VALKYRIE COMODO

Summary

File Name: a9J3j.exe

File Type: PE32 executable (GUI) Intel 80386, for MS Windows

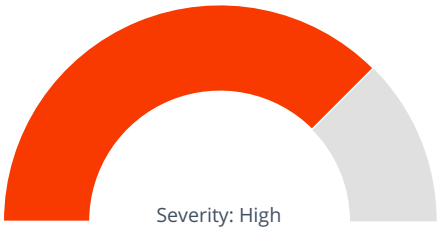
SHA1: 3451a3b7b9125b705aaecb9fc8aa4d80e77c860f

MD5: df515c7944862ef4982cacfc151085f5

MALWARE

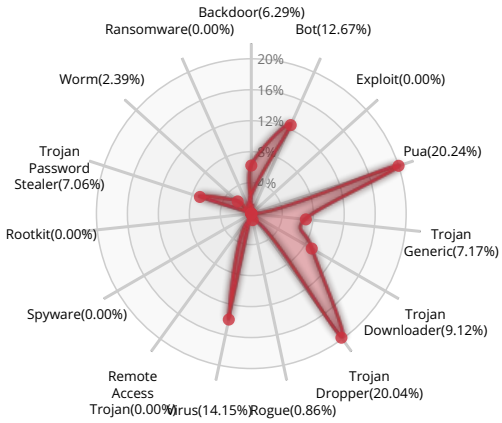
Valkyrie Final Verdict

DETECTION SECTION

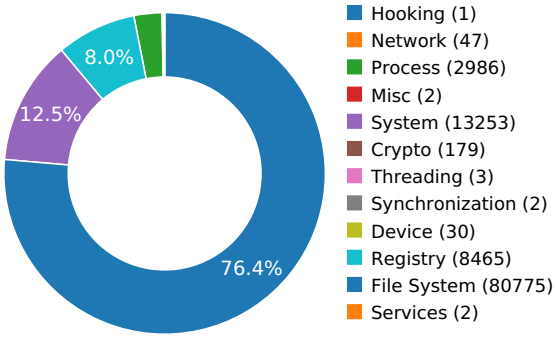


Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

VALKYRIE COMODO

Activity Details

PACKER

The binary likely contains encrypted or compressed data. Show sources

NETWORKING

Attempts to connect to a dead IP:Port (1 unique times) Show sources

MALWARE ANALYSIS SYSTEM EVASION

A process attempted to delay the analysis task. Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

