro Devices, Inc.
ProductName	Catalyst\xae Control Center
ProductVersion	3.5.0.0
FileDescription	Catalyst\xae Control Center Launcher
OriginalFilename	CLIStart.exe
Translation	0x0409 0x04b0
Entry Point	0x5d400a ()
Machine Type	Intel 386 or later - 32Bit
File Size	1899768
Ssdeep	49152:LjSQNZIqYM2edF0AoAuKs7LpV6RDZWqTgQ:XSuYMvBsXuFZWqcQ
Sha256	17afcbb091442bb609220b6470baa5fe772f4fd4164692f446743bf58c5d024f
Exifinfo	[{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/2/e/2/8/2e2889879b93f72664c66329ea4162de53774477', u'EXE:OriginalFileName': u'CLIStart.exe', u'EXE:ProductName': u'Catalyst\xae Control Center', u'EXE:InternalName': u'CLIStart', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2018:05:18 21:36:01+00:00', u'EXE:InitializedDataSize': 857600, u'File:FileModifyDate': u'2018:05:18 21:36:01+00:00', u'EXE:FileVersionNumber': u'3.5.0.0', u'EXE:FileVersion': u'3.5.0.0', u'File:FileSize': u'1855 kB', u'EXE:CharacterSet': u'Unicode', u'EXE:MachineType': u'Intel 386 or later, and compatibles', u'EXE:FileOS': u'Win32', u'EXE:ProductVersion': u'3.5.0.0', u'EXE:ObjectFileType': u'Executable application', u'File:FileType': u'Win32 EXE', u'EXE:CompanyName': u'Advanced Micro Devices, Inc.', u'File:FileName': u'2e2889879b93f72664c66329ea4162de53774477', u'EXE:ImageVersion': 0.0, u'File:FileTypeExtension': u'exe', u'EXE:OSVersion': 4.0, u'EXE:PEType': u'PE32', u'EXE:TimeStamp': u'2017:08:08 20:37:48+00:00', u'EXE:FileFlagsMask': u'0x0017', u'EXE:LegalCopyright': u'\xa9 2015 Advanced Micro Devices, Inc.', u'EXE:LinkerVersion': 8.0, u'EXE:FileFlags': u'(none)', u'EXE:Subsystem': u'Windows GUI', u'File:Directory': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/2/e/2/8', u'EXE:FileDescription': u'Catalyst\xae Control Center Launcher', u'EXE:EntryPoint': u'0x1d400a', u'EXE:SubsystemVersion': 4.0, u'EXE:CodeSize': 1033216, u'File:FileInodeChangeDate': u'2018:05:18 21:36:01+00:00', u'EXE:UninitializedDataSize': 0, u'EXE:LanguageCode': u'English (U.S.)', u'ExifTool:ExifToolVersion': 10.1, u'EXE:ProductVersionNumber': u'3.5.0.0'}]
Mime Type	application/x-dosexec
Imphash	f34d5f2d4577ed6d9ceec516c1f5a744

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
{M%`H	0x2000	0x61428	0x61600	7.99958608113	276854111692cdf0ae9985676c60ac06
.text	0x64000	0xfc138	0xfc200	7.96472139295	c006565bab0856e546f093148418d0e0
.rsrc	0x162000	0x6fcf0	0x6fe00	3.18146907244	d2489abb1d8e75ec0d1a7c865ec07386
.reloc	0x1d2000	0xc	0x200	0.0980041756627	920cc09fa5e65f8da072f87a9506fe46
	0x1d4000	0x10	0x200	0.142635768149	21c207900d82717c19fa277a030a46f8

