VALKYRIE COMODO

Summary

File Name: primopdfsetup.exe

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

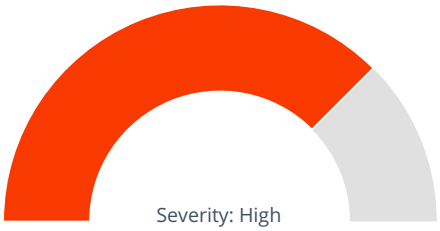
SHA1: 5732b93642462b9c529ac1888286d778f044f6b1

MD5: d7a9a897aa8a40bf3017356782de442d

MALWARE

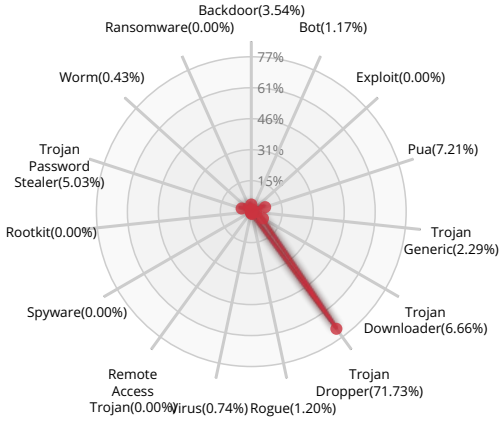
Valkyrie Final Verdict

DETECTION SECTION

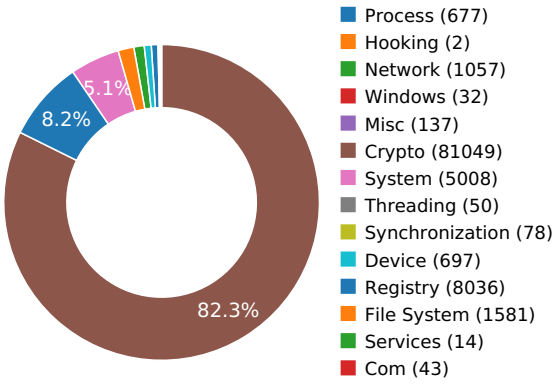


Verdict: Malware

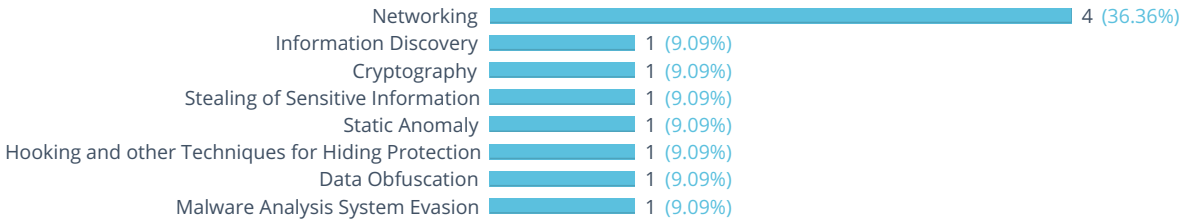
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



VALKYRIE COMODO

Activity Details

INFORMATION DISCOVERY

Reads data out of its own binary image	Show sources

NETWORKING

Attempts to connect to a dead IP:Port (14 unique times)	Show sources
HTTP traffic contains suspicious features which may be indicative of malware related traffic	Show sources
Performs some HTTP requests	Show sources
Network activity contains more than one unique useragent.	Show sources

CRYPTOGRAPHY

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

STEALING OF SENSITIVE INFORMATION

Attempts to modify proxy settings

STATIC ANOMALY

Anomalous binary characteristics	Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory	Show sources

DATA OBFUSCATION

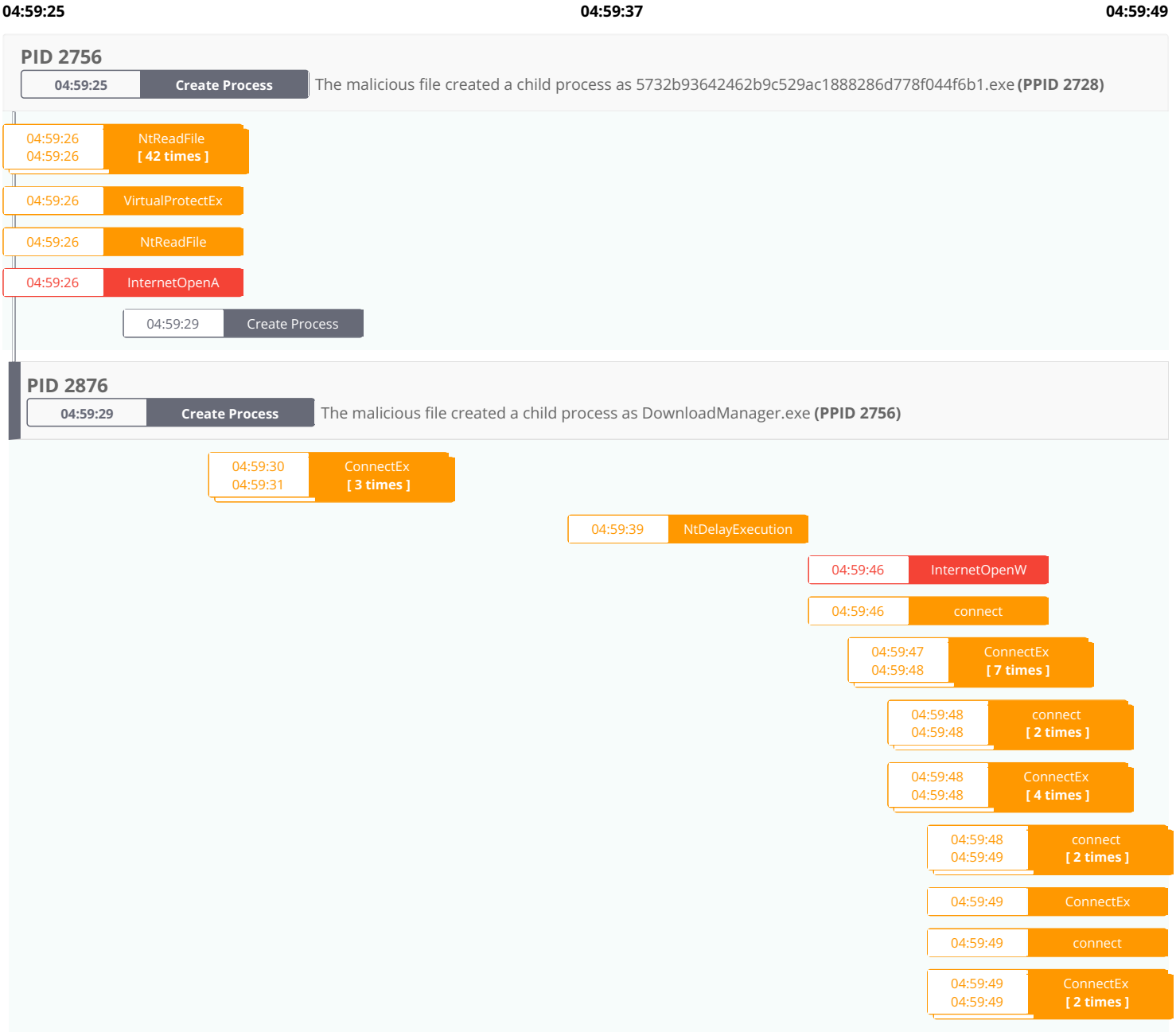
Drops a binary and executes it	Show sources

MALWARE ANALYSIS SYSTEM EVASION

A process attempted to delay the analysis task. Show sources

VALKYRIE COMODO

Behavior Graph



VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

\Device\KsecDD
C:\Users\user\AppData\Local\Temp\SHFOLDER.DLL
C:\Windows\System32\shfolder.dll
\??\MountPointManager
C:\Users\user\AppData\Local\Temp\
C:\Users\user\AppData\Local\Temp
C:\Users\user\AppData\Local\Temp\nskA722.tmp
C:\Users\user\AppData\Local\Temp\5732b93642462b9c529ac1888286d778f044f6b1.exe
C:\Users\user\AppData\Local\Temp\nsfA752.tmp
C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Local
C:\Users\user\AppData\Local\Temp\nsfA752.tmp\UserInfo.dll
C:\Users\user\AppData\Local\Temp\nsfA752.tmp\pwgen.dll
C:\Users\user\AppData\Local\Temp\DM_yDk9Jw0okW
C:\Users\user\AppData\Local\Temp\DM_yDk9Jw0okW\DownloadManager.exe
C:\Users\user\AppData\Local\Temp\nsfA752.tmp\System.dll
C:\Users\user\AppData\Local\Temp\nsvA7B1.tmp
C:\Users\user\AppData\Local\Temp\nsfA752.tmp\inetc.dll
C:\ProgramData\Microsoft\Network\Connections\Pbk\rasphone.pbk
C:\ProgramData\Microsoft\Network\Connections\Pbk*.pbk
C:\Windows\System32\ras*.pbk
C:\Users\user\AppData\Roaming\Microsoft\Network\Connections\Pbk\rasphone.pbk
C:\Users\user\AppData\Roaming\Microsoft\Network\Connections\Pbk*.pbk
C:\
C:\Users\user\AppData\Local\Temp\DM_yDk9Jw0okW*.*
C:\Users\user\AppData\Local\Temp\DM_yDk9Jw0okW\ApplicationDebug.log
C:\Users\user\AppData\Local\Temp\DM_yDk9Jw0okW\
C:\Users\user\AppData\Local\Temp\nsfA752.tmp*.*
C:\Users\user\AppData\Local\Temp\nsfA752.tmp\
C:\Windows\sysnative\MSCOREE.DLL.local