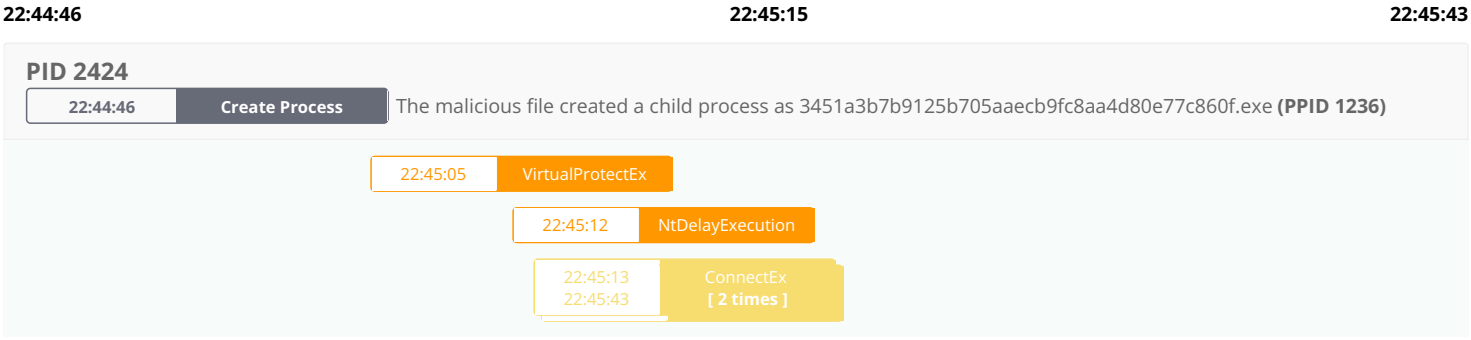
Creates RWX memory Show sources

CRYPTOGRAPHY

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

VALKYRIE COMODO

Behavior Graph



VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Windows\nebifozajuxe
C:\Users\user\AppData\Local\Temp\luvifodipatomaxiyizekejore fisocudejotefofo fenohoseva pisi.DLL
C:\Windows\System32\luvifodipatomaxiyizekejore fisocudejotefofo fenohoseva pisi.DLL
C:\Windows\system\luvifodipatomaxiyizekejore fisocudejotefofo fenohoseva pisi.DLL
C:\Windows\luvifodipatomaxiyizekejore fisocudejotefofo fenohoseva pisi.DLL
C:\ProgramData\Oracle\Java\javapath\luvifodipatomaxiyizekejore fisocudejotefofo fenohoseva pisi.DLL
C:\Windows\System32\wbem\luvifodipatomaxiyizekejore fisocudejotefofo fenohoseva pisi.DLL
C:\Windows\System32\WindowsPowerShell\v1.0\luvifodipatomaxiyizekejore fisocudejotefofo fenohoseva pisi.DLL
C:\Program Files\Microsoft Network Monitor 3\luvifodipatomaxiyizekejore fisocudejotefofo fenohoseva pisi.DLL
C:\Program Files (x86)\Universal Extractor\luvifodipatomaxiyizekejore fisocudejotefofo fenohoseva pisi.DLL
C:\Program Files (x86)\Universal Extractor\bin\luvifodipatomaxiyizekejore fisocudejotefofo fenohoseva pisi.DLL
C:\Program Files (x86)\Windows Kits\8.1\Windows Performance Toolkit\luvifodipatomaxiyizekejore fisocudejotefofo fenohoseva pisi.DLL
C:\Python27\luvifodipatomaxiyizekejore fisocudejotefofo fenohoseva pisi.DLL
C:\Python27\Scripts\luvifodipatomaxiyizekejore fisocudejotefofo fenohoseva pisi.DLL
C:\tools\sysinternals\luvifodipatomaxiyizekejore fisocudejotefofo fenohoseva pisi.DLL
C:\tools\luvifodipatomaxiyizekejore fisocudejotefofo fenohoseva pisi.DLL
C:\tools\IDA_Pro_v6\python\luvifodipatomaxiyizekejore fisocudejotefofo fenohoseva pisi.DLL
C:\Windows\Fonts\xehopalomasusujamamomunaxifiga maramubuhebu fuhakerupe garopekakeposuwufinamorawopo nafefoze\xevamibavazavomibi jekobifadoyi cobosekukoxehituxecugiciwewome
C:\Users\user\AppData\Local\Temp\xehopalomasusujamamomunaxifiga maramubuhebu fuhakerupe garopekakeposuwufinamorawopo nafefoze\xevamibavazavomibi jekobifadoyi cobosekukoxehituxecugiciwewome
C:\Windows\System32\xehopalomasusujamamomunaxifiga maramubuhebu fuhakerupe garopekakeposuwufinamorawopo nafefoze\xevamibavazavomibi jekobifadoyi cobosekukoxehituxecugiciwewome
C:\Windows\system\xehopalomasusujamamomunaxifiga maramubuhebu fuhakerupe garopekakeposuwufinamorawopo nafefoze\xevamibavazavomibi jekobifadoyi cobosekukoxehituxecugiciwewome
C:\Windows\xehopalomasusujamamomunaxifiga maramubuhebu fuhakerupe garopekakeposuwufinamorawopo nafefoze\xevamibavazavomibi jekobifadoyi cobosekukoxehituxecugiciwewome
C:\ProgramData\Oracle\Java\javapath\xehopalomasusujamamomunaxifiga maramubuhebu fuhakerupe garopekakeposuwufinamorawopo nafefoze\xevamibavazavomibi jekobifadoyi cobosekukoxehituxecugiciwewome
C:\Windows\System32\wbem\xehopalomasusujamamomunaxifiga maramubuhebu fuhakerupe garopekakeposuwufinamorawopo nafefoze\xevamibavazavomibi jekobifadoyi cobosekukoxehituxecugiciwewome
C:\Windows\System32\WindowsPowerShell\v1.0\xehopalomasusujamamomunaxifiga maramubuhebu fuhakerupe garopekakeposuwufinamorawopo nafefoze\xevamibavazavomibi jekobifadoyi cobosekukoxehituxecugiciwewome
C:\Program Files\Microsoft Network Monitor 3\xehopalomasusujamamomunaxifiga maramubuhebu fuhakerupe garopekakeposuwufinamorawopo nafefoze\xevamibavazavomibi jekobifadoyi cobosekukoxehituxecugiciwewome
C:\Program Files (x86)\Universal Extractor\xehopalomasusujamamomunaxifiga maramubuhebu fuhakerupe garopekakeposuwufinamorawopo nafefoze\xevamibavazavomibi jekobifadoyi cobosekukoxehituxecugiciwewome
C:\Program Files (x86)\Universal Extractor\bin\xehopalomasusujamamomunaxifiga maramubuhebu fuhakerupe garopekakeposuwufinamorawopo