PE Imports

- mscoree.dll
  - _CorExeMain

PE Resources

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1451708, u'sha256': u'da09ab1c12acdd9815b8df420226aeddf849a99c766e56ce9600ad54c683a160', u'type': u'dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 2576943512, next used block 37017', u'size': 744}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1452452, u'sha256': u'e4fd8a33f78b10d286d182af6fb53f26ce8c0e6c38d042028be9c5314276f9b0', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 296}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1452748, u'sha256': u'936cfce16f6e348ebc4cdaadd5e777a76a5c3c9e5657b0b706130cdda3bf0571', u'type': u'dBase IV DBT of \\300.DBF, block length 9216, next free block index 40, next free block 0, next used block 0', u'size': 11432}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1464180, u'sha256': u'0b53e2d503246cd1b35060e713dde05b6a4c05a6f59cc42a7438646cb89bd4bc', u'type': u'data', u'size': 7112}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1471292, u'sha256': u'4f030f86682277d4640319914ae29aee8c88f4879fff8728f206e6708fa13434', u'type': u'dBase IV DBT of \\200.DBF, blocks size 0, block length 4096, next free block index 40, next free block 0, next used block 0', u'size': 5672}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1476964, u'sha256': u'14588ffd5d43262de28c2f5d0e5aad120ea31578d26f343ae7eaf78b7f825429', u'type': u'data', u'size': 5144}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1482108, u'sha256': u'f40173f67aab148122000c3ca24bc3c5a69b935c7227389e7bf55cac8774eee3', u'type': u'data', u'size': 3752}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1485860, u'sha256': u'832a12a561d2d47475752421eb41cb6be1ffad704d69b3d9e6760d5ca2b4d0a4', u'type': u'data', u'size': 2984}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1488844, u'sha256': u'3f842cb2845452e3fea47d2b9559ff28fc1d2d4a053939d73e2611e1a4f9ea82', u'type': u'dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 0, next used block 0', u'size': 2216}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1491060, u'sha256': u'0db02f39f322156b560c00176ff77afbf8efbee285392da33121a979e8b57fd4', u'type': u'data', u'size': 1736}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1492796, u'sha256': u'528de6a15c69c67f8444085d8a916916101ae00ce0c75b510428657441e04ec8', u'type': u'data', u'size': 1544}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1494340, u'sha256': u'5e00a8d4451ba0ce891150037247511b7d180fbb2f5c4a8f154fc84bec34ae7e', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1384}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1495724, u'sha256': u'94b5ef5008a5174ece882793d8b6855059b73eac6640dcde4634c49c567fadaf', u'type': u'PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced', u'size': 2158}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1497884, u'sha256': u'a170a0a2570a43ecda78164a3f32999d254e3454e0093b60be8c783eebe576c3', u'type': u'data', u'size': 38056}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1535940, u'sha256': u'4cfd23338afbf0315ae3214dbb6c464033f015bc6835467ce605156ed72a8172', u'type': u'data', u'size': 21640}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1557580, u'sha256': u'aa822264d0766af83d391dd0f2b5ebfcb2ea23c44ba478909b49b0cb32fb4377', u'type': u'dBase IV DBT of \\200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 4294967295, next used block 4294903552', u'size': 16936}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1574516, u'sha256': u'01fe12b04e641e5aba54ffe47266264d3f951e943ac33a7f858591c18df63014', u'type': u'data', u'size': 14920}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1589436, u'sha256': u'e4cab87847b0c11cf9b3ef4d5ae8d768df9dc9d8d56c87131291385f6ccd4bd9', u'type': u'data', u'size': 9640}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1599076, u'sha256': u'58760b72dc9cdbc910fb0199c72d9c2b39673a9112a2defcbd28c5bbf781276d', u'type': u'data', u'size': 6760}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1605836, u'sha256': u'38bc585f424d4e4838534b67a30b2786d338424002e261a906c94a0ce0f6cd01', u'type': u'data', u'size': 4264}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1610100, u'sha256': u'33f9dcbb9a8d3276d58f83f5fd1a16d148210a7aa26906213746dba8772dcab2', u'type': u'data', u'size': 2440}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1612540, u'sha256': u'0a8286c47d2fe26cc8c7df13357818d13ccfbc9b38bd57f72ea74629fa059e02', u'type': u'data', u'size': 1720}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1614260, u'sha256':