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscoreei.dll
C:\Windows\Microsoft.NET\Framework64*
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\clr.dll
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorwks.dll
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clr.dll
C:\Users\user\AppData\Local\Temp\DM_yDk9Jw0okW\DownloadManager.exe.config
C:\Users\user\AppData\Local\Temp\DM_yDk9Jw0okW\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\sysnative\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\system\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\ProgramData\Oracle\Java\javapath\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\sysnative\wbem\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\sysnative\WindowsPowerShell\v1.0\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Program Files\Microsoft Network Monitor 3\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Program Files (x86)\Universal Extractor\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Program Files (x86)\Universal Extractor\bin\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Program Files (x86)\Windows Kits\8.1\Windows Performance Toolkit\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Python27\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Python27\Scripts\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\tools\sysinternals\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\tools\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\tools\IDA_Pro_v6\python\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Users\user\AppData\Local\Temp\DM_yDk9Jw0okW\DownloadManager.exe.Local\
C:\Windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_88df89932faf0bf6
C:\Windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_88df89932faf0bf6\msvcr80.dll
C:\Windows
C:\Windows\winsxs
C:\Windows\Microsoft.NET\Framework64\v4.0.30319
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\fusion.localgac
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\security.config
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\security.config.cch
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\enterprisesec.config
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\enterprisesec.config.cch
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\64bit\security.config

C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\64bit\security.config.cch
C:\Windows\assembly\NativeImages_v2.0.50727_64\index142.dat
C:\Windows\assembly\NativeImages_v2.0.50727_64\mscorlib\9469491f37d9c35b596968b206615309\mscorlib.ni.dll
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.INI
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorsec.dll
C:\Windows\winsxs\amd64_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_a4d6a923711520a9
C:\Windows\winsxs\amd64_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_a4d6a923711520a9\comctl32.dll
C:\Windows\sysnative\p2pcollab.dll
C:\Windows\sysnative\QAGENTRT.DLL

READ REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\UseFilter
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\UserInfo.dll
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\pwgen.dll
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\System.dll
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\CurrentVersion
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\crypt32\DebugHeapFlags
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\DisableImprovedZoneCheck
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Security_HKLM_only
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\inetc.dll
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{26656EAA-54EB-4E6F-8F85-4F0EF901A406}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{8A40A45D-055C-4B62-ABD7-6D613E2CEAEC}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{55272A00-42CB-11CE-8135-00AA004BB851}\ProxyStubClsid32\(Default)

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\InprocServer32\InprocServer32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\InprocServer32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\InprocServer32\ThreadingModel
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{BCD1DE7E-2DB1-418B-B047-4A74E101F8C1}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{2A1C9EB2-DF62-4154-B800-63278FCB8037}\ProxyStubClsid32\(Default)
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecision
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecisionTime
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\WpadExpirationDays
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\WpadLastNetwork
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoProxyDetectType
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\5732b93642462b9c529ac1888286d778f044f6b1_RASAPI32\EnableFileTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\5732b93642462b9c529ac1888286d778f044f6b1_RASAPI32\FileTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\5732b93642462b9c529ac1888286d778f044f6b1_RASAPI32\EnableConsoleTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\5732b93642462b9c529ac1888286d778f044f6b1_RASAPI32\ConsoleTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\5732b93642462b9c529ac1888286d778f044f6b1_RASAPI32\MaxFileSize
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\5732b93642462b9c529ac1888286d778f044f6b1_RASAPI32\FileDirectory
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\5732b93642462b9c529ac1888286d778f044f6b1_RASMANCS\EnableFileTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\5732b93642462b9c529ac1888286d778f044f6b1_RASMANCS\FileTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\5732b93642462b9c529ac1888286d778f044f6b1_RASMANCS\EnableConsoleTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\5732b93642462b9c529ac1888286d778f044f6b1_RASMANCS\ConsoleTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\5732b93642462b9c529ac1888286d778f044f6b1_RASMANCS\MaxFileSize
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\5732b93642462b9c529ac1888286d778f044f6b1_RASMANCS\FileDirectory
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\ProgramData
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\AppData
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2298303332-66077612-2598613238-1000\ProfileImagePath
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\InstallRoot
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\CLRLoadLogDir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\UseLegacyV2RuntimeActivationPolicyDefaultValue
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\OnlyUseLatestCLR
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NoClientChecks
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\GCStressStart

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\GCStressStartAtJit
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\DisableConfigCache
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\CacheLocation
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\DownloadCacheQuotaInKB
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\EnableLog
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\LoggingLevel
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\ForceLog
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\LogFailures
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\VersioningLog
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\LogResourceBinds
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\UseLegacyIdentityFormat
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\DisableMSIPeek
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DevOverrideEnable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\LatestIndex
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\index142\NIUsageMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\index142\ILUsageMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\ConfigMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_64\NI\181938c6\7950e2c5\82\ConfigString

MODIFIED FILES

C:\Users\user\AppData\Local\Temp\nsfA752.tmp\UserInfo.dll
C:\Users\user\AppData\Local\Temp\nsfA752.tmp\pwgen.dll
C:\Users\user\AppData\Local\Temp\DM_yDk9Jw0okW\DownloadManager.exe
C:\Users\user\AppData\Local\Temp\nsfA752.tmp\System.dll
C:\Users\user\AppData\Local\Temp\nsfA752.tmp\inetc.dll
C:\Users\user\AppData\Local\Temp\nsvA7B1.tmp
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\7D266D9E1E69FA1EEFB9699B009B34C8_1D5A876A9113EC07224C45E5A870E3BD
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\7D266D9E1E69FA1EEFB9699B009B34C8_1D5A876A9113EC07224C45E5A870E3BD
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\B3BB9C1BA2D19E090AE305B2683903A0_608E9093E4033CB74CFDFDB1E83A5BC5
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\B3BB9C1BA2D19E090AE305B2683903A0_608E9093E4033CB74CFDFDB1E83A5BC5
C:\Users\user\AppData\Local\Temp\DM_yDk9Jw0okW\ApplicationDebug.log
C:\Users\user\AppData\Local\GDIPFONTCACHEV1.DAT

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\index.dat

C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\070E0202839D9D67350CD2613E78E416

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\070E0202839D9D67350CD2613E78E416

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

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

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\B66240B0F6C84BD4857ABA60CF5CE4A0_5043E0F5DF723415C9EECC201C838A62

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\B66240B0F6C84BD4857ABA60CF5CE4A0_5043E0F5DF723415C9EECC201C838A62

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\6A2279C2CA42EBEE26F14589F0736E50

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\6A2279C2CA42EBEE26F14589F0736E50

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\BAD725C80F9E10846F35D039A996E4A8_88B6AE015495C1ECC395D19C1DD02894

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\BAD725C80F9E10846F35D039A996E4A8_88B6AE015495C1ECC395D19C1DD02894

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\75CA58072B9926F763A91F0CC2798706_93E4B2BA79A897B3100CCB27F2D3BF4F

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\75CA58072B9926F763A91F0CC2798706_93E4B2BA79A897B3100CCB27F2D3BF4F

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\FC5A820A001B41D68902E051F36A5282_E98D75262B3D5D962FC8706E05221C8A

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\FC5A820A001B41D68902E051F36A5282_E98D75262B3D5D962FC8706E05221C8A

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\v2[1].txt

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\8828F39C7C0CE9A14B25C7EB321181BA_BD8B98368542C3BBAE3413A0EF3BB623

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\8828F39C7C0CE9A14B25C7EB321181BA_BD8B98368542C3BBAE3413A0EF3BB623

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\3FA0F92EA40DC353FF9E95B9F7D06EAF_02A7BB8D663AB0A2D3E0CE44422ED38B

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\3FA0F92EA40DC353FF9E95B9F7D06EAF_02A7BB8D663AB0A2D3E0CE44422ED38B

C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012018080720180808\index.dat

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\0DA515F703BB9B49479E8697ADB0B955_7DC3E633EDFAEFC3AA3C99552548EC2F

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\0DA515F703BB9B49479E8697ADB0B955_7DC3E633EDFAEFC3AA3C99552548EC2F

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\nr-1071.min[1].js

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\B398B80134F72209547439DB21AB308D_9487BC0D4381A7CDEB9A8CC43F66D27C

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\B398B80134F72209547439DB21AB308D_9487BC0D4381A7CDEB9A8CC43F66D27C

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\4344B8AF97AF3A423D9EE52899963CDE_6BF99D49F7848CB4DF1BBF4D7AE05358

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\4344B8AF97AF3A423D9EE52899963CDE_6BF99D49F7848CB4DF1BBF4D7AE05358

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\b9d332c3e7[1]