nafefoze\xevamibavazavomibi jekobifadoyi cobosekukoxehituxecugiciwewome
C:\Program Files (x86)\Windows Kits\8.1\Windows Performance Toolkit\xehopalomasusujamamomunaxifiga maramubuhebu fuhakerupe garopekakeposuwufinamorawopo nafefoze\xevamibavazavomibi jekobifadoyi cobosekukoxehituxecugiciwewome
C:\Python27\xehopalomasusujamamomunaxifiga maramubuhebu fuhakerupe garopekakeposuwufinamorawopo nafefoze\xevamibavazavomibi jekobifadoyi cobosekukoxehituxecugiciwewome
C:\Python27\Scripts\xehopalomasusujamamomunaxifiga maramubuhebu fuhakerupe garopekakeposuwufinamorawopo nafefoze\xevamibavazavomibi jekobifadoyi cobosekukoxehituxecugiciwewome
C:\tools\sysinternals\xehopalomasusujamamomunaxifiga maramubuhebu fuhakerupe garopekakeposuwufinamorawopo nafefoze\xevamibavazavomibi jekobifadoyi cobosekukoxehituxecugiciwewome
C:\tools\xehopalomasusujamamomunaxifiga maramubuhebu fuhakerupe garopekakeposuwufinamorawopo nafefoze\xevamibavazavomibi jekobifadoyi cobosekukoxehituxecugiciwewome
C:\tools\IDA_Pro_v6\python\xehopalomasusujamamomunaxifiga maramubuhebu fuhakerupe garopekakeposuwufinamorawopo nafefoze\xevamibavazavomibi jekobifadoyi cobosekukoxehituxecugiciwewome
C:\Users\user\AppData\Local\Temp\msvcr100.dll
C:\Windows\System32\msvcr100.dll
C:\Windows\system\msvcr100.dll
C:\Windows\msvcr100.dll
C:\ProgramData\Oracle\Java\javapath\msvcr100.dll
C:\Windows\System32\wbem\msvcr100.dll
C:\Windows\System32\WindowsPowerShell\v1.0\msvcr100.dll
C:\Program Files\Microsoft Network Monitor 3\msvcr100.dll
C:\Program Files (x86)\Universal Extractor\msvcr100.dll
C:\Program Files (x86)\Universal Extractor\bin\msvcr100.dll
C:\Program Files (x86)\Windows Kits\8.1\Windows Performance Toolkit\msvcr100.dll
C:\Python27\msvcr100.dll
C:\Python27\Scripts\msvcr100.dll
C:\tools\sysinternals\msvcr100.dll
C:\tools\msvcr100.dll
C:\tools\IDA_Pro_v6\python\msvcr100.dll
C:\Users\user\AppData\Local*
C:
C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Local
C:\Users\user\AppData\Local\2259afc4852c5c7311722091fb1069f452d5de8d
C:\
C:\Users\user\AppData\Local\2259afc4852c5c7311722091fb1069f452d5de8d\container.dat

C:\Users\user\AppData\Local\2259afc4852c5c7311722091fb1069f452d5de8d\container.dat.tmp
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

