VALKYRIE COMODO

Summary

File Name: igrmwns.exe

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

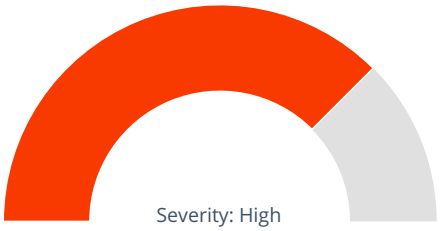
SHA1: 2ee131baf9fd1e163bde6124d6137c050fcc98b4

MD5: 5cdf1c6855a682405062959b4f4af891

MALWARE

Valkyrie Final Verdict

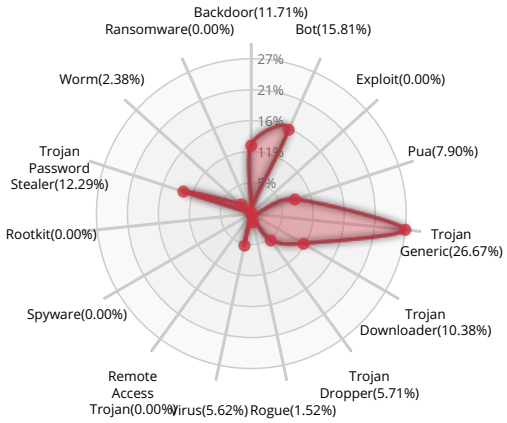
DETECTION SECTION



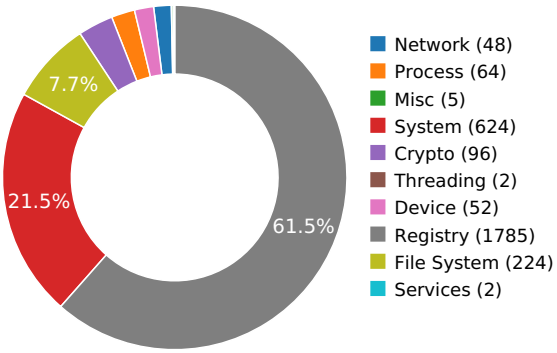
Severity: High

Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

VALKYRIE COMODO

Activity Details

PACKER

The binary likely contains encrypted or compressed data. Show sources

NETWORKING

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

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory Show sources

Behavior Graph

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\sysnative\p2pcollab.dll
C:\Windows\sysnative\QAGENTRT.DLL
C:\Windows\sysnative\dnsapi.dll
C:\Windows\sysnative\en-US\DNSAPI.dll.mui
C:\Windows\sysnative\fveui.dll
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
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:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\CRLs*
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\CTLs*
C:\Windows\sysnative\en-US\WINHTTP.dll.mui

C:\Users\user\AppData\LocalLow
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506
C:\Users\user\AppData\Local\Temp
C:\Users\user\AppData\Local\Temp\Cab50A1.tmp
C:\Users\user\AppData\Local\Temp\Tar50A2.tmp
C:\Users\user\AppData\Local\Temp\
C:\Windows\inf\

READ REGISTRY KEYS

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\SecurityProviders\SCHANNEL\UserContextLockCount
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SecurityProviders\SCHANNEL\UserContextListCount
HKEY_LOCAL_MACHINE\SOFTWARE\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\Microsoft\Cryptography\OID\EncodingType 0\CryptDllFindOIDInfo\1.3.6.1.4.1.311.47.1.1!7\Name
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\qagentrt.dll,-10
HKEY_LOCAL_MACHINE\SOFTWARE\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\Microsoft\Cryptography\OID\EncodingType 0\CryptDllFindOIDInfo\1.3.6.1.4.1.311.67.1.1!7\Name
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\System32\fveui.dll,-843
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CryptDllFindOIDInfo\1.3.6.1.4.1.311.67.1.2!7\Name
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\System32\fveui.dll,-844
HKEY_LOCAL_MACHINE\SOFTWARE\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\6431723036FD26DEA502792FA5959224930 30F97\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

MODIFIED FILES

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

C:\Users\user\AppData\Local\Temp\Cab50A1.tmp

C:\Users\user\AppData\Local\Temp\Tar50A2.tmp

RESOLVED APIS

kernel32.dll.VirtualAlloc

kernel32.dll.LoadLibraryA

kernel32.dll.GetProcAddress

kernel32.dll.VirtualProtect

kernel32.dll.UnmapViewOfFile

kernel32.dll.AddVectoredExceptionHandler

kernel32.dll.RemoveVectoredExceptionHandler

kernel32.dll.FreeConsole

kernel32.dll.GetLastError
kernel32.dll.HeapAlloc
kernel32.dll.HeapDestroy
kernel32.dll.HeapCreate
kernel32.dll.HeapFree
kernel32.dll.GetModuleHandleA
kernel32.dll.ExitProcess
kernel32.dll.GetTickCount
kernel32.dll.VirtualFree
ntdll.dll.memset
ntdll.dll.memcpy
ntdll.dll.RtlUnwind
ntdll.dll.NtQueryVirtualMemory
ntdll.dll.NtSetValueKey
ntdll.dll.NtQueryValueKey
ntdll.dll.NtOpenKey
ntdll.dll.NtCreateKey
ntdll.dll.RtlInitUnicodeString
ntdll.dll.strrchr
ntdll.dll.NtOpenSection
ntdll.dll.NtMapViewOfSection
ntdll.dll.NtUnmapViewOfSection
ntdll.dll.NtCreateSection
ntdll.dll.NtQueryInformationToken
ntdll.dll.NtOpenProcessToken
ntdll.dll.NtClose
ntdll.dll.NtQueryInformationProcess
ntdll.dll._wcsupr
ntdll.dll.NtProtectVirtualMemory
ntdll.dll.wcsrchr
ntdll.dll.NtResumeProcess
ntdll.dll.NtSuspendProcess
ntdll.dll._strupr
ntdll.dll.mbstowcs
ntdll.dll._snwprintf

ntdll.dll.RtlNtStatusToDosError
ntdll.dll.wcstombs
ntdll.dll.strchr
ntdll.dll.strcpy
ntdll.dll.sprintf
ntdll.dll._snprintf
ntdll.dll._aulldiv
ntdll.dll._allmul
ntdll.dll.wcschr
ntdll.dll.RtlImageNtHeader
shlwapi.dll.StrToIntExA
shlwapi.dll.StrTrimA
shlwapi.dll.StrStrIA
shlwapi.dll.PathFindExtensionW
shlwapi.dll.PathFindFileNameW
shlwapi.dll.StrStrIW
shlwapi.dll.PathCombineW
kernel32.dll.SetWaitableTimer
kernel32.dll.QueueUserAPC
kernel32.dll.GetCurrentThreadId
kernel32.dll.InterlockedIncrement
kernel32.dll.Sleep
kernel32.dll.InterlockedDecrement
kernel32.dll.OpenThread
kernel32.dll.CreateWaitableTimerA
kernel32.dll.OpenFileMappingW
kernel32.dll.GetFileSize
kernel32.dll.GetTempFileNameW
kernel32.dll.ReadFile
kernel32.dll.lstrcatW
kernel32.dll.GetSystemTimeAsFileTime
kernel32.dll.CreateWaitableTimerW
kernel32.dll.WaitForMultipleObjects