RESOLVED APIS

cryptbase.dll.SystemFunction036

uxtheme.dll.ThemeInitApiHook

user32.dll.IsProcessDPIAware
shfolder.dll.SHGetFolderPathA
setupapi.dll.CM_Get_Device_Interface_List_Size_ExW
setupapi.dll.CM_Get_Device_Interface_List_ExW
kernel32.dll.GetUserDefaultUILanguage
userinfo.dll.GetAccountType
advapi32.dll.CheckTokenMembership
pwgen.dll.GeneratePassword
cryptsp.dll.CryptAcquireContextA
cryptsp.dll.CryptGenRandom
cryptsp.dll.CryptReleaseContext
system.dll.Alloc
system.dll.Call
ole32.dll.CoCreateGuid
ole32.dll.StringFromGUID2
kernel32.dll.WideCharToMultiByte
system.dll.Free
kernel32.dll.GetSystemDefaultLangID
kernel32.dll.GetLocaleInfoA
user32.dll.GetSystemMetrics
user32.dll.GetWindowDC
gdi32.dll.GetDeviceCaps
inetc.dll.get
dwmapi.dll.DwmIsCompositionEnabled
comctl32.dll.RegisterClassNameW
wininet.dll.FtpCommandA
rasapi32.dll.RasConnectionNotificationW
sechost.dll.NotifyServiceStatusChangeA
ole32.dll.CoInitializeEx
advapi32.dll.RegDeleteTreeA
advapi32.dll.RegDeleteTreeW
ole32.dll.CoCreateInstance
ole32.dll.CoTaskMemAlloc
oleaut32.dll.#8
oleaut32.dll.#9

oleaut32.dll.DllGetClassObject
oleaut32.dll.DllCanUnloadNow
advapi32.dll.RegOpenKeyW
ole32.dll.CoTaskMemFree
ole32.dll.StringFromIID
iphlpapi.dll.GetAdaptersAddresses
dhcpcsvc.dll.DhcpRequestParams
oleaut32.dll.#2
oleaut32.dll.#6
ole32.dll.CoUninitialize
oleaut32.dll.#500
ole32.dll.CoRevokeInitializeSpy
comctl32.dll.#388
rpcrt4.dll.RpcBindingFree
advapi32.dll.UnregisterTraceGuids
comctl32.dll.#321
advapi32.dll.RegOpenKeyExW
advapi32.dll.RegQueryInfoKeyW
advapi32.dll.RegEnumKeyExW
advapi32.dll.RegEnumValueW
advapi32.dll.RegCloseKey
advapi32.dll.RegQueryValueExW
kernel32.dll.FlsAlloc
kernel32.dll.FlsFree
kernel32.dll.FlsGetValue
kernel32.dll.FlsSetValue
kernel32.dll.InitializeCriticalSectionEx
kernel32.dll.CreateEventExW
kernel32.dll.CreateSemaphoreExW
kernel32.dll.SetThreadStackGuarantee
kernel32.dll.CreateThreadpoolTimer
kernel32.dll.SetThreadpoolTimer
kernel32.dll.WaitForThreadpoolTimerCallbacks
kernel32.dll.CloseThreadpoolTimer

kernel32.dll.CreateThreadpoolWait
kernel32.dll.SetThreadpoolWait
kernel32.dll.CloseThreadpoolWait
kernel32.dll.FlushProcessWriteBuffers
kernel32.dll.FreeLibraryWhenCallbackReturns

DELETED FILES

C:\Users\user\AppData\Local\Temp\nskA722.tmp
C:\Users\user\AppData\Local\Temp\nsfA752.tmp
C:\Users\user\AppData\Local\Temp\nsvA7B1.tmp
C:\Users\user\AppData\Local\Temp\DM_yDk9Jw0okW\ApplicationDebug.log
C:\Users\user\AppData\Local\Temp\DM_yDk9Jw0okW\DownloadManager.exe
C:\Users\user\AppData\Local\Temp\DM_yDk9Jw0okW\
C:\Users\user\AppData\Local\Temp\nsfA752.tmp\inetc.dll
C:\Users\user\AppData\Local\Temp\nsfA752.tmp\pwgen.dll
C:\Users\user\AppData\Local\Temp\nsfA752.tmp\System.dll
C:\Users\user\AppData\Local\Temp\nsfA752.tmp\UserInfo.dll
C:\Users\user\AppData\Local\Temp\nsfA752.tmp\
C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012016042520160426\index.dat
C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012016042520160426\
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\security.config.cch.2876.36832703
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\enterprisesec.config.cch.2876.36832703
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\64bit\security.config.cch.2876.36832718

DELETED REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL

REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\UseFilter
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\UserInfo.dll
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\pwgen.dll
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NET Framework Setup\NDP\v2.0.50727
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\System.dll
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\CurrentVersion
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\crypt32
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\crypt32\DebugHeapFlags
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\DisableImprovedZoneCheck
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Security_HKLM_only
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\inetc.dll
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale\Alternate Sorts
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Language Groups
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_CURRENT_USER
HKEY_CURRENT_USER\Software\Classes

HKEY_CURRENT_USER\Software\Classes\Interface\{26656EAA-54EB-4E6F-8F85-4F0EF901A406}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{26656EAA-54EB-4E6F-8F85-4F0EF901A406}\ProxyStubClsid32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{26656EAA-54EB-4E6F-8F85-4F0EF901A406}\ProxyStubClsid32\(Default)
HKEY_CURRENT_USER\Software\Classes\Interface\{8A40A45D-055C-4B62-ABD7-6D613E2CEAEC}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{8A40A45D-055C-4B62-ABD7-6D613E2CEAEC}\ProxyStubClsid32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{8A40A45D-055C-4B62-ABD7-6D613E2CEAEC}\ProxyStubClsid32\(Default)
HKEY_CURRENT_USER\Software\Classes\Interface\{55272A00-42CB-11CE-8135-00AA004BB851}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{55272A00-42CB-11CE-8135-00AA004BB851}\ProxyStubClsid32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{55272A00-42CB-11CE-8135-00AA004BB851}\ProxyStubClsid32\(Default)
HKEY_CURRENT_USER\Software\Classes\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\TreatAs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\Progid
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\Progid
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\InprocServer32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\InprocServer32\InprocServer32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\InprocServer32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\InprocServer32\ThreadingModel
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\InprocHandler32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{B196B286-BAB4-101A-B69C-00AA00341D07}\InprocHandler
HKEY_LOCAL_MACHINE\Software\Microsoft\OleAut
HKEY_CURRENT_USER\Software\Classes\Interface\{BCD1DE7E-2DB1-418B-B047-4A74E101F8C1}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{BCD1DE7E-2DB1-418B-B047-4A74E101F8C1}\ProxyStubClsid32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{BCD1DE7E-2DB1-418B-B047-4A74E101F8C1}\ProxyStubClsid32\(Default)
HKEY_CURRENT_USER\Software\Classes\Interface\{2A1C9EB2-DF62-4154-B800-63278FCB8037}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{2A1C9EB2-DF62-4154-B800-63278FCB8037}\ProxyStubClsid32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{2A1C9EB2-DF62-4154-B800-63278FCB8037}\ProxyStubClsid32\(Default)
HKEY_CURRENT_USER\Software\Microsoft\windows\CurrentVersion\Internet Settings\Wpad
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecision
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecisionTime
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\WpadExpirationDays
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\WpadLastNetwork
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoProxyDetectType
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-

A8A2D5F46E6B}\WpadDecisionReason
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadNetworkName
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecisionReason
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecisionTime
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecision
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\0a-00-27-00-00-00

READ FILES

\Device\KsecDD
C:\Windows\System32\shfolder.dll
C:\Users\user\AppData\Local\Temp\nskA722.tmp
C:\Users\user\AppData\Local\Temp\5732b93642462b9c529ac1888286d778f044f6b1.exe
C:\Users\user\AppData\Local\Temp\nsfA752.tmp
C:\Users\user\AppData\Local\Temp\nsfA752.tmp\UserInfo.dll
C:\Users\user\AppData\Local\Temp\nsfA752.tmp\pwgen.dll
C:\Users\user\AppData\Local\Temp\nsfA752.tmp\System.dll
C:\Users\user\AppData\Local\Temp\nsvA7B1.tmp
C:\Users\user\AppData\Local\Temp\nsfA752.tmp\inetc.dll
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscoreei.dll
C:\Users\user\AppData\Local\Temp\DM_yDk9Jw0okW\DownloadManager.exe.config
C:\Users\user\AppData\Local\Temp\DM_yDk9Jw0okW\DownloadManager.exe
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorwks.dll
C:\Windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_88df89932faf0bf6\msvcr80.dll
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\security.config
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\security.config.cch
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\enterprisesec.config
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\enterprisesec.config.cch
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\64bit\security.config
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\64bit\security.config.cch
C:\Windows\assembly\NativeImages_v2.0.50727_64\index142.dat
C:\Windows\assembly\NativeImages_v2.0.50727_64\mscorlib\9469491f37d9c35b596968b206615309\mscorlib.ni.dll
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorsec.dll
C:\Windows\winsxs\amd64_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_a4d6a923711520a9\comctl32.dll

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\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\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\7D266D9E1E69FA1EEFB9699B009B34C8_1D5A876A9113EC07224C45E5A870E3BD
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\7D266D9E1E69FA1EEFB9699B009B34C8_1D5A876A9113EC07224C45E5A870E3BD
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\B3BB9C1BA2D19E090AE305B2683903A0_608E9093E4033CB74CFDFDB1E83A5BC5
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\B3BB9C1BA2D19E090AE305B2683903A0_608E9093E4033CB74CFDFDB1E83A5BC5
C:\Windows\sysnative\l_intl.nls
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorjit.dll

C:\Windows\assembly\pubpol20.dat
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\Culture.dll
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorrc.dll
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\sorttbls.nlp
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\sortkey.nlp
C:\Windows\assembly\NativeImages_v2.0.50727_64\System\adff7dd9fe8e541775c46b6363401b22\System.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Configuration\091b931d0f6408001747dbbbb05dbe66\System.Configuration.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Xml\ee795155543768ea67eecddc686a1e9e\System.Xml.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Drawing\5910828a337dbe848dc90c7ae0a7dee2\System.Drawing.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Windows.Forms\6c352ff9e3603b0e69d969ff7e7632f5\System.Windows.Forms.ni.dll
C:\Windows\assembly\GAC_MSIL\System.Windows.Forms\2.0.0.0__b77a5c561934e089\System.Windows.Forms.dll
C:\Windows\winsxs\amd64_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_2b24536c71ed437a\GdiPlus.dll
C:\Users\user\AppData\Local\GDIPFONTCACHEV1.DAT
C:\Windows\Fonts\tahoma.ttf
C:\Windows\Fonts\msjh.ttf

MUTEXES

IESQMMUTEX_0_208
Global\CLR_CASOFF_MUTEX
Local\WininetStartupMutex
Local_!MSFTHISTORY!_
Local\c:!users!user!appdata!local!microsoft!windows!temporary internet files!content.ie5!
Local\c:!users!user!appdata!roaming!microsoft!windows!cookies!
Local\c:!users!user!appdata!local!microsoft!windows!history!history.ie5!
Local\WininetConnectionMutex
Local\WininetProxyRegistryMutex
Local\ZonesCounterMutex
Local\ZoneAttributeCacheCounterMutex
Local\ZonesCacheCounterMutex
Local\ZonesLockedCacheCounterMutex
Local\!IETld!Mutex
CicLoadWinStaWinSta0
Local\MSCTF.CtfMonitorInstMutexDefault1
!SHMSFTHISTORY!
Local\c:!users!user!appdata!local!microsoft!windows!history!history.ie5!mshist012018080720180808!