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\0
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SESSION MANAGER\SafeProcessSearchMode
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SecurityProviders\SCHANNEL\UserContextLockCount
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SecurityProviders\SCHANNEL\UserContextListCount
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\SYSTEM\ControlSet001\services\crypt32\DiagLevel
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\crypt32\DiagMatchAnyMask
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
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\WeakRsaPubKeyTime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\ChainCacheResyncFiletime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\WeakMD5ThirdPartyFlags
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\WeakMD5AllFlags
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\WeakSHA1ThirdPartyFlags
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\WeakSHA1AllFlags
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\WeakRSAThirdPartyFlags
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\WeakRSAAllFlags
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\WeakDSAThirdPartyFlags
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\WeakDSAAllFlags
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\WeakECDSAThirdPartyFlags
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\WeakECDSAAllFlags
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2298303332-66077612-2598613238-1000\ProfileImagePath
HKEY_CURRENT_USER\Software\Microsoft\SystemCertificates\CA\Certificates\9317D002FC43BDA932B8397B6E729B83D48EEB8D\Blob
HKEY_CURRENT_USER\Software\Microsoft\SystemCertificates\CA\Certificates\E6A3B45B062D509B3382282D196EFE97D5956CCB\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\CA\Certificates\109F1CAED645BB78B3EA2B94C0697C740733031C\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\CA\Certificates\D559A586669B08F46A30A133F8A9ED3D038E2EA8\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\CA\Certificates\FEE449EE0E3965A5246F000E87FDE2A065FD89D4\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\CA\CRLs\A377D1B1C0538833035211F4083D00FECC414DAB\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\Disallowed\Certificates\1916A2AF346D399F50313C393200F14140456616\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\Disallowed\Certificates\2A83E9020591A55FC6DDAD3FB102794C52B24E70\Blob

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\Disallowed\Certificates\2B84BFBB34EE2EF949FE1CBE30AA026416EB2216\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\Disallowed\Certificates\305F8BD17AA2CBC483A4C41B19A39A0C75DA39D6\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\Disallowed\Certificates\367D4B3B4FCBBC0B767B2EC0CDB2A36EAB71A4EB\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\Disallowed\Certificates\3A850044D8A195CD401A680C012CB0A3B5F8DC08\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\Disallowed\Certificates\40AA38731BD189F9CDB5B9DC35E2136F38777AF4\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\Disallowed\Certificates\43D9BCB568E039D073A74A71D8511F7476089CC3\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\Disallowed\Certificates\471C949A8143DB5AD5CDF1C972864A2504FA23C9\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\Disallowed\Certificates\51C3247D60F356C7CA3BAF4C3F429DAC93EE7B74\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\Disallowed\Certificates\5DE83EE82AC5090AEA9D6AC4E7A6E213F946E179\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\Disallowed\Certificates\61793FCBFA4F9008309BBA5FF12D2CB29CD4151A\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\Disallowed\Certificates\637162CC59A3A1E25956FA5FA8F60D2E1C52EAC6\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\Disallowed\Certificates\63FEAE960BAA91E343CE2BD8B71798C76BDB77D0\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\Disallowed\Certificates\6431723036FD26DEA502792FA595922493030F97\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\Disallowed\Certificates\7D7F4414CCEF168ADF6BF40753B5BECD78375931\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\Disallowed\Certificates\80962AE4D6C5B442894E95A13E4A699E07D694CF\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\Disallowed\Certificates\86E817C81A5CA672FE000F36F878C19518D6F844\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\Disallowed\Certificates\8E5BD50D6AE686D65252F843A9D4B96D197730AB\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\Disallowed\Certificates\9845A431D51959CAF225322B4A4FE9F223CE6D15\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\Disallowed\Certificates\B533345D06F64516403C00DA03187D3BFEF59156\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\Disallowed\Certificates\B86E791620F759F17B8D25E38CA8BE32E7D5EAC2\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\Disallowed\Certificates\C060ED44CBD881BD0EF86C0BA287DDCF8167478C\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\Disallowed\Certificates\CEA586B2CE593EC7D939898337C57814708AB2BE\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\Disallowed\Certificates\D018B62DC518907247DF50925BB09ACF4A5CB3AD\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\Disallowed\Certificates\F8A54E03AADC5692B850496A4C4630FFEAA29D83\Blob
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\Disallowed\Certificates\FA6660A94AB45F6A88C0D7874D89A863D74DEE97\Blob
HKEY_CURRENT_USER\Software\Microsoft\SystemCertificates\Root\Certificates\9317D002FC43BDA932B8397B6E729B83D48EEB8D\Blob
HKEY_CURRENT_USER\Software\Microsoft\SystemCertificates\Root\Certificates\95EEF9A37407C5B87BCF95D69B01DCFDAFD07635\Blob