REGISTRY KEYS

HKEY_CURRENT_USER\Identities\{BC747A38-9DB1-AA66-8A41-008F24D29CEE}
HKEY_CURRENT_USER\Identities\{BC747A38-9DB1-AA66-8A41-008F24D29CEE}\Monitorcode
HKEY_CURRENT_USER\Identities\{BC747A38-9DB1-AA66-8A41-008F24D29CEE}\Currentmedia
HKEY_USERS\S-1-5-21-2298303332-66077612-2598613238-1000\Software\Microsoft\Windows\CurrentVersion\Run
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\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\Microsoft\Cryptography\OID\EncodingType 0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CryptDllFindOIDInfo
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\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\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\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\Microsoft\Cryptography\OID\EncodingType 0\CryptDllFindOIDInfo\1.3.6.1.4.1.311.47.1.1!7\Name
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\qagentrt.dll,-10
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\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\Name
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\dnsapi.dll,-103
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CryptDllFindOIDInfo\1.3.6.1.4.1.311.67.1.1!7
HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\OID\EncodingType 0\CryptDllFindOIDInfo\1.3.6.1.4.1.311.67.1.1!7
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CryptDllFindOIDInfo\1.3.6.1.4.1.311.67.1.1!7\Name
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\System32\fveui.dll,-843

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CryptDllFindOIDInfo\1.3.6.1.4.1.311.67.1.2!7
HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\OID\EncodingType 0\CryptDllFindOIDInfo\1.3.6.1.4.1.311.67.1.2!7
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CryptDllFindOIDInfo\1.3.6.1.4.1.311.67.1.2!7\Name
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\System32\fveui.dll,-844
HKEY_LOCAL_MACHINE\SOFTWARE\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\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

READ FILES

C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\sysnative\p2pcollab.dll
C:\Windows\sysnative\QAGENTRT.DLL
C:\Windows\sysnative\en-US\DNSAPI.dll.mui
C:\Windows\sysnative\fveui.dll
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\sysnative\en-US\WINHTTP.dll.mui

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

C:\Users\user\AppData\Local\Temp\Cab50A1.tmp

C:\Users\user\AppData\Local\Temp\Tar50A2.tmp

MODIFIED REGISTRY KEYS

HKEY_CURRENT_USER\Identities\{BC747A38-9DB1-AA66-8A41-008F24D29CEE}

HKEY_CURRENT_USER\Identities\{BC747A38-9DB1-AA66-8A41-008F24D29CEE}\Monitorcode

HKEY_CURRENT_USER\Identities\{BC747A38-9DB1-AA66-8A41-008F24D29CEE}\Currentmedia

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\qagentrt.dll,-10

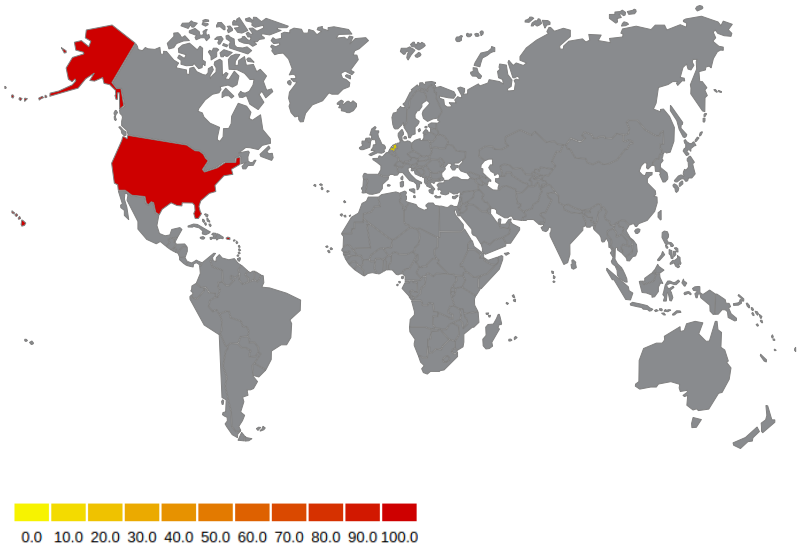
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\dnsapi.dll,-103

HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\System32\fveui.dll,-843

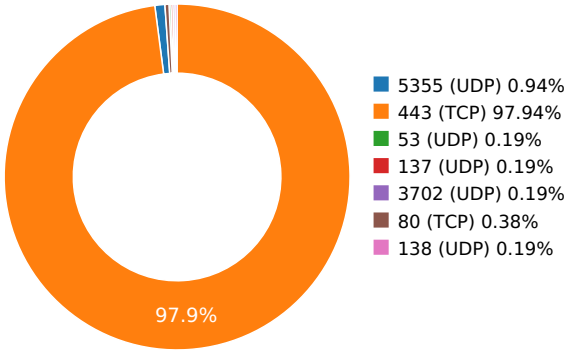
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\System32\fveui.dll,-844

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
	184.26.44.97	United States	20940	Akamai Technologies, Inc.	OS Process
ctldl.windowsupdate.com	65.152.202.18	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	17.356085062

Path: /msdownload/update/v3/static/trustedr/en/authrootstl.cab?e2e4bd038d3769b7
URI: http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab?e2e4bd038d3769b7

DNS QUERIES

Request	Type
ctldl.windowsupdate.com	A

Answers
- ctldl.windowsupdate.nsatc.net (CNAME)
- 184.26.44.97 (A)
- a1621.g.akamai.net (CNAME)
- ctldl.windowsupdate.com.edgesuite.net (CNAME)
- 184.26.44.105 (A)

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
10.9073889256	Sandbox	86.105.18.236	443