DBWinMutex

Global\.net clr networking

MODIFIED REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecisionReason

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecisionTime

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecision

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadNetworkName

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecisionReason

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecisionTime

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecision

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\WpadLastNetwork

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

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012018080720180808

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012018080720180808\CachePath

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012018080720180808\CachePrefix

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012018080720180808\CacheLimit

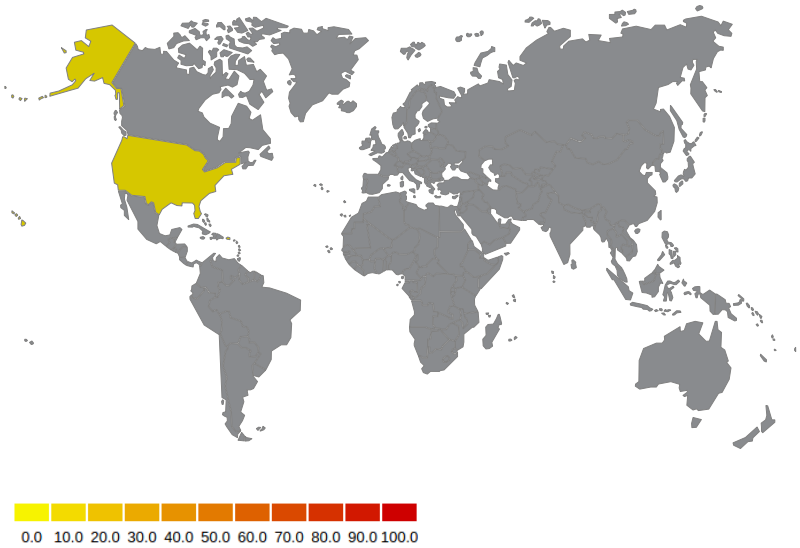
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012018080720180808\CacheOptions

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012018080720180808\CacheRepair

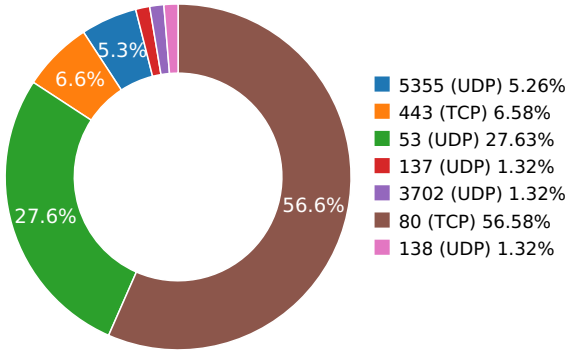
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\WindowsSearch\Version

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
	151.101.2.110	United States	54113	Fastly	Malware Process
	151.101.2.133	United States	54113	Fastly	Malware Process
	162.247.242.20	United States	23467	New Relic	Malware Process
	172.217.10.142	United States	15169	Google LLC	Malware Process
	184.26.44.97	United States	20940	Akamai Technologies, Inc.	OS Process
	184.26.44.98	United States	20940	Akamai Technologies, Inc.	OS Process
	52.85.98.129	United States	16509	Amazon Technologies Inc.	Malware Process
	52.85.98.136	United States	16509	Amazon Technologies Inc.	Malware Process
	52.85.98.18	United States	16509	Amazon Technologies Inc.	Malware Process
	52.85.98.251	United States	16509	Amazon Technologies Inc.	Malware Process
	52.85.98.27	United States	16509	Amazon Technologies Inc.	Malware Process
	52.85.98.91	United States	16509	Amazon Technologies Inc.	Malware Process
api.xtrdlapi.com	54.76.182.212	Ireland	16509	Amazon Technologies Inc.	Malware Process
crl.microsoft.com	208.185.118.88	United States	6461	Zayo Bandwidth	OS Process
s.symcd.com	23.4.187.27	United States	16625	Akamai Technologies, Inc.	Malware Process
crl.globalsign.net	151.101.22.133	United States	54113	Fastly	Malware Process
s.ss2.us	52.84.31.183	United States	16509	Amazon Technologies Inc.	Malware Process
evcs-ocsp.ws.symantec.com	23.4.187.27	United States	16625	Akamai Technologies, Inc.	Malware Process
ocsp.sca1b.amazontrust.com	52.84.31.246	United States	16509	Amazon Technologies Inc.	Malware Process
d1gx3pzah7uolr.cloudfront.net	13.35.87.220	United States	16509	Amazon Technologies Inc.	Malware Process
bam.nr-data.net	162.247.242.19	United States	23467	New Relic	Malware Process
ocsp.verisign.com	23.4.187.27	United States	16625	Akamai Technologies, Inc.	Malware Process

Name	IP	Country	ASN	ASN Name	Trigger Process Type
js-agent.newrelic.com	151.101.22.110	United States	54113	Fastly	Malware Process
ocsp.rootca1.amazontrust.com	52.84.31.141	United States	16509	Amazon Technologies Inc.	Malware Process
o.ss2.us	52.84.31.52	United States	16509	Amazon Technologies Inc.	Malware Process
ocsp.globalsign.com	151.101.22.133	United States	54113	Fastly	Malware Process
ocsp.rootg2.amazontrust.com	52.84.31.141	United States	16509	Amazon Technologies Inc.	Malware Process
ocsp.digicert.com	72.21.91.29	United States	15133	MCI Communications Servic...	Malware Process
x.ss2.us	52.84.31.31	United States	16509	Amazon Technologies Inc.	Malware Process
ctldl.windowsupdate.com	208.185.118.89	United States	6461	Zayo Bandwidth	OS Process
www.google-analytics.com	172.217.6.238	United States	15169	Google LLC	Malware Process
status.geotrust.com	72.21.91.29	United States	15133	MCI Communications Servic...	Malware Process

HTTP PACKETS

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
www.google-analytics.com	80	GET	1.1	Mozilla/4.0 (compatible; en..	1	12.7160959244
Path: /__utm.gif?utmwv=5.3.6&utmhn=&utmr=-&utmp=&utmac=UA-44288146-1&utmcc=__utma%3D999.999.999.999.999.1%3B&utms=1&utmvid=0xEB9CD1823A0C473C&guid=on&utmt=event&utme=5(DownloadManager*NET%20Framework*Installed)&utmsr=800x600&utmsc=32-bit **URI:** http://www.google-analytics.com/__utm.gif?utmwv=5.3.6&utmhn=&utmr=-&utmp=&utmac=UA-44288146-1&utmcc=__utma%3D999.999.999.999.999.1%3B&utms=1&utmvid=0xEB9CD1823A0C473C&guid=on&utmt=event&utme=5(DownloadManager*NET%20Framework*Installed)&utmsr=800x600&utmsc=32-bit						
ctldl.windowsupdate.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	14.6860868931
Path: /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?d3cfbfcef0ceddab **URI:** http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?d3cfbfcef0ceddab						
ocsp.verisign.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	14.9629428387
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBS56bKHAoUD%2BOyl%2B0LhPg9JxyQm4gQUf9Nlp8Ld7LvwMAnzQzn6Aq8zMTMCEGxZ76nhAOEO4wa6j%2BApJVk%3D **URI:** http://ocsp.verisign.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBS56bKHAoUD%2BOyl%2B0LhPg9JxyQm4gQUf9Nlp8Ld7LvwMAnzQzn6Aq8zMTMCEGxZ76nhAOEO4wa6j%2BApJVk%3D						
evcs-ocsp.ws.symantec.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	15.0978929996
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBQckPwgwK2Thdm9JYVwXQ4ERz3XDQQUo47PGUI9MeGrIYmEbcvZeaKysloCECLU1%2BUEK%2BnCmZywXEyiu08%3D **URI:** http://evcs-ocsp.ws.symantec.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQckPwgwK2Thdm9JYVwXQ4ERz3XDQQUo47PGUI9MeGrIYmEbcvZeaKysloCECLU1%2BUEK%2BnCmZywXEyiu08%3D						
x.ss2.us	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	31.0565438271
Path: /x.cer **URI:** http://x.ss2.us/x.cer						
ctldl.windowsupdate.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	31.2065768242
Path: /msdownload/update/v3/static/trustedr/en/authrootstl.cab?1e0d8ed553287452 **URI:** http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab?1e0d8ed553287452						
o.ss2.us	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	31.5011999607