MODIFIED FILES

C:\Users\user\AppData\Local\2259afc4852c5c7311722091fb1069f452d5de8d\container.dat.tmp
C:\Users\user\AppData\Local\2259afc4852c5c7311722091fb1069f452d5de8d\container.dat

RESOLVED APIS

kernel32.dll.FlsAlloc
kernel32.dll.FlsGetValue
kernel32.dll.FlsSetValue

kernel32.dll.FlsFree
kernel32.dll.GlobalAlloc
uxtheme.dll.ThemeInitApiHook
user32.dll.IsProcessDPIAware
kernel32.dll.LoadLibraryA
kernel32.dll.VirtualAlloc
kernel32.dll.VirtualProtect
kernel32.dll.VirtualFree
kernel32.dll.GetVersionExA
kernel32.dll.TerminateProcess
kernel32.dll.SetEnvironmentVariableA
kernel32.dll.FlushInstructionCache
kernel32.dll.Sleep
kernel32.dll.ExitProcess
kernel32.dll.ReadProcessMemory
kernel32.dll.GetSystemInfo
kernel32.dll.GetCurrentProcess
kernel32.dll.GetProcAddress
kernel32.dll.GetModuleHandleA
kernel32.dll.UnhandledExceptionFilter
kernel32.dll.RtlUnwind
kernel32.dll.SetUnhandledExceptionFilter
advapi32.dll.CryptHashData
advapi32.dll.CryptCreateHash
advapi32.dll.CryptReleaseContext
advapi32.dll.CryptDestroyHash
advapi32.dll.CryptAcquireContextW
advapi32.dll.CryptGetHashParam
msvcrt.dll.strlen
msvcrt.dll.memcmp
msvcrt.dll.memcpy
msvcrt.dll.memmove
msvcrt.dll.puts
msvcrt.dll.abort

msvcrt.dll.memset
msvcrt.dll.free
msvcrt.dll.malloc
msvcrt.dll.???3@YAXPAX@Z
msvcrt.dll.???2@YAPAXI@Z
ntdll.dll.NtQueryVirtualMemory
cryptsp.dll.CryptAcquireContextW
cryptsp.dll.CryptCreateHash
cryptsp.dll.CryptHashData
cryptsp.dll.CryptGetHashParam
cryptsp.dll.CryptDestroyHash
cryptsp.dll.CryptReleaseContext
kernel32.dll.CreateFileW
kernel32.dll.SetFilePointer
kernel32.dll.WriteFile
kernel32.dll.GetFileAttributesW
kernel32.dll.DeleteFileW
kernel32.dll.GetEnvironmentVariableA
kernel32.dll.VirtualQuery
kernel32.dll.FlushFileBuffers
kernel32.dll.CopyFileW
kernel32.dll.GetShortPathNameW
kernel32.dll.GetCommandLineW
kernel32.dll.OpenEventW
kernel32.dll.SetErrorMode
kernel32.dll.GetModuleFileNameW
kernel32.dll.CreateProcessW
kernel32.dll.RemoveDirectoryW
kernel32.dll.OpenMutexA
kernel32.dll.GetComputerNameW
kernel32.dll.GetSystemDirectoryW
kernel32.dll.ResumeThread
kernel32.dll.CreateEventA
kernel32.dll.GetEnvironmentVariableW
kernel32.dll.CreateMutexA

kernel32.dll.FindFirstFileW
kernel32.dll.FindNextFileW
kernel32.dll.FindClose
kernel32.dll.OpenProcess