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
17.356085062	Sandbox	184.26.44.97	80
17.7829670906	Sandbox	86.105.18.236	443
18.1563310623	Sandbox	86.105.18.236	443
18.5207099915	Sandbox	86.105.18.236	443
18.8759388924	Sandbox	86.105.18.236	443
19.2392148972	Sandbox	86.105.18.236	443
19.6037459373	Sandbox	86.105.18.236	443
19.9725298882	Sandbox	86.105.18.236	443
20.3417429924	Sandbox	86.105.18.236	443
20.7106668949	Sandbox	86.105.18.236	443
21.0741150379	Sandbox	86.105.18.236	443
21.438297987	Sandbox	86.105.18.236	443
21.7998468876	Sandbox	86.105.18.236	443
22.1715140343	Sandbox	86.105.18.236	443
22.536853075	Sandbox	86.105.18.236	443
22.8989500999	Sandbox	86.105.18.236	443
23.2606320381	Sandbox	86.105.18.236	443
23.6191720963	Sandbox	86.105.18.236	443
23.9760890007	Sandbox	86.105.18.236	443
24.3438689709	Sandbox	86.105.18.236	443
24.7070229053	Sandbox	86.105.18.236	443
25.0684540272	Sandbox	86.105.18.236	443
25.4315719604	Sandbox	86.105.18.236	443
25.7985041142	Sandbox	86.105.18.236	443
26.157088995	Sandbox	86.105.18.236	443
26.5275409222	Sandbox	86.105.18.236	443
26.8969659805	Sandbox	86.105.18.236	443
27.2667930126	Sandbox	86.105.18.236	443
27.6281290054	Sandbox	86.105.18.236	443
27.9899311066	Sandbox	86.105.18.236	443
28.3502109051	Sandbox	86.105.18.236	443
28.7063550949	Sandbox	86.105.18.236	443
29.0624539852	Sandbox	86.105.18.236	443
29.4273281097	Sandbox	86.105.18.236	443
29.7834711075	Sandbox	86.105.18.236	443
30.1429669857	Sandbox	86.105.18.236	443
30.4972379208	Sandbox	86.105.18.236	443

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
30.8510119915	Sandbox	86.105.18.236	443
31.2085309029	Sandbox	86.105.18.236	443
31.5758700371	Sandbox	86.105.18.236	443
31.9374980927	Sandbox	86.105.18.236	443
32.3006939888	Sandbox	86.105.18.236	443
32.6706008911	Sandbox	86.105.18.236	443
33.0356628895	Sandbox	86.105.18.236	443
33.3925089836	Sandbox	86.105.18.236	443
33.7569429874	Sandbox	86.105.18.236	443
34.1254010201	Sandbox	86.105.18.236	443
34.4888958931	Sandbox	86.105.18.236	443
34.8558549881	Sandbox	86.105.18.236	443
35.2154870033	Sandbox	86.105.18.236	443
35.568846941	Sandbox	86.105.18.236	443
35.9307079315	Sandbox	86.105.18.236	443
36.2928860188	Sandbox	86.105.18.236	443
36.6546940804	Sandbox	86.105.18.236	443
37.0069470406	Sandbox	86.105.18.236	443
37.3641600609	Sandbox	86.105.18.236	443
37.7333950996	Sandbox	86.105.18.236	443
38.0992329121	Sandbox	86.105.18.236	443
38.4642920494	Sandbox	86.105.18.236	443
38.8310670853	Sandbox	86.105.18.236	443
39.1907439232	Sandbox	86.105.18.236	443
39.5457201004	Sandbox	86.105.18.236	443
39.9096329212	Sandbox	86.105.18.236	443
40.2812199593	Sandbox	86.105.18.236	443
40.6478509903	Sandbox	86.105.18.236	443
41.0104210377	Sandbox	86.105.18.236	443
41.3718240261	Sandbox	86.105.18.236	443
41.7335240841	Sandbox	86.105.18.236	443
42.0968160629	Sandbox	86.105.18.236	443
42.4604389668	Sandbox	86.105.18.236	443
42.8305499554	Sandbox	86.105.18.236	443
43.1881239414	Sandbox	86.105.18.236	443
43.5467739105	Sandbox	86.105.18.236	443
43.9138989449	Sandbox	86.105.18.236	443

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
44.2745249271	Sandbox	86.105.18.236	443
44.6323120594	Sandbox	86.105.18.236	443
44.9975709915	Sandbox	86.105.18.236	443
45.3598120213	Sandbox	86.105.18.236	443
45.7274301052	Sandbox	86.105.18.236	443
46.0902869701	Sandbox	86.105.18.236	443
46.4561979771	Sandbox	86.105.18.236	443
46.8169240952	Sandbox	86.105.18.236	443
47.1808860302	Sandbox	86.105.18.236	443
47.5480599403	Sandbox	86.105.18.236	443
47.9088740349	Sandbox	86.105.18.236	443
48.2693340778	Sandbox	86.105.18.236	443
48.6306939125	Sandbox	86.105.18.236	443
48.9909861088	Sandbox	86.105.18.236	443
49.3500249386	Sandbox	86.105.18.236	443
49.7071359158	Sandbox	86.105.18.236	443
50.0682299137	Sandbox	86.105.18.236	443
50.4293870926	Sandbox	86.105.18.236	443
50.7915370464	Sandbox	86.105.18.236	443
51.1522700787	Sandbox	86.105.18.236	443
51.5121119022	Sandbox	86.105.18.236	443
51.8669219017	Sandbox	86.105.18.236	443
52.2285320759	Sandbox	86.105.18.236	443
52.5898029804	Sandbox	86.105.18.236	443
52.956412077	Sandbox	86.105.18.236	443
53.3190429211	Sandbox	86.105.18.236	443
53.6861538887	Sandbox	86.105.18.236	443
54.0485889912	Sandbox	86.105.18.236	443
54.433300972	Sandbox	86.105.18.236	443
54.7956290245	Sandbox	86.105.18.236	443
55.1503500938	Sandbox	86.105.18.236	443
55.5164220333	Sandbox	86.105.18.236	443
55.8826489449	Sandbox	86.105.18.236	443
56.2431540489	Sandbox	86.105.18.236	443
56.6040298939	Sandbox	86.105.18.236	443
56.9630479813	Sandbox	86.105.18.236	443
57.3176989555	Sandbox	86.105.18.236	443