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
Path: //MEowSDBGMEQwQjAJBgUrDgMCGgUABBSLwZ6EW5gdYc9UaSEaaLjjETNtkAQUv1%2B30c7dH4b0W1Ws3NcQwg6piOcCCQCnDkpMNIK3fw%3D%3D **URI:** http://o.ss2.us//MEowSDBGMEQwQjAJBgUrDgMCGgUABBSLwZ6EW5gdYc9UaSEaaLjjETNtkAQUv1%2B30c7dH4b0W1Ws3NcQwg6piOcCCQCnDkpMNIK3fw%3D%3D						
o.ss2.us	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	31.5584719181
Path: //MEowSDBGMEQwQjAJBgUrDgMCGgUABBSLwZ6EW5gdYc9UaSEaaLjjETNtkAQUv1%2B30c7dH4b0W1Ws3NcQwg6piOcCCQCnDkpMNIK3fw%3D%3D **URI:** http://o.ss2.us//MEowSDBGMEQwQjAJBgUrDgMCGgUABBSLwZ6EW5gdYc9UaSEaaLjjETNtkAQUv1%2B30c7dH4b0W1Ws3NcQwg6piOcCCQCnDkpMNIK3fw%3D%3D						
s.ss2.us	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	31.6614518166
Path: /r.crl **URI:** http://s.ss2.us/r.crl						
ocsp.rootg2.amazontrust.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	31.8453769684
Path: /MFQwUjBQME4wTDAJBgUrDgMCGgUABBSIfaREXmfqfJR3TkMYnD7O5MhzEgQUnF8A36oB1zArOIiiuG1KnPIRkYMCEwZ%2FlEoqJ83z%2BsKuKwH5CO65xMY%3D **URI:** http://ocsp.rootg2.amazontrust.com/MFQwUjBQME4wTDAJBgUrDgMCGgUABBSIfaREXmfqfJR3TkMYnD7O5MhzEgQUnF8A36oB1zArOIiiuG1KnPIRkYMCEwZ%2FlEoqJ83z%2BsKuKwH5CO65xMY%3D						
ocsp.rootca1.amazontrust.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	31.9718239307
Path: /MFQwUjBQME4wTDAJBgUrDgMCGgUABBRPWaOUU8%2B5VZ5%2Fa9jFTaU9pkK3FAQUhBjMhTTsvAyUlC4IWZzHshBOCggCEwZ%2FlFeFh%2Bisd96yUzJbvJmLVg0%3D **URI:** http://ocsp.rootca1.amazontrust.com/MFQwUjBQME4wTDAJBgUrDgMCGgUABBRPWaOUU8%2B5VZ5%2Fa9jFTaU9pkK3FAQUhBjMhTTsvAyUlC4IWZzHshBOCggCEwZ%2FlFeFh%2Bisd96yUzJbvJmLVg0%3D						
ocsp.sca1b.amazontrust.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	32.0945599079
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBQz9arGHWbnBV0DFzpNHz4YcTiFDQQUWaRmBlKge5WSPKOUByeWdFv5PdACEAnEcGcK1jMsIIACRqKgD8o%3D **URI:** http://ocsp.sca1b.amazontrust.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQz9arGHWbnBV0DFzpNHz4YcTiFDQQUWaRmBlKge5WSPKOUByeWdFv5PdACEAnEcGcK1jMsIIACRqKgD8o%3D						
s.symcd.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	2	32.5070137978
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBS56bKHAoUD%2BOyl%2B0LhPg9JxyQm4gQUf9Nlp8Ld7LvwMAnzQzn6Aq8zMTMCEGMYDTj7gJd4qdA1oxYY%2BEA%3D **URI:** http://s.symcd.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBS56bKHAoUD%2BOyl%2B0LhPg9JxyQm4gQUf9Nlp8Ld7LvwMAnzQzn6Aq8zMTMCEGMYDTj7gJd4qdA1oxYY%2BEA%3D						
ocsp.digicert.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	2	32.6113889217
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEWVxDlQQUTiJUIBiV5uNu5g%2F6%2BrkS7QYXjzkCEAyO4MkNaokViAQGHuJB%2Ba8%3D **URI:** http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEWVxDlQQUTiJUIBiV5uNu5g%2F6%2BrkS7QYXjzkCEAyO4MkNaokViAQGHuJB%2Ba8%3D						
ocsp.globalsign.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	33.1738929749
Path: /rootr1/ME8wTTBLMEkwRzAJBgUrDgMCGgUABBS3V7W2nAf4FiMTjpDJKg6%2BMgGqMQQUYHtmGkUNl8qJUC99BM00qP%2F8%2FUsCDkbwjNvPLFRm7zMB3V80 **URI:** http://ocsp.globalsign.com/rootr1/ME8wTTBLMEkwRzAJBgUrDgMCGgUABBS3V7W2nAf4FiMTjpDJKg6%2BMgGqMQQUYHtmGkUNl8qJUC99BM00qP%2F8%2FUsCDkbwjNvPLFRm7zMB3V80						
ocsp.digicert.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	33.4167149067

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAVG%2Fhgj9%2BGUHaOfzhTEYXM%3D **URI:** http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAVG%2Fhgj9%2BGUHaOfzhTEYXM%3D						
status.geotrust.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	33.5432939529
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBR3enuod9bxDxzpICGW%2B2sabjf17QQUkFj%2FsJx1qFFUd7Ht8qNDFjiebMUCEA1fNxT7Zt2V3O1CaWimmzM%3D **URI:** http://status.geotrust.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBR3enuod9bxDxzpICGW%2B2sabjf17QQUkFj%2FsJx1qFFUd7Ht8qNDFjiebMUCEA1fNxT7Zt2V3O1CaWimmzM%3D						
api.xtrdlapi.com	80	POST	1.1		1	34.0646388531
Path: /layout_exception.php?v=1.0.0.15962 **URI:** http://api.xtrdlapi.com/layout_exception.php?v=1.0.0.15962						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	47.345582962
Path: /pki/crl/products/tspca.crl **URI:** http://crl.microsoft.com/pki/crl/products/tspca.crl						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	47.7602009773
Path: /pki/crl/products/CodeSignPCA2.crl **URI:** http://crl.microsoft.com/pki/crl/products/CodeSignPCA2.crl						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	47.9836699963
Path: /pki/crl/products/WinPCA.crl **URI:** http://crl.microsoft.com/pki/crl/products/WinPCA.crl						
crl.globalsign.net	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	48.3301949501
Path: /primobject.crl **URI:** http://crl.globalsign.net/primobject.crl						

DNS QUERIES

Request	Type
www.google-analytics.com	A
Answers - www-google-analytics.l.google.com (CNAME) - 172.217.10.142 (A)	
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)	
ocsp.verisign.com	A
Answers - ocsp-ds.ws.symantec.com.edgekey.net (CNAME) - e8218.dscb1.akamaiedge.net (CNAME) - 23.4.187.27 (A)	
evcs-ocsp.ws.symantec.com	A

Request	Type
api.xtrdlapi.com	A
Answers - 54.76.182.212 (A) - xtrdlapi-vpc01-waf-1155237989.eu-west-1.elb.amazonaws.com (CNAME) - 54.171.217.47 (A)	
x.ss2.us	A
Answers - 52.85.98.94 (A) - 52.85.98.136 (A) - 52.85.98.207 (A) - 52.85.98.11 (A)	
o.ss2.us	A
Answers - 52.85.98.71 (A) - 52.85.98.15 (A) - 52.85.98.18 (A) - 52.85.98.85 (A)	
s.ss2.us	A
Answers - 52.85.98.50 (A) - 52.85.98.190 (A) - 52.85.98.251 (A) - 52.85.98.63 (A)	
ocsp.rootg2.amazontrust.com	A
Answers - 52.85.98.123 (A) - 52.85.98.91 (A) - 52.85.98.75 (A) - 52.85.98.148 (A)	
ocsp.rootca1.amazontrust.com	A
ocsp.sca1b.amazontrust.com	A
Answers - 52.85.98.129 (A) - 52.85.98.184 (A) - 52.85.98.189 (A) - 52.85.98.140 (A)	
d1gx3pzah7uolr.cloudfront.net	A
Answers - 52.85.98.117 (A) - 52.85.98.27 (A) - 52.85.98.135 (A)	
s.symcd.com	A
ocsp.digicert.com	A
Answers - cs9.wac.phicdn.net (CNAME) - 72.21.91.29 (A)	
js-agent.newrelic.com	A

Request	Type
Answers - 151.101.2.110 (A) - f4.shared.global.fastly.net (CNAME) - 151.101.194.110 (A) - 151.101.66.110 (A) - 151.101.130.110 (A)	
ocsp.globalsign.com	A
Answers - 151.101.66.133 (A) - 151.101.2.133 (A) - global.prd.cdn.globalsign.com (CNAME) - 151.101.194.133 (A) - 151.101.130.133 (A) - prod.globalsign.map.fastly.net (CNAME)	
bam.nr-data.net	A
Answers - 162.247.242.18 (A) - 162.247.242.20 (A) - 162.247.242.21 (A) - 162.247.242.19 (A)	
status.geotrust.com	A
Answers - ocsp.digicert.com (CNAME)	
crl.microsoft.com	A
Answers - 184.26.44.98 (A) - crl.www.ms.akadns.net (CNAME) - a1363.dscg.akamai.net (CNAME)	
crl.globalsign.net	A

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
12.7160959244	Sandbox	172.217.10.142	80
14.6860868931	Sandbox	184.26.44.97	80
14.9629428387	Sandbox	23.4.187.27	80
15.0978929996	Sandbox	23.4.187.27	80
30.6328628063	Sandbox	54.76.182.212	443
31.0565438271	Sandbox	52.85.98.136	80
31.2065768242	Sandbox	184.26.44.97	80
31.5011999607	Sandbox	52.85.98.18	80
31.6614518166	Sandbox	52.85.98.251	80
31.8453769684	Sandbox	52.85.98.91	80
31.9718239307	Sandbox	52.85.98.91	80
32.0945599079	Sandbox	52.85.98.129	80
32.3654639721	Sandbox	52.85.98.27	443
32.365888834	Sandbox	52.85.98.27	443
32.5070137978	Sandbox	23.4.187.27	80
32.5233919621	Sandbox	23.4.187.27	80
32.6113889217	Sandbox	72.21.91.29	80
32.6231398582	Sandbox	72.21.91.29	80
33.0464940071	Sandbox	151.101.2.110	443
33.1738929749	Sandbox	151.101.2.133	80
33.3054687977	Sandbox	162.247.242.20	443
33.4167149067	Sandbox	72.21.91.29	80
33.5432939529	Sandbox	72.21.91.29	80
34.0646388531	Sandbox	54.76.182.212	80
47.345582962	Sandbox	184.26.44.98	80
48.3301949501	Sandbox	151.101.2.133	80