u'64388b9d1cabb50c529103662cac51ac8ca87d5bf1db3106fee985142d221971', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1128}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1615388, u'sha256': u'16798a6c46332c96fccd3132b16be48b45a1be56166289f4abda7c75033a0242', u'type': u'dBase IV DBT, blocks size 0, block length 8192, next free block index 40, next free block 0, next used block 0', u'size': 270376}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1885764, u'sha256': u'9506e74027e78e2244a1c8fd423d41a171ad7ed57929bb8145d02d17db67115c', u'type': u'data', u'size': 9640}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1895404, u'sha256': u'03aa931e854bdc541a1b00fc09149d387c03b618acb74ea6611baf2034613760', u'type': u'data', u'size': 5512}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1900916, u'sha256': u'a390240b93e67c5fc8bc3768db1bd209997103d18bd594d126577352985201b6', u'type': u'data', u'size': 2440}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1903356, u'sha256': u'f7f0be0bade32dc78776c64d6a60da38efc722b8ddc87abb5a26626b4d43d2b8', u'type': u'data', u'size': 1720}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1905076, u'sha256': u'3a4437b4be4e1637fde5b6dcae1cb8ebb9f3061790df3d09d590ba08b6fc1f75', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1128}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_ICON', u'offset': 1906204, u'sha256': u'd2d1f2681387c72916e509fc1a52624ef576ef038a10a267c196a077040cb648', u'type': u'MS Windows icon resource - 6 icons, 256x256', u'size': 90}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_ICON', u'offset': 1906296, u'sha256': u'7e2b9be377f905a64ddf56f472ab582265f17fd36ca9bfd28cb99adc90a621c5', u'type': u'MS Windows icon resource - 23 icons, 32x32, 16 colors', u'size': 328}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_VERSION', u'offset': 1906624, u'sha256': u'b5a54b120d83d47144b44c9ac23f56e8ea3ee14524022e9fafa15172711159c3', u'type': u'data', u'size': 832}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_MANIFEST', u'offset': 1907456, 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

- Success ✔

[+] F3D LIMITED	
Status	NoError ✔
Start Date	2017-09-12 03:00:00
End Date	2018-09-13 02:59:59
Sha256	c47d0aff71985019286c4059b2c789d27b2d4636df97c482d71149a8a1d96efc
Serial	4F3FEB4BAF377AEA90A463C5DEE63884
Subject Key Identifier	52 d9 05 e0 0e 92 09 f9 65 22 5f a4 88 f5 6d 1f c7 d8 90 59
Issuer Name	thawte SHA256 Code Signing CA
Issuer Key Identifier	57 86 9b 54 b8 be a6 29 8a e4 f6 c2 e2 13 18 89 85 cd dc b7
Crl link	http://tl.symcb.com/tl.crl
Key Usage	Digital Signature (80)
Extended Usage	Code Signing (1.3.6.1.5.5.7.3.3)

[+] thawte SHA256 Code Signing CA	
Status	NoError ✔
Start Date	2013-12-10 02:00:00
End Date	2023-12-10 01:59:59
Sha256	d542ad03871f39ed7a47a057892a67f6d76b973134a8a129d2ba1ace821de2e4
Serial	71A0B73695DDB1AFC23B2B9A18EE54CB
Subject Key Identifier	57 86 9b 54 b8 be a6 29 8a e4 f6 c2 e2 13 18 89 85 cd dc b7
Issuer Name	thawte Primary Root CA
Issuer Key Identifier	7b 5b 45 cf af ce cb 7a fd 31 92 1a 6a b6 f3 46 eb 57 48 50
Crl link	http://t1.symcb.com/ThawtePCA.crl
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	Client Authentication (1.3.6.1.5.5.7.3.2)

[+] thawte Primary Root CA	
Status	NoError ✔
Start Date	2006-11-17 02:00:00
End Date	2036-07-17 02:59:59
Sha256	d6a37f73bd37d7adacb96997064639215d4806b63a4ccee5416e3da8d68a3b1f
Serial	344ED55720D5EDEC49F42FCE37DB2B6D
Subject Key Identifier	7b 5b 45 cf af ce cb 7a fd 31 92 1a 6a b6 f3 46 eb 57 48 50
Issuer Name	thawte Primary Root CA
Issuer Key Identifier	undefined
Crl link	undefined
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	undefined

[+] thawte Primary Root CA	
Status	NoError ✔
Start Date	2006-11-17 02:00:00
End Date	2036-07-17 02:59:59
Sha256	d6a37f73bd37d7adacb96997064639215d4806b63a4ccee5416e3da8d68a3b1f
Serial	344ED55720D5EDEC49F42FCE37DB2B6D
Subject Key Identifier	7b 5b 45 cf af ce cb 7a fd 31 92 1a 6a b6 f3 46 eb 57 48 50
Issuer Name	thawte Primary Root CA
Issuer Key Identifier	undefined
Crl link	undefined
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	undefined

SCREENSHOTS