REGISTRY KEYS

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Codepage
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\0
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\SYSTEM\ControlSet001\Control\SESSION MANAGER\SafeProcessSearchMode
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\Schannel
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SecurityProviders\SCHANNEL\UserContextLockCount
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SecurityProviders\SCHANNEL\UserContextListCount
HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\OID
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptDllFindOIDInfo
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptDllFindOIDInfo\1.3.6.1.4.1.311.44.3.4!7
HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\OID\EncodingType 0\CryptDllFindOIDInfo\1.3.6.1.4.1.311.44.3.4!7
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\CurrentControlSet\Control\MUI\StringCacheSettings
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\MUI\StringCacheSettings\StringCacheGeneration
HKEY_CURRENT_USER
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6d\52C64B7E
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_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptDllFindOIDInfo\1.3.6.1.4.1.311.47.1.1!7
HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\OID\EncodingType 0\CryptDllFindOIDInfo\1.3.6.1.4.1.311.47.1.1!7
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
HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\OID\EncodingType 0\CryptDllFindOIDInfo\1.3.6.1.4.1.311.64.1.1!7
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\Cryptography\OID\EncodingType 0\CryptDllFindOIDInfo\1.3.6.1.4.1.311.76.6.1!7
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\Services\crypt32
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\crypt32\DiagLevel
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\crypt32\DiagMatchAnyMask
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\SystemCertificates\Root\ProtectedRoots
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\SystemCertificates\AuthRoot
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\SystemCertificates\AuthRoot\DisableRootAutoUpdate
HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config
HKEY_LOCAL_MACHINE\Software\Microsoft\SystemCertificates\AuthRoot\AutoUpdate
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\AutoUpdate\DisallowedCertSyncDeltaTime
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\SystemCertificates\ChainEngine\Config
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
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\WeakRsaPubKeyTime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\ChainCacheResyncFiletime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\Default
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\WeakMD5ThirdPartyFlags
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\WeakMD5AllFlags
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\WeakSHA1ThirdPartyFlags
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\WeakSHA1AllFlags
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\WeakRSAThirdPartyFlags
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\WeakRSAAllFlags

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\WeakDSAThirdPartyFlags
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\WeakDSAAllFlags
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\WeakECDSAThirdPartyFlags
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config\WeakECDSAAllFlags
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CertDllOpenStoreProv
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CertDllOpenStoreProv\#16
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0\CertDllOpenStoreProv\Ldap
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 1
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 1\CertDllOpenStoreProv
HKEY_USERS\S-1-5-21-2298303332-66077612-2598613238-1000
HKEY_CURRENT_USER\Software\Microsoft\SystemCertificates\My\PhysicalStores
HKEY_CURRENT_USER\Software\Microsoft\SystemCertificates\My
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2298303332-66077612-2598613238-1000
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2298303332-66077612-2598613238-1000\ProfileImagePath

READ FILES

C:\Windows\nebifozajuxe
C:\Users\user\AppData\Local\2259afc4852c5c7311722091fb1069f452d5de8d\container.dat
C:\Users\user\AppData\Local\2259afc4852c5c7311722091fb1069f452d5de8d\container.dat.tmp
C:\Windows\System32\p2pcollab.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

MODIFIED REGISTRY KEYS

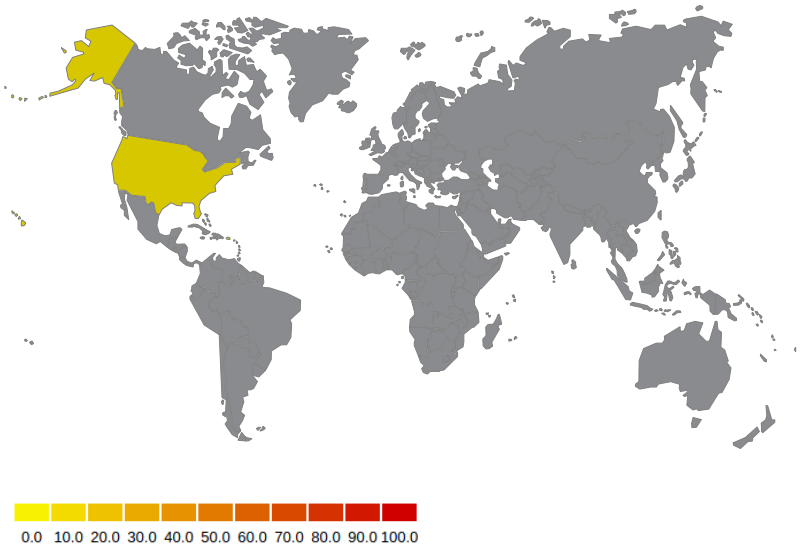
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\LanguageList