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
6.90875887871	Sandbox	224.0.0.252	5355
6.91052389145	Sandbox	224.0.0.252	5355
6.92577290535	Sandbox	239.255.255.250	3702
6.94428801537	Sandbox	192.168.56.255	137
9.46007180214	Sandbox	224.0.0.252	5355
10.0733189583	Sandbox	224.0.0.252	5355
12.6673419476	Sandbox	8.8.4.4	53
12.9593119621	Sandbox	192.168.56.255	138
14.5094649792	Sandbox	8.8.4.4	53
14.9090378284	Sandbox	8.8.4.4	53
15.0382750034	Sandbox	8.8.4.4	53
30.4375557899	Sandbox	8.8.4.4	53
30.9786038399	Sandbox	8.8.4.4	53
31.4478979111	Sandbox	8.8.4.4	53
31.6092100143	Sandbox	8.8.4.4	53
31.7326710224	Sandbox	8.8.4.4	53
31.915968895	Sandbox	8.8.4.4	53
32.0332188606	Sandbox	8.8.4.4	53
32.2889239788	Sandbox	8.8.4.4	53
32.4625909328	Sandbox	8.8.4.4	53
32.470925808	Sandbox	8.8.4.4	53
32.5876438618	Sandbox	8.8.4.4	53
32.9989159107	Sandbox	8.8.4.4	53
33.12864995	Sandbox	8.8.4.4	53
33.2734029293	Sandbox	8.8.4.4	53
33.495721817	Sandbox	8.8.4.4	53
47.1940569878	Sandbox	8.8.4.4	53
48.2404429913	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\DM_yDk9Jw0okW\ApplicationDebug.Log	**Type :** ASCII text, with CRLF line terminators **MD5 :** c085d5451020159ec84ad5063d0faff7 **SHA-1 :** c32a9b21952ec1a2cb5dfffc8a6ddb0f5070692a **SHA-256 :** 5e82a976a9e3a193b2366954d94b8e919ab4d75 **SHA-512 :** 6deb0d3ca9c7368dfff5ac08da8d700debeda9c1(**Size :** 0.114 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\7D266D9E1E69FA1EEFB9699B009B34C8_1D5A876A9113EC07224C45E5A870E3BD	**Type :** data **MD5 :** 547178fdb77ad5c4c45b26d59000cf03 **SHA-1 :** 0d78b3681b84cfa1a9037df5c292b819a6fa3cd3 **SHA-256 :** 8199b723d52c0efc0c229f3bd9e5b04c112bf39b8 **SHA-512 :** 8e9b1e3168c5e8e451dc43211390beb1160043b **Size :** 1.754 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157	**Type :** Microsoft Cabinet archive data, 6509 bytes, 1 file **MD5 :** 33b39e2a516ef730a8fa922894f0fbd5 **SHA-1 :** 03d455583dda59215d945af76af6293b202f586f **SHA-256 :** 9446e8f2056fea3ac1365a809ada04602606242c **SHA-512 :** 75763aa13b43eb96294b0f84e13106611198872(**Size :** 6.509 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\FC5A820A001B41D68902E051F36A5282_E98D75262B3D5D962FC8706E05221C8A	**Type :** data **MD5 :** 8debb52d796ec3c66d821dd85883a64d **SHA-1 :** 7a35b6b8240bfdb156a078da17344de0fc81d3d0 **SHA-256 :** 95d11288275bc6ff8e75c09ef5d25b3b59a05994(**SHA-512 :** 6f44b7fc7a158b253b1a44af74fc91cb416484c25 **Size :** 0.471 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsvA7B1.Tmp	**Type :** GIF image data, version 89a, 1 x 1 **MD5 :** 28d6814f309ea289f847c69cf91194c6 **SHA-1 :** 0f4e929dd5bb2564f7ab9c76338e04e292a42ace **SHA-256 :** 8337212354871836e6763a41e615916c89bac5b3 **SHA-512 :** 1d68b92e8d822fe82dc7563edd7b37f3418a02a8 **Size :** 0.035 Kilobytes.
C:\Users\User\AppData\Local\Temp\DM_yDk9Jw0okW\DownloadManager.Exe	**Type :** PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows **MD5 :** 19fb006a1aa00ec8517f021a87c35e08 **SHA-1 :** 00c02fd53c775e6d35ceb4d0b5091bd9b3bd5785 **SHA-256 :** 72b9e4f2ca323e96bf94ca0633980ab0b25a8020 **SHA-512 :** 25fef7a05178f42b08e3de7e71bf05305b9c9ec03 **Size :** 1447.984 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsfA752.Tmp\Pwgen.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 (stripped to external PDB), for MS Windows **MD5 :** a555472395178ac8c733d90928e05017 **SHA-1 :** f44b192d66473f01a6540aaec4b6c9ac4c611d35 **SHA-256 :** 82ae08fced4a1f9a7df123634da5f4cb12af4593a(**SHA-512 :** e6d87b030c45c655d93b2e76d7437ad900df5da7 **Size :** 17.269 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\FC5A820A001B41D68902E051F36A5282_E98D75262B3D5D962FC8706E05221C8A	**Type :** data **MD5 :** 88b1779fb750632a8672655aca6adeda **SHA-1 :** d2c2eaa08b9d6adcdb396f212660e4a1e6768a85 **SHA-256 :** ed4534b84ef2aba6121b3748c89ee9d1c24d2d3b **SHA-512 :** b3818ad79cf34124e5c03a818032b892def6acf45 **Size :** 0.444 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\B9d332c3e7[1]	**Type :** ASCII text, with no line terminators **MD5 :** 5c9da71976fb9d00f82e61c7e496ba06 **SHA-1 :** 58884fb0e24a399213205ad35db27e6011bd149c **SHA-256 :** f69a13217482dc43f25e74cfcb9391d0f06d22501 **SHA-512 :** dbc11417f6342430d30220b7a4f141f05801520c **Size :** 0.057 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\070E0202839D9D67350CD2613E78E416	**Type :** data **MD5 :** 55540a230bdab55187a841cfe1aa1545 **SHA-1 :** 363e4734f757bdeb89868efe94907774a327695e **SHA-256 :** d73494e3446b02167573b3cde3ae1c8584ac26e **SHA-512 :** c899cb1d31d3214fd9dc8626a55e40580d3b222 **Size :** 1.302 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\75CA58072B9926F763A91F0CC2798706_93E4B2BA79A897B3100CCB27F2D3BF4F	**Type :** data **MD5 :** c8860acd1d387fd2094820c0270f5a14 **SHA-1 :** 30fcc6fe87507c906ea7cca16223d348b6a2d907 **SHA-256 :** d4e35f29a6c87b8e28eb78d648da5f83214116d3 **SHA-512 :** 736e5201a0da3b9b86866d82cfcf1d3d0dcae0d6 **Size :** 0.442 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157	**Type :** data **MD5 :** a001280dde88dafe3b9d7db33597aa98 **SHA-1 :** 1df19de7af5f00fcc114e8cd4468de056fcb39dd **SHA-256 :** 84e08a41b2500b8d151b7dc0e9a6814465e4307 **SHA-512 :** 150b89020c5be14ac6496d1df8d395c81dc0267f **Size :** 0.342 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsfA752.Tmp\Inetc.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** c498ae64b4971132bba676873978de1e **SHA-1 :** 92e4009cd776b6c8616d8bffade7668ef3cb3c27 **SHA-256 :** 5552bdde7e4113393f683ef501e4cc84dccc071b **SHA-512 :** 8e5ca35493f749a39ceae6796d2658ba10f7d8d9 **Size :** 20.992 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\4344B8AF97AF3A423D9EE52899963CDE_6BF99D49F7848CB4DF1BBF4D7AE05358	**Type :** data **MD5 :** 649b0351f163aff39b16ec14a01e6333 **SHA-1 :** c58aaf58210149d2a6a9ec01752958fc54511c48 **SHA-256 :** baed1542002db71e7fc191ec2ef92fde9e269367 **SHA-512 :** 2f6ea63734c46e5c2ff77c48df367f12fd282ab487 **Size :** 0.471 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\3FA0F92EA40DC353FF9E95B9F7D06EAF_02A7BB8D663AB0A2D3E0CE44422ED38B	**Type :** data **MD5 :** 34e51a091f2d18de0c9a1b1412f2b166 **SHA-1 :** 765a37a38fa4d85379db0e320d3e79dcb2b72c29 **SHA-256 :** 6ee73f56176ede6023f305e6a6fe99cc5022b4ec4 **SHA-512 :** e3e33c93081735b60e8c6428136ddc49f2fd65c2 **Size :** 0.446 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\BAD725C80F9E10846F35D039A996E4A8_88B6AE015495C1ECC395D19C1DD02894	**Type :** data **MD5 :** 3aaae1fde39aafa2494465860f228a67 **SHA-1 :** 2348fb1d0c6da3ca6801a0f809e51d9a4589df68 **SHA-256 :** 24b64af7649f3ad4681befcf49932785098553d9 **SHA-512 :** f100a6265a8ee60f9440ee89c21531a88eee6947 **Size :** 0.432 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	**Type :** Microsoft Cabinet archive data, 54153 bytes, 1 file **MD5 :** 767760b1b3b838b2de0599d0e76d1c76 **SHA-1 :** c56b126f887495918e8abcf813957780f0b9466a **SHA-256 :** c0f37380971fb93ecb0cfa3c2bd6d91cc77f254f0a **SHA-512 :** bacdd86b37e70fe36274c6ae9076f0ac89e82245 **Size :** 54.153 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\B398B80134F72209547439DB21AB308D_9487BC0D4381A7CDEB9A8CC43F66D27C	**Type :** data **MD5 :** 0d4156cba92557fbc94e896514c0137e **SHA-1 :** 0eac50c4c130b057064282142305f92b5e983912 **SHA-256 :** 144f10e6127476f51f8bb04b30fe97a740554959b **SHA-512 :** d8839b4dd3431ced4a7f6b553cad0d54fc64400e **Size :** 0.438 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012018080720180808\Index.Dat	**Type :** Internet Explorer cache file version Ver 5.2 **MD5 :** 90e5d874fdb4e4b184137b9a27edcdbb **SHA-1 :** 7844c5caf5be10d6099b96611525310fb3a61d75 **SHA-256 :** ae008a4ceb02affe65f487d4ca8fc8bdf956a0c642 **SHA-512 :** 2abac58d6e34ab05fa765f9dd51d183383bacca6 **Size :** 32.768 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\B66240B0F6C84BD4857ABA60CF5CE4A0_5043E0F5DF723415C9EECC201C838A62	**Type :** data **MD5 :** 51bc42361c20e7e9939970ea2d27050d **SHA-1 :** 7a3779d340c8b0c01165ff8c2e4fdf0bc3a26023 **SHA-256 :** 07e89dfd3faac0f1754f4805d95090a154d429e45 **SHA-512 :** 314400a26eff48547e9d443c19f9c5fed45bc1926 **Size :** 1.744 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\B3BB9C1BA2D19E090AE305B2683903A0_608E9093E4033CB74CFDFDB1E83A5BC5	**Type :** data **MD5 :** b4b4d360140edfe55e6b4a6543188232 **SHA-1 :** 7c806e13c328172d4e3a2ae94eba59b00bc251a4 **SHA-256 :** 4f0cbe1122da69edd00559b565241146714b7a5 **SHA-512 :** 3fa668cae19794aed41d9034097deb3a382e60b7 **Size :** 1.618 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsfA752.Tmp\UserInfo.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** 7579ade7ae1747a31960a228ce02e666 **SHA-1 :** 8ec8571a296737e819dcf86353a43fcf8ec63351 **SHA-256 :** 564c80dec62d76c53497c40094db360ff8a36e0d **SHA-512 :** a88bc56e938374c333b0e33cb72951635b5d5a9 **Size :** 4.096 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\3FA0F92EA40DC353FF9E95B9F7D06EAF_02A7BB8D663AB0A2D3E0CE44422ED38B	**Type :** data **MD5 :** 961d918dea1c184f7964c5f4daa6520f **SHA-1 :** dd2de222d5139f105b1e2a7a20bd55197fe71ae5 **SHA-256 :** 35c0d40b16f955e7280f87c2a6e5c2651fc33d9f6 **SHA-512 :** 792000debd0e177af7af2490858b70caced38443 **Size :** 0.471 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\6A2279C2CA42EBEE26F14589F0736E50	**Type :** data **MD5 :** b2c9ba50e62d18f4e2785722add68e38 **SHA-1 :** b0df4cef3333850d9fcaa97b71a62cc7bfa01dd1 **SHA-256 :** 3120410e55500e919b71457931b5026270d3b27 **SHA-512 :** 9f0cd897c91b8b7e3f17a9ec46f645fcc0da1d195 **Size :** 0.2 Kilobytes.
C:\Users\User\AppData\Local\Temp\NsfA752.Tmp\System.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386, for MS Windows **MD5 :** c17103ae9072a06da581dec998343fc1 **SHA-1 :** b72148c6bdfaada8b8c3f950e610ee7cf1da1f8d **SHA-256 :** dc58d8ad81cacb0c1ed72e33bff8f23ea40b5252b **SHA-512 :** d32a71aaef18e993f28096d536e41c4d01685072 **Size :** 11.264 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	**Type :** data **MD5 :** 00e8a9ec3aec582447613c9410169411 **SHA-1 :** 3ca7722bd586c2b6d4a03266d98ac3b07ab3e4de **SHA-256 :** 025960248dd97da6b955ff6539765ded191adafd **SHA-512 :** e7230eb0ade2829c1149af2b865201118b5537e **Size :** 0.328 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\0DA515F703BB9B49479E8697ADB0B955_7DC3E633EDFAEFC3AA3C99552548EC2F	**Type :** data **MD5 :** fcfb11d4615983dc117c5e24b945d9c7 **SHA-1 :** 16214f2e5a173aa4950d184aa27407a35f949a72 **SHA-256 :** b8b59308999a1884493d661f573587af4893c9ea **SHA-512 :** bc0e4e2a33d579b1b26fdb985a743b80ac465ee **Size :** 0.5 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\4344B8AF97AF3A423D9EE52899963CDE_6BF99D49F7848CB4DF1BBF4D7AE05358	**Type :** data **MD5 :** f81ec50a62ceaa0c6931b16b93dd6b1c **SHA-1 :** 7c998a5b44412058eb7ae79ca51307ca77094d51 **SHA-256 :** 6708be129ede23466e240a3b48ffca81a91a3740 **SHA-512 :** be3c23267272c7600f59ea0820aae5eae41d5d13 **Size :** 0.438 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\B3BB9C1BA2D19E090AE305B2683903A0_608E9093E4033CB74CFDFDB1E83A5BC5	**Type :** data **MD5 :** 9c21b7e3af584d327ceabba283faa1d3 **SHA-1 :** 54208532103c81e149097cb62543628491cebc23 **SHA-256 :** e06c21e97565ca325380e44ab9147e687fcff0f3c **SHA-512 :** 5172c1248a8fbd23cb061b49becf6425853672a0 **Size :** 0.42 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\B66240B0F6C84BD4857ABA60CF5CE4A0_5043E0F5DF723415C9EECC201C838A62	**Type :** data **MD5 :** e9ac65e179cef11ab5eb582eeb2a51ac **SHA-1 :** 86a955c72bd23fffa97a6f3738ee49f637353133 **SHA-256 :** 2451b2596d5a3b1e78afdd3dcd048bd8c1520aff **SHA-512 :** 051caf15b81e6d5e730e787938097b632718fb29 **Size :** 0.458 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\BAD725C80F9E10846F35D039A996E4A8_88B6AE015495C1ECC395D19C1DD02894	**Type :** data **MD5 :** 209b9bf6f389767b8e5ac07d7bf8b45f **SHA-1 :** fd17cca7b8cd8cf2290e8752b867838ef2ce07ff **SHA-256 :** e273bd2f24107fea88ba514117131d0baa9e0b67 **SHA-512 :** 9333367a8bea608077b149243d458375295ec06 **Size :** 1.548 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\B398B80134F72209547439DB21AB308D_9487BC0D4381A7CDEB9A8CC43F66D27C	**Type :** data **MD5 :** cef93d7bbae0314746028989c24988ad **SHA-1 :** 613172cc1edb0924bd9a538e92ddcf906325a149 **SHA-256 :** 6f59dae3c46cd9d3ad9cbd4e768295813550cb63 **SHA-512 :** 6e87076b4cd5fb70b869119f030653db82dba75a **Size :** 0.471 Kilobytes.
C:\Users\User\AppData\Local\GDIPFONTCACHEV1.DAT	**Type :** data **MD5 :** 696bad2ef23da7f0ccaaa7f76ab9fdf0 **SHA-1 :** 0efe907b47e8331cf56a95c0c06d324257ece202 **SHA-256 :** bd27979561fac15e4043fc980ad62f24f00738cba **SHA-512 :** fb1a4afdbf5f9e3d7e55eb806f660057927d6c357 **Size :** 84.528 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\8828F39C7C0CE9A14B25C7EB321181BA_BD8B98368542C3BBAE3413A0EF3BB623	**Type :** data **MD5 :** 3ca1bdd33df367134cc91857e7af68ce **SHA-1 :** 41254ea87c5825d63c499b7ed4e4196cab80b4c9 **SHA-256 :** 8e61e38ca9addef2141a035bcbdd8754d166e67(**SHA-512 :** 3476d03232238cf52fa8e192fc7befa82be55bdbe **Size :** 0.396 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\8828F39C7C0CE9A14B25C7EB321181BA_BD8B98368542C3BBAE3413A0EF3BB623	**Type :** data **MD5 :** eec3c77f2b72318bc4d1b010231b47cd **SHA-1 :** 23449e3de417382dc32263b101dbff47d16f413c **SHA-256 :** 5f724019362d7a2c363896416c0ddc477fd2cb2fa **SHA-512 :** d6d46de3afd6a861dabcfdc0891426fc162c50934 **Size :** 1.754 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\75CA58072B9926F763A91F0CC2798706_93E4B2BA79A897B3100CCB27F2D3BF4F	**Type :** data **MD5 :** cfb59c6876796ad6954f416b2143c6f0 **SHA-1 :** 44ec95593e0e025be8a2efb391f65547d4c3d808 **SHA-256 :** e41f5b25f4ede5897684fa4927d5ec7e1c09fda05 **SHA-512 :** 16a3b4ff73f614ad300d55e3a3903f296fa6250ce **Size :** 1.426 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\7D266D9E1E69FA1EEFB9699B009B34C8_1D5A876A9113EC07224C45E5A870E3BD	**Type :** data **MD5 :** 48aadf58b4af3f7da0ddbfcdc221c812 **SHA-1 :** e7376f3b4c50f964b4e1fd16a5197baa080e8ff2 **SHA-256 :** dd571ec73f4aedb266e343bd033b4ecdb629ec3f **SHA-512 :** 88a095bef92a0cbcca55777fcd6b235748ba0dcf9 **Size :** 0.408 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\6A2279C2CA42EBEE26F14589F0736E50	**Type :** data **MD5 :** 77ca4289661000b3a8b8e912e7d2138b **SHA-1 :** deec92073bea4176589f4840121ecf6f2750b1b4 **SHA-256 :** a7692aa2b5b2664de344b922a091b7ba6f4fa01a **SHA-512 :** f8dc07c60abeab1b60ded14c3d51c25a41f28fa7e **Size :** 0.434 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\0DA515F703BB9B49479E8697ADB0B955_7DC3E633EDFAEFC3AA3C99552548EC2F	**Type :** data **MD5 :** 0439925669525c6a542a7ed674c96a36 **SHA-1 :** 6cb9f346c4a89776b113036f5482c0776d0c110e **SHA-256 :** 8369e6da8d5db40ac2a8624e11fa8fd16d60b949 **SHA-512 :** 37f2e54fc9eb3ab2c654f9a1d40fb676105643d50 **Size :** 1.52 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\Nr-1071.Min[1].Js	**Type :** ASCII text, with very long lines, with no line terminators **MD5 :** a1a545c95f313a230157b47dca555c25 **SHA-1 :** 3c6346aea5d04121ca868e984a819c68512b697d **SHA-256 :** 56097e8b7ceb27db42a5e102af6d11dfdcaee13d **SHA-512 :** 32e6f74e7c3098dd8360d4f27cb98276b23119f5 **Size :** 23.651 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\070E0202839D9D67350CD2613E78E416	**Type :** data **MD5 :** 5dc9dc09f0a5fd5d4bd2abf239ef349a **SHA-1 :** 4966105c94d7ba2c4d9751253f96c2df950a5b3f **SHA-256 :** c0c9cd9ecf0ed9c3d563ae9dd169b230721b0c48 **SHA-512 :** d4164bc5412f44e773c8ec7ddd8061e17afd9cad **Size :** 0.23 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	primopdfsetup.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	5732b93642462b9c529ac1888286d778f044f6b1
MD5:	d7a9a897aa8a40bf3017356782de442d
First Seen Date:	2018-08-07 01:02:32.055145 (5 months ago)
Number Of Clients Seen:	1
Last Analysis Date:	2018-08-07 01:02:32.055145 (5 months ago)
Human Expert Analysis Result:	No human expert analysis verdict given to this sample yet.

VALKYRIE COMODO

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[]
Number Of Sections	5
Trid	[]
Compilation Time Stamp	0x4B1AE3CC [Sat Dec 5 22:50:52 2009 UTC]
Entry Point	0x4030fa (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	760720
Ssdeep	
Sha256	7202325e3163e756f24f4c93c17630358a582e17baa608341b8c7f8605c7cb27
Exifinfo	[]
Mime Type	application/x-dosexec
Imphash	

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x5c4c	0x5e00	6.4401055495	856b32eb77dfd6fb67f21d6543272da5
.rdata	0x7000	0x129c	0x1400	5.04683530791	dc77f8a1e6985a4361c55642680ddb4f
.data	0x9000	0x25c58	0x400	4.80100375272	7922d4ce117d7d5b3ac2cffe4b0b5e4f
.ndata	0x2f000	0x9000	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.rsrc	0x38000	0x96a0	0x9800	6.46794824264	9db491049faa17da4c23752a499c4e67

PE Resources

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 230160, u'sha256': u'3007981afb2289a983ecdccfced0f0e6ea190fc60b5463135a083d9ab597c6f3', u'type': u'PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced', u'size': 12841}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 243008, u'sha256': u'03d6a74140c7c2e39bfab31e909e16749a6f52029b98cde1f115af72ff9eefc9', u'type': u'dBase III DBT, version number 0, next free block index 40', u'size': 9640}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 252648, u'sha256': u'56e50e40ca96c822f551210a66b14cd21d4cbc66c91416494f442e0074884fc3', u'type': u'data', u'size': 4264}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 256912, u'sha256': u'62fbb015b4e82e0992886c0e589c1c9084a65728c71886bc10184f7459da6cfd', u'type': u'data', u'size': 3752}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 260664, u'sha256': u'7f8ced43c2e5c0cdc87db69ed238ee916151251599c454088a450b065452caa4', u'type': u'data', u'size': 2216}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 262880, u'sha256': u'f2ed0d176730d00be8aaa18961885715bcf57bea64816bfc2073dfa482ca87c4', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1384}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 264264, u'sha256': u'fc46fd34cc3beb5da5feb6d54b2dd32442280c706216c78227c50c78a8508e72', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1128}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 265392, u'sha256': u'7efc7114648e0832e7b437c0ab9aaeed7cbf79957ede6854f76ba3aa57b9a87b', u'type': u'data', u'size': 744}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 266136, u'sha256': u'8e6d9e02b8bbf3430dc46c698f9b1bb6e56da174da1580a7fe08b1352f746911', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 296}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_DIALOG', u'offset': 266432, u'sha256': u'fecdb955f8d7f1c219ff8167f90b64f3cb52e53337494577ff73c0ac1dafcd96', u'type': u'data', u'size': 256}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_DIALOG', u'offset': 266688, u'sha256': u'69897c784f1491eb3024b0d52c2897196a2e245974497fda1915db5fefcf8729', u'type': u'data', u'size': 284}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_DIALOG', u'offset': 266976, u'sha256': u'85025c8556952f6a651c2468c8a0d58853b0ba482be9ad5cd3060f216540dfc0', u'type': u'data', u'size': 96}

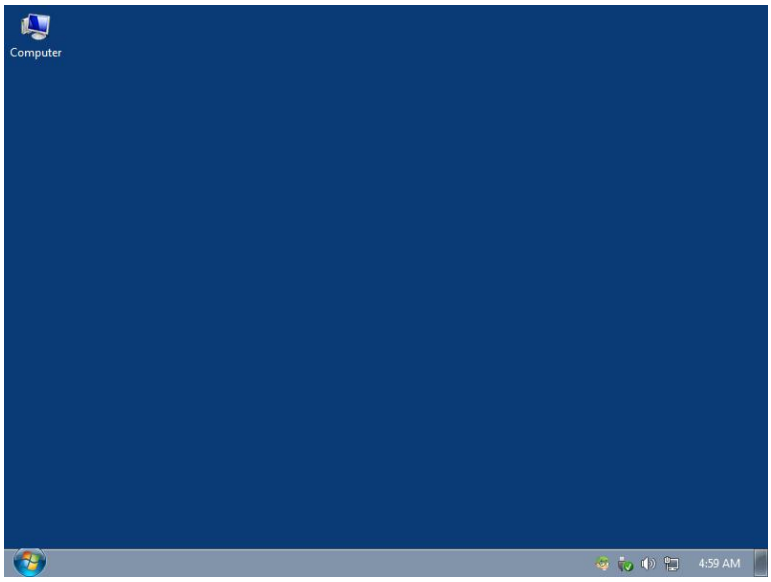
{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_ICON', u'offset': 267072, u'sha256': u'f4659a766f45a08245e3473d39c8f78bdebbe0f2fab5f9dd44d4d2cfef329b0a', u'type': u'MS Windows icon resource - 9 icons, 32x32, 16 colors', u'size': 132}

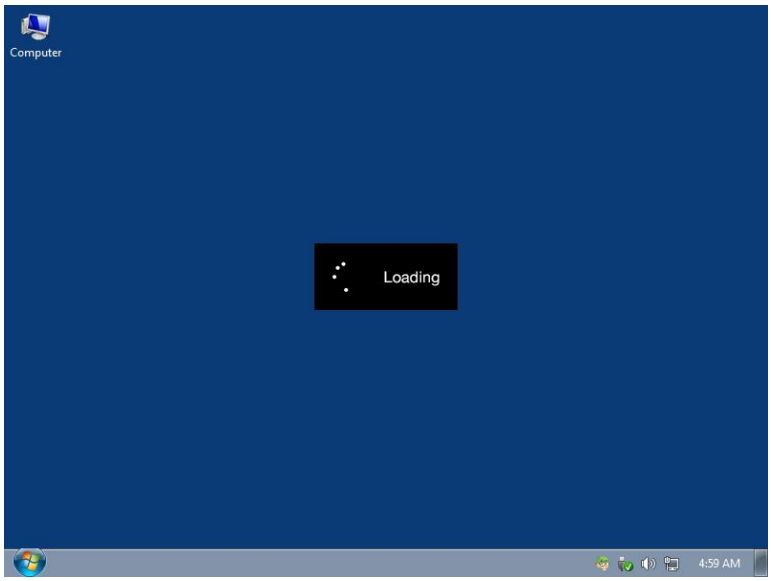
{u'lang': u'LANG_ENGLISH', u'name': u'RT_MANIFEST', u'offset': 267208, u'sha256': u'0a8ea44c423c7094712bf091f4a40cf1446ae63345a69b396367f29d7da83df5', u'type': u'XML 1.0 document, ASCII text, with very long lines, with no line terminators', u'size': 727}

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS




Computer
Loading
4:59 AM


Computer
4:59 AM