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
57.6771600246	Sandbox	86.105.18.236	443
58.0321650505	Sandbox	86.105.18.236	443
58.3963670731	Sandbox	86.105.18.236	443
58.7633709908	Sandbox	86.105.18.236	443
59.1245400906	Sandbox	86.105.18.236	443
59.501693964	Sandbox	86.105.18.236	443
59.8584458828	Sandbox	86.105.18.236	443
60.227132082	Sandbox	86.105.18.236	443
60.5936069489	Sandbox	86.105.18.236	443
60.9596569538	Sandbox	86.105.18.236	443
61.3184320927	Sandbox	86.105.18.236	443
61.6734669209	Sandbox	86.105.18.236	443
62.035228014	Sandbox	86.105.18.236	443
62.3907740116	Sandbox	86.105.18.236	443
62.7587099075	Sandbox	86.105.18.236	443
63.1320569515	Sandbox	86.105.18.236	443
63.5002911091	Sandbox	86.105.18.236	443
63.8628408909	Sandbox	86.105.18.236	443
64.2276370525	Sandbox	86.105.18.236	443
64.5953299999	Sandbox	86.105.18.236	443
64.958739996	Sandbox	86.105.18.236	443
65.3184440136	Sandbox	86.105.18.236	443
65.6847119331	Sandbox	86.105.18.236	443
66.0444090366	Sandbox	86.105.18.236	443
66.4112620354	Sandbox	86.105.18.236	443
66.7742400169	Sandbox	86.105.18.236	443
67.1384088993	Sandbox	86.105.18.236	443
67.5042660236	Sandbox	86.105.18.236	443
67.8711249828	Sandbox	86.105.18.236	443
68.230684042	Sandbox	86.105.18.236	443
68.5882608891	Sandbox	86.105.18.236	443
68.9561440945	Sandbox	86.105.18.236	443
69.3157060146	Sandbox	86.105.18.236	443
69.6715860367	Sandbox	86.105.18.236	443
70.032834053	Sandbox	86.105.18.236	443
70.3969929218	Sandbox	86.105.18.236	443
70.7629420757	Sandbox	86.105.18.236	443

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
71.1164269447	Sandbox	86.105.18.236	443
71.4753799438	Sandbox	86.105.18.236	443
71.8379359245	Sandbox	86.105.18.236	443
72.1979179382	Sandbox	86.105.18.236	443
72.5519199371	Sandbox	86.105.18.236	443
72.9125669003	Sandbox	86.105.18.236	443
73.2738959789	Sandbox	86.105.18.236	443
73.635833025	Sandbox	86.105.18.236	443
73.9975988865	Sandbox	86.105.18.236	443
74.361371994	Sandbox	86.105.18.236	443
74.7226560116	Sandbox	86.105.18.236	443
75.082349062	Sandbox	86.105.18.236	443
75.4361569881	Sandbox	86.105.18.236	443
75.790102005	Sandbox	86.105.18.236	443
76.1473379135	Sandbox	86.105.18.236	443
76.5090420246	Sandbox	86.105.18.236	443
76.8706459999	Sandbox	86.105.18.236	443
77.2295410633	Sandbox	86.105.18.236	443
77.5845420361	Sandbox	86.105.18.236	443
77.9434969425	Sandbox	86.105.18.236	443
78.2978329659	Sandbox	86.105.18.236	443
78.6556520462	Sandbox	86.105.18.236	443
79.0244390965	Sandbox	86.105.18.236	443
79.3874459267	Sandbox	86.105.18.236	443
79.7491579056	Sandbox	86.105.18.236	443
80.1096110344	Sandbox	86.105.18.236	443
80.4744670391	Sandbox	86.105.18.236	443
80.8469569683	Sandbox	86.105.18.236	443
81.2158339024	Sandbox	86.105.18.236	443
81.5765650272	Sandbox	86.105.18.236	443
81.9331240654	Sandbox	86.105.18.236	443
82.2932319641	Sandbox	86.105.18.236	443
82.6490709782	Sandbox	86.105.18.236	443
83.0108299255	Sandbox	86.105.18.236	443
83.3718008995	Sandbox	86.105.18.236	443
83.7358388901	Sandbox	86.105.18.236	443
84.1029219627	Sandbox	86.105.18.236	443

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
84.4645609856	Sandbox	86.105.18.236	443
84.8285269737	Sandbox	86.105.18.236	443
85.1984550953	Sandbox	86.105.18.236	443
85.5645289421	Sandbox	86.105.18.236	443
85.9337720871	Sandbox	86.105.18.236	443
86.2994771004	Sandbox	86.105.18.236	443
86.6595098972	Sandbox	86.105.18.236	443
87.0264821053	Sandbox	86.105.18.236	443
87.3897199631	Sandbox	86.105.18.236	443
87.7588779926	Sandbox	86.105.18.236	443
88.1281108856	Sandbox	86.105.18.236	443
88.4941680431	Sandbox	86.105.18.236	443
88.8513450623	Sandbox	86.105.18.236	443
89.2160570621	Sandbox	86.105.18.236	443
89.5731210709	Sandbox	86.105.18.236	443
89.9544329643	Sandbox	86.105.18.236	443
90.3133370876	Sandbox	86.105.18.236	443
90.6707780361	Sandbox	86.105.18.236	443
91.0369429588	Sandbox	86.105.18.236	443
91.4085469246	Sandbox	86.105.18.236	443
91.7748429775	Sandbox	86.105.18.236	443
92.1368429661	Sandbox	86.105.18.236	443
92.4956200123	Sandbox	86.105.18.236	443
92.8566789627	Sandbox	86.105.18.236	443
93.2104580402	Sandbox	86.105.18.236	443
93.5665159225	Sandbox	86.105.18.236	443
93.9277570248	Sandbox	86.105.18.236	443
94.2883050442	Sandbox	86.105.18.236	443
94.6480240822	Sandbox	86.105.18.236	443
95.0082879066	Sandbox	86.105.18.236	443
95.3689720631	Sandbox	86.105.18.236	443
95.7293739319	Sandbox	86.105.18.236	443
96.0882279873	Sandbox	86.105.18.236	443
96.4417459965	Sandbox	86.105.18.236	443
96.7953579426	Sandbox	86.105.18.236	443
97.1511108875	Sandbox	86.105.18.236	443
97.5144679546	Sandbox	86.105.18.236	443

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
97.8815779686	Sandbox	86.105.18.236	443
98.2430040836	Sandbox	86.105.18.236	443
98.605684042	Sandbox	86.105.18.236	443
98.9728341103	Sandbox	86.105.18.236	443
99.3369350433	Sandbox	86.105.18.236	443
99.7008109093	Sandbox	86.105.18.236	443
100.059400082	Sandbox	86.105.18.236	443
100.416861057	Sandbox	86.105.18.236	443
100.780723095	Sandbox	86.105.18.236	443
101.137720108	Sandbox	86.105.18.236	443
101.498636007	Sandbox	86.105.18.236	443
101.857769012	Sandbox	86.105.18.236	443
102.215787888	Sandbox	86.105.18.236	443
102.585510015	Sandbox	86.105.18.236	443
102.953475952	Sandbox	86.105.18.236	443
103.316469908	Sandbox	86.105.18.236	443
103.678556919	Sandbox	86.105.18.236	443
104.037278891	Sandbox	86.105.18.236	443
104.393326998	Sandbox	86.105.18.236	443
104.760526896	Sandbox	86.105.18.236	443
105.12383008	Sandbox	86.105.18.236	443
105.490271091	Sandbox	86.105.18.236	443
105.849070072	Sandbox	86.105.18.236	443
106.2043221	Sandbox	86.105.18.236	443
106.559983015	Sandbox	86.105.18.236	443
106.919116974	Sandbox	86.105.18.236	443
107.277997017	Sandbox	86.105.18.236	443
107.642011881	Sandbox	86.105.18.236	443
107.997684956	Sandbox	86.105.18.236	443
108.357204914	Sandbox	86.105.18.236	443
108.714799881	Sandbox	86.105.18.236	443
109.082568884	Sandbox	86.105.18.236	443
109.449645996	Sandbox	86.105.18.236	443
109.811512947	Sandbox	86.105.18.236	443
110.170517921	Sandbox	86.105.18.236	443
110.524307013	Sandbox	86.105.18.236	443
110.881481886	Sandbox	86.105.18.236	443

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
111.246916056	Sandbox	86.105.18.236	443
111.604227066	Sandbox	86.105.18.236	443
111.970135927	Sandbox	86.105.18.236	443
112.329550982	Sandbox	86.105.18.236	443
112.685734987	Sandbox	86.105.18.236	443
113.050471067	Sandbox	86.105.18.236	443
113.417625904	Sandbox	86.105.18.236	443
113.782171965	Sandbox	86.105.18.236	443
114.149182081	Sandbox	86.105.18.236	443
114.510001898	Sandbox	86.105.18.236	443
114.866779089	Sandbox	86.105.18.236	443
115.229783058	Sandbox	86.105.18.236	443
115.590322971	Sandbox	86.105.18.236	443
115.951360941	Sandbox	86.105.18.236	443
116.312031984	Sandbox	86.105.18.236	443
116.669392109	Sandbox	86.105.18.236	443
117.039258957	Sandbox	86.105.18.236	443
117.399934053	Sandbox	86.105.18.236	443
117.758578062	Sandbox	86.105.18.236	443
118.113528967	Sandbox	86.105.18.236	443
118.479397058	Sandbox	86.105.18.236	443
118.849057913	Sandbox	86.105.18.236	443
119.215498924	Sandbox	86.105.18.236	443
119.574418068	Sandbox	86.105.18.236	443
119.930135012	Sandbox	86.105.18.236	443
120.293329954	Sandbox	86.105.18.236	443
120.659960032	Sandbox	86.105.18.236	443
121.02106905	Sandbox	86.105.18.236	443
121.379998922	Sandbox	86.105.18.236	443
121.735661983	Sandbox	86.105.18.236	443
122.097501993	Sandbox	86.105.18.236	443
122.461088896	Sandbox	86.105.18.236	443
122.830427885	Sandbox	86.105.18.236	443
123.192513943	Sandbox	86.105.18.236	443
123.555625916	Sandbox	86.105.18.236	443
123.924170017	Sandbox	86.105.18.236	443
124.293441057	Sandbox	86.105.18.236	443

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
124.664051056	Sandbox	86.105.18.236	443
125.032445908	Sandbox	86.105.18.236	443
125.398140907	Sandbox	86.105.18.236	443
125.754471064	Sandbox	86.105.18.236	443
126.114028931	Sandbox	86.105.18.236	443
126.471705914	Sandbox	86.105.18.236	443
126.840069056	Sandbox	86.105.18.236	443
127.201297045	Sandbox	86.105.18.236	443
127.559894085	Sandbox	86.105.18.236	443
127.916897058	Sandbox	86.105.18.236	443
128.281039	Sandbox	86.105.18.236	443
128.635289907	Sandbox	86.105.18.236	443
128.991086006	Sandbox	86.105.18.236	443
129.352505922	Sandbox	86.105.18.236	443
129.712245941	Sandbox	86.105.18.236	443
130.06733799	Sandbox	86.105.18.236	443
130.430562973	Sandbox	86.105.18.236	443
130.798300982	Sandbox	86.105.18.236	443
131.160145044	Sandbox	86.105.18.236	443
131.521481037	Sandbox	86.105.18.236	443
131.882945061	Sandbox	86.105.18.236	443
132.246213913	Sandbox	86.105.18.236	443
132.614418983	Sandbox	86.105.18.236	443
132.974555016	Sandbox	86.105.18.236	443
133.332221985	Sandbox	86.105.18.236	443
133.699713945	Sandbox	86.105.18.236	443
134.06208992	Sandbox	86.105.18.236	443
134.42524004	Sandbox	86.105.18.236	443
134.790343046	Sandbox	86.105.18.236	443
135.147557974	Sandbox	86.105.18.236	443
135.51257205	Sandbox	86.105.18.236	443
135.868937016	Sandbox	86.105.18.236	443
136.228542089	Sandbox	86.105.18.236	443
136.586177111	Sandbox	86.105.18.236	443
136.952061892	Sandbox	86.105.18.236	443
137.305668116	Sandbox	86.105.18.236	443
137.659141064	Sandbox	86.105.18.236	443

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
138.013118982	Sandbox	86.105.18.236	443
138.370635986	Sandbox	86.105.18.236	443
138.735523939	Sandbox	86.105.18.236	443
139.104937077	Sandbox	86.105.18.236	443
139.468540907	Sandbox	86.105.18.236	443
139.836411953	Sandbox	86.105.18.236	443
140.194550037	Sandbox	86.105.18.236	443
140.561249971	Sandbox	86.105.18.236	443
140.92130208	Sandbox	86.105.18.236	443
141.277226925	Sandbox	86.105.18.236	443
141.643992901	Sandbox	86.105.18.236	443
142.00741601	Sandbox	86.105.18.236	443
142.37638092	Sandbox	86.105.18.236	443
142.745604038	Sandbox	86.105.18.236	443
143.113154888	Sandbox	86.105.18.236	443
143.474809885	Sandbox	86.105.18.236	443
143.841464043	Sandbox	86.105.18.236	443
144.208216906	Sandbox	86.105.18.236	443
144.566119909	Sandbox	86.105.18.236	443
144.933521032	Sandbox	86.105.18.236	443
145.29737401	Sandbox	86.105.18.236	443
145.663491011	Sandbox	86.105.18.236	443
146.025345087	Sandbox	86.105.18.236	443
146.386693954	Sandbox	86.105.18.236	443
146.748558998	Sandbox	86.105.18.236	443
147.111392975	Sandbox	86.105.18.236	443
147.472867012	Sandbox	86.105.18.236	443
147.846330881	Sandbox	86.105.18.236	443
148.208606005	Sandbox	86.105.18.236	443
148.568366051	Sandbox	86.105.18.236	443
148.92417407	Sandbox	86.105.18.236	443
149.286469936	Sandbox	86.105.18.236	443
149.650002003	Sandbox	86.105.18.236	443
150.012794971	Sandbox	86.105.18.236	443
150.375612974	Sandbox	86.105.18.236	443
150.740573883	Sandbox	86.105.18.236	443
151.108463049	Sandbox	86.105.18.236	443

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
151.475418091	Sandbox	86.105.18.236	443
151.836730003	Sandbox	86.105.18.236	443
152.199780941	Sandbox	86.105.18.236	443
152.566452026	Sandbox	86.105.18.236	443
152.929944038	Sandbox	86.105.18.236	443
153.299108982	Sandbox	86.105.18.236	443
153.661004066	Sandbox	86.105.18.236	443
154.024281025	Sandbox	86.105.18.236	443
154.391371012	Sandbox	86.105.18.236	443
154.755307913	Sandbox	86.105.18.236	443
155.124218941	Sandbox	86.105.18.236	443
155.484122992	Sandbox	86.105.18.236	443
155.837625027	Sandbox	86.105.18.236	443
156.19380188	Sandbox	86.105.18.236	443
156.556502104	Sandbox	86.105.18.236	443
156.918967962	Sandbox	86.105.18.236	443
157.27895999	Sandbox	86.105.18.236	443
157.635333061	Sandbox	86.105.18.236	443
158.002680063	Sandbox	86.105.18.236	443
158.364073038	Sandbox	86.105.18.236	443
158.727488995	Sandbox	86.105.18.236	443
159.097428083	Sandbox	86.105.18.236	443
159.467772961	Sandbox	86.105.18.236	443
159.837611914	Sandbox	86.105.18.236	443
160.208276033	Sandbox	86.105.18.236	443
160.570446968	Sandbox	86.105.18.236	443
160.933757067	Sandbox	86.105.18.236	443
161.301455975	Sandbox	86.105.18.236	443
161.664973974	Sandbox	86.105.18.236	443
162.024019957	Sandbox	86.105.18.236	443
162.379782915	Sandbox	86.105.18.236	443
162.742549896	Sandbox	86.105.18.236	443
163.106046915	Sandbox	86.105.18.236	443
163.473982096	Sandbox	86.105.18.236	443
163.835472107	Sandbox	86.105.18.236	443
164.196448088	Sandbox	86.105.18.236	443
164.560204029	Sandbox	86.105.18.236	443

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
164.926378012	Sandbox	86.105.18.236	443
165.285644054	Sandbox	86.105.18.236	443
165.656194925	Sandbox	86.105.18.236	443
166.0223701	Sandbox	86.105.18.236	443
166.381352901	Sandbox	86.105.18.236	443
166.737365961	Sandbox	86.105.18.236	443
167.100315094	Sandbox	86.105.18.236	443
167.466850996	Sandbox	86.105.18.236	443
167.82879591	Sandbox	86.105.18.236	443
168.188935041	Sandbox	86.105.18.236	443
168.550481081	Sandbox	86.105.18.236	443
168.904108047	Sandbox	86.105.18.236	443
169.261141062	Sandbox	86.105.18.236	443
169.624572992	Sandbox	86.105.18.236	443
169.989633083	Sandbox	86.105.18.236	443
170.345767975	Sandbox	86.105.18.236	443
170.707400084	Sandbox	86.105.18.236	443
171.067468882	Sandbox	86.105.18.236	443
171.428189039	Sandbox	86.105.18.236	443
171.784243107	Sandbox	86.105.18.236	443
172.145153046	Sandbox	86.105.18.236	443
172.505712032	Sandbox	86.105.18.236	443
172.86421895	Sandbox	86.105.18.236	443
173.236639023	Sandbox	86.105.18.236	443
173.599950075	Sandbox	86.105.18.236	443
173.964339018	Sandbox	86.105.18.236	443
174.321577072	Sandbox	86.105.18.236	443
174.687150002	Sandbox	86.105.18.236	443
175.051101923	Sandbox	86.105.18.236	443
175.421276093	Sandbox	86.105.18.236	443
175.791095972	Sandbox	86.105.18.236	443
176.157255888	Sandbox	86.105.18.236	443
176.521614075	Sandbox	86.105.18.236	443
176.888524055	Sandbox	86.105.18.236	443
177.251239061	Sandbox	86.105.18.236	443
177.618249893	Sandbox	86.105.18.236	443
177.981442928	Sandbox	86.105.18.236	443

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
178.34877491	Sandbox	86.105.18.236	443
178.708684921	Sandbox	86.105.18.236	443
179.066601992	Sandbox	86.105.18.236	443
179.430372	Sandbox	86.105.18.236	443
179.797487974	Sandbox	86.105.18.236	443
180.15854907	Sandbox	86.105.18.236	443
180.521208048	Sandbox	86.105.18.236	443
180.877453089	Sandbox	86.105.18.236	443
181.240135908	Sandbox	86.105.18.236	443
181.599909067	Sandbox	86.105.18.236	443
181.953531027	Sandbox	86.105.18.236	443
182.311172962	Sandbox	86.105.18.236	443
182.68163991	Sandbox	86.105.18.236	443
183.050549984	Sandbox	86.105.18.236	443
183.412256002	Sandbox	86.105.18.236	443
183.771373034	Sandbox	86.105.18.236	443
184.127262115	Sandbox	86.105.18.236	443
184.492558002	Sandbox	86.105.18.236	443
184.857031107	Sandbox	86.105.18.236	443
185.215147018	Sandbox	86.105.18.236	443
185.581482887	Sandbox	86.105.18.236	443
185.942792892	Sandbox	86.105.18.236	443
186.303946972	Sandbox	86.105.18.236	443
186.666762114	Sandbox	86.105.18.236	443
187.035957098	Sandbox	86.105.18.236	443
187.399483919	Sandbox	86.105.18.236	443
187.755506992	Sandbox	86.105.18.236	443
188.118582964	Sandbox	86.105.18.236	443
188.488149881	Sandbox	86.105.18.236	443
188.856004953	Sandbox	86.105.18.236	443
189.214771032	Sandbox	86.105.18.236	443
189.568850994	Sandbox	86.105.18.236	443
189.925007105	Sandbox	86.105.18.236	443
190.287846088	Sandbox	86.105.18.236	443
190.65544796	Sandbox	86.105.18.236	443
191.012171984	Sandbox	86.105.18.236	443
191.375926971	Sandbox	86.105.18.236	443

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
191.740087986	Sandbox	86.105.18.236	443
192.108314037	Sandbox	86.105.18.236	443
192.470767021	Sandbox	86.105.18.236	443
192.825416088	Sandbox	86.105.18.236	443
193.182934046	Sandbox	86.105.18.236	443
193.550542116	Sandbox	86.105.18.236	443
193.912461996	Sandbox	86.105.18.236	443
194.275676966	Sandbox	86.105.18.236	443
194.642556906	Sandbox	86.105.18.236	443
195.000492096	Sandbox	86.105.18.236	443
195.36618495	Sandbox	86.105.18.236	443
195.724590063	Sandbox	86.105.18.236	443
196.08890605	Sandbox	86.105.18.236	443
196.452027082	Sandbox	86.105.18.236	443
196.810069084	Sandbox	86.105.18.236	443
197.179097891	Sandbox	86.105.18.236	443
197.544908047	Sandbox	86.105.18.236	443
197.906280994	Sandbox	86.105.18.236	443
198.268127918	Sandbox	86.105.18.236	443
198.628393888	Sandbox	86.105.18.236	443
198.982254028	Sandbox	86.105.18.236	443
199.340128899	Sandbox	86.105.18.236	443
199.706521034	Sandbox	86.105.18.236	443
200.070909023	Sandbox	86.105.18.236	443
200.430346012	Sandbox	86.105.18.236	443
200.788553953	Sandbox	86.105.18.236	443
201.15013504	Sandbox	86.105.18.236	443
201.511709929	Sandbox	86.105.18.236	443
201.872437954	Sandbox	86.105.18.236	443
202.233634949	Sandbox	86.105.18.236	443
202.593055964	Sandbox	86.105.18.236	443
202.950340986	Sandbox	86.105.18.236	443
203.314194918	Sandbox	86.105.18.236	443
203.684159994	Sandbox	86.105.18.236	443
204.050590992	Sandbox	86.105.18.236	443
204.407963991	Sandbox	86.105.18.236	443
204.77343297	Sandbox	86.105.18.236	443

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
205.131973028	Sandbox	86.105.18.236	443
205.500077009	Sandbox	86.105.18.236	443
205.860372066	Sandbox	86.105.18.236	443
206.219113111	Sandbox	86.105.18.236	443

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.16446399689	Sandbox	192.168.56.255	137
3.20336294174	Sandbox	224.0.0.252	5355
3.25052595139	Sandbox	224.0.0.252	5355
3.56428790092	Sandbox	239.255.255.250	3702
5.81398105621	Sandbox	224.0.0.252	5355
9.20409393311	Sandbox	192.168.56.255	138
11.9112679958	Sandbox	224.0.0.252	5355
14.6341040134	Sandbox	224.0.0.252	5355
17.2000689507	Sandbox	8.8.4.4	53

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\Tar50A2.Tmp	**Type :** data **MD5 :** ef3913c6ab2445516e54d3fb4584e66d **SHA-1 :** 4d4562bbcca6889b0ab854e144f82ba514323546 **SHA-256 :** cc36d25f632741e4fb40cb3b5216ad3b1f477078 **SHA-512 :** 7de7eb527ccf6fdffd652d6187adc95afa2868d44 **Size :** 129.579 Kilobytes.
C:\Users\User\AppData\Local\Temp\Cab50A1.Tmp **C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506**	**Type :** Microsoft Cabinet archive data, 53748 bytes, 1 file **MD5 :** e6be5d4fe0366f48e21b7293824b5b94 **SHA-1 :** 36ec9da5ab19880fe614bdc35a67430708cc57cd **SHA-256 :** 4150ae6b41c104f149f95245d84bc6f8678fe8f98 **SHA-512 :** 359443d9200b6009aa1aeb9cb88fbaa6c802b40f **Size :** 53.748 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	**Type :** data **MD5 :** 3fa8fd98e8f6cbf39cde0439bf4f7b2c **SHA-1 :** ab6cbe734f9df2fba6447f03423424ffad0f3b16 **SHA-256 :** 0ede3d2e3d11b39a37ae562d4eee1aecfc5c403f **SHA-512 :** 899e1049a9d4ecf98e8bea6f58c8e8faae9145a72 **Size :** 0.33 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	igrmwns.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	2ee131baf9fd1e163bde6124d6137c050fcc98b4
MD5:	5cdf1c6855a682405062959b4f4af891
First Seen Date:	2018-05-18 15:51:04.078773 (10 months ago)
Number Of Clients Seen:	7
Last Analysis Date:	2018-05-18 15:51:04.078773 (10 months ago)
Human Expert Analysis Result:	No human expert analysis verdict given to this sample yet.

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[{u'Path': u'Lqcp5p34o52v32v534823mb2345234.pdb', u'GUID': u'{6a9e3c1a-e8ba-4391-a958-38c3ad81d18f}', u'timestamp': u'2018-05-18 16:28:30'}]
Number Of Sections	6
Trid	[[43.5, u'Win32 Dynamic Link Library (generic)'], [29.8, u'Win32 Executable (generic)'], [13.2, u'Generic Win/DOS Executable'], [13.2, u'DOS Executable Generic']]
Compilation Time Stamp	0x5582C5E4 [Thu Jun 18 13:21:40 2015 UTC]
Translation	0x0409 0x04b0
Entry Point	0x401930 (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	153952
Ssdeep	3072:w3bgfEhr1tBY1Fhx+Osbk1+XWd/2wnFfrpo7iLmZwIUmy:wbf5sPh00SWRnFDeyQrs
Sha256	9c710b420d66e79faa56e54b268baaa443ca17fba645dd4e57a81ad137ba227f
Exifinfo	[{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/2/e/e/1/2ee131baf9fd1e163bde6124d6137c050fcc98b4', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2018:05:18 15:50:19+00:00', u'EXE:InitializedDataSize': 135168, u'File:FileModifyDate': u'2018:05:18 15:50:19+00:00', u'EXE:FileVersionNumber': u'6.1.7600.16385', u'File:FileSize': u'150 kB', u'EXE:MachineType': u'Intel 386 or later, and compatibles', u'EXE:FileOS': u'Windows NT 32-bit', u'EXE:ObjectFileType': u'Dynamic link library', u'File:FileType': u'Win32 EXE', u'EXE:UninitializedDataSize': 0, u'File:FileName': u'2ee131baf9fd1e163bde6124d6137c050fcc98b4', u'EXE:ImageVersion': 0.0, u'File:FileTypeExtension': u'exe', u'EXE:OSVersion': 5.0, u'EXE:PEType': u'PE32', u'EXE:TimeStamp': u'2015:06:18 13:21:40+00:00', u'EXE:FileFlagsMask': u'0x003f', u'EXE:LinkerVersion': 24.0, u'EXE:FileFlags': u'(none)', u'EXE:Subsystem': u'Windows GUI', u'File:Directory': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/2/e/e/1', u'EXE:EntryPoint': u'0x1930', u'EXE:SubsystemVersion': 5.0, u'EXE:CodeSize': 16384, u'File:FileInodeChangeDate': u'2018:05:18 15:50:19+00:00', u'ExifTool:ExifToolVersion': 10.1, u'EXE:ProductVersionNumber': u'6.1.7600.16385'}]
Mime Type	application/x-dosexec
Imphash	086ab08e2c86bb86fe2a7558519aa3cb

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x305c	0x4000	5.26702667311	bf8bb80592ead51f993c345eb2111603
.rdata	0x5000	0xbd18	0xc000	7.68360921167	6e7c6c88de8cece45ad74eaef20b916f
.data	0x11000	0x3594	0x2000	3.83240677943	1eabb671188283a21c184d5ebe0bbf57
.code	0x15000	0xaa3e	0xb000	7.65237799164	8d2ca4ebf08a6a5c8ab2036f59b278c3
.crt	0x20000	0x3572	0x4000	6.95833617392	acda9f9dccdedc44f9b650f6f82036d9
.rsrc	0x24000	0x1930	0x2000	4.26324944076	c87397c4e46b66b0133cea036898ffc9

PE Imports

- NETAPI32.dll
  - NetGetAnyDCName
- CRYPT32.dll
  - CryptMsgDuplicate
- SETUPAPI.dll
  - SetupGetStringFieldA
- GDI32.dll
  - GetRgnBox
  - IntersectClipRect
  - GetEnhMetaFileDescriptionA
- USER32.dll
  - UnionRect
  - DdeGetLastError
  - GetAncestor
  - GetInputState
- KERNEL32.dll
  - MoveFileW
  - GetSystemInfo
  - CancelIoEx
  - GetProcessVersion
  - WritePrivateProfileStructA
  - SetCommTimeouts
- msvcrt.dll
  - fputs
- WININET.dll
  - HttpEndRequestW

PE Resources

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 150560, u'sha256': u'd77cc718990aaff88d58f8a0d7c517f7b4cf90ae4a6b292351224c71eb65ae75', u'type': u'data', u'size': 2440}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 147808, u'sha256': u'cb58180d2d4b0b405daaa4e957d56946a041601ae9084a5c00b69cb9b2d53f76', u'type': u'data', u'size': 2094}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 149904, u'sha256': u'b7d508d99d999ad4edb64404ec9a86fd206911cb462c66285264b7edcaebca4f', u'type': u'data', u'size': 586}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_ICON', u'offset': 150496, u'sha256': u'bb1523613848d859f9af07f321acb4513471bec8fc1b1161710679368398f630', u'type': u'MS Windows icon resource - 4 icons, 48x48', u'size': 62}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_VERSION', u'offset': 153000, u'sha256': u'e9dcd0ea179b0aa0eff363de51adf0d8d065ebf9e8c43b336a17b3b52526b11f', u'type': u'data', u'size': 904}

CERTIFICATE VALIDATION

- SubjectCertificateRevoked ✖

[+] All Media, SIA	
Status	Revoked ✖
Start Date	2018-04-03 03:00:00
End Date	2019-03-31 01:59:59
Sha256	8f55bde3986a9c93aed512512cbc594bf11465371f52c411247a8d598a56d149
Serial	475AEA339356AD6F09E07E96A723935D
Subject Key Identifier	66 5b 30 69 f3 fc 9c 79 c6 de 0c 02 4f 8b c1 80 1b 22 27 7d
Issuer Name	COMODO RSA Code Signing CA
Issuer Key Identifier	29 91 60 ff 8a 4d fa eb f9 a6 6a b8 cf f9 e6 4b bd 49 ce 12
Crl link	http://crl.comodoca.com/COMODORSACodeSigningCA.crl
Key Usage	Digital Signature (80)
Extended Usage	Code Signing (1.3.6.1.5.5.7.3.3)

[+] COMODO RSA Code Signing CA	
Status	NoError ✔
Start Date	2013-05-09 03:00:00
End Date	2028-05-09 02:59:59
Sha256	be4b37864cefc39611d4b6a1de110074e5f282de90016aa5d36849ab452eab2c
Serial	2E7C87CC0E934A52FE94FD1CB7CD34AF
Subject Key Identifier	29 91 60 ff 8a 4d fa eb f9 a6 6a b8 cf f9 e6 4b bd 49 ce 12
Issuer Name	COMODO RSA Certification Authority
Issuer Key Identifier	bb af 7e 02 3d fa a6 f1 3c 84 8e ad ee 38 98 ec d9 32 32 d4
Crl link	http://crl.comodoca.com/COMODORSACertificationAuthority.crl
Key Usage	Digital Signature,Certificate Signing,Off-line CRL Signing,CRL Signing (86)
Extended Usage	Code Signing (1.3.6.1.5.5.7.3.3)

[+] COMODO RSA Certification Authority	
Status	NoError ✔
Start Date	2010-01-19 02:00:00
End Date	2038-01-19 01:59:59
Sha256	f1bc8293a80c7d1bb2fd1d6e9b714b06e6b66686ca9b26a76d91e06e2934fa83
Serial	4CAAF9CADB636FE01FF74ED85B03869D
Subject Key Identifier	bb af 7e 02 3d fa a6 f1 3c 84 8e ad ee 38 98 ec d9 32 32 d4
Issuer Name	COMODO RSA Certification Authority
Issuer Key Identifier	undefined
Crl link	undefined
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	undefined

[+] GlobalSign Timestamping CA - G2	
Status	NoError ✔
Start Date	2011-04-13 13:00:00
End Date	2028-01-28 14:00:00
Sha256	0f870989c6b1f8082f91361833e8a61864a760c50594398911ffe34531cd1065
Serial	0400000000012F4EE152D7
Subject Key Identifier	46 d8 3e ff dc e3 be ff 83 e6 f4 85 9b b0 dd 6a d6 14 a9 c1
Issuer Name	GlobalSign Root CA
Issuer Key Identifier	60 7b 66 1a 45 0d 97 ca 89 50 2f 7d 04 cd 34 a8 ff fc fd 4b
Crl link	http://crl.globalsign.net/root.crl
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	undefined

[+] GlobalSign Root CA	
Status	NoError ✔
Start Date	1998-09-01 15:00:00
End Date	2028-01-28 14:00:00
Sha256	8890262a3cd37c0b6c37c0239b9533f33244fb4ec82b6d846f6bd379ed2184b7
Serial	040000000001154B5AC394
Subject Key Identifier	60 7b 66 1a 45 0d 97 ca 89 50 2f 7d 04 cd 34 a8 ff fc fd 4b
Issuer Name	GlobalSign Root CA
Issuer Key Identifier	undefined
Crl link	undefined
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	undefined

SCREENSHOTS