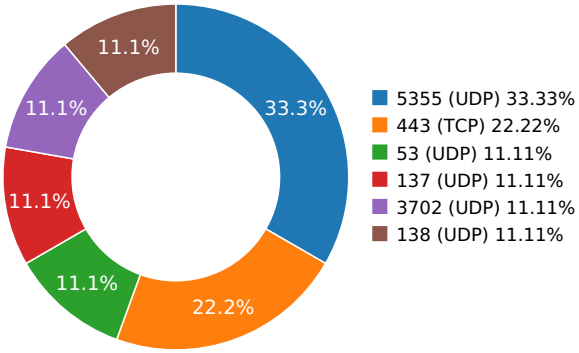
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\p2pcollab.dll,-8042

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
	172.217.10.238		15169	Google LLC	Malware Process

DNS QUERIES

Request	Type
google.com	A
Answers - 172.217.10.238 (A)	

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
31.7819311619	Sandbox	172.217.10.238	443
62.4188771248	Sandbox	172.217.10.238	443

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.07362604141	Sandbox	224.0.0.252	5355
3.09593200684	Sandbox	224.0.0.252	5355
3.10057210922	Sandbox	239.255.255.250	3702
3.14032506943	Sandbox	192.168.56.255	137
5.67320203781	Sandbox	224.0.0.252	5355
9.15583920479	Sandbox	192.168.56.255	138
31.7013981342	Sandbox	8.8.4.4	53

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\2259afc4852c5c7311722091fb1069f452d5de8d\Container.Dat.Tmp **C:\Users\User\AppData\Local\2259afc4852c5c7311722091fb1069f452d5de8d\Container.Dat**	**Type :** data **MD5 :** c3adb397a215dbc346d94c643aeddf3f **SHA-1 :** f76c3535a1c58c7d6139bd13264d4c28eb8f0af2 **SHA-256 :** 1261dc597c1725b1297383a75383f636171f2f2f3 **SHA-512 :** 87c64dd93674107f24242db75c4f8897f205ee6b **Size :** 0.464 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	a9J3j.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	3451a3b7b9125b705aaecb9fc8aa4d80e77c860f
MD5:	df515c7944862ef4982cacfc151085f5
First Seen Date:	2018-03-21 17:11:27.794132 (11 months ago)
Number Of Clients Seen:	7
Last Analysis Date:	2018-03-21 17:11:27.794132 (11 months ago)
Human Expert Analysis Date:	2018-03-21 19:30:14.483935 (11 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	[]
Compilation Time Stamp	0x5AB28169 [Wed Mar 21 15:59:37 2018 UTC]
Entry Point	0x1000183e (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	286208
Ssdeep	
Sha256	163268c02f5d7d6431d21e9ce84ebe8e9b625491ededacb28ec6c8db0ca82aff
Exifinfo	[]
Mime Type	application/x-dosexec
Imphash	

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x4910	0x4a00	6.47482263813	e9cb00b4e602dc84930168bd45f4ce23
.rdata	0x6000	0x292c	0x2a00	4.78030662465	9fb2137948d37a2fffd62f1718f745dc
.data	0x9000	0x60c740	0xe00	2.2040815877	28042e36a0b6a521301656930053ffcb
.rsrc	0x616000	0x3a350	0x3a400	7.99765854329	1cd8c23a0f3eae43f02d8efde1586d19
.reloc	0x651000	0x3258	0x3400	1.35510232447	93996007f1695f325e28aea0f27c3f96

PE Resources

{u'lang': u'LANG_NEUTRAL', u'name': u'IHDXMBTPMS', u'offset': 6381896, u'sha256': u'0622f3b635a9b050523d343ef1e1cef253add3f17a34ea05c9fe64bd06d20fdc', u'type': u'data', u'size': 233715}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 6615612, u'sha256': u'7346933011a4275d9d43e88c5cc4b632ec2600b1d58c521e397b1c3060763676', u'type': u'data', u'size': 4264}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ACCELERATOR', u'offset': 6619876, u'sha256': u'71e5738309a82c861a7cc62b9ecaced80e668bd1b1061f2d781d9098357fda5c', u'type': u'data', u'size': 88}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_ICON', u'offset': 6619964, u'sha256': u'a14e70ed824f3f17d3a51136aa08839954d6d3ccadaa067415c7bfc08e6636b0', u'type': u'MS Windows icon resource - 1 icon, 32x32', u'size': 20}

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS