Summary

File Name: 2

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

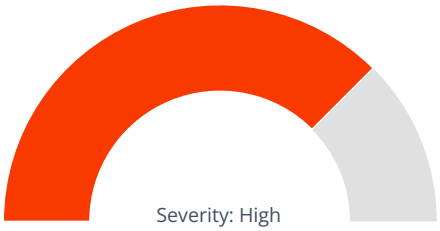
SHA1: 0dddca0add163af6238f2b68bc25a88ada1f35d5

MD5: cc52ba8f6f250704f6ed9139a242382f

MALWARE

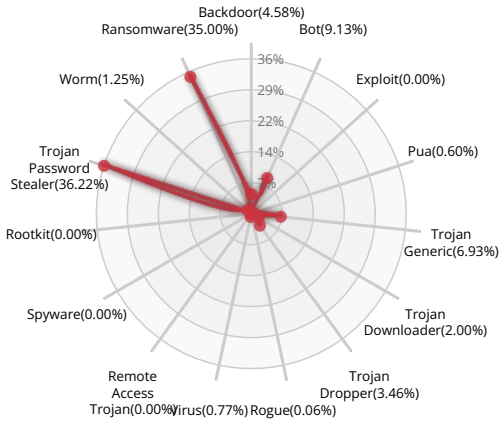
Valkyrie Final Verdict

DETECTION SECTION

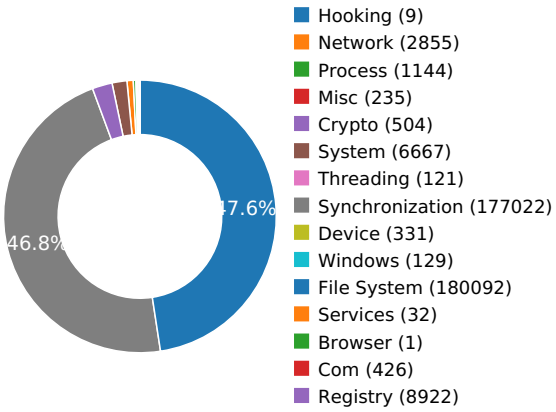


Verdict: Malware

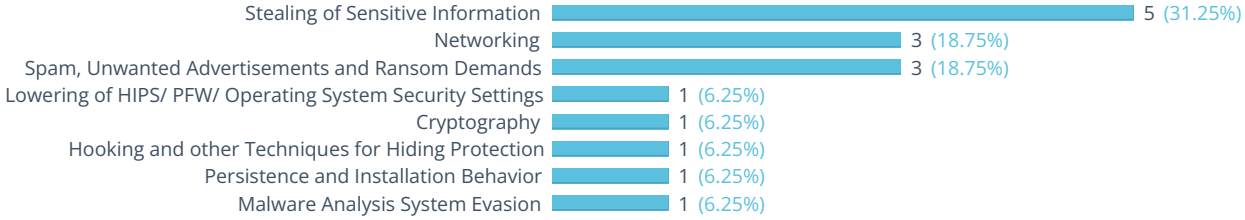
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



VALKYRIE COMODO

Activity Details

NETWORKING

Attempts to connect to a dead IP:Port (11 unique times)	Show sources
Performs some HTTP requests	Show sources
Network activity contains more than one unique useragent.	Show sources

LOWERING OF HIPS/ PFW/ OPERATING SYSTEM SECURITY SETTINGS

Attempts to block SafeBoot use by removing registry keys	Show sources

CRYPTOGRAPHY

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

STEALING OF SENSITIVE INFORMATION

Collects information to fingerprint the system	Show sources
Attempts to access Bitcoin/ALTCoin wallets	Show sources
Steals private information from local Internet browsers	Show sources
Attempts to modify proxy settings	
Harvests information related to installed mail clients	Show sources

SPAM, UNWANTED ADVERTISEMENTS AND RANSOM DEMANDS

Attempts to modify desktop wallpaper	
Exhibits behavior characteristic of Cerber ransomware	
Writes a potential ransom message to disk	Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory	Show sources

PERSISTENCE AND INSTALLATION BEHAVIOR

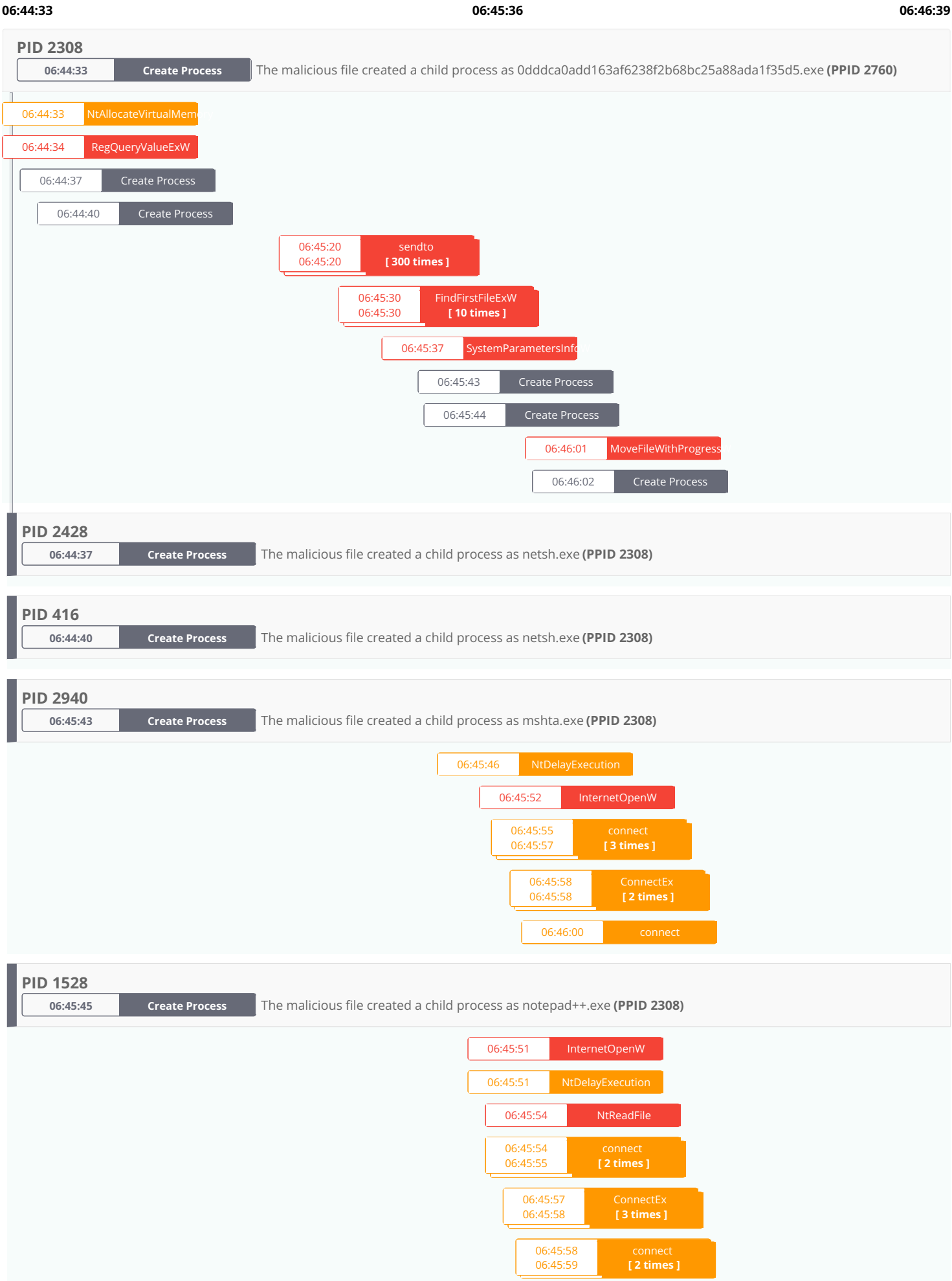
Deletes its original binary from disk Show sources

MALWARE ANALYSIS SYSTEM EVASION

A process attempted to delay the analysis task. Show sources

VALKYRIE COMODO

Behavior Graph



PID 1256

06:46:03 | Create Process | The malicious file created a child process as cmd.exe **(PPID 2308)**

06:46:04 | Create Process

06:46:38 | Create Process

PID 2908

06:46:04 | Create Process | The malicious file created a child process as taskkill.exe **(PPID 1256)**

PID 548

06:46:39 | Create Process | The malicious file created a child process as PING.EXE **(PPID 1256)**

PID 584

06:44:53 | Create Process | The malicious file created a child process as svchost.exe **(PPID 460)**

06:45:43 | Create Process

06:46:27 | Create Process

PID 1452

06:45:44 | Create Process | The malicious file created a child process as dllhost.exe **(PPID 584)**

PID 1612

06:46:27 | Create Process | The malicious file created a child process as WmiPrvSE.exe **(PPID 584)**

06:46:29 | NtDelayExecution

PID 1500

06:44:59 | Create Process | The malicious file created a child process as svchost.exe **(PPID 460)**

06:45:02 | RegOpenKeyExW

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Users\user\AppData\Local\Temp\0dddca0add163af6238f2b68bc25a88ada1f35d5.exe.Local\
C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80
C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80\GdiPlus.dll
C:\Users\user\AppData\Local\Temp\0dddca0add163af6238f2b68bc25a88ada1f35d5.exe
C:\test\cerber_debug.txt
C:\Users\user\AppData\Local\Temp\8902607b\cafe.tmp
C:\Program Files (x86)\Windows Defender*
C:\Program Files (x86)\Windows Defender\en-US*
C:\test\cerber_debug2.txt
C:
D:
C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Local
C:\Users\user\AppData\Local\Temp
C:\Users\user\AppData\Local\Temp\8902607b
C:\Users\user\AppData\Local\Temp\8902607b\40b9.tmp
C:\Windows\System32
C:\
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent*.lnk
\??\MountPointManager
C:*
D:\
D:*
C:\$Recycle.Bin\
D:\$RECYCLE.BIN\
C:\program files\
D:\samples\
C:\program files (x86)\
D:\samples*
C:\programdata\

C:\Python27\
C:\Sandbox\
C:\Sandbox*
C:\Sandbox\user\
C:\Sandbox\user*
C:\Sandbox\user\BSA\
C:\Sandbox\user\BSA*
C:\Sandbox\user\bsa_advanced\
C:\Sandbox\user\bsa_advanced*
C:\system volume information\
C:\tools\
C:\tools*
C:\Users\
C:\Users*
C:\Users\Default\
C:\Users\Public\
C:\Users\Public*
C:\Users\Public\Desktop\
C:\Users\Public\documents\
C:\Users\Public\documents*
C:\Users\Public\downloads\
C:\Users\Public\downloads*
C:\Users\Public\favorites\
C:\Users\Public\libraries\
C:\Users\Public\Music\
C:\Users\Public\Music*
C:\Users\Public\Music\sample music\
C:\Users\Public\Pictures\
C:\Users\Public\Pictures*
C:\Users\Public\Pictures\sample pictures\
C:\Users\Public\recorded tv\
C:\Users\Public\recorded tv*
C:\Users\Public\recorded tv\sample media\
C:\Users\Public\recorded tv\sample media*
C:\Users\Public\Videos\

C:\Users\Public\Videos*
C:\Users\Public\Videos\sample videos\
C:\Users\user\
C:\Windows\
C:\program files (x86)\bitcoin
C:\program files (x86)\bitcoin*
C:\programdata\bitcoin
C:\programdata\bitcoin*
C:\Windows\System32\config\systemprofile\AppData\Roaming\bitcoin

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{3050F55D-98B5-11CF-BB82-00AA00BDCE0B}\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\Hostname
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\Domain
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{D4781CD6-E5D3-44DF-AD94-930EFE48A887}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9556DC99-828C-11CF-A37E-00AA003240C7}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\InprocServer32\InprocServer32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\InprocServer32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\InprocServer32\ThreadingModel
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{027947E1-D731-11CE-A357-000000000001}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\InprocServer32\InprocServer32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\InprocServer32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\InprocServer32\ThreadingModel
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{1C1C45EE-4395-11D2-B60B-00104B703EFD}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{423EC01E-2E35-11D2-B604-00104B703EFD}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDrives
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-18\ProfileImagePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-19\ProfileImagePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-20\ProfileImagePath
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\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\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFilePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane7
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane8
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane9
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane10
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane11
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane12
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane13
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane14
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane15
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane16
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesMyComputer
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesRecycleBin
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoControlPanel
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoSetFolders
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoInternetIcon

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoCommonGroups
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Drive\shellex\FolderExtensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}\DriveMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\AllowFileCLSIDJunctions
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\DontShowSuperHidden
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.hta\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\htafile\DocObject
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\htafile\BrowseInPlace
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.hta\Content Type
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\htafile\CLSID\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\htafile\IsShortcut
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\htafile\AlwaysShowExt
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\htafile\NeverShowExt
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\KindMap\.hta
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\htafile\Shell\Open\Command\DelegateExecute
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.asp\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.bas\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.bat\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.cer\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.chm\(Default)

MODIFIED FILES

C:\Users\user\AppData\Local\Temp\8902607b\40b9.tmp
C:\Users\user\AppData\Local\Temp\8902607b\cafe.tmp
D:\agent.pyw
C:\Users\user\AppData\Roaming\microsoft\Outlook\Outlook.srs
D:\CPbJPOO7nE.97bf
D:_R_E_A_D___T_H_I_S___V5BE_.hta
C:\Users\user\AppData\Roaming\microsoft\Outlook\U0zWeuumVq.97bf
C:\Users\user\AppData\Roaming\microsoft\Outlook_R_E_A_D___T_H_I_S___JN4MMCO_.hta
D:_R_E_A_D___T_H_I_S___SIZ9T2UH_.txt
C:\Users\user\AppData\Roaming\microsoft\Outlook_R_E_A_D___T_H_I_S___0Y9M_.txt
C:\Users\user\AppData\Roaming\microsoft\Outlook\Outlook.xml
C:\Users\user\AppData\Roaming\microsoft\Outlook\0g4yPMug6i.97bf
C:\Users\user\AppData\Local\microsoft\Outlook\Outlook.pst
C:\Users\user\AppData\Local\microsoft\Outlook\RxPSr5YUl7.97bf

C:\Users\user\AppData\Local\microsoft\Outlook_R_E_A_D___T_H_I_S___DPA5L_.hta
C:\Users\user\AppData\Local\microsoft\Outlook_R_E_A_D___T_H_I_S___UNV87_.txt
C:\Users\user\AppData\Local\Temp\tmpC50.bmp
C:\Users\user\Desktop_R_E_A_D___T_H_I_S___6JVNRXN_.hta
C:\Users\user\Desktop_R_E_A_D___T_H_I_S___RRH6J_.txt
\??\VBoxMiniRdrDN
\??\PIPE\wkssvc
\Device\LanmanDatagramReceiver
\??\PIPE\DAV RPC SERVICE
\Device\Http\Communication
\??\PIPE\samr
C:\Windows\sysnative\wbem\repository\WRITABLE.TST
C:\Windows\sysnative\wbem\repository\MAPPING1.MAP
C:\Windows\sysnative\wbem\repository\MAPPING2.MAP
C:\Windows\sysnative\wbem\repository\MAPPING3.MAP
C:\Windows\sysnative\wbem\repository\OBJECTS.DATA
C:\Windows\sysnative\wbem\repository\INDEX.BTR
\??\pipe\PIPE_EVENTROOT\CIMV2WMI SELF-INSTRUMENTATION EVENT PROVIDER
\??\pipe\PIPE_EVENTROOT\CIMV2PROVIDERSUBSYSTEM
C:\Users\user\AppData\Roaming\Microsoft\Windows\IETldCache\index.dat
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\ACF244F1A10D4DBED0D88EBA0C43A9B5_3FB9EBFC1D18D5E09631A5E5A62F6EF3
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\ACF244F1A10D4DBED0D88EBA0C43A9B5_3FB9EBFC1D18D5E09631A5E5A62F6EF3
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\BD5208ADDEC1165FD57AF2BF2F455EAA_263FE4237EA516DF2897E98DDA15C41D
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\BD5208ADDEC1165FD57AF2BF2F455EAA_263FE4237EA516DF2897E98DDA15C41D
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\all[1]
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\1016d7ceff188e9fe32e68e9761bd811f354cfb31d7d106ec3c4f3ebce7f7a50[1]
C:\Users\user\AppData\Roaming\Notepad++\plugins\config\PluginManager.ini
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\E49827401028F7A0F97B5576C77A26CB_7CE95D8DCA26FE957E7BD7D76F353B08
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\E49827401028F7A0F97B5576C77A26CB_7CE95D8DCA26FE957E7BD7D76F353B08
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\399B5D4120C9EA3BF46CD1435D520D37
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\399B5D4120C9EA3BF46CD1435D520D37
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\plugins.md5[1].txt

C:\Users\user\AppData\Roaming\Notepad++\plugins\config\PluginManagerPlugins.zip
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\plugins[1].zip
C:\Users\user\AppData\Roaming\Notepad++\plugins\config\PluginManagerPlugins.xml
\??\NUL

RESOLVED APIS

kernel32.dll.LoadLibraryExA
kernel32.dll.GetModuleHandleA
kernel32.dll.WriteFile
kernel32.dll.CloseHandle
kernel32.dll.VirtualFree
kernel32.dll.UnmapViewOfFile
kernel32.dll.GetProcAddress
kernel32.dll.VirtualAlloc
kernel32.dll.SetFilePointer
kernel32.dll.GetTempPathA
kernel32.dll.VirtualProtect
kernel32.dll.CreateFileA
kernel32.dll.lstrlenA
kernel32.dll.lstrcatA
ntdll.dll.memmove
ntdll.dll.isspace
ntdll.dll.tolower
ntdll.dll._aulldvrm
ntdll.dll.memset
ntdll.dll.memcpy
ntdll.dll._allmul
ntdll.dll._alldiv
ntdll.dll.RtlUnwind
ntdll.dll.NtQueryVirtualMemory
cryptsp.dll.CryptAcquireContextW
cryptsp.dll.CryptImportKey
cryptsp.dll.CryptEncrypt
cryptsp.dll.CryptDestroyKey
cryptsp.dll.CryptGenRandom

cryptsp.dll.CryptGetKeyParam
cryptsp.dll.CryptCreateHash
cryptsp.dll.CryptHashData
cryptsp.dll.CryptGetHashParam
cryptsp.dll.CryptDestroyHash
kernel32.dll.IsWow64Process
cryptbase.dll.SystemFunction036
uxtheme.dll.ThemeInitApiHook
user32.dll.IsProcessDPIAware
kernel32.dll.GetThreadPreferredUILanguages
kernel32.dll.SetThreadPreferredUILanguages
kernel32.dll.LocaleNameToLCID
kernel32.dll.GetLocaleInfoEx
kernel32.dll.LCIDToLocaleName
kernel32.dll.GetSystemDefaultLocaleName
oleaut32.dll.#283
oleaut32.dll.#284
ntdll.dll.EtwUnregisterTraceGuids
oleaut32.dll.#500
dwmapi.dll.DwmIsCompositionEnabled
setupapi.dll.CM_Get_Device_Interface_List_Size_ExW
setupapi.dll.CM_Get_Device_Interface_List_ExW
comctl32.dll.#386
gdi32.dll.GetLayout
gdi32.dll.GdiRealizationInfo
gdi32.dll.FontIsLinked
advapi32.dll.RegOpenKeyExW
advapi32.dll.RegQueryValueExW
advapi32.dll.RegCloseKey
gdi32.dll.GetFontAssocStatus
advapi32.dll.RegQueryValueExA
advapi32.dll.RegQueryInfoKeyW
advapi32.dll.RegEnumKeyExW
gdi32.dll.GetTextFaceAliasW
gdi32.dll.GdiIsMetaPrintDC

ole32.dll.OleInitialize
propsys.dll.PSCreateMemoryPropertyStore
propsys.dll.PSPropertyBag_WriteDWORD
propsys.dll.PSPropertyBag_ReadDWORD
propsys.dll.PSPropertyBag_ReadBSTR
propsys.dll.PSPropertyBag_ReadStrAlloc
propsys.dll.#430
advapi32.dll.RegGetValueW
ole32.dll.CoTaskMemRealloc
propsys.dll.InitPropVariantFromStringAsVector
propsys.dll.PSCoerceToCanonicalValue
propsys.dll.PropVariantToStringAlloc

DELETED FILES

D:\agent.pyw
C:\Users\user\AppData\Roaming\microsoft\Outlook\Outlook.srs
C:\Users\user\AppData\Roaming\microsoft\Outlook\Outlook.xml
C:\Users\user\AppData\Local\microsoft\Outlook\Outlook.pst
C:\Users\user\AppData\Local\Temp\tmpC50.tmp
C:\Users\user\AppData\Local\Temp\0dddca0add163af6238f2b68bc25a88ada1f35d5.exe
C:\Users\user\AppData\Roaming\Notepad++\plugins\config\plugin_install_temp
C:\Users\user\AppData\Roaming\Notepad++\plugins\config\PluginManagerGpup.xml
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\user@downloads.sourceforge[1].txt

DELETED REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\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_CLASSES_ROOT\interface\{3050F55D-98B5-11CF-BB82-00AA00BDCE0B}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{3050F55D-98B5-11CF-BB82-00AA00BDCE0B}\(Default)

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide\AssemblyStorageRoots
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\Hostname
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\System\DNSclient
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\Domain
HKEY_CURRENT_USER\Software\Classes
HKEY_CURRENT_USER\Software\Classes\Interface\{D4781CD6-E5D3-44DF-AD94-930EFE48A887}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{D4781CD6-E5D3-44DF-AD94-930EFE48A887}\ProxyStubClsid32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{D4781CD6-E5D3-44DF-AD94-930EFE48A887}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\CustomLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\ExtendedLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en
HKEY_CURRENT_USER\Software\Classes\Interface\{9556DC99-828C-11CF-A37E-00AA003240C7}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9556DC99-828C-11CF-A37E-00AA003240C7}\ProxyStubClsid32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{9556DC99-828C-11CF-A37E-00AA003240C7}\ProxyStubClsid32\(Default)
HKEY_CURRENT_USER\Software\Classes\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\TreatAs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\Progid
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\Progid
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\InprocServer32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\InprocServer32\InprocServer32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\InprocServer32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\InprocServer32\ThreadingModel
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\InprocHandler32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\InprocHandler
HKEY_CURRENT_USER\Software\Classes\Interface\{027947E1-D731-11CE-A357-000000000001}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{027947E1-D731-11CE-A357-000000000001}\ProxyStubClsid32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{027947E1-D731-11CE-A357-000000000001}\ProxyStubClsid32\(Default)
HKEY_CURRENT_USER\Software\Classes\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\TreatAs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\Progid

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\Progid
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\InprocServer32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\InprocServer32\InprocServer32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\InprocServer32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\InprocServer32\ThreadingModel
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\InprocHandler32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\InprocHandler
HKEY_CURRENT_USER\Software\Classes\Interface\{1C1C45EE-4395-11D2-B60B-00104B703EFD}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{1C1C45EE-4395-11D2-B60B-00104B703EFD}\ProxyStubClsid32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{1C1C45EE-4395-11D2-B60B-00104B703EFD}\ProxyStubClsid32\(Default)
HKEY_CURRENT_USER\Software\Classes\Interface\{423EC01E-2E35-11D2-B604-00104B703EFD}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{423EC01E-2E35-11D2-B604-00104B703EFD}\ProxyStubClsid32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\Interface\{423EC01E-2E35-11D2-B604-00104B703EFD}\ProxyStubClsid32\(Default)
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDrives
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-18
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-18\ProfileImagePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-19
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-19\ProfileImagePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-20
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-20\ProfileImagePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2298303332-66077612-2598613238-1000
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2298303332-66077612-2598613238-1000\ProfileImagePath
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

EXECUTED COMMANDS

C:\Windows\system32\netsh.exe advfirewall set allprofiles state on
C:\Windows\system32\netsh.exe advfirewall reset
"C:\Windows\SysWOW64\mshta.exe" "C:\Users\user\Desktop_R_E_A_D___T_H_I_S___6JVNRXN_.hta"
C:\Users\user\Desktop_R_E_A_D___T_H_I_S___6JVNRXN_.hta
"C:\Program Files (x86)\Notepad++\notepad++.exe" "C:\Users\user\Desktop_R_E_A_D___T_H_I_S___RRH6J_.txt"
C:\Users\user\Desktop_R_E_A_D___T_H_I_S___RRH6J_.txt
C:\Windows\system32\DllHost.exe /Processid:{AB8902B4-09CA-4BB6-B78D-A8F59079A8D5}
C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
taskkill /f /im "0dddca0add163af6238f2b68bc25a88ada1f35d5.exe"
C:\Windows\system32\PING.EXE ping -n 1 127.0.0.1

READ FILES

C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80\GdiPlus.dll
C:\Users\user\AppData\Local\Temp\0dddca0add163af6238f2b68bc25a88ada1f35d5.exe
C:\Users\user\AppData\Local\Temp\8902607b\cafe.tmp
D:\agent.pyw
C:\Users\user\AppData\Roaming\microsoft\Outlook\Outlook.srs
C:\Users\user\AppData\Roaming\microsoft\Outlook\Outlook.xml
C:\Users\user\AppData\Local\microsoft\Outlook\Outlook.pst
C:\Windows\Fonts\staticcache.dat
C:\Users\user\AppData\Local\Temp\tmpC50.tmp
C:\Windows\SysWOW64\mshta.exe
C:\Program Files (x86)\Notepad++\notepad++.exe
\??\VBoxMiniRdrDN
\??\PIPE\wkssvc
\Device\LanmanDatagramReceiver
C:\Windows\SysWOW64\en-US\KERNELBASE.dll.mui

\??\PIPE\DAV RPC SERVICE
\Device\NamedPipe\
\Device\KsecDD
\Device\Http\Communication
C:\Windows\SysWOW64\en-US\FWCFG.DLL.mui
C:\Windows\System32\p2pcollab.dll
C:\Windows\System32\dnsapi.dll
C:\Windows\SysWOW64\en-US\DNSAPI.dll.mui
C:\Windows\System32\DHCPQEC.DLL
C:\Windows\System32\napipsec.dll
C:\Windows\System32\en-US\napipsec.dll.mui
C:\Windows\System32\tsgqec.dll
C:\Windows\System32\EAPQEC.DLL
C:\Windows\System32\en-US\eapqec.dll.mui
C:\Windows\SysWOW64\en-US\P2PNETSH.DLL.mui
\??\PIPE\samr
C:\Windows\sysnative\wbem\repository\MAPPING1.MAP
C:\Windows\sysnative\wbem\repository\MAPPING2.MAP
C:\Windows\sysnative\wbem\repository\MAPPING3.MAP
C:\Windows\sysnative\wbem\repository\OBJECTS.DATA
C:\Windows\sysnative\wbem\repository\INDEX.BTR
\??\pipe\PIPE_EVENTROOT\CIMV2WMI SELF-INSTRUMENTATION EVENT PROVIDER
\??\pipe\PIPE_EVENTROOT\CIMV2PROVIDERSUBSYSTEM
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Users\user\Desktop_R_E_A_D___T_H_I_S___6JVNRXN_.hta
C:\Users\user\AppData\Roaming\Microsoft\Windows\IETldCache\index.dat
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\SysWOW64\schannel.dll
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\ACF244F1A10D4DBED0D88EBA0C43A9B5_3FB9EBFC1D18D5E09631A5E5A62F6EF3
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\ACF244F1A10D4DBED0D88EBA0C43A9B5_3FB9EBFC1D18D5E09631A5E5A62F6EF3
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\BD5208ADDEC1165FD57AF2BF2F455EAA_263FE4237EA516DF2897E98DDA15C41D
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\BD5208ADDEC1165FD57AF2BF2F455EAA_263FE4237EA516DF2897E98DDA15C41D
C:\Program Files (x86)\Notepad++\SciLexer.dll
C:\Windows\System32\msimg32.dll
C:\Windows\SysWOW64\shell32.dll
C:\
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x000000000000004a.db
C:\Users\desktop.ini
C:\Users

MUTEXES

shell.{894DBB4C-C85C-6AA1-3632-71663E84D0E6}
Local\ZoneAttributeCacheCounterMutex
Local\ZonesCacheCounterMutex
Local\ZonesLockedCacheCounterMutex
CicLoadWinStaWinSta0
Local\MSCTF.CtfMonitorInstMutexDefault1
IESQMMUTEX_0_208

Local\c:!users!user!appdata!roaming!microsoft!windows!ietldcache!
nppInstance
DBWinMutex
Local\ZonesCounterMutex
Local\!IETld!Mutex

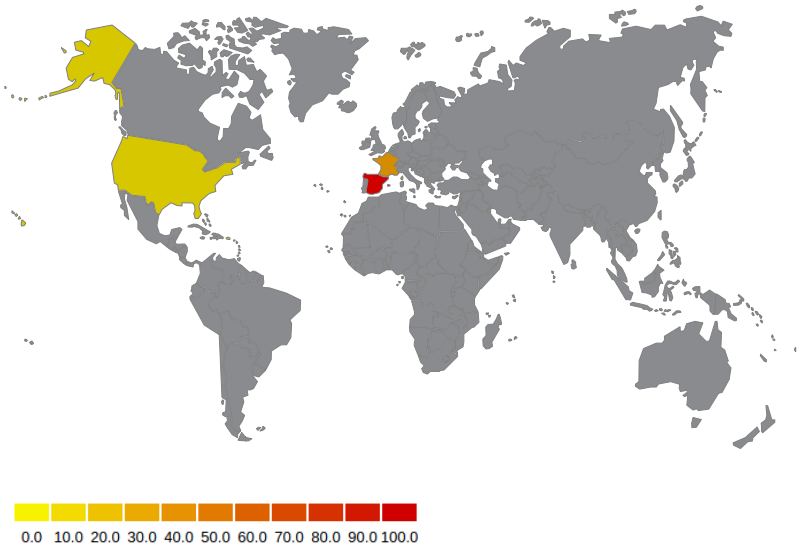
MODIFIED REGISTRY KEYS

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\Classes\Local Settings\MuiCache\6D\52C64B7E\LanguageList
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\p2pcollab.dll,-8042
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\dnsapi.dll,-103
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\dhcpqec.dll,-100
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\dhcpqec.dll,-101
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\dhcpqec.dll,-103
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\dhcpqec.dll,-102
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\napipsec.dll,-1
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\napipsec.dll,-2
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\napipsec.dll,-4
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\napipsec.dll,-3
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\tsgqec.dll,-100
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\tsgqec.dll,-101
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\tsgqec.dll,-102
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\tsgqec.dll,-103
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\eapqec.dll,-100
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\eapqec.dll,-101
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\eapqec.dll,-102
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\eapqec.dll,-103
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\LastServiceStart
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Transports\Decoupled\Server
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Server\CreationTime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Server\MarshaledProxy
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Server\ProcessIdentifier
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\ConfigValueEssNeedsLoading
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\List of event-active namespaces

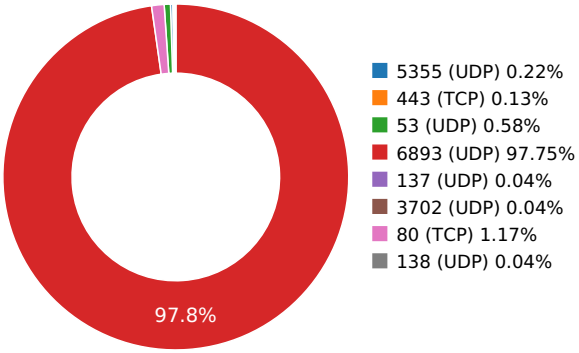
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\ESS\//./root/CIMV2\SCM Event Provider
HKEY_LOCAL_MACHINE\Software\Microsoft\Tracing\mshta_RASAPI32
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\mshta_RASAPI32\EnableFileTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\mshta_RASAPI32\EnableConsoleTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\mshta_RASAPI32\FileTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\mshta_RASAPI32\ConsoleTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\mshta_RASAPI32\MaxFileSize
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\mshta_RASAPI32\FileDirectory
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\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

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type
	8.8.4.4	United States	15169	Level 3 Parent, LLC	Malware Process
	104.16.152.172	United States	13335	Cloudflare, Inc.	Malware Process
	184.26.44.105	United States	20940	Akamai Technologies, Inc.	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
	54.175.70.194	United States	14618	Amazon Technologies Inc.	Malware Process
	104.16.149.172		13335	Cloudflare, Inc.	Malware Process
	23.218.156.113		20940	Akamai Technologies, Inc.	OS Process
	184.26.44.103		20940	Akamai Technologies, Inc.	Malware Process
	104.31.74.124		13335	Cloudflare, Inc.	Malware Process
	52.2.101.52		14618	Amazon Technologies Inc.	Malware Process
	104.31.74.124		13335	Cloudflare, Inc.	Malware Process
	119.28.153.89		132203	Tencent cloud computing (Beijing) ...	Malware Process
	74.82.59.181		6939	Hurricane Electric LLC	Malware Process
	184.26.44.103		20940	Akamai Technologies, Inc.	Malware Process
	188.226.138.244		14061		Malware Process
	104.31.75.124		13335	Cloudflare, Inc.	Malware Process
	66.61.174.137		7843	Time Warner Cable Internet LLC	OS Process
	216.105.38.13		6130	Internet Express	Malware Process

HTTP PACKETS

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
downloads.sourceforge.net	80	GET	1.1	Notepad++/Plugin-Manag...	1	87.8053319454
Path: /project/npppluginmgr/xml/plugins.md5.txt **URI:** http://downloads.sourceforge.net/project/npppluginmgr/xml/plugins.md5.txt						
api.blockcypher.com	80	GET	1.1	Mozilla/4.0 (compatible; M...	1	88.9128448963
Path: /v1/btc/main/addrs/17gd1msp5FnMcEMF1MitTNSsYs7w7AQyCt?_=1524383141575 **URI:** http://api.blockcypher.com/v1/btc/main/addrs/17gd1msp5FnMcEMF1MitTNSsYs7w7AQyCt?_=1524383141575						
btc.blockr.io	80	GET	1.1	Mozilla/4.0 (compatible; M...	1	90.1869680882
Path: /api/v1/address/txs/17gd1msp5FnMcEMF1MitTNSsYs7w7AQyCt?_=1524384986825 **URI:** http://btc.blockr.io/api/v1/address/txs/17gd1msp5FnMcEMF1MitTNSsYs7w7AQyCt?_=1524384986825						
ctldl.windowsupdate.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	90.3344919682
Path: /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?5f7ede18f3015712 **URI:** http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?5f7ede18f3015712						
isrg.trustid.ocsp.identrust.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	91.0866289139
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBRv9GhNQxLSSGKBnMArPUcsHYovpgQUxKexpHsscfrb4UuQdf%2FEFWCFiRACEAoBQUIAAAFThXNqC4Xspwg%3D **URI:** http://isrg.trustid.ocsp.identrust.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBRv9GhNQxLSSGKBnMArPUcsHYovpgQUxKexpHsscfrb4UuQdf%2FEFWCFiRACEAoBQUIAAAFThXNqC4Xspwg%3D						
ocsp.globalsign.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	91.1775760651
Path: /rootr1/MEwwSjBIMEYwRDAJBgUrDgMCGgUABBS3V7W2nAf4FiMTjpDJKg6%2BMgGqMQQUYHtmGkUNl8qJUC99BM00qP%2F8%2FUsCCwQAAAAAAURO8D4g **URI:** http://ocsp.globalsign.com/rootr1/MEwwSjBIMEYwRDAJBgUrDgMCGgUABBS3V7W2nAf4FiMTjpDJKg6%2BMgGqMQQUYHtmGkUNl8qJUC99BM00qP%2F8%2FUsCCwQAAAAAAURO8D4g						
ocsp.int-x3.letsencrypt.org	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	91.6210770607
Path: /MFMwUTBPME0wSzAJBgUrDgMCGgUABBR%2B5mrncpqz%2FPiiIGRsFqEtYHEIXQQUqEpqYwR93brm0Tm3pkVl7%2FOo7KECEgSMnuKt8tKyyjnODwjC1ZYVOw%3D%3D **URI:** http://ocsp.int-x3.letsencrypt.org/MFMwUTBPME0wSzAJBgUrDgMCGgUABBR%2B5mrncpqz%2FPiiIGRsFqEtYHEIXQQUqEpqYwR93brm0Tm3pkVl7%2FOo7KECEgSMnuKt8tKyyjnODwjC1ZYVOw%3D%3D						
ocsp2.globalsign.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	91.6724069118
Path: /gsdomainvalsha2g2/ME0wSzBJMEcwRTAJBgUrDgMCGgUABBTR8bV2%2Be7AwQ96%2FHwxJKnDYl18YQQU6k581IAt5RWBhiaMgm3AmKTPlw8CDAIeKarC7MJ2RYOA9A%3D%3D **URI:** http://ocsp2.globalsign.com/gsdomainvalsha2g2/ME0wSzBJMEcwRTAJBgUrDgMCGgUABBTR8bV2%2Be7AwQ96%2FHwxJKnDYl18YQQU6k581IAt5RWBhiaMgm3AmKTPlw8CDAIeKarC7MJ2RYOA9A%3D%3D						
downloads.sourceforge.net	80	GET	1.1	Notepad++/Plugin-Manag...	1	92.1610920429
Path: /project/npppluginmgr/xml/plugins.zip **URI:** http://downloads.sourceforge.net/project/npppluginmgr/xml/plugins.zip						
p27dokhpz2n7nvgr.1j9r76.top	80	GET	1.1	Mozilla/4.0 (compatible; M...	1	93.9412550926
Path: /56BE-BE2A-3B89-0446-990F?iframe&_=1524386779887 **URI:** http://p27dokhpz2n7nvgr.1j9r76.top/56BE-BE2A-3B89-0446-990F?iframe&_=1524386779887						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	130.268583059
Path: /pki/crl/products/tspca.crl **URI:** http://crl.microsoft.com/pki/crl/products/tspca.crl						

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	130.682323933
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	131.439166069
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	132.081161976
Path: /primobject.crl **URI:** http://crl.globalsign.net/primobject.crl						

DNS QUERIES

Request	Type
downloads.sourceforge.net	A
Answers - 216.105.38.13 (A)	
cytranet.dl.sourceforge.net	A
Answers - 74.82.59.181 (A)	
api.blockcypher.com	A
Answers - 54.175.70.194 (A) - 52.2.101.52 (A)	
btc.blockr.io	A
Answers - 104.16.148.172 (A) - 104.16.152.172 (A) - 104.16.150.172 (A) - 104.16.151.172 (A) - 104.16.149.172 (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)	
bitaps.com	A
Answers - 198.211.122.103 (A) - 188.226.138.244 (A)	
isrg.trustid.ocsp.identrust.com	A

Request	Type
Answers - 184.26.44.103 (A) - 184.26.44.106 (A) - a279.dscq.akamai.net (CNAME) - isrg.trustid.ocsp.identrust.com.edgesuite.net (CNAME)	
ocsp.globalsign.com	A
Answers - 104.31.75.124 (A) - global.prd.cdn.globalsign.com (CNAME) - cdn.globalsigncdn.com.cdn.cloudflare.net (CNAME) - 104.31.74.124 (A)	
ocsp.int-x3.letsencrypt.org	A
Answers - a771.dscq.akamai.net (CNAME) - ocsp.int-x3.letsencrypt.org.edgesuite.net (CNAME)	
ocsp2.globalsign.com	A
p27dokhpz2n7nvgr.1j9r76.top	A
Answers - 119.28.153.89 (A)	
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
87.8053319454	Sandbox	216.105.38.13	80
88.3809330463	Sandbox	74.82.59.181	443
88.9128448963	Sandbox	54.175.70.194	80
90.1869680882	Sandbox	104.16.152.172	80
90.3344919682	Sandbox	184.26.44.97	80
90.3983700275	Sandbox	188.226.138.244	443
91.0866289139	Sandbox	184.26.44.103	80
91.1775760651	Sandbox	104.31.74.124	80
91.6210770607	Sandbox	184.26.44.105	80
91.6724069118	Sandbox	104.31.75.124	80
92.1610920429	Sandbox	216.105.38.13	80
92.3350570202	Sandbox	74.82.59.181	443
93.9412550926	Sandbox	119.28.153.89	80
130.268583059	Sandbox	184.26.44.98	80
132.081161976	Sandbox	104.31.75.124	80

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
7.01524496078	Sandbox	224.0.0.252	5355
7.04289293289	Sandbox	224.0.0.252	5355
7.06518006325	Sandbox	239.255.255.250	3702
7.07647490501	Sandbox	192.168.56.255	137
9.6396150589	Sandbox	224.0.0.252	5355
13.0758750439	Sandbox	192.168.56.255	138
53.8743300438	Sandbox	178.33.158.0	6893
53.8745830059	Sandbox	178.33.158.1	6893
53.8747799397	Sandbox	178.33.158.2	6893
53.8749420643	Sandbox	178.33.158.3	6893
53.8751180172	Sandbox	178.33.158.4	6893
53.8752710819	Sandbox	178.33.158.5	6893
53.8753890991	Sandbox	178.33.158.6	6893
53.875510931	Sandbox	178.33.158.7	6893
53.8756279945	Sandbox	178.33.158.8	6893
53.8757419586	Sandbox	178.33.158.9	6893
53.8758568764	Sandbox	178.33.158.10	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
53.8759720325	Sandbox	178.33.158.11	6893
53.8761329651	Sandbox	178.33.158.12	6893
53.8762500286	Sandbox	178.33.158.13	6893
53.8763680458	Sandbox	178.33.158.14	6893
53.8764829636	Sandbox	178.33.158.15	6893
53.8765978813	Sandbox	178.33.158.16	6893
53.8767120838	Sandbox	178.33.158.17	6893
53.8768260479	Sandbox	178.33.158.18	6893
53.8769390583	Sandbox	178.33.158.19	6893
53.8770840168	Sandbox	178.33.158.20	6893
53.8771998882	Sandbox	178.33.158.21	6893
53.8773169518	Sandbox	178.33.158.22	6893
53.8774318695	Sandbox	178.33.158.23	6893
53.877546072	Sandbox	178.33.158.24	6893
53.8776600361	Sandbox	178.33.158.25	6893
53.8777730465	Sandbox	178.33.158.26	6893
53.8778870106	Sandbox	178.33.158.27	6893
53.878000021	Sandbox	178.33.158.28	6893
53.8781139851	Sandbox	178.33.158.29	6893
53.8782279491	Sandbox	178.33.158.30	6893
53.8783419132	Sandbox	178.33.158.31	6893
53.8784630299	Sandbox	178.33.159.0	6893
53.8785789013	Sandbox	178.33.159.1	6893
53.8786931038	Sandbox	178.33.159.2	6893
53.8788099289	Sandbox	178.33.159.3	6893
53.878923893	Sandbox	178.33.159.4	6893
53.8790369034	Sandbox	178.33.159.5	6893
53.8791520596	Sandbox	178.33.159.6	6893
53.8792660236	Sandbox	178.33.159.7	6893
53.879379034	Sandbox	178.33.159.8	6893
53.8794929981	Sandbox	178.33.159.9	6893
53.8796069622	Sandbox	178.33.159.10	6893
53.8797240257	Sandbox	178.33.159.11	6893
53.8798379898	Sandbox	178.33.159.12	6893
53.8799519539	Sandbox	178.33.159.13	6893
53.8800768852	Sandbox	178.33.159.14	6893
53.8801920414	Sandbox	178.33.159.15	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
53.8803060055	Sandbox	178.33.159.16	6893
53.8804180622	Sandbox	178.33.159.17	6893
53.8805339336	Sandbox	178.33.159.18	6893
53.8806490898	Sandbox	178.33.159.19	6893
53.8807640076	Sandbox	178.33.159.20	6893
53.8808789253	Sandbox	178.33.159.21	6893
53.8810908794	Sandbox	178.33.159.22	6893
53.8812069893	Sandbox	178.33.159.23	6893
53.8813209534	Sandbox	178.33.159.24	6893
53.8814358711	Sandbox	178.33.159.25	6893
53.881551981	Sandbox	178.33.159.26	6893
53.8816680908	Sandbox	178.33.159.27	6893
53.8817830086	Sandbox	178.33.159.28	6893
53.8818979263	Sandbox	178.33.159.29	6893
53.8820130825	Sandbox	178.33.159.30	6893
53.8821299076	Sandbox	178.33.159.31	6893
53.8822860718	Sandbox	178.33.160.0	6893
53.8824028969	Sandbox	178.33.160.1	6893
53.8825170994	Sandbox	178.33.160.2	6893
53.8826348782	Sandbox	178.33.160.3	6893
53.8827490807	Sandbox	178.33.160.4	6893
53.8828639984	Sandbox	178.33.160.5	6893
53.8829798698	Sandbox	178.33.160.6	6893
53.883095026	Sandbox	178.33.160.7	6893
53.8832089901	Sandbox	178.33.160.8	6893
53.8833250999	Sandbox	178.33.160.9	6893
53.883439064	Sandbox	178.33.160.10	6893
53.8835539818	Sandbox	178.33.160.11	6893
53.8836688995	Sandbox	178.33.160.12	6893
53.8837840557	Sandbox	178.33.160.13	6893
53.8838989735	Sandbox	178.33.160.14	6893
53.8840498924	Sandbox	178.33.160.15	6893
53.8841719627	Sandbox	178.33.160.16	6893
53.8842868805	Sandbox	178.33.160.17	6893
53.884401083	Sandbox	178.33.160.18	6893
53.8845150471	Sandbox	178.33.160.19	6893
53.8846290112	Sandbox	178.33.160.20	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
53.884747982	Sandbox	178.33.160.21	6893
53.8848640919	Sandbox	178.33.160.22	6893
53.884978056	Sandbox	178.33.160.23	6893
53.8850939274	Sandbox	178.33.160.24	6893
53.8852090836	Sandbox	178.33.160.25	6893
53.8853230476	Sandbox	178.33.160.26	6893
53.8854398727	Sandbox	178.33.160.27	6893
53.8855550289	Sandbox	178.33.160.28	6893
53.885668993	Sandbox	178.33.160.29	6893
53.8857839108	Sandbox	178.33.160.30	6893
53.8858990669	Sandbox	178.33.160.31	6893
53.886013031	Sandbox	178.33.160.32	6893
53.8861269951	Sandbox	178.33.160.33	6893
53.8862419128	Sandbox	178.33.160.34	6893
53.8863549232	Sandbox	178.33.160.35	6893
53.8864688873	Sandbox	178.33.160.36	6893
53.8865818977	Sandbox	178.33.160.37	6893
53.8866970539	Sandbox	178.33.160.38	6893
53.886813879	Sandbox	178.33.160.39	6893
53.8869299889	Sandbox	178.33.160.40	6893
53.8870439529	Sandbox	178.33.160.41	6893
53.8871588707	Sandbox	178.33.160.42	6893
53.8872718811	Sandbox	178.33.160.43	6893
53.8874249458	Sandbox	178.33.160.44	6893
53.8876080513	Sandbox	178.33.160.45	6893
53.8877270222	Sandbox	178.33.160.46	6893
53.887845993	Sandbox	178.33.160.47	6893
53.8879599571	Sandbox	178.33.160.48	6893
53.8880820274	Sandbox	178.33.160.49	6893
53.888199091	Sandbox	178.33.160.50	6893
53.888313055	Sandbox	178.33.160.51	6893
53.8884270191	Sandbox	178.33.160.52	6893
53.8885400295	Sandbox	178.33.160.53	6893
53.8886580467	Sandbox	178.33.160.54	6893
53.8887770176	Sandbox	178.33.160.55	6893
53.888892889	Sandbox	178.33.160.56	6893
53.8890080452	Sandbox	178.33.160.57	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
53.8891220093	Sandbox	178.33.160.58	6893
53.889236927	Sandbox	178.33.160.59	6893
53.8893520832	Sandbox	178.33.160.60	6893
53.8894660473	Sandbox	178.33.160.61	6893
53.889580965	Sandbox	178.33.160.62	6893
53.8896949291	Sandbox	178.33.160.63	6893
53.8898100853	Sandbox	178.33.160.64	6893
53.8899240494	Sandbox	178.33.160.65	6893
53.8900380135	Sandbox	178.33.160.66	6893
53.8901510239	Sandbox	178.33.160.67	6893
53.8902649879	Sandbox	178.33.160.68	6893
53.8903799057	Sandbox	178.33.160.69	6893
53.8904950619	Sandbox	178.33.160.70	6893
53.890609026	Sandbox	178.33.160.71	6893
53.89072299	Sandbox	178.33.160.72	6893
53.8908419609	Sandbox	178.33.160.73	6893
53.890955925	Sandbox	178.33.160.74	6893
53.8910689354	Sandbox	178.33.160.75	6893
53.8911819458	Sandbox	178.33.160.76	6893
53.8912959099	Sandbox	178.33.160.77	6893
53.8914110661	Sandbox	178.33.160.78	6893
53.8915250301	Sandbox	178.33.160.79	6893
53.8916399479	Sandbox	178.33.160.80	6893
53.891753912	Sandbox	178.33.160.81	6893
53.8918678761	Sandbox	178.33.160.82	6893
53.8919949532	Sandbox	178.33.160.83	6893
53.8921160698	Sandbox	178.33.160.84	6893
53.8922300339	Sandbox	178.33.160.85	6893
53.892385006	Sandbox	178.33.160.86	6893
53.8925030231	Sandbox	178.33.160.87	6893
53.8926169872	Sandbox	178.33.160.88	6893
53.8927309513	Sandbox	178.33.160.89	6893
53.8928439617	Sandbox	178.33.160.90	6893
53.8929579258	Sandbox	178.33.160.91	6893
53.8930709362	Sandbox	178.33.160.92	6893
53.8931839466	Sandbox	178.33.160.93	6893
53.8932991028	Sandbox	178.33.160.94	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
53.8934130669	Sandbox	178.33.160.95	6893
53.8935270309	Sandbox	178.33.160.96	6893
53.893640995	Sandbox	178.33.160.97	6893
53.8937549591	Sandbox	178.33.160.98	6893
53.8939640522	Sandbox	178.33.160.99	6893
53.8940908909	Sandbox	178.33.160.100	6893
53.8942079544	Sandbox	178.33.160.101	6893
53.8943250179	Sandbox	178.33.160.102	6893
53.8944408894	Sandbox	178.33.160.103	6893
53.8945550919	Sandbox	178.33.160.104	6893
53.8946700096	Sandbox	178.33.160.105	6893
53.89478302	Sandbox	178.33.160.106	6893
53.8948969841	Sandbox	178.33.160.107	6893
53.8950109482	Sandbox	178.33.160.108	6893
53.8951249123	Sandbox	178.33.160.109	6893
53.8952410221	Sandbox	178.33.160.110	6893
53.895359993	Sandbox	178.33.160.111	6893
53.895526886	Sandbox	178.33.160.112	6893
53.8956460953	Sandbox	178.33.160.113	6893
53.8957629204	Sandbox	178.33.160.114	6893
53.8958790302	Sandbox	178.33.160.115	6893
53.8960199356	Sandbox	178.33.160.116	6893
53.8961539268	Sandbox	178.33.160.117	6893
53.896271944	Sandbox	178.33.160.118	6893
53.8963871002	Sandbox	178.33.160.119	6893
53.8965010643	Sandbox	178.33.160.120	6893
53.8966159821	Sandbox	178.33.160.121	6893
53.8967320919	Sandbox	178.33.160.122	6893
53.896846056	Sandbox	178.33.160.123	6893
53.8969600201	Sandbox	178.33.160.124	6893
53.8970780373	Sandbox	178.33.160.125	6893
53.8971951008	Sandbox	178.33.160.126	6893
53.8973090649	Sandbox	178.33.160.127	6893
53.8974239826	Sandbox	178.33.160.128	6893
53.8975739479	Sandbox	178.33.160.129	6893
53.8976900578	Sandbox	178.33.160.130	6893
53.8978049755	Sandbox	178.33.160.131	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
53.8979189396	Sandbox	178.33.160.132	6893
53.89803195	Sandbox	178.33.160.133	6893
53.8981480598	Sandbox	178.33.160.134	6893
53.8982629776	Sandbox	178.33.160.135	6893
53.8983778954	Sandbox	178.33.160.136	6893
53.8984920979	Sandbox	178.33.160.137	6893
53.8986110687	Sandbox	178.33.160.138	6893
53.8987259865	Sandbox	178.33.160.139	6893
53.8988399506	Sandbox	178.33.160.140	6893
53.8989539146	Sandbox	178.33.160.141	6893
53.8990690708	Sandbox	178.33.160.142	6893
53.8991839886	Sandbox	178.33.160.143	6893
53.8993010521	Sandbox	178.33.160.144	6893
53.8994140625	Sandbox	178.33.160.145	6893
53.8995280266	Sandbox	178.33.160.146	6893
53.8996429443	Sandbox	178.33.160.147	6893
53.8997569084	Sandbox	178.33.160.148	6893
53.8998720646	Sandbox	178.33.160.149	6893
53.8999938965	Sandbox	178.33.160.150	6893
53.9001159668	Sandbox	178.33.160.151	6893
53.9002308846	Sandbox	178.33.160.152	6893
53.900343895	Sandbox	178.33.160.153	6893
53.9004590511	Sandbox	178.33.160.154	6893
53.9005720615	Sandbox	178.33.160.155	6893
53.9006888866	Sandbox	178.33.160.156	6893
53.9008030891	Sandbox	178.33.160.157	6893
53.9009189606	Sandbox	178.33.160.158	6893
53.9010839462	Sandbox	178.33.160.159	6893
53.9012019634	Sandbox	178.33.160.160	6893
53.9013168812	Sandbox	178.33.160.161	6893
53.9014310837	Sandbox	178.33.160.162	6893
53.9015440941	Sandbox	178.33.160.163	6893
53.9016580582	Sandbox	178.33.160.164	6893
53.9017720222	Sandbox	178.33.160.165	6893
53.9018919468	Sandbox	178.33.160.166	6893
53.9020059109	Sandbox	178.33.160.167	6893
53.902121067	Sandbox	178.33.160.168	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
53.9022359848	Sandbox	178.33.160.169	6893
53.9023509026	Sandbox	178.33.160.170	6893
53.9025020599	Sandbox	178.33.160.171	6893
53.9026210308	Sandbox	178.33.160.172	6893
53.9027359486	Sandbox	178.33.160.173	6893
53.9028539658	Sandbox	178.33.160.174	6893
53.9029688835	Sandbox	178.33.160.175	6893
53.9030840397	Sandbox	178.33.160.176	6893
53.999808073	Sandbox	178.33.160.177	6893
54.0000588894	Sandbox	178.33.160.178	6893
54.0002560616	Sandbox	178.33.160.179	6893
54.0004220009	Sandbox	178.33.160.180	6893
54.0005838871	Sandbox	178.33.160.181	6893
54.0007410049	Sandbox	178.33.160.182	6893
54.0008950233	Sandbox	178.33.160.183	6893
54.0010199547	Sandbox	178.33.160.184	6893
54.0011370182	Sandbox	178.33.160.185	6893
54.0013160706	Sandbox	178.33.160.186	6893
54.0015029907	Sandbox	178.33.160.187	6893
54.0016200542	Sandbox	178.33.160.188	6893
54.0017418861	Sandbox	178.33.160.189	6893
54.0018599033	Sandbox	178.33.160.190	6893
54.0019760132	Sandbox	178.33.160.191	6893
54.0020930767	Sandbox	178.33.160.192	6893
54.0022079945	Sandbox	178.33.160.193	6893
54.0023241043	Sandbox	178.33.160.194	6893
54.0024399757	Sandbox	178.33.160.195	6893
54.0025639534	Sandbox	178.33.160.196	6893
54.0027420521	Sandbox	178.33.160.197	6893
54.002863884	Sandbox	178.33.160.198	6893
54.0029809475	Sandbox	178.33.160.199	6893
54.0030970573	Sandbox	178.33.160.200	6893
54.0032129288	Sandbox	178.33.160.201	6893
54.0033290386	Sandbox	178.33.160.202	6893
54.0034499168	Sandbox	178.33.160.203	6893
54.003567934	Sandbox	178.33.160.204	6893
54.0036849976	Sandbox	178.33.160.205	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
54.0038020611	Sandbox	178.33.160.206	6893
54.0039188862	Sandbox	178.33.160.207	6893
54.004076004	Sandbox	178.33.160.208	6893
54.0042309761	Sandbox	178.33.160.209	6893
54.0043509007	Sandbox	178.33.160.210	6893
54.0044848919	Sandbox	178.33.160.211	6893
54.0046041012	Sandbox	178.33.160.212	6893
54.0047199726	Sandbox	178.33.160.213	6893
54.0048348904	Sandbox	178.33.160.214	6893
54.0049490929	Sandbox	178.33.160.215	6893
54.0050621033	Sandbox	178.33.160.216	6893
54.0051748753	Sandbox	178.33.160.217	6893
54.0052890778	Sandbox	178.33.160.218	6893
54.0054049492	Sandbox	178.33.160.219	6893
54.0055189133	Sandbox	178.33.160.220	6893
54.0056340694	Sandbox	178.33.160.221	6893
54.0057909489	Sandbox	178.33.160.222	6893
54.0059089661	Sandbox	178.33.160.223	6893
54.0060238838	Sandbox	178.33.160.224	6893
54.00613904	Sandbox	178.33.160.225	6893
54.0062549114	Sandbox	178.33.160.226	6893
54.0063960552	Sandbox	178.33.160.227	6893
54.0065140724	Sandbox	178.33.160.228	6893
54.006633997	Sandbox	178.33.160.229	6893
54.0067498684	Sandbox	178.33.160.230	6893
54.0068650246	Sandbox	178.33.160.231	6893
54.0069799423	Sandbox	178.33.160.232	6893
54.0070950985	Sandbox	178.33.160.233	6893
54.0072119236	Sandbox	178.33.160.234	6893
54.0073270798	Sandbox	178.33.160.235	6893
54.0074419975	Sandbox	178.33.160.236	6893
54.007557869	Sandbox	178.33.160.237	6893
54.0076720715	Sandbox	178.33.160.238	6893
54.0077869892	Sandbox	178.33.160.239	6893
54.0079050064	Sandbox	178.33.160.240	6893
54.0080299377	Sandbox	178.33.160.241	6893
54.0081450939	Sandbox	178.33.160.242	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
54.0082600117	Sandbox	178.33.160.243	6893
54.0083730221	Sandbox	178.33.160.244	6893
54.0084888935	Sandbox	178.33.160.245	6893
54.0086040497	Sandbox	178.33.160.246	6893
54.0087189674	Sandbox	178.33.160.247	6893
54.0088329315	Sandbox	178.33.160.248	6893
54.008949995	Sandbox	178.33.160.249	6893
54.0090649128	Sandbox	178.33.160.250	6893
54.009180069	Sandbox	178.33.160.251	6893
54.0092940331	Sandbox	178.33.160.252	6893
54.0094089508	Sandbox	178.33.160.253	6893
54.0095238686	Sandbox	178.33.160.254	6893
55.0687549114	Sandbox	178.33.160.255	6893
55.068967104	Sandbox	178.33.161.0	6893
55.0690979958	Sandbox	178.33.161.1	6893
55.0692200661	Sandbox	178.33.161.2	6893
55.0693399906	Sandbox	178.33.161.3	6893
55.0694589615	Sandbox	178.33.161.4	6893
55.0695769787	Sandbox	178.33.161.5	6893
55.0696959496	Sandbox	178.33.161.6	6893
55.0698158741	Sandbox	178.33.161.7	6893
55.0699388981	Sandbox	178.33.161.8	6893
55.0700569153	Sandbox	178.33.161.9	6893
55.0701799393	Sandbox	178.33.161.10	6893
55.0702989101	Sandbox	178.33.161.11	6893
55.0704159737	Sandbox	178.33.161.12	6893
55.0705339909	Sandbox	178.33.161.13	6893
55.0706529617	Sandbox	178.33.161.14	6893
55.0707719326	Sandbox	178.33.161.15	6893
55.0708899498	Sandbox	178.33.161.16	6893
55.0710070133	Sandbox	178.33.161.17	6893
55.0711228848	Sandbox	178.33.161.18	6893
55.0712399483	Sandbox	178.33.161.19	6893
55.0713570118	Sandbox	178.33.161.20	6893
55.0714728832	Sandbox	178.33.161.21	6893
55.0715909004	Sandbox	178.33.161.22	6893
55.0717110634	Sandbox	178.33.161.23	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
55.0718290806	Sandbox	178.33.161.24	6893
55.0719540119	Sandbox	178.33.161.25	6893
55.0721280575	Sandbox	178.33.161.26	6893
55.0722498894	Sandbox	178.33.161.27	6893
55.0723659992	Sandbox	178.33.161.28	6893
55.0724790096	Sandbox	178.33.161.29	6893
55.0725939274	Sandbox	178.33.161.30	6893
55.0727109909	Sandbox	178.33.161.31	6893
55.0728280544	Sandbox	178.33.161.32	6893
55.0729448795	Sandbox	178.33.161.33	6893
55.0730619431	Sandbox	178.33.161.34	6893
55.0732228756	Sandbox	178.33.161.35	6893
55.0733420849	Sandbox	178.33.161.36	6893
55.07345891	Sandbox	178.33.161.37	6893
55.0735859871	Sandbox	178.33.161.38	6893
55.0737059116	Sandbox	178.33.161.39	6893
55.07385993	Sandbox	178.33.161.40	6893
55.0740070343	Sandbox	178.33.161.41	6893
55.0741529465	Sandbox	178.33.161.42	6893
55.0743000507	Sandbox	178.33.161.43	6893
55.0744440556	Sandbox	178.33.161.44	6893
55.0745890141	Sandbox	178.33.161.45	6893
55.0747349262	Sandbox	178.33.161.46	6893
55.0748810768	Sandbox	178.33.161.47	6893
55.0750260353	Sandbox	178.33.161.48	6893
55.0751709938	Sandbox	178.33.161.49	6893
55.0754129887	Sandbox	178.33.161.50	6893
55.0755679607	Sandbox	178.33.161.51	6893
55.0757138729	Sandbox	178.33.161.52	6893
55.0758628845	Sandbox	178.33.161.53	6893
55.076020956	Sandbox	178.33.161.54	6893
55.0761680603	Sandbox	178.33.161.55	6893
55.0763130188	Sandbox	178.33.161.56	6893
55.0764579773	Sandbox	178.33.161.57	6893
55.0766050816	Sandbox	178.33.161.58	6893
55.0767500401	Sandbox	178.33.161.59	6893
55.0768959522	Sandbox	178.33.161.60	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
55.0770421028	Sandbox	178.33.161.61	6893
55.077188015	Sandbox	178.33.161.62	6893
55.0773329735	Sandbox	178.33.161.63	6893
55.077477932	Sandbox	178.33.161.64	6893
55.0776278973	Sandbox	178.33.161.65	6893
55.0777740479	Sandbox	178.33.161.66	6893
55.0779190063	Sandbox	178.33.161.67	6893
55.0780670643	Sandbox	178.33.161.68	6893
55.0782170296	Sandbox	178.33.161.69	6893
55.0783638954	Sandbox	178.33.161.70	6893
55.0785079002	Sandbox	178.33.161.71	6893
55.0786540508	Sandbox	178.33.161.72	6893
55.0787980556	Sandbox	178.33.161.73	6893
55.0789420605	Sandbox	178.33.161.74	6893
55.079087019	Sandbox	178.33.161.75	6893
55.0792319775	Sandbox	178.33.161.76	6893
55.0793809891	Sandbox	178.33.161.77	6893
55.0795280933	Sandbox	178.33.161.78	6893
55.0796730518	Sandbox	178.33.161.79	6893
55.079816103	Sandbox	178.33.161.80	6893
55.0799610615	Sandbox	178.33.161.81	6893
55.0801160336	Sandbox	178.33.161.82	6893
55.0802659988	Sandbox	178.33.161.83	6893
55.0804109573	Sandbox	178.33.161.84	6893
55.0805549622	Sandbox	178.33.161.85	6893
55.0806999207	Sandbox	178.33.161.86	6893
55.0808448792	Sandbox	178.33.161.87	6893
55.0809879303	Sandbox	178.33.161.88	6893
55.0811328888	Sandbox	178.33.161.89	6893
55.0812780857	Sandbox	178.33.161.90	6893
55.0814220905	Sandbox	178.33.161.91	6893
55.0815649033	Sandbox	178.33.161.92	6893
55.0817139149	Sandbox	178.33.161.93	6893
55.0818600655	Sandbox	178.33.161.94	6893
55.082005024	Sandbox	178.33.161.95	6893
55.0821499825	Sandbox	178.33.161.96	6893
55.0822949409	Sandbox	178.33.161.97	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
55.0824429989	Sandbox	178.33.161.98	6893
55.0825889111	Sandbox	178.33.161.99	6893
55.0827338696	Sandbox	178.33.161.100	6893
55.0828790665	Sandbox	178.33.161.101	6893
55.0830249786	Sandbox	178.33.161.102	6893
55.0831739902	Sandbox	178.33.161.103	6893
55.083327055	Sandbox	178.33.161.104	6893
55.0834739208	Sandbox	178.33.161.105	6893
55.0836200714	Sandbox	178.33.161.106	6893
55.0837640762	Sandbox	178.33.161.107	6893
55.0839090347	Sandbox	178.33.161.108	6893
55.084086895	Sandbox	178.33.161.109	6893
55.0842370987	Sandbox	178.33.161.110	6893
55.0843830109	Sandbox	178.33.161.111	6893
55.084528923	Sandbox	178.33.161.112	6893
55.0846779346	Sandbox	178.33.161.113	6893
55.0848240852	Sandbox	178.33.161.114	6893
55.0849690437	Sandbox	178.33.161.115	6893
55.0851960182	Sandbox	178.33.161.116	6893
55.0853729248	Sandbox	178.33.161.117	6893
55.0855209827	Sandbox	178.33.161.118	6893
55.085668087	Sandbox	178.33.161.119	6893
55.0858180523	Sandbox	178.33.161.120	6893
55.0859639645	Sandbox	178.33.161.121	6893
55.0861098766	Sandbox	178.33.161.122	6893
55.0862550735	Sandbox	178.33.161.123	6893
55.0864009857	Sandbox	178.33.161.124	6893
55.0865459442	Sandbox	178.33.161.125	6893
55.0866920948	Sandbox	178.33.161.126	6893
55.0868370533	Sandbox	178.33.161.127	6893
55.0869870186	Sandbox	178.33.161.128	6893
55.0871369839	Sandbox	178.33.161.129	6893
55.0872819424	Sandbox	178.33.161.130	6893
55.087428093	Sandbox	178.33.161.131	6893
55.0875730515	Sandbox	178.33.161.132	6893
55.0877170563	Sandbox	178.33.161.133	6893
55.0878629684	Sandbox	178.33.161.134	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
55.0880179405	Sandbox	178.33.161.135	6893
55.0881640911	Sandbox	178.33.161.136	6893
55.0883169174	Sandbox	178.33.161.137	6893
55.0884618759	Sandbox	178.33.161.138	6893
55.0886080265	Sandbox	178.33.161.139	6893
55.088752985	Sandbox	178.33.161.140	6893
55.0888988972	Sandbox	178.33.161.141	6893
55.0890450478	Sandbox	178.33.161.142	6893
55.089195013	Sandbox	178.33.161.143	6893
55.0893409252	Sandbox	178.33.161.144	6893
55.0894858837	Sandbox	178.33.161.145	6893
55.0896310806	Sandbox	178.33.161.146	6893
55.0897769928	Sandbox	178.33.161.147	6893
55.0899260044	Sandbox	178.33.161.148	6893
55.0900709629	Sandbox	178.33.161.149	6893
55.0902168751	Sandbox	178.33.161.150	6893
55.0903630257	Sandbox	178.33.161.151	6893
55.0905079842	Sandbox	178.33.161.152	6893
55.0906529427	Sandbox	178.33.161.153	6893
55.0908820629	Sandbox	178.33.161.154	6893
55.091039896	Sandbox	178.33.161.155	6893
55.0911870003	Sandbox	178.33.161.156	6893
55.0913319588	Sandbox	178.33.161.157	6893
55.0914819241	Sandbox	178.33.161.158	6893
55.0916280746	Sandbox	178.33.161.159	6893
55.0917730331	Sandbox	178.33.161.160	6893
55.0919189453	Sandbox	178.33.161.161	6893
55.09207201	Sandbox	178.33.161.162	6893
55.0922188759	Sandbox	178.33.161.163	6893
55.0923640728	Sandbox	178.33.161.164	6893
55.0925090313	Sandbox	178.33.161.165	6893
55.0926558971	Sandbox	178.33.161.166	6893
55.0928010941	Sandbox	178.33.161.167	6893
55.0929470062	Sandbox	178.33.161.168	6893
55.0930919647	Sandbox	178.33.161.169	6893
55.0932369232	Sandbox	178.33.161.170	6893
55.093403101	Sandbox	178.33.161.171	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
55.0935499668	Sandbox	178.33.161.172	6893
55.0936980247	Sandbox	178.33.161.173	6893
55.0938448906	Sandbox	178.33.161.174	6893
55.0939979553	Sandbox	178.33.161.175	6893
55.0941429138	Sandbox	178.33.161.176	6893
55.0942890644	Sandbox	178.33.161.177	6893
55.0944340229	Sandbox	178.33.161.178	6893
55.0945789814	Sandbox	178.33.161.179	6893
55.0947229862	Sandbox	178.33.161.180	6893
55.0948719978	Sandbox	178.33.161.181	6893
55.0950191021	Sandbox	178.33.161.182	6893
55.0951640606	Sandbox	178.33.161.183	6893
55.0953090191	Sandbox	178.33.161.184	6893
55.0954539776	Sandbox	178.33.161.185	6893
55.0955979824	Sandbox	178.33.161.186	6893
55.0957429409	Sandbox	178.33.161.187	6893
55.0959010124	Sandbox	178.33.161.188	6893
55.0960741043	Sandbox	178.33.161.189	6893
55.0962228775	Sandbox	178.33.161.190	6893
55.0963690281	Sandbox	178.33.161.191	6893
55.0965139866	Sandbox	178.33.161.192	6893
55.0966589451	Sandbox	178.33.161.193	6893
55.0968050957	Sandbox	178.33.161.194	6893
55.0969500542	Sandbox	178.33.161.195	6893
55.0970959663	Sandbox	178.33.161.196	6893
55.0972409248	Sandbox	178.33.161.197	6893
55.0973880291	Sandbox	178.33.161.198	6893
55.0975339413	Sandbox	178.33.161.199	6893
55.0976788998	Sandbox	178.33.161.200	6893
55.0978250504	Sandbox	178.33.161.201	6893
55.0979700089	Sandbox	178.33.161.202	6893
55.0981209278	Sandbox	178.33.161.203	6893
55.0982670784	Sandbox	178.33.161.204	6893
55.0984098911	Sandbox	178.33.161.205	6893
55.0985610485	Sandbox	178.33.161.206	6893
55.0987100601	Sandbox	178.33.161.207	6893
55.0988550186	Sandbox	178.33.161.208	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
55.0990009308	Sandbox	178.33.161.209	6893
55.0991470814	Sandbox	178.33.161.210	6893
55.0992910862	Sandbox	178.33.161.211	6893
55.0994360447	Sandbox	178.33.161.212	6893
55.0995800495	Sandbox	178.33.161.213	6893
55.0997269154	Sandbox	178.33.161.214	6893
55.0998718739	Sandbox	178.33.161.215	6893
55.1000249386	Sandbox	178.33.161.216	6893
55.1001720428	Sandbox	178.33.161.217	6893
55.1003210545	Sandbox	178.33.161.218	6893
55.100466013	Sandbox	178.33.161.219	6893
55.1006100178	Sandbox	178.33.161.220	6893
55.1007540226	Sandbox	178.33.161.221	6893
55.1008989811	Sandbox	178.33.161.222	6893
55.1010439396	Sandbox	178.33.161.223	6893
55.1011879444	Sandbox	178.33.161.224	6893
55.1013319492	Sandbox	178.33.161.225	6893
55.1014750004	Sandbox	178.33.161.226	6893
55.1016209126	Sandbox	178.33.161.227	6893
55.1017639637	Sandbox	178.33.161.228	6893
55.1019070148	Sandbox	178.33.161.229	6893
55.102052927	Sandbox	178.33.161.230	6893
55.1021990776	Sandbox	178.33.161.231	6893
55.1023440361	Sandbox	178.33.161.232	6893
55.1024949551	Sandbox	178.33.161.233	6893
55.1026389599	Sandbox	178.33.161.234	6893
55.1027829647	Sandbox	178.33.161.235	6893
55.1029260159	Sandbox	178.33.161.236	6893
55.1030700207	Sandbox	178.33.161.237	6893
55.1032159328	Sandbox	178.33.161.238	6893
55.1033608913	Sandbox	178.33.161.239	6893
55.103511095	Sandbox	178.33.161.240	6893
55.1036550999	Sandbox	178.33.161.241	6893
55.1037991047	Sandbox	178.33.161.242	6893
55.1039428711	Sandbox	178.33.161.243	6893
55.1041209698	Sandbox	178.33.161.244	6893
55.1042668819	Sandbox	178.33.161.245	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
55.1044120789	Sandbox	178.33.161.246	6893
55.1045560837	Sandbox	178.33.161.247	6893
55.1047050953	Sandbox	178.33.161.248	6893
55.1048491001	Sandbox	178.33.161.249	6893
55.1049931049	Sandbox	178.33.161.250	6893
55.1052660942	Sandbox	178.33.161.251	6893
55.1054799557	Sandbox	178.33.161.252	6893
55.1056261063	Sandbox	178.33.161.253	6893
55.1057710648	Sandbox	178.33.161.254	6893
56.1481559277	Sandbox	178.33.161.255	6893
56.1483108997	Sandbox	178.33.162.0	6893
56.1484129429	Sandbox	178.33.162.1	6893
56.1485040188	Sandbox	178.33.162.2	6893
56.1485950947	Sandbox	178.33.162.3	6893
56.1486809254	Sandbox	178.33.162.4	6893
56.1487660408	Sandbox	178.33.162.5	6893
56.1488549709	Sandbox	178.33.162.6	6893
56.1489369869	Sandbox	178.33.162.7	6893
56.1490180492	Sandbox	178.33.162.8	6893
56.1491000652	Sandbox	178.33.162.9	6893
56.1491820812	Sandbox	178.33.162.10	6893
56.1492629051	Sandbox	178.33.162.11	6893
56.1493449211	Sandbox	178.33.162.12	6893
56.1494278908	Sandbox	178.33.162.13	6893
56.1495099068	Sandbox	178.33.162.14	6893
56.1495919228	Sandbox	178.33.162.15	6893
56.1496729851	Sandbox	178.33.162.16	6893
56.1497550011	Sandbox	178.33.162.17	6893
56.1498360634	Sandbox	178.33.162.18	6893
56.1499168873	Sandbox	178.33.162.19	6893
56.1499989033	Sandbox	178.33.162.20	6893
56.150083065	Sandbox	178.33.162.21	6893
56.150247097	Sandbox	178.33.162.22	6893
56.1504049301	Sandbox	178.33.162.23	6893
56.1504979134	Sandbox	178.33.162.24	6893
56.1505789757	Sandbox	178.33.162.25	6893
56.1506609917	Sandbox	178.33.162.26	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
56.150742054	Sandbox	178.33.162.27	6893
56.1508250237	Sandbox	178.33.162.28	6893
56.1509120464	Sandbox	178.33.162.29	6893
56.1509940624	Sandbox	178.33.162.30	6893
56.1510748863	Sandbox	178.33.162.31	6893
56.1511569023	Sandbox	178.33.162.32	6893
56.1512379646	Sandbox	178.33.162.33	6893
56.1513190269	Sandbox	178.33.162.34	6893
56.1514000893	Sandbox	178.33.162.35	6893
56.15148592	Sandbox	178.33.162.36	6893
56.1515679359	Sandbox	178.33.162.37	6893
56.1516499519	Sandbox	178.33.162.38	6893
56.1517310143	Sandbox	178.33.162.39	6893
56.1518120766	Sandbox	178.33.162.40	6893
56.1518929005	Sandbox	178.33.162.41	6893
56.1519739628	Sandbox	178.33.162.42	6893
56.152105093	Sandbox	178.33.162.43	6893
56.1521909237	Sandbox	178.33.162.44	6893
56.152271986	Sandbox	178.33.162.45	6893
56.1523530483	Sandbox	178.33.162.46	6893
56.1524350643	Sandbox	178.33.162.47	6893
56.1525170803	Sandbox	178.33.162.48	6893
56.1525969505	Sandbox	178.33.162.49	6893
56.1526780128	Sandbox	178.33.162.50	6893
56.1527619362	Sandbox	178.33.162.51	6893
56.1528720856	Sandbox	178.33.162.52	6893
56.1529560089	Sandbox	178.33.162.53	6893
56.1530370712	Sandbox	178.33.162.54	6893
56.1531209946	Sandbox	178.33.162.55	6893
56.1532049179	Sandbox	178.33.162.56	6893
56.1532869339	Sandbox	178.33.162.57	6893
56.1533689499	Sandbox	178.33.162.58	6893
56.1534509659	Sandbox	178.33.162.59	6893
56.1535329819	Sandbox	178.33.162.60	6893
56.1536850929	Sandbox	178.33.162.61	6893
56.1537709236	Sandbox	178.33.162.62	6893
56.1538519859	Sandbox	178.33.162.63	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
56.1539330482	Sandbox	178.33.162.64	6893
56.1540129185	Sandbox	178.33.162.65	6893
56.1540970802	Sandbox	178.33.162.66	6893
56.1541779041	Sandbox	178.33.162.67	6893
56.1542608738	Sandbox	178.33.162.68	6893
56.1543409824	Sandbox	178.33.162.69	6893
56.1544229984	Sandbox	178.33.162.70	6893
56.1545040607	Sandbox	178.33.162.71	6893
56.1545848846	Sandbox	178.33.162.72	6893
56.1546669006	Sandbox	178.33.162.73	6893
56.1547470093	Sandbox	178.33.162.74	6893
56.1548280716	Sandbox	178.33.162.75	6893
56.1549088955	Sandbox	178.33.162.76	6893
56.1549909115	Sandbox	178.33.162.77	6893
56.1550750732	Sandbox	178.33.162.78	6893
56.1551558971	Sandbox	178.33.162.79	6893
56.1552369595	Sandbox	178.33.162.80	6893
56.1553249359	Sandbox	178.33.162.81	6893
56.1554059982	Sandbox	178.33.162.82	6893
56.1554870605	Sandbox	178.33.162.83	6893
56.1555728912	Sandbox	178.33.162.84	6893
56.1556549072	Sandbox	178.33.162.85	6893
56.1557350159	Sandbox	178.33.162.86	6893
56.1558160782	Sandbox	178.33.162.87	6893
56.1558959484	Sandbox	178.33.162.88	6893
56.1559770107	Sandbox	178.33.162.89	6893
56.1560940742	Sandbox	178.33.162.90	6893
56.1561770439	Sandbox	178.33.162.91	6893
56.1562600136	Sandbox	178.33.162.92	6893
56.1563420296	Sandbox	178.33.162.93	6893
56.1564230919	Sandbox	178.33.162.94	6893
56.1565039158	Sandbox	178.33.162.95	6893
56.1565890312	Sandbox	178.33.162.96	6893
56.1566710472	Sandbox	178.33.162.97	6893
56.1567509174	Sandbox	178.33.162.98	6893
56.1568319798	Sandbox	178.33.162.99	6893
56.1569149494	Sandbox	178.33.162.100	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
56.1569979191	Sandbox	178.33.162.101	6893
56.1570808887	Sandbox	178.33.162.102	6893
56.1571629047	Sandbox	178.33.162.103	6893
56.1572449207	Sandbox	178.33.162.104	6893
56.1573269367	Sandbox	178.33.162.105	6893
56.1574089527	Sandbox	178.33.162.106	6893
56.1574950218	Sandbox	178.33.162.107	6893
56.1575779915	Sandbox	178.33.162.108	6893
56.1576609612	Sandbox	178.33.162.109	6893
56.1577699184	Sandbox	178.33.162.110	6893
56.1578578949	Sandbox	178.33.162.111	6893
56.1579458714	Sandbox	178.33.162.112	6893
56.1580278873	Sandbox	178.33.162.113	6893
56.1581110954	Sandbox	178.33.162.114	6893
56.1581919193	Sandbox	178.33.162.115	6893
56.158274889	Sandbox	178.33.162.116	6893
56.1583580971	Sandbox	178.33.162.117	6893
56.1584398746	Sandbox	178.33.162.118	6893
56.1585218906	Sandbox	178.33.162.119	6893
56.1586070061	Sandbox	178.33.162.120	6893
56.1586899757	Sandbox	178.33.162.121	6893
56.1587710381	Sandbox	178.33.162.122	6893
56.158853054	Sandbox	178.33.162.123	6893
56.15893507	Sandbox	178.33.162.124	6893
56.159017086	Sandbox	178.33.162.125	6893
56.1591029167	Sandbox	178.33.162.126	6893
56.1591849327	Sandbox	178.33.162.127	6893
56.159265995	Sandbox	178.33.162.128	6893
56.159348011	Sandbox	178.33.162.129	6893
56.159430027	Sandbox	178.33.162.130	6893
56.1595110893	Sandbox	178.33.162.131	6893
56.1595931053	Sandbox	178.33.162.132	6893
56.1596779823	Sandbox	178.33.162.133	6893
56.1597599983	Sandbox	178.33.162.134	6893
56.1598410606	Sandbox	178.33.162.135	6893
56.1599218845	Sandbox	178.33.162.136	6893
56.1600110531	Sandbox	178.33.162.137	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
56.1600930691	Sandbox	178.33.162.138	6893
56.1601769924	Sandbox	178.33.162.139	6893
56.1602590084	Sandbox	178.33.162.140	6893
56.1603438854	Sandbox	178.33.162.141	6893
56.1604249477	Sandbox	178.33.162.142	6893
56.1605060101	Sandbox	178.33.162.143	6893
56.1605870724	Sandbox	178.33.162.144	6893
56.1606678963	Sandbox	178.33.162.145	6893
56.1607489586	Sandbox	178.33.162.146	6893
56.1608300209	Sandbox	178.33.162.147	6893
56.1609110832	Sandbox	178.33.162.148	6893
56.1609930992	Sandbox	178.33.162.149	6893
56.1610739231	Sandbox	178.33.162.150	6893
56.1611549854	Sandbox	178.33.162.151	6893
56.1612360477	Sandbox	178.33.162.152	6893
56.1613309383	Sandbox	178.33.162.153	6893
56.1614220142	Sandbox	178.33.162.154	6893
56.1615099907	Sandbox	178.33.162.155	6893
56.1616020203	Sandbox	178.33.162.156	6893
56.1616899967	Sandbox	178.33.162.157	6893
56.1617779732	Sandbox	178.33.162.158	6893
56.1618680954	Sandbox	178.33.162.159	6893
56.1619560719	Sandbox	178.33.162.160	6893
56.1620430946	Sandbox	178.33.162.161	6893
56.1621310711	Sandbox	178.33.162.162	6893
56.1622169018	Sandbox	178.33.162.163	6893
56.1623048782	Sandbox	178.33.162.164	6893
56.162391901	Sandbox	178.33.162.165	6893
56.1624779701	Sandbox	178.33.162.166	6893
56.1625659466	Sandbox	178.33.162.167	6893
56.1626520157	Sandbox	178.33.162.168	6893
56.1627380848	Sandbox	178.33.162.169	6893
56.1628239155	Sandbox	178.33.162.170	6893
56.1629478931	Sandbox	178.33.162.171	6893
56.1630420685	Sandbox	178.33.162.172	6893
56.1631290913	Sandbox	178.33.162.173	6893
56.1632390022	Sandbox	178.33.162.174	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
56.1633269787	Sandbox	178.33.162.175	6893
56.1634149551	Sandbox	178.33.162.176	6893
56.1635379791	Sandbox	178.33.162.177	6893
56.1636281013	Sandbox	178.33.162.178	6893
56.1637148857	Sandbox	178.33.162.179	6893
56.1638031006	Sandbox	178.33.162.180	6893
56.1638898849	Sandbox	178.33.162.181	6893
56.1639769077	Sandbox	178.33.162.182	6893
56.1641049385	Sandbox	178.33.162.183	6893
56.1641950607	Sandbox	178.33.162.184	6893
56.1642849445	Sandbox	178.33.162.185	6893
56.1643760204	Sandbox	178.33.162.186	6893
56.1644630432	Sandbox	178.33.162.187	6893
56.1645510197	Sandbox	178.33.162.188	6893
56.1646380424	Sandbox	178.33.162.189	6893
56.1647260189	Sandbox	178.33.162.190	6893
56.1648139954	Sandbox	178.33.162.191	6893
56.1649019718	Sandbox	178.33.162.192	6893
56.1649899483	Sandbox	178.33.162.193	6893
56.1650769711	Sandbox	178.33.162.194	6893
56.1651659012	Sandbox	178.33.162.195	6893
56.165252924	Sandbox	178.33.162.196	6893
56.1653399467	Sandbox	178.33.162.197	6893
56.1654279232	Sandbox	178.33.162.198	6893
56.1655139923	Sandbox	178.33.162.199	6893
56.165610075	Sandbox	178.33.162.200	6893
56.1657009125	Sandbox	178.33.162.201	6893
56.1657879353	Sandbox	178.33.162.202	6893
56.165874958	Sandbox	178.33.162.203	6893
56.1659650803	Sandbox	178.33.162.204	6893
56.1660530567	Sandbox	178.33.162.205	6893
56.1661400795	Sandbox	178.33.162.206	6893
56.1662271023	Sandbox	178.33.162.207	6893
56.1663138866	Sandbox	178.33.162.208	6893
56.1664009094	Sandbox	178.33.162.209	6893
56.1664869785	Sandbox	178.33.162.210	6893
56.1665759087	Sandbox	178.33.162.211	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
56.1666629314	Sandbox	178.33.162.212	6893
56.1667499542	Sandbox	178.33.162.213	6893
56.166836977	Sandbox	178.33.162.214	6893
56.1669239998	Sandbox	178.33.162.215	6893
56.1670138836	Sandbox	178.33.162.216	6893
56.1671020985	Sandbox	178.33.162.217	6893
56.1671879292	Sandbox	178.33.162.218	6893
56.1672759056	Sandbox	178.33.162.219	6893
56.1673638821	Sandbox	178.33.162.220	6893
56.1674520969	Sandbox	178.33.162.221	6893
56.1675400734	Sandbox	178.33.162.222	6893
56.1676280499	Sandbox	178.33.162.223	6893
56.1677138805	Sandbox	178.33.162.224	6893
56.1678009033	Sandbox	178.33.162.225	6893
56.1678879261	Sandbox	178.33.162.226	6893
56.1679749489	Sandbox	178.33.162.227	6893
56.1681149006	Sandbox	178.33.162.228	6893
56.1682069302	Sandbox	178.33.162.229	6893
56.1682949066	Sandbox	178.33.162.230	6893
56.1683859825	Sandbox	178.33.162.231	6893
56.168473959	Sandbox	178.33.162.232	6893
56.1685609818	Sandbox	178.33.162.233	6893
56.1686470509	Sandbox	178.33.162.234	6893
56.1687340736	Sandbox	178.33.162.235	6893
56.1688230038	Sandbox	178.33.162.236	6893
56.1689128876	Sandbox	178.33.162.237	6893
56.1689999104	Sandbox	178.33.162.238	6893
56.1690869331	Sandbox	178.33.162.239	6893
56.1692650318	Sandbox	178.33.162.240	6893
56.1693570614	Sandbox	178.33.162.241	6893
56.1694440842	Sandbox	178.33.162.242	6893
56.1695299149	Sandbox	178.33.162.243	6893
56.1696178913	Sandbox	178.33.162.244	6893
56.1697039604	Sandbox	178.33.162.245	6893
56.1697990894	Sandbox	178.33.162.246	6893
56.1698870659	Sandbox	178.33.162.247	6893
56.1699740887	Sandbox	178.33.162.248	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
56.1700639725	Sandbox	178.33.162.249	6893
56.1701519489	Sandbox	178.33.162.250	6893
56.1703190804	Sandbox	178.33.162.251	6893
56.1704809666	Sandbox	178.33.162.252	6893
56.1705760956	Sandbox	178.33.162.253	6893
56.170664072	Sandbox	178.33.162.254	6893
57.2293329239	Sandbox	178.33.162.255	6893
57.2294991016	Sandbox	178.33.163.0	6893
57.2295949459	Sandbox	178.33.163.1	6893
57.2296829224	Sandbox	178.33.163.2	6893
57.2297699451	Sandbox	178.33.163.3	6893
57.2298550606	Sandbox	178.33.163.4	6893
57.2299480438	Sandbox	178.33.163.5	6893
57.2300310135	Sandbox	178.33.163.6	6893
57.2301199436	Sandbox	178.33.163.7	6893
57.2302029133	Sandbox	178.33.163.8	6893
57.2302849293	Sandbox	178.33.163.9	6893
57.2303669453	Sandbox	178.33.163.10	6893
57.2304499149	Sandbox	178.33.163.11	6893
57.2305328846	Sandbox	178.33.163.12	6893
57.2306160927	Sandbox	178.33.163.13	6893
57.2306969166	Sandbox	178.33.163.14	6893
57.2307789326	Sandbox	178.33.163.15	6893
57.2308619022	Sandbox	178.33.163.16	6893
57.2309429646	Sandbox	178.33.163.17	6893
57.2310268879	Sandbox	178.33.163.18	6893
57.2311079502	Sandbox	178.33.163.19	6893
57.2311980724	Sandbox	178.33.163.20	6893
57.2312810421	Sandbox	178.33.163.21	6893
57.2313621044	Sandbox	178.33.163.22	6893
57.2314450741	Sandbox	178.33.163.23	6893
57.2315270901	Sandbox	178.33.163.24	6893
57.231730938	Sandbox	178.33.163.25	6893
57.2318210602	Sandbox	178.33.163.26	6893
57.2319049835	Sandbox	178.33.163.27	6893
57.2319989204	Sandbox	178.33.163.28	6893
57.2321140766	Sandbox	178.33.163.29	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
57.232198	Sandbox	178.33.163.30	6893
57.2322800159	Sandbox	178.33.163.31	6893
57.2323679924	Sandbox	178.33.163.32	6893
57.2324528694	Sandbox	178.33.163.33	6893
57.2325360775	Sandbox	178.33.163.34	6893
57.2326231003	Sandbox	178.33.163.35	6893
57.2327070236	Sandbox	178.33.163.36	6893
57.2327890396	Sandbox	178.33.163.37	6893
57.2328701019	Sandbox	178.33.163.38	6893
57.2329530716	Sandbox	178.33.163.39	6893
57.2330350876	Sandbox	178.33.163.40	6893
57.2331171036	Sandbox	178.33.163.41	6893
57.2332279682	Sandbox	178.33.163.42	6893
57.2333118916	Sandbox	178.33.163.43	6893
57.2333939075	Sandbox	178.33.163.44	6893
57.2334759235	Sandbox	178.33.163.45	6893
57.2335579395	Sandbox	178.33.163.46	6893
57.2336468697	Sandbox	178.33.163.47	6893
57.2337300777	Sandbox	178.33.163.48	6893
57.2338120937	Sandbox	178.33.163.49	6893
57.2338969707	Sandbox	178.33.163.50	6893
57.2339808941	Sandbox	178.33.163.51	6893
57.2340629101	Sandbox	178.33.163.52	6893
57.2341458797	Sandbox	178.33.163.53	6893
57.2342290878	Sandbox	178.33.163.54	6893
57.2343111038	Sandbox	178.33.163.55	6893
57.2343928814	Sandbox	178.33.163.56	6893
57.2344748974	Sandbox	178.33.163.57	6893
57.2345569134	Sandbox	178.33.163.58	6893
57.2346410751	Sandbox	178.33.163.59	6893
57.2347240448	Sandbox	178.33.163.60	6893
57.2348070145	Sandbox	178.33.163.61	6893
57.2348890305	Sandbox	178.33.163.62	6893
57.2349710464	Sandbox	178.33.163.63	6893
57.2350518703	Sandbox	178.33.163.64	6893
57.2351379395	Sandbox	178.33.163.65	6893
57.2352209091	Sandbox	178.33.163.66	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
57.2353038788	Sandbox	178.33.163.67	6893
57.2353880405	Sandbox	178.33.163.68	6893
57.2355420589	Sandbox	178.33.163.69	6893
57.2357189655	Sandbox	178.33.163.70	6893
57.235861063	Sandbox	178.33.163.71	6893
57.235943079	Sandbox	178.33.163.72	6893
57.2360310555	Sandbox	178.33.163.73	6893
57.2361190319	Sandbox	178.33.163.74	6893
57.2362039089	Sandbox	178.33.163.75	6893
57.2362859249	Sandbox	178.33.163.76	6893
57.2363679409	Sandbox	178.33.163.77	6893
57.2364480495	Sandbox	178.33.163.78	6893
57.2365300655	Sandbox	178.33.163.79	6893
57.2366170883	Sandbox	178.33.163.80	6893
57.236700058	Sandbox	178.33.163.81	6893
57.2367839813	Sandbox	178.33.163.82	6893
57.2368659973	Sandbox	178.33.163.83	6893
57.2369480133	Sandbox	178.33.163.84	6893
57.2370319366	Sandbox	178.33.163.85	6893
57.237112999	Sandbox	178.33.163.86	6893
57.2371940613	Sandbox	178.33.163.87	6893
57.2372760773	Sandbox	178.33.163.88	6893
57.2373590469	Sandbox	178.33.163.89	6893
57.2374410629	Sandbox	178.33.163.90	6893
57.2375218868	Sandbox	178.33.163.91	6893
57.2376039028	Sandbox	178.33.163.92	6893
57.2376840115	Sandbox	178.33.163.93	6893
57.2377650738	Sandbox	178.33.163.94	6893
57.2378499508	Sandbox	178.33.163.95	6893
57.2379310131	Sandbox	178.33.163.96	6893
57.2380130291	Sandbox	178.33.163.97	6893
57.2381260395	Sandbox	178.33.163.98	6893
57.2382099628	Sandbox	178.33.163.99	6893
57.2382919788	Sandbox	178.33.163.100	6893
57.2383749485	Sandbox	178.33.163.101	6893
57.2384569645	Sandbox	178.33.163.102	6893
57.2385439873	Sandbox	178.33.163.103	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
57.2386260033	Sandbox	178.33.163.104	6893
57.2387080193	Sandbox	178.33.163.105	6893
57.2387890816	Sandbox	178.33.163.106	6893
57.2388710976	Sandbox	178.33.163.107	6893
57.2389528751	Sandbox	178.33.163.108	6893
57.2390339375	Sandbox	178.33.163.109	6893
57.2391219139	Sandbox	178.33.163.110	6893
57.239207983	Sandbox	178.33.163.111	6893
57.2392909527	Sandbox	178.33.163.112	6893
57.2393729687	Sandbox	178.33.163.113	6893
57.2394559383	Sandbox	178.33.163.114	6893
57.2395379543	Sandbox	178.33.163.115	6893
57.2396240234	Sandbox	178.33.163.116	6893
57.2397060394	Sandbox	178.33.163.117	6893
57.2397880554	Sandbox	178.33.163.118	6893
57.2398719788	Sandbox	178.33.163.119	6893
57.2399539948	Sandbox	178.33.163.120	6893
57.2400450706	Sandbox	178.33.163.121	6893
57.2401280403	Sandbox	178.33.163.122	6893
57.2402100563	Sandbox	178.33.163.123	6893
57.2402939796	Sandbox	178.33.163.124	6893
57.2403800488	Sandbox	178.33.163.125	6893
57.2404639721	Sandbox	178.33.163.126	6893
57.2405459881	Sandbox	178.33.163.127	6893
57.2406289577	Sandbox	178.33.163.128	6893
57.2407100201	Sandbox	178.33.163.129	6893
57.2407948971	Sandbox	178.33.163.130	6893
57.2408790588	Sandbox	178.33.163.131	6893
57.2409620285	Sandbox	178.33.163.132	6893
57.2410449982	Sandbox	178.33.163.133	6893
57.2411279678	Sandbox	178.33.163.134	6893
57.2412099838	Sandbox	178.33.163.135	6893
57.2412939072	Sandbox	178.33.163.136	6893
57.2413780689	Sandbox	178.33.163.137	6893
57.2414619923	Sandbox	178.33.163.138	6893
57.2415440083	Sandbox	178.33.163.139	6893
57.241631031	Sandbox	178.33.163.140	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
57.241713047	Sandbox	178.33.163.141	6893
57.2417960167	Sandbox	178.33.163.142	6893
57.2418780327	Sandbox	178.33.163.143	6893
57.2419610023	Sandbox	178.33.163.144	6893
57.242043972	Sandbox	178.33.163.145	6893
57.2421278954	Sandbox	178.33.163.146	6893
57.2422099113	Sandbox	178.33.163.147	6893
57.2422940731	Sandbox	178.33.163.148	6893
57.2423770428	Sandbox	178.33.163.149	6893
57.2424590588	Sandbox	178.33.163.150	6893
57.2425398827	Sandbox	178.33.163.151	6893
57.2426218987	Sandbox	178.33.163.152	6893
57.2427048683	Sandbox	178.33.163.153	6893
57.2427880764	Sandbox	178.33.163.154	6893
57.2428739071	Sandbox	178.33.163.155	6893
57.2429978848	Sandbox	178.33.163.156	6893
57.2433168888	Sandbox	178.33.163.157	6893
57.2434411049	Sandbox	178.33.163.158	6893
57.2437200546	Sandbox	178.33.163.159	6893
57.2438120842	Sandbox	178.33.163.160	6893
57.2438960075	Sandbox	178.33.163.161	6893
57.2439789772	Sandbox	178.33.163.162	6893
57.2441079617	Sandbox	178.33.163.163	6893
57.2441940308	Sandbox	178.33.163.164	6893
57.2442770004	Sandbox	178.33.163.165	6893
57.2443590164	Sandbox	178.33.163.166	6893
57.2444419861	Sandbox	178.33.163.167	6893
57.2445240021	Sandbox	178.33.163.168	6893
57.2446060181	Sandbox	178.33.163.169	6893
57.2446949482	Sandbox	178.33.163.170	6893
57.2447769642	Sandbox	178.33.163.171	6893
57.2448589802	Sandbox	178.33.163.172	6893
57.2449400425	Sandbox	178.33.163.173	6893
57.2450220585	Sandbox	178.33.163.174	6893
57.2451040745	Sandbox	178.33.163.175	6893
57.2451848984	Sandbox	178.33.163.176	6893
57.2452669144	Sandbox	178.33.163.177	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
57.2453489304	Sandbox	178.33.163.178	6893
57.2454299927	Sandbox	178.33.163.179	6893
57.245513916	Sandbox	178.33.163.180	6893
57.2455968857	Sandbox	178.33.163.181	6893
57.2456800938	Sandbox	178.33.163.182	6893
57.2457618713	Sandbox	178.33.163.183	6893
57.2458429337	Sandbox	178.33.163.184	6893
57.2459280491	Sandbox	178.33.163.185	6893
57.2460119724	Sandbox	178.33.163.186	6893
57.2460949421	Sandbox	178.33.163.187	6893
57.2461779118	Sandbox	178.33.163.188	6893
57.2462620735	Sandbox	178.33.163.189	6893
57.2463829517	Sandbox	178.33.163.190	6893
57.2464709282	Sandbox	178.33.163.191	6893
57.2465529442	Sandbox	178.33.163.192	6893
57.2466349602	Sandbox	178.33.163.193	6893
57.2467160225	Sandbox	178.33.163.194	6893
57.2467989922	Sandbox	178.33.163.195	6893
57.2468829155	Sandbox	178.33.163.196	6893
57.2469649315	Sandbox	178.33.163.197	6893
57.2470479012	Sandbox	178.33.163.198	6893
57.2471299171	Sandbox	178.33.163.199	6893
57.247220993	Sandbox	178.33.163.200	6893
57.2473039627	Sandbox	178.33.163.201	6893
57.2475528717	Sandbox	178.33.163.202	6893
57.2476429939	Sandbox	178.33.163.203	6893
57.2477259636	Sandbox	178.33.163.204	6893
57.2478079796	Sandbox	178.33.163.205	6893
57.2478890419	Sandbox	178.33.163.206	6893
57.2479701042	Sandbox	178.33.163.207	6893
57.2480590343	Sandbox	178.33.163.208	6893
57.248142004	Sandbox	178.33.163.209	6893
57.24822402	Sandbox	178.33.163.210	6893
57.248306036	Sandbox	178.33.163.211	6893
57.2484140396	Sandbox	178.33.163.212	6893
57.2485039234	Sandbox	178.33.163.213	6893
57.2485859394	Sandbox	178.33.163.214	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
57.248677969	Sandbox	178.33.163.215	6893
57.2487618923	Sandbox	178.33.163.216	6893
57.2488451004	Sandbox	178.33.163.217	6893
57.248926878	Sandbox	178.33.163.218	6893
57.249008894	Sandbox	178.33.163.219	6893
57.24909091	Sandbox	178.33.163.220	6893
57.2491719723	Sandbox	178.33.163.221	6893
57.2492549419	Sandbox	178.33.163.222	6893
57.2493360043	Sandbox	178.33.163.223	6893
57.2494189739	Sandbox	178.33.163.224	6893
57.2495000362	Sandbox	178.33.163.225	6893
57.2495810986	Sandbox	178.33.163.226	6893
57.2496628761	Sandbox	178.33.163.227	6893
57.2497439384	Sandbox	178.33.163.228	6893
57.2498250008	Sandbox	178.33.163.229	6893
57.2499098778	Sandbox	178.33.163.230	6893
57.2499930859	Sandbox	178.33.163.231	6893
57.2500739098	Sandbox	178.33.163.232	6893
57.2501549721	Sandbox	178.33.163.233	6893
57.2502360344	Sandbox	178.33.163.234	6893
57.2503170967	Sandbox	178.33.163.235	6893
57.2503969669	Sandbox	178.33.163.236	6893
57.2504789829	Sandbox	178.33.163.237	6893
57.2505609989	Sandbox	178.33.163.238	6893
57.2506430149	Sandbox	178.33.163.239	6893
57.2507240772	Sandbox	178.33.163.240	6893
57.2508099079	Sandbox	178.33.163.241	6893
57.2508950233	Sandbox	178.33.163.242	6893
57.2509770393	Sandbox	178.33.163.243	6893
57.2510590553	Sandbox	178.33.163.244	6893
57.2511460781	Sandbox	178.33.163.245	6893
57.2512290478	Sandbox	178.33.163.246	6893
57.2513110638	Sandbox	178.33.163.247	6893
57.2513940334	Sandbox	178.33.163.248	6893
57.2514750957	Sandbox	178.33.163.249	6893
57.2515568733	Sandbox	178.33.163.250	6893
57.2516379356	Sandbox	178.33.163.251	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
57.2517199516	Sandbox	178.33.163.252	6893
57.2518029213	Sandbox	178.33.163.253	6893
57.2518839836	Sandbox	178.33.163.254	6893
58.2995688915	Sandbox	178.33.163.255	6893
70.4512898922	Sandbox	178.33.158.0	6893
70.4514980316	Sandbox	178.33.158.1	6893
70.4515938759	Sandbox	178.33.158.2	6893
70.4516820908	Sandbox	178.33.158.3	6893
70.4517679214	Sandbox	178.33.158.4	6893
70.4518530369	Sandbox	178.33.158.5	6893
70.4519369602	Sandbox	178.33.158.6	6893
70.4520270824	Sandbox	178.33.158.7	6893
70.4521110058	Sandbox	178.33.158.8	6893
70.4521949291	Sandbox	178.33.158.9	6893
70.4522800446	Sandbox	178.33.158.10	6893
70.4523639679	Sandbox	178.33.158.11	6893
70.4524478912	Sandbox	178.33.158.12	6893
70.4525310993	Sandbox	178.33.158.13	6893
70.4526128769	Sandbox	178.33.158.14	6893
70.4526948929	Sandbox	178.33.158.15	6893
70.452778101	Sandbox	178.33.158.16	6893
70.4528610706	Sandbox	178.33.158.17	6893
70.4529418945	Sandbox	178.33.158.18	6893
70.4530239105	Sandbox	178.33.158.19	6893
70.453109026	Sandbox	178.33.158.20	6893
70.4532210827	Sandbox	178.33.158.21	6893
70.4533059597	Sandbox	178.33.158.22	6893
70.4533879757	Sandbox	178.33.158.23	6893
70.4534709454	Sandbox	178.33.158.24	6893
70.453553915	Sandbox	178.33.158.25	6893
70.453635931	Sandbox	178.33.158.26	6893
70.4537808895	Sandbox	178.33.158.27	6893
70.4538989067	Sandbox	178.33.158.28	6893
70.4539849758	Sandbox	178.33.158.29	6893
70.4540679455	Sandbox	178.33.158.30	6893
70.4541509151	Sandbox	178.33.158.31	6893
70.4542388916	Sandbox	178.33.159.0	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
70.4543230534	Sandbox	178.33.159.1	6893
70.4544069767	Sandbox	178.33.159.2	6893
70.4544899464	Sandbox	178.33.159.3	6893
70.454572916	Sandbox	178.33.159.4	6893
70.454654932	Sandbox	178.33.159.5	6893
70.4547379017	Sandbox	178.33.159.6	6893
70.4548199177	Sandbox	178.33.159.7	6893
70.4549028873	Sandbox	178.33.159.8	6893
70.4549849033	Sandbox	178.33.159.9	6893
70.4550669193	Sandbox	178.33.159.10	6893
70.455149889	Sandbox	178.33.159.11	6893
70.455231905	Sandbox	178.33.159.12	6893
70.4553148746	Sandbox	178.33.159.13	6893
70.4553968906	Sandbox	178.33.159.14	6893
70.4554800987	Sandbox	178.33.159.15	6893
70.4555618763	Sandbox	178.33.159.16	6893
70.4556438923	Sandbox	178.33.159.17	6893
70.4557580948	Sandbox	178.33.159.18	6893
70.4558439255	Sandbox	178.33.159.19	6893
70.4559268951	Sandbox	178.33.159.20	6893
70.4560439587	Sandbox	178.33.159.21	6893
70.4561309814	Sandbox	178.33.159.22	6893
70.4562389851	Sandbox	178.33.159.23	6893
70.4563250542	Sandbox	178.33.159.24	6893
70.4564070702	Sandbox	178.33.159.25	6893
70.4564890862	Sandbox	178.33.159.26	6893
70.4565720558	Sandbox	178.33.159.27	6893
70.4566540718	Sandbox	178.33.159.28	6893
70.4567360878	Sandbox	178.33.159.29	6893
70.4568190575	Sandbox	178.33.159.30	6893
70.4568998814	Sandbox	178.33.159.31	6893
70.4569880962	Sandbox	178.33.160.0	6893
70.4570710659	Sandbox	178.33.160.1	6893
70.4571530819	Sandbox	178.33.160.2	6893
70.4572350979	Sandbox	178.33.160.3	6893
70.4573168755	Sandbox	178.33.160.4	6893
70.4573988914	Sandbox	178.33.160.5	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
70.4574809074	Sandbox	178.33.160.6	6893
70.4575629234	Sandbox	178.33.160.7	6893
70.4576449394	Sandbox	178.33.160.8	6893
70.4577269554	Sandbox	178.33.160.9	6893
70.4578080177	Sandbox	178.33.160.10	6893
70.4578909874	Sandbox	178.33.160.11	6893
70.4579739571	Sandbox	178.33.160.12	6893
70.4580569267	Sandbox	178.33.160.13	6893
70.4581398964	Sandbox	178.33.160.14	6893
70.4582300186	Sandbox	178.33.160.15	6893
70.4583609104	Sandbox	178.33.160.16	6893
70.45845294	Sandbox	178.33.160.17	6893
70.4585380554	Sandbox	178.33.160.18	6893
70.4586200714	Sandbox	178.33.160.19	6893
70.4587059021	Sandbox	178.33.160.20	6893
70.4587888718	Sandbox	178.33.160.21	6893
70.4588720798	Sandbox	178.33.160.22	6893
70.4589540958	Sandbox	178.33.160.23	6893
70.4590370655	Sandbox	178.33.160.24	6893
70.4591190815	Sandbox	178.33.160.25	6893
70.4592020512	Sandbox	178.33.160.26	6893
70.4592840672	Sandbox	178.33.160.27	6893
70.4593710899	Sandbox	178.33.160.28	6893
70.4594531059	Sandbox	178.33.160.29	6893
70.4595360756	Sandbox	178.33.160.30	6893
70.4596190453	Sandbox	178.33.160.31	6893
70.4597010612	Sandbox	178.33.160.32	6893
70.4597840309	Sandbox	178.33.160.33	6893
70.4598650932	Sandbox	178.33.160.34	6893
70.4599480629	Sandbox	178.33.160.35	6893
70.4600429535	Sandbox	178.33.160.36	6893
70.4601340294	Sandbox	178.33.160.37	6893
70.4602169991	Sandbox	178.33.160.38	6893
70.4602999687	Sandbox	178.33.160.39	6893
70.4603819847	Sandbox	178.33.160.40	6893
70.4604640007	Sandbox	178.33.160.41	6893
70.4605469704	Sandbox	178.33.160.42	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
70.46062994	Sandbox	178.33.160.43	6893
70.4607150555	Sandbox	178.33.160.44	6893
70.4608049393	Sandbox	178.33.160.45	6893
70.460901022	Sandbox	178.33.160.46	6893
70.4609930515	Sandbox	178.33.160.47	6893
70.4610769749	Sandbox	178.33.160.48	6893
70.4611589909	Sandbox	178.33.160.49	6893
70.4612410069	Sandbox	178.33.160.50	6893
70.4613230228	Sandbox	178.33.160.51	6893
70.4614069462	Sandbox	178.33.160.52	6893
70.4614899158	Sandbox	178.33.160.53	6893
70.461575985	Sandbox	178.33.160.54	6893
70.4616589546	Sandbox	178.33.160.55	6893
70.461742878	Sandbox	178.33.160.56	6893
70.461824894	Sandbox	178.33.160.57	6893
70.4619090557	Sandbox	178.33.160.58	6893
70.4619910717	Sandbox	178.33.160.59	6893
70.462074995	Sandbox	178.33.160.60	6893
70.4621710777	Sandbox	178.33.160.61	6893
70.4622550011	Sandbox	178.33.160.62	6893
70.4623379707	Sandbox	178.33.160.63	6893
70.4624209404	Sandbox	178.33.160.64	6893
70.4625039101	Sandbox	178.33.160.65	6893
70.4625868797	Sandbox	178.33.160.66	6893
70.4626700878	Sandbox	178.33.160.67	6893
70.4627530575	Sandbox	178.33.160.68	6893
70.4628369808	Sandbox	178.33.160.69	6893
70.4629199505	Sandbox	178.33.160.70	6893
70.4630029202	Sandbox	178.33.160.71	6893
70.4630858898	Sandbox	178.33.160.72	6893
70.4631679058	Sandbox	178.33.160.73	6893
70.4632759094	Sandbox	178.33.160.74	6893
70.4633600712	Sandbox	178.33.160.75	6893
70.4634439945	Sandbox	178.33.160.76	6893
70.4635279179	Sandbox	178.33.160.77	6893
70.4636120796	Sandbox	178.33.160.78	6893
70.4636950493	Sandbox	178.33.160.79	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
70.46378088	Sandbox	178.33.160.80	6893
70.4638640881	Sandbox	178.33.160.81	6893
70.4639470577	Sandbox	178.33.160.82	6893
70.4640359879	Sandbox	178.33.160.83	6893
70.4641211033	Sandbox	178.33.160.84	6893
70.4642050266	Sandbox	178.33.160.85	6893
70.4642879963	Sandbox	178.33.160.86	6893
70.464370966	Sandbox	178.33.160.87	6893
70.4644539356	Sandbox	178.33.160.88	6893
70.4645369053	Sandbox	178.33.160.89	6893
70.464619875	Sandbox	178.33.160.90	6893
70.464703083	Sandbox	178.33.160.91	6893
70.4647870064	Sandbox	178.33.160.92	6893
70.464869976	Sandbox	178.33.160.93	6893
70.4649538994	Sandbox	178.33.160.94	6893
70.4650380611	Sandbox	178.33.160.95	6893
70.4651210308	Sandbox	178.33.160.96	6893
70.4652030468	Sandbox	178.33.160.97	6893
70.4652860165	Sandbox	178.33.160.98	6893
70.4653689861	Sandbox	178.33.160.99	6893
70.4654529095	Sandbox	178.33.160.100	6893
70.4655370712	Sandbox	178.33.160.101	6893
70.4656209946	Sandbox	178.33.160.102	6893
70.4657039642	Sandbox	178.33.160.103	6893
70.4657878876	Sandbox	178.33.160.104	6893
70.4658710957	Sandbox	178.33.160.105	6893
70.4659569263	Sandbox	178.33.160.106	6893
70.466039896	Sandbox	178.33.160.107	6893
70.4661240578	Sandbox	178.33.160.108	6893
70.466258049	Sandbox	178.33.160.109	6893
70.4663450718	Sandbox	178.33.160.110	6893
70.4664289951	Sandbox	178.33.160.111	6893
70.4665119648	Sandbox	178.33.160.112	6893
70.4665949345	Sandbox	178.33.160.113	6893
70.4666779041	Sandbox	178.33.160.114	6893
70.4667608738	Sandbox	178.33.160.115	6893
70.4668459892	Sandbox	178.33.160.116	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
70.4669299126	Sandbox	178.33.160.117	6893
70.4670128822	Sandbox	178.33.160.118	6893
70.4670960903	Sandbox	178.33.160.119	6893
70.4671781063	Sandbox	178.33.160.120	6893
70.467261076	Sandbox	178.33.160.121	6893
70.4673440456	Sandbox	178.33.160.122	6893
70.4674270153	Sandbox	178.33.160.123	6893
70.4675109386	Sandbox	178.33.160.124	6893
70.4675939083	Sandbox	178.33.160.125	6893
70.467676878	Sandbox	178.33.160.126	6893
70.4677600861	Sandbox	178.33.160.127	6893
70.4678430557	Sandbox	178.33.160.128	6893
70.4679260254	Sandbox	178.33.160.129	6893
70.4680418968	Sandbox	178.33.160.130	6893
70.4681329727	Sandbox	178.33.160.131	6893
70.4682199955	Sandbox	178.33.160.132	6893
70.4683039188	Sandbox	178.33.160.133	6893
70.4684090614	Sandbox	178.33.160.134	6893
70.4684948921	Sandbox	178.33.160.135	6893
70.4685781002	Sandbox	178.33.160.136	6893
70.4686620235	Sandbox	178.33.160.137	6893
70.4687469006	Sandbox	178.33.160.138	6893
70.4688298702	Sandbox	178.33.160.139	6893
70.4689149857	Sandbox	178.33.160.140	6893
70.468998909	Sandbox	178.33.160.141	6893
70.4690830708	Sandbox	178.33.160.142	6893
70.4691669941	Sandbox	178.33.160.143	6893
70.4692509174	Sandbox	178.33.160.144	6893
70.4693350792	Sandbox	178.33.160.145	6893
70.4694180489	Sandbox	178.33.160.146	6893
70.4695010185	Sandbox	178.33.160.147	6893
70.4695849419	Sandbox	178.33.160.148	6893
70.4696679115	Sandbox	178.33.160.149	6893
70.4697520733	Sandbox	178.33.160.150	6893
70.469835043	Sandbox	178.33.160.151	6893
70.4699180126	Sandbox	178.33.160.152	6893
70.4700009823	Sandbox	178.33.160.153	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
70.4700849056	Sandbox	178.33.160.154	6893
70.4701678753	Sandbox	178.33.160.155	6893
70.470252037	Sandbox	178.33.160.156	6893
70.4703359604	Sandbox	178.33.160.157	6893
70.4704220295	Sandbox	178.33.160.158	6893
70.4705059528	Sandbox	178.33.160.159	6893
70.4705898762	Sandbox	178.33.160.160	6893
70.4706730843	Sandbox	178.33.160.161	6893
70.4707560539	Sandbox	178.33.160.162	6893
70.4708390236	Sandbox	178.33.160.163	6893
70.4709229469	Sandbox	178.33.160.164	6893
70.4710080624	Sandbox	178.33.160.165	6893
70.4710919857	Sandbox	178.33.160.166	6893
70.4711749554	Sandbox	178.33.160.167	6893
70.4714150429	Sandbox	178.33.160.168	6893
70.4716310501	Sandbox	178.33.160.169	6893
70.4717578888	Sandbox	178.33.160.170	6893
70.4718620777	Sandbox	178.33.160.171	6893
70.4720110893	Sandbox	178.33.160.172	6893
70.4721329212	Sandbox	178.33.160.173	6893
70.4722850323	Sandbox	178.33.160.174	6893
70.4724369049	Sandbox	178.33.160.175	6893
70.4725880623	Sandbox	178.33.160.176	6893
70.4727430344	Sandbox	178.33.160.177	6893
70.4728960991	Sandbox	178.33.160.178	6893
70.4730470181	Sandbox	178.33.160.179	6893
70.4732038975	Sandbox	178.33.160.180	6893
70.4733669758	Sandbox	178.33.160.181	6893
70.4735279083	Sandbox	178.33.160.182	6893
70.4736878872	Sandbox	178.33.160.183	6893
70.4738500118	Sandbox	178.33.160.184	6893
70.474009037	Sandbox	178.33.160.185	6893
70.4741668701	Sandbox	178.33.160.186	6893
70.4743249416	Sandbox	178.33.160.187	6893
70.4744870663	Sandbox	178.33.160.188	6893
70.4746470451	Sandbox	178.33.160.189	6893
70.4748079777	Sandbox	178.33.160.190	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
70.4749701023	Sandbox	178.33.160.191	6893
70.4751319885	Sandbox	178.33.160.192	6893
70.4752919674	Sandbox	178.33.160.193	6893
70.4754509926	Sandbox	178.33.160.194	6893
70.4756090641	Sandbox	178.33.160.195	6893
70.4757990837	Sandbox	178.33.160.196	6893
70.4759740829	Sandbox	178.33.160.197	6893
70.4761469364	Sandbox	178.33.160.198	6893
70.4763090611	Sandbox	178.33.160.199	6893
70.4764668941	Sandbox	178.33.160.200	6893
70.476626873	Sandbox	178.33.160.201	6893
70.4767830372	Sandbox	178.33.160.202	6893
70.4769339561	Sandbox	178.33.160.203	6893
70.477093935	Sandbox	178.33.160.204	6893
70.4772520065	Sandbox	178.33.160.205	6893
70.4774079323	Sandbox	178.33.160.206	6893
70.4775619507	Sandbox	178.33.160.207	6893
70.4777169228	Sandbox	178.33.160.208	6893
70.4778709412	Sandbox	178.33.160.209	6893
70.4780340195	Sandbox	178.33.160.210	6893
70.4781939983	Sandbox	178.33.160.211	6893
70.4783530235	Sandbox	178.33.160.212	6893
70.4785161018	Sandbox	178.33.160.213	6893
70.4786729813	Sandbox	178.33.160.214	6893
70.4787940979	Sandbox	178.33.160.215	6893
70.4788858891	Sandbox	178.33.160.216	6893
70.4789719582	Sandbox	178.33.160.217	6893
70.4790570736	Sandbox	178.33.160.218	6893
70.4791409969	Sandbox	178.33.160.219	6893
70.4792258739	Sandbox	178.33.160.220	6893
70.4793109894	Sandbox	178.33.160.221	6893
70.4793949127	Sandbox	178.33.160.222	6893
70.4794790745	Sandbox	178.33.160.223	6893
70.4795620441	Sandbox	178.33.160.224	6893
70.4796459675	Sandbox	178.33.160.225	6893
70.4797298908	Sandbox	178.33.160.226	6893
70.4798140526	Sandbox	178.33.160.227	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
70.4798979759	Sandbox	178.33.160.228	6893
70.4799900055	Sandbox	178.33.160.229	6893
70.4801020622	Sandbox	178.33.160.230	6893
70.4801869392	Sandbox	178.33.160.231	6893
70.4802730083	Sandbox	178.33.160.232	6893
70.4803578854	Sandbox	178.33.160.233	6893
70.4804420471	Sandbox	178.33.160.234	6893
70.4805259705	Sandbox	178.33.160.235	6893
70.4806139469	Sandbox	178.33.160.236	6893
70.480700016	Sandbox	178.33.160.237	6893
70.4807839394	Sandbox	178.33.160.238	6893
70.4808700085	Sandbox	178.33.160.239	6893
70.4809520245	Sandbox	178.33.160.240	6893
70.4810369015	Sandbox	178.33.160.241	6893
70.4811210632	Sandbox	178.33.160.242	6893
70.4812049866	Sandbox	178.33.160.243	6893
70.481290102	Sandbox	178.33.160.244	6893
70.4813740253	Sandbox	178.33.160.245	6893
70.4814579487	Sandbox	178.33.160.246	6893
70.481541872	Sandbox	178.33.160.247	6893
70.4816260338	Sandbox	178.33.160.248	6893
70.4817099571	Sandbox	178.33.160.249	6893
70.4817938805	Sandbox	178.33.160.250	6893
70.4818770885	Sandbox	178.33.160.251	6893
70.4820189476	Sandbox	178.33.160.252	6893
70.4821059704	Sandbox	178.33.160.253	6893
70.4821910858	Sandbox	178.33.160.254	6893
71.4813330173	Sandbox	178.33.160.255	6893
71.4814660549	Sandbox	178.33.161.0	6893
71.4815700054	Sandbox	178.33.161.1	6893
71.4816761017	Sandbox	178.33.161.2	6893
71.4818050861	Sandbox	178.33.161.3	6893
71.4819118977	Sandbox	178.33.161.4	6893
71.482008934	Sandbox	178.33.161.5	6893
71.4820959568	Sandbox	178.33.161.6	6893
71.4821820259	Sandbox	178.33.161.7	6893
71.482268095	Sandbox	178.33.161.8	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
71.482352972	Sandbox	178.33.161.9	6893
71.4824368954	Sandbox	178.33.161.10	6893
71.4825220108	Sandbox	178.33.161.11	6893
71.4826068878	Sandbox	178.33.161.12	6893
71.4826910496	Sandbox	178.33.161.13	6893
71.4827740192	Sandbox	178.33.161.14	6893
71.4828579426	Sandbox	178.33.161.15	6893
71.4829409122	Sandbox	178.33.161.16	6893
71.483025074	Sandbox	178.33.161.17	6893
71.4831290245	Sandbox	178.33.161.18	6893
71.4832139015	Sandbox	178.33.161.19	6893
71.4833080769	Sandbox	178.33.161.20	6893
71.4833939075	Sandbox	178.33.161.21	6893
71.4834768772	Sandbox	178.33.161.22	6893
71.4835619926	Sandbox	178.33.161.23	6893
71.4836449623	Sandbox	178.33.161.24	6893
71.4837288857	Sandbox	178.33.161.25	6893
71.4838120937	Sandbox	178.33.161.26	6893
71.4838960171	Sandbox	178.33.161.27	6893
71.4839799404	Sandbox	178.33.161.28	6893
71.4840989113	Sandbox	178.33.161.29	6893
71.4841849804	Sandbox	178.33.161.30	6893
71.4842689037	Sandbox	178.33.161.31	6893
71.4843530655	Sandbox	178.33.161.32	6893
71.4844379425	Sandbox	178.33.161.33	6893
71.4845209122	Sandbox	178.33.161.34	6893
71.4846050739	Sandbox	178.33.161.35	6893
71.4846880436	Sandbox	178.33.161.36	6893
71.4847719669	Sandbox	178.33.161.37	6893
71.4848549366	Sandbox	178.33.161.38	6893
71.4849390984	Sandbox	178.33.161.39	6893
71.4850230217	Sandbox	178.33.161.40	6893
71.485106945	Sandbox	178.33.161.41	6893
71.4852190018	Sandbox	178.33.161.42	6893
71.4853060246	Sandbox	178.33.161.43	6893
71.4853909016	Sandbox	178.33.161.44	6893
71.4854750633	Sandbox	178.33.161.45	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
71.485558033	Sandbox	178.33.161.46	6893
71.4856419563	Sandbox	178.33.161.47	6893
71.485724926	Sandbox	178.33.161.48	6893
71.4858090878	Sandbox	178.33.161.49	6893
71.4858930111	Sandbox	178.33.161.50	6893
71.4859778881	Sandbox	178.33.161.51	6893
71.4860610962	Sandbox	178.33.161.52	6893
71.4861450195	Sandbox	178.33.161.53	6893
71.486232996	Sandbox	178.33.161.54	6893
71.4863159657	Sandbox	178.33.161.55	6893
71.4863989353	Sandbox	178.33.161.56	6893
71.4864840508	Sandbox	178.33.161.57	6893
71.4865670204	Sandbox	178.33.161.58	6893
71.4866499901	Sandbox	178.33.161.59	6893
71.4867339134	Sandbox	178.33.161.60	6893
71.4868168831	Sandbox	178.33.161.61	6893
71.4869000912	Sandbox	178.33.161.62	6893
71.4869830608	Sandbox	178.33.161.63	6893
71.4870660305	Sandbox	178.33.161.64	6893
71.4871499538	Sandbox	178.33.161.65	6893
71.4872338772	Sandbox	178.33.161.66	6893
71.4873170853	Sandbox	178.33.161.67	6893
71.4874000549	Sandbox	178.33.161.68	6893
71.4874830246	Sandbox	178.33.161.69	6893
71.4875659943	Sandbox	178.33.161.70	6893
71.4876489639	Sandbox	178.33.161.71	6893
71.4877309799	Sandbox	178.33.161.72	6893
71.4878160954	Sandbox	178.33.161.73	6893
71.487899065	Sandbox	178.33.161.74	6893
71.4879889488	Sandbox	178.33.161.75	6893
71.4881000519	Sandbox	178.33.161.76	6893
71.4881858826	Sandbox	178.33.161.77	6893
71.4882700443	Sandbox	178.33.161.78	6893
71.4883539677	Sandbox	178.33.161.79	6893
71.4884409904	Sandbox	178.33.161.80	6893
71.4885270596	Sandbox	178.33.161.81	6893
71.4886119366	Sandbox	178.33.161.82	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
71.4886960983	Sandbox	178.33.161.83	6893
71.4887800217	Sandbox	178.33.161.84	6893
71.488863945	Sandbox	178.33.161.85	6893
71.4889478683	Sandbox	178.33.161.86	6893
71.4890320301	Sandbox	178.33.161.87	6893
71.4891149998	Sandbox	178.33.161.88	6893
71.4891989231	Sandbox	178.33.161.89	6893
71.4892830849	Sandbox	178.33.161.90	6893
71.4893670082	Sandbox	178.33.161.91	6893
71.4894499779	Sandbox	178.33.161.92	6893
71.4895329475	Sandbox	178.33.161.93	6893
71.4896168709	Sandbox	178.33.161.94	6893
71.4897010326	Sandbox	178.33.161.95	6893
71.4897830486	Sandbox	178.33.161.96	6893
71.4898679256	Sandbox	178.33.161.97	6893
71.4899520874	Sandbox	178.33.161.98	6893
71.4900350571	Sandbox	178.33.161.99	6893
71.4901180267	Sandbox	178.33.161.100	6893
71.4902019501	Sandbox	178.33.161.101	6893
71.4903149605	Sandbox	178.33.161.102	6893
71.4904010296	Sandbox	178.33.161.103	6893
71.4904859066	Sandbox	178.33.161.104	6893
71.490571022	Sandbox	178.33.161.105	6893
71.4906580448	Sandbox	178.33.161.106	6893
71.4907419682	Sandbox	178.33.161.107	6893
71.4908280373	Sandbox	178.33.161.108	6893
71.4909119606	Sandbox	178.33.161.109	6893
71.4909958839	Sandbox	178.33.161.110	6893
71.4910809994	Sandbox	178.33.161.111	6893
71.491163969	Sandbox	178.33.161.112	6893
71.4912478924	Sandbox	178.33.161.113	6893
71.4913320541	Sandbox	178.33.161.114	6893
71.4914150238	Sandbox	178.33.161.115	6893
71.4914989471	Sandbox	178.33.161.116	6893
71.4915819168	Sandbox	178.33.161.117	6893
71.4916648865	Sandbox	178.33.161.118	6893
71.4917490482	Sandbox	178.33.161.119	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
71.4918310642	Sandbox	178.33.161.120	6893
71.4919159412	Sandbox	178.33.161.121	6893
71.4920060635	Sandbox	178.33.161.122	6893
71.4920909405	Sandbox	178.33.161.123	6893
71.4921751022	Sandbox	178.33.161.124	6893
71.4922580719	Sandbox	178.33.161.125	6893
71.4923419952	Sandbox	178.33.161.126	6893
71.4924249649	Sandbox	178.33.161.127	6893
71.4925079346	Sandbox	178.33.161.128	6893
71.49259305	Sandbox	178.33.161.129	6893
71.492677927	Sandbox	178.33.161.130	6893
71.4927620888	Sandbox	178.33.161.131	6893
71.4928469658	Sandbox	178.33.161.132	6893
71.4929308891	Sandbox	178.33.161.133	6893
71.4930140972	Sandbox	178.33.161.134	6893
71.4930970669	Sandbox	178.33.161.135	6893
71.4931800365	Sandbox	178.33.161.136	6893
71.4932639599	Sandbox	178.33.161.137	6893
71.4933478832	Sandbox	178.33.161.138	6893
71.4934310913	Sandbox	178.33.161.139	6893
71.493514061	Sandbox	178.33.161.140	6893
71.4935979843	Sandbox	178.33.161.141	6893
71.4936819077	Sandbox	178.33.161.142	6893
71.4937660694	Sandbox	178.33.161.143	6893
71.4938480854	Sandbox	178.33.161.144	6893
71.4939320087	Sandbox	178.33.161.145	6893
71.4940159321	Sandbox	178.33.161.146	6893
71.4940989017	Sandbox	178.33.161.147	6893
71.4941818714	Sandbox	178.33.161.148	6893
71.4942660332	Sandbox	178.33.161.149	6893
71.4943490028	Sandbox	178.33.161.150	6893
71.4944319725	Sandbox	178.33.161.151	6893
71.4945149422	Sandbox	178.33.161.152	6893
71.4945991039	Sandbox	178.33.161.153	6893
71.4946830273	Sandbox	178.33.161.154	6893
71.4947669506	Sandbox	178.33.161.155	6893
71.4948508739	Sandbox	178.33.161.156	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
71.4949350357	Sandbox	178.33.161.157	6893
71.4950211048	Sandbox	178.33.161.158	6893
71.4951040745	Sandbox	178.33.161.159	6893
71.495210886	Sandbox	178.33.161.160	6893
71.4952991009	Sandbox	178.33.161.161	6893
71.4953839779	Sandbox	178.33.161.162	6893
71.4954669476	Sandbox	178.33.161.163	6893
71.495552063	Sandbox	178.33.161.164	6893
71.4956359863	Sandbox	178.33.161.165	6893
71.4957199097	Sandbox	178.33.161.166	6893
71.4958050251	Sandbox	178.33.161.167	6893
71.4958899021	Sandbox	178.33.161.168	6893
71.4959740639	Sandbox	178.33.161.169	6893
71.4960930347	Sandbox	178.33.161.170	6893
71.4961800575	Sandbox	178.33.161.171	6893
71.4962649345	Sandbox	178.33.161.172	6893
71.4963490963	Sandbox	178.33.161.173	6893
71.496432066	Sandbox	178.33.161.174	6893
71.496516943	Sandbox	178.33.161.175	6893
71.4965999126	Sandbox	178.33.161.176	6893
71.4966850281	Sandbox	178.33.161.177	6893
71.4967699051	Sandbox	178.33.161.178	6893
71.4968540668	Sandbox	178.33.161.179	6893
71.4970359802	Sandbox	178.33.161.180	6893
71.4971940517	Sandbox	178.33.161.181	6893
71.4972989559	Sandbox	178.33.161.182	6893
71.4973840714	Sandbox	178.33.161.183	6893
71.4974720478	Sandbox	178.33.161.184	6893
71.4975578785	Sandbox	178.33.161.185	6893
71.4976429939	Sandbox	178.33.161.186	6893
71.4977269173	Sandbox	178.33.161.187	6893
71.4978120327	Sandbox	178.33.161.188	6893
71.4978981018	Sandbox	178.33.161.189	6893
71.4979820251	Sandbox	178.33.161.190	6893
71.4980659485	Sandbox	178.33.161.191	6893
71.4981489182	Sandbox	178.33.161.192	6893
71.4982349873	Sandbox	178.33.161.193	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
71.4983189106	Sandbox	178.33.161.194	6893
71.4984030724	Sandbox	178.33.161.195	6893
71.4984869957	Sandbox	178.33.161.196	6893
71.4985730648	Sandbox	178.33.161.197	6893
71.4986579418	Sandbox	178.33.161.198	6893
71.4987409115	Sandbox	178.33.161.199	6893
71.4988238811	Sandbox	178.33.161.200	6893
71.4989080429	Sandbox	178.33.161.201	6893
71.4989929199	Sandbox	178.33.161.202	6893
71.4990758896	Sandbox	178.33.161.203	6893
71.4991600513	Sandbox	178.33.161.204	6893
71.4992439747	Sandbox	178.33.161.205	6893
71.499327898	Sandbox	178.33.161.206	6893
71.4994120598	Sandbox	178.33.161.207	6893
71.4994950294	Sandbox	178.33.161.208	6893
71.4995799065	Sandbox	178.33.161.209	6893
71.4996678829	Sandbox	178.33.161.210	6893
71.4997529984	Sandbox	178.33.161.211	6893
71.4998369217	Sandbox	178.33.161.212	6893
71.4999210835	Sandbox	178.33.161.213	6893
71.500043869	Sandbox	178.33.161.214	6893
71.500138998	Sandbox	178.33.161.215	6893
71.500223875	Sandbox	178.33.161.216	6893
71.500344038	Sandbox	178.33.161.217	6893
71.5004310608	Sandbox	178.33.161.218	6893
71.5005159378	Sandbox	178.33.161.219	6893
71.5006000996	Sandbox	178.33.161.220	6893
71.5006849766	Sandbox	178.33.161.221	6893
71.5007688999	Sandbox	178.33.161.222	6893
71.5008540154	Sandbox	178.33.161.223	6893
71.5009379387	Sandbox	178.33.161.224	6893
71.5010221004	Sandbox	178.33.161.225	6893
71.5011069775	Sandbox	178.33.161.226	6893
71.5011909008	Sandbox	178.33.161.227	6893
71.5012750626	Sandbox	178.33.161.228	6893
71.5013589859	Sandbox	178.33.161.229	6893
71.5014429092	Sandbox	178.33.161.230	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
71.501527071	Sandbox	178.33.161.231	6893
71.5016109943	Sandbox	178.33.161.232	6893
71.5016958714	Sandbox	178.33.161.233	6893
71.5017800331	Sandbox	178.33.161.234	6893
71.5018639565	Sandbox	178.33.161.235	6893
71.5019519329	Sandbox	178.33.161.236	6893
71.5020370483	Sandbox	178.33.161.237	6893
71.5021219254	Sandbox	178.33.161.238	6893
71.502204895	Sandbox	178.33.161.239	6893
71.5022890568	Sandbox	178.33.161.240	6893
71.5023739338	Sandbox	178.33.161.241	6893
71.5024580956	Sandbox	178.33.161.242	6893
71.5025410652	Sandbox	178.33.161.243	6893
71.5026249886	Sandbox	178.33.161.244	6893
71.502710104	Sandbox	178.33.161.245	6893
71.5027940273	Sandbox	178.33.161.246	6893
71.5028779507	Sandbox	178.33.161.247	6893
71.5029609203	Sandbox	178.33.161.248	6893
71.5030460358	Sandbox	178.33.161.249	6893
71.5031299591	Sandbox	178.33.161.250	6893
71.5032138824	Sandbox	178.33.161.251	6893
71.5032980442	Sandbox	178.33.161.252	6893
71.5033819675	Sandbox	178.33.161.253	6893
71.5034658909	Sandbox	178.33.161.254	6893
72.5553319454	Sandbox	178.33.161.255	6893
72.5554699898	Sandbox	178.33.162.0	6893
72.5555620193	Sandbox	178.33.162.1	6893
72.555644989	Sandbox	178.33.162.2	6893
72.5557620525	Sandbox	178.33.162.3	6893
72.555850029	Sandbox	178.33.162.4	6893
72.555932045	Sandbox	178.33.162.5	6893
72.5560529232	Sandbox	178.33.162.6	6893
72.556137085	Sandbox	178.33.162.7	6893
72.5562160015	Sandbox	178.33.162.8	6893
72.5562949181	Sandbox	178.33.162.9	6893
72.556374073	Sandbox	178.33.162.10	6893
72.5564539433	Sandbox	178.33.162.11	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
72.5565330982	Sandbox	178.33.162.12	6893
72.5566129684	Sandbox	178.33.162.13	6893
72.5567040443	Sandbox	178.33.162.14	6893
72.556789875	Sandbox	178.33.162.15	6893
72.5568749905	Sandbox	178.33.162.16	6893
72.5569601059	Sandbox	178.33.162.17	6893
72.5570449829	Sandbox	178.33.162.18	6893
72.5571300983	Sandbox	178.33.162.19	6893
72.5572140217	Sandbox	178.33.162.20	6893
72.557297945	Sandbox	178.33.162.21	6893
72.5573818684	Sandbox	178.33.162.22	6893
72.5574660301	Sandbox	178.33.162.23	6893
72.5575489998	Sandbox	178.33.162.24	6893
72.5576319695	Sandbox	178.33.162.25	6893
72.5577440262	Sandbox	178.33.162.26	6893
72.55783391	Sandbox	178.33.162.27	6893
72.5579190254	Sandbox	178.33.162.28	6893
72.5580029488	Sandbox	178.33.162.29	6893
72.5580880642	Sandbox	178.33.162.30	6893
72.5581719875	Sandbox	178.33.162.31	6893
72.558257103	Sandbox	178.33.162.32	6893
72.5583400726	Sandbox	178.33.162.33	6893
72.5584230423	Sandbox	178.33.162.34	6893
72.5585069656	Sandbox	178.33.162.35	6893
72.5585899353	Sandbox	178.33.162.36	6893
72.558672905	Sandbox	178.33.162.37	6893
72.5587570667	Sandbox	178.33.162.38	6893
72.5588409901	Sandbox	178.33.162.39	6893
72.5589239597	Sandbox	178.33.162.40	6893
72.5590069294	Sandbox	178.33.162.41	6893
72.5590910912	Sandbox	178.33.162.42	6893
72.5591728687	Sandbox	178.33.162.43	6893
72.5592560768	Sandbox	178.33.162.44	6893
72.5594139099	Sandbox	178.33.162.45	6893
72.5595040321	Sandbox	178.33.162.46	6893
72.5595879555	Sandbox	178.33.162.47	6893
72.5596709251	Sandbox	178.33.162.48	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
72.5597538948	Sandbox	178.33.162.49	6893
72.5598380566	Sandbox	178.33.162.50	6893
72.5599219799	Sandbox	178.33.162.51	6893
72.5600149632	Sandbox	178.33.162.52	6893
72.5601029396	Sandbox	178.33.162.53	6893
72.5601871014	Sandbox	178.33.162.54	6893
72.560270071	Sandbox	178.33.162.55	6893
72.560352087	Sandbox	178.33.162.56	6893
72.560434103	Sandbox	178.33.162.57	6893
72.5605220795	Sandbox	178.33.162.58	6893
72.5606050491	Sandbox	178.33.162.59	6893
72.5606870651	Sandbox	178.33.162.60	6893
72.5607709885	Sandbox	178.33.162.61	6893
72.5608539581	Sandbox	178.33.162.62	6893
72.5609369278	Sandbox	178.33.162.63	6893
72.5610198975	Sandbox	178.33.162.64	6893
72.5611031055	Sandbox	178.33.162.65	6893
72.5611870289	Sandbox	178.33.162.66	6893
72.5612699986	Sandbox	178.33.162.67	6893
72.5613529682	Sandbox	178.33.162.68	6893
72.5614359379	Sandbox	178.33.162.69	6893
72.5615200996	Sandbox	178.33.162.70	6893
72.5616030693	Sandbox	178.33.162.71	6893
72.5616869926	Sandbox	178.33.162.72	6893
72.5617699623	Sandbox	178.33.162.73	6893
72.5618538857	Sandbox	178.33.162.74	6893
72.5619840622	Sandbox	178.33.162.75	6893
72.5621509552	Sandbox	178.33.162.76	6893
72.5623099804	Sandbox	178.33.162.77	6893
72.5624010563	Sandbox	178.33.162.78	6893
72.562484026	Sandbox	178.33.162.79	6893
72.5625660419	Sandbox	178.33.162.80	6893
72.5626730919	Sandbox	178.33.162.81	6893
72.5627589226	Sandbox	178.33.162.82	6893
72.5628418922	Sandbox	178.33.162.83	6893
72.5629279613	Sandbox	178.33.162.84	6893
72.5630118847	Sandbox	178.33.162.85	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
72.5630950928	Sandbox	178.33.162.86	6893
72.5631780624	Sandbox	178.33.162.87	6893
72.5632619858	Sandbox	178.33.162.88	6893
72.5633449554	Sandbox	178.33.162.89	6893
72.5634288788	Sandbox	178.33.162.90	6893
72.5635120869	Sandbox	178.33.162.91	6893
72.5635950565	Sandbox	178.33.162.92	6893
72.5636780262	Sandbox	178.33.162.93	6893
72.5637609959	Sandbox	178.33.162.94	6893
72.5638439655	Sandbox	178.33.162.95	6893
72.5639278889	Sandbox	178.33.162.96	6893
72.5640170574	Sandbox	178.33.162.97	6893
72.5640990734	Sandbox	178.33.162.98	6893
72.5641820431	Sandbox	178.33.162.99	6893
72.5642650127	Sandbox	178.33.162.100	6893
72.5643489361	Sandbox	178.33.162.101	6893
72.5644319057	Sandbox	178.33.162.102	6893
72.5645160675	Sandbox	178.33.162.103	6893
72.5645990372	Sandbox	178.33.162.104	6893
72.5646820068	Sandbox	178.33.162.105	6893
72.5647640228	Sandbox	178.33.162.106	6893
72.5648469925	Sandbox	178.33.162.107	6893
72.5649299622	Sandbox	178.33.162.108	6893
72.5650129318	Sandbox	178.33.162.109	6893
72.5650999546	Sandbox	178.33.162.110	6893
72.5651829243	Sandbox	178.33.162.111	6893
72.5652658939	Sandbox	178.33.162.112	6893
72.565349102	Sandbox	178.33.162.113	6893
72.5654320717	Sandbox	178.33.162.114	6893
72.5655150414	Sandbox	178.33.162.115	6893
72.565598011	Sandbox	178.33.162.116	6893
72.5656819344	Sandbox	178.33.162.117	6893
72.5657660961	Sandbox	178.33.162.118	6893
72.5658490658	Sandbox	178.33.162.119	6893
72.5659298897	Sandbox	178.33.162.120	6893
72.5660130978	Sandbox	178.33.162.121	6893
72.5660948753	Sandbox	178.33.162.122	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
72.5661780834	Sandbox	178.33.162.123	6893
72.5662620068	Sandbox	178.33.162.124	6893
72.5663449764	Sandbox	178.33.162.125	6893
72.5664279461	Sandbox	178.33.162.126	6893
72.5665109158	Sandbox	178.33.162.127	6893
72.5665929317	Sandbox	178.33.162.128	6893
72.5666759014	Sandbox	178.33.162.129	6893
72.5667579174	Sandbox	178.33.162.130	6893
72.5668408871	Sandbox	178.33.162.131	6893
72.5669229031	Sandbox	178.33.162.132	6893
72.5670058727	Sandbox	178.33.162.133	6893
72.5670890808	Sandbox	178.33.162.134	6893
72.5671720505	Sandbox	178.33.162.135	6893
72.56726408	Sandbox	178.33.162.136	6893
72.5673480034	Sandbox	178.33.162.137	6893
72.5674328804	Sandbox	178.33.162.138	6893
72.5675148964	Sandbox	178.33.162.139	6893
72.5675981045	Sandbox	178.33.162.140	6893
72.5676820278	Sandbox	178.33.162.141	6893
72.5678069592	Sandbox	178.33.162.142	6893
72.5678958893	Sandbox	178.33.162.143	6893
72.5679810047	Sandbox	178.33.162.144	6893
72.568103075	Sandbox	178.33.162.145	6893
72.5681889057	Sandbox	178.33.162.146	6893
72.5682730675	Sandbox	178.33.162.147	6893
72.5683550835	Sandbox	178.33.162.148	6893
72.5684480667	Sandbox	178.33.162.149	6893
72.5685310364	Sandbox	178.33.162.150	6893
72.5686149597	Sandbox	178.33.162.151	6893
72.5686969757	Sandbox	178.33.162.152	6893
72.5687789917	Sandbox	178.33.162.153	6893
72.568862915	Sandbox	178.33.162.154	6893
72.5689470768	Sandbox	178.33.162.155	6893
72.5690300465	Sandbox	178.33.162.156	6893
72.5691130161	Sandbox	178.33.162.157	6893
72.5691969395	Sandbox	178.33.162.158	6893
72.5693159103	Sandbox	178.33.162.159	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
72.5694038868	Sandbox	178.33.162.160	6893
72.5694890022	Sandbox	178.33.162.161	6893
72.5695779324	Sandbox	178.33.162.162	6893
72.5696620941	Sandbox	178.33.162.163	6893
72.5697479248	Sandbox	178.33.162.164	6893
72.5698349476	Sandbox	178.33.162.165	6893
72.5699188709	Sandbox	178.33.162.166	6893
72.5700039864	Sandbox	178.33.162.167	6893
72.570125103	Sandbox	178.33.162.168	6893
72.5702140331	Sandbox	178.33.162.169	6893
72.5702979565	Sandbox	178.33.162.170	6893
72.5703840256	Sandbox	178.33.162.171	6893
72.5704679489	Sandbox	178.33.162.172	6893
72.5705549717	Sandbox	178.33.162.173	6893
72.570638895	Sandbox	178.33.162.174	6893
72.5707249641	Sandbox	178.33.162.175	6893
72.5708088875	Sandbox	178.33.162.176	6893
72.5708940029	Sandbox	178.33.162.177	6893
72.5709788799	Sandbox	178.33.162.178	6893
72.5710890293	Sandbox	178.33.162.179	6893
72.5711960793	Sandbox	178.33.162.180	6893
72.5713040829	Sandbox	178.33.162.181	6893
72.5714120865	Sandbox	178.33.162.182	6893
72.5715200901	Sandbox	178.33.162.183	6893
72.5716269016	Sandbox	178.33.162.184	6893
72.5717339516	Sandbox	178.33.162.185	6893
72.5718419552	Sandbox	178.33.162.186	6893
72.5719490051	Sandbox	178.33.162.187	6893
72.5720648766	Sandbox	178.33.162.188	6893
72.5721549988	Sandbox	178.33.162.189	6893
72.5722410679	Sandbox	178.33.162.190	6893
72.5723259449	Sandbox	178.33.162.191	6893
72.5724110603	Sandbox	178.33.162.192	6893
72.5724949837	Sandbox	178.33.162.193	6893
72.5725800991	Sandbox	178.33.162.194	6893
72.5726881027	Sandbox	178.33.162.195	6893
72.57279706	Sandbox	178.33.162.196	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
72.5729050636	Sandbox	178.33.162.197	6893
72.5730130672	Sandbox	178.33.162.198	6893
72.5730979443	Sandbox	178.33.162.199	6893
72.5731830597	Sandbox	178.33.162.200	6893
72.5732710361	Sandbox	178.33.162.201	6893
72.5733559132	Sandbox	178.33.162.202	6893
72.5734400749	Sandbox	178.33.162.203	6893
72.5735249519	Sandbox	178.33.162.204	6893
72.5736100674	Sandbox	178.33.162.205	6893
72.5736949444	Sandbox	178.33.162.206	6893
72.5737791061	Sandbox	178.33.162.207	6893
72.5738630295	Sandbox	178.33.162.208	6893
72.5739469528	Sandbox	178.33.162.209	6893
72.5740320683	Sandbox	178.33.162.210	6893
72.5741159916	Sandbox	178.33.162.211	6893
72.5741999149	Sandbox	178.33.162.212	6893
72.5742850304	Sandbox	178.33.162.213	6893
72.5743710995	Sandbox	178.33.162.214	6893
72.5744559765	Sandbox	178.33.162.215	6893
72.5745410919	Sandbox	178.33.162.216	6893
72.5746259689	Sandbox	178.33.162.217	6893
72.5747098923	Sandbox	178.33.162.218	6893
72.5747950077	Sandbox	178.33.162.219	6893
72.574878931	Sandbox	178.33.162.220	6893
72.5750589371	Sandbox	178.33.162.221	6893
72.5751481056	Sandbox	178.33.162.222	6893
72.575232029	Sandbox	178.33.162.223	6893
72.575316906	Sandbox	178.33.162.224	6893
72.5754010677	Sandbox	178.33.162.225	6893
72.5754859447	Sandbox	178.33.162.226	6893
72.5755698681	Sandbox	178.33.162.227	6893
72.5756540298	Sandbox	178.33.162.228	6893
72.5757679939	Sandbox	178.33.162.229	6893
72.5758559704	Sandbox	178.33.162.230	6893
72.5759420395	Sandbox	178.33.162.231	6893
72.5760350227	Sandbox	178.33.162.232	6893
72.5761210918	Sandbox	178.33.162.233	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
72.5762059689	Sandbox	178.33.162.234	6893
72.5762898922	Sandbox	178.33.162.235	6893
72.576374054	Sandbox	178.33.162.236	6893
72.5764598846	Sandbox	178.33.162.237	6893
72.5765440464	Sandbox	178.33.162.238	6893
72.5766298771	Sandbox	178.33.162.239	6893
72.5767168999	Sandbox	178.33.162.240	6893
72.5768010616	Sandbox	178.33.162.241	6893
72.5768859386	Sandbox	178.33.162.242	6893
72.5769729614	Sandbox	178.33.162.243	6893
72.5770568848	Sandbox	178.33.162.244	6893
72.5771420002	Sandbox	178.33.162.245	6893
72.5772280693	Sandbox	178.33.162.246	6893
72.5773119926	Sandbox	178.33.162.247	6893
72.5773980618	Sandbox	178.33.162.248	6893
72.5774819851	Sandbox	178.33.162.249	6893
72.5775659084	Sandbox	178.33.162.250	6893
72.5776500702	Sandbox	178.33.162.251	6893
72.5777349472	Sandbox	178.33.162.252	6893
72.5778479576	Sandbox	178.33.162.253	6893
72.5779399872	Sandbox	178.33.162.254	6893
73.6308469772	Sandbox	178.33.162.255	6893
73.6309840679	Sandbox	178.33.163.0	6893
73.6310908794	Sandbox	178.33.163.1	6893
73.6311759949	Sandbox	178.33.163.2	6893
73.6312599182	Sandbox	178.33.163.3	6893
73.6313419342	Sandbox	178.33.163.4	6893
73.6314220428	Sandbox	178.33.163.5	6893
73.6315019131	Sandbox	178.33.163.6	6893
73.6315820217	Sandbox	178.33.163.7	6893
73.6316599846	Sandbox	178.33.163.8	6893
73.6317410469	Sandbox	178.33.163.9	6893
73.6318259239	Sandbox	178.33.163.10	6893
73.6319069862	Sandbox	178.33.163.11	6893
73.6319930553	Sandbox	178.33.163.12	6893
73.632076025	Sandbox	178.33.163.13	6893
73.6321558952	Sandbox	178.33.163.14	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
73.6322350502	Sandbox	178.33.163.15	6893
73.6323149204	Sandbox	178.33.163.16	6893
73.6323940754	Sandbox	178.33.163.17	6893
73.6324739456	Sandbox	178.33.163.18	6893
73.6325531006	Sandbox	178.33.163.19	6893
73.6326320171	Sandbox	178.33.163.20	6893
73.6327109337	Sandbox	178.33.163.21	6893
73.6327910423	Sandbox	178.33.163.22	6893
73.6328690052	Sandbox	178.33.163.23	6893
73.6329479218	Sandbox	178.33.163.24	6893
73.6330280304	Sandbox	178.33.163.25	6893
73.6331079006	Sandbox	178.33.163.26	6893
73.6331870556	Sandbox	178.33.163.27	6893
73.6332659721	Sandbox	178.33.163.28	6893
73.6333479881	Sandbox	178.33.163.29	6893
73.6334280968	Sandbox	178.33.163.30	6893
73.6335060596	Sandbox	178.33.163.31	6893
73.6335849762	Sandbox	178.33.163.32	6893
73.6336638927	Sandbox	178.33.163.33	6893
73.6337430477	Sandbox	178.33.163.34	6893
73.6338229179	Sandbox	178.33.163.35	6893
73.6339039803	Sandbox	178.33.163.36	6893
73.6339828968	Sandbox	178.33.163.37	6893
73.6340620518	Sandbox	178.33.163.38	6893
73.6341400146	Sandbox	178.33.163.39	6893
73.6342179775	Sandbox	178.33.163.40	6893
73.6342968941	Sandbox	178.33.163.41	6893
73.634376049	Sandbox	178.33.163.42	6893
73.6344549656	Sandbox	178.33.163.43	6893
73.6345338821	Sandbox	178.33.163.44	6893
73.6346130371	Sandbox	178.33.163.45	6893
73.6346919537	Sandbox	178.33.163.46	6893
73.6347699165	Sandbox	178.33.163.47	6893
73.6348490715	Sandbox	178.33.163.48	6893
73.6349279881	Sandbox	178.33.163.49	6893
73.6350069046	Sandbox	178.33.163.50	6893
73.6350860596	Sandbox	178.33.163.51	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
73.6351649761	Sandbox	178.33.163.52	6893
73.6352438927	Sandbox	178.33.163.53	6893
73.635322094	Sandbox	178.33.163.54	6893
73.6354019642	Sandbox	178.33.163.55	6893
73.6354808807	Sandbox	178.33.163.56	6893
73.6356060505	Sandbox	178.33.163.57	6893
73.6356890202	Sandbox	178.33.163.58	6893
73.6357688904	Sandbox	178.33.163.59	6893
73.635848999	Sandbox	178.33.163.60	6893
73.6359269619	Sandbox	178.33.163.61	6893
73.6360468864	Sandbox	178.33.163.62	6893
73.6361310482	Sandbox	178.33.163.63	6893
73.6362099648	Sandbox	178.33.163.64	6893
73.6362888813	Sandbox	178.33.163.65	6893
73.6363680363	Sandbox	178.33.163.66	6893
73.6364459991	Sandbox	178.33.163.67	6893
73.6365249157	Sandbox	178.33.163.68	6893
73.6366028786	Sandbox	178.33.163.69	6893
73.6366820335	Sandbox	178.33.163.70	6893
73.6367630959	Sandbox	178.33.163.71	6893
73.6368410587	Sandbox	178.33.163.72	6893
73.6369199753	Sandbox	178.33.163.73	6893
73.6369979382	Sandbox	178.33.163.74	6893
73.637075901	Sandbox	178.33.163.75	6893
73.637155056	Sandbox	178.33.163.76	6893
73.6372330189	Sandbox	178.33.163.77	6893
73.6373109818	Sandbox	178.33.163.78	6893
73.6373898983	Sandbox	178.33.163.79	6893
73.6374680996	Sandbox	178.33.163.80	6893
73.6375479698	Sandbox	178.33.163.81	6893
73.6377120018	Sandbox	178.33.163.82	6893
73.6377949715	Sandbox	178.33.163.83	6893
73.637873888	Sandbox	178.33.163.84	6893
73.637953043	Sandbox	178.33.163.85	6893
73.6380310059	Sandbox	178.33.163.86	6893
73.6381089687	Sandbox	178.33.163.87	6893
73.6381909847	Sandbox	178.33.163.88	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
73.6382710934	Sandbox	178.33.163.89	6893
73.6383490562	Sandbox	178.33.163.90	6893
73.6384260654	Sandbox	178.33.163.91	6893
73.638504982	Sandbox	178.33.163.92	6893
73.6385819912	Sandbox	178.33.163.93	6893
73.6386590004	Sandbox	178.33.163.94	6893
73.6387369633	Sandbox	178.33.163.95	6893
73.6388139725	Sandbox	178.33.163.96	6893
73.638892889	Sandbox	178.33.163.97	6893
73.6389710903	Sandbox	178.33.163.98	6893
73.6390490532	Sandbox	178.33.163.99	6893
73.6391270161	Sandbox	178.33.163.100	6893
73.6392059326	Sandbox	178.33.163.101	6893
73.6392850876	Sandbox	178.33.163.102	6893
73.6393630505	Sandbox	178.33.163.103	6893
73.6394410133	Sandbox	178.33.163.104	6893
73.6395199299	Sandbox	178.33.163.105	6893
73.6396000385	Sandbox	178.33.163.106	6893
73.6396780014	Sandbox	178.33.163.107	6893
73.6397559643	Sandbox	178.33.163.108	6893
73.6398329735	Sandbox	178.33.163.109	6893
73.6399109364	Sandbox	178.33.163.110	6893
73.6400001049	Sandbox	178.33.163.111	6893
73.6400809288	Sandbox	178.33.163.112	6893
73.6401629448	Sandbox	178.33.163.113	6893
73.6402440071	Sandbox	178.33.163.114	6893
73.6403229237	Sandbox	178.33.163.115	6893
73.6404008865	Sandbox	178.33.163.116	6893
73.6405050755	Sandbox	178.33.163.117	6893
73.6405849457	Sandbox	178.33.163.118	6893
73.6406641006	Sandbox	178.33.163.119	6893
73.6407420635	Sandbox	178.33.163.120	6893
73.6408209801	Sandbox	178.33.163.121	6893
73.6408998966	Sandbox	178.33.163.122	6893
73.6409790516	Sandbox	178.33.163.123	6893
73.6410570145	Sandbox	178.33.163.124	6893
73.641135931	Sandbox	178.33.163.125	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
73.6412129402	Sandbox	178.33.163.126	6893
73.6412909031	Sandbox	178.33.163.127	6893
73.6413679123	Sandbox	178.33.163.128	6893
73.6414458752	Sandbox	178.33.163.129	6893
73.6415240765	Sandbox	178.33.163.130	6893
73.641602993	Sandbox	178.33.163.131	6893
73.6416809559	Sandbox	178.33.163.132	6893
73.6417589188	Sandbox	178.33.163.133	6893
73.6418380737	Sandbox	178.33.163.134	6893
73.6419150829	Sandbox	178.33.163.135	6893
73.6419930458	Sandbox	178.33.163.136	6893
73.6420719624	Sandbox	178.33.163.137	6893
73.6421499252	Sandbox	178.33.163.138	6893
73.6422278881	Sandbox	178.33.163.139	6893
73.6423089504	Sandbox	178.33.163.140	6893
73.6423869133	Sandbox	178.33.163.141	6893
73.6424648762	Sandbox	178.33.163.142	6893
73.6425418854	Sandbox	178.33.163.143	6893
73.6426200867	Sandbox	178.33.163.144	6893
73.6426990032	Sandbox	178.33.163.145	6893
73.6427769661	Sandbox	178.33.163.146	6893
73.642854929	Sandbox	178.33.163.147	6893
73.6429328918	Sandbox	178.33.163.148	6893
73.6430120468	Sandbox	178.33.163.149	6893
73.6430900097	Sandbox	178.33.163.150	6893
73.6431679726	Sandbox	178.33.163.151	6893
73.6432459354	Sandbox	178.33.163.152	6893
73.6433238983	Sandbox	178.33.163.153	6893
73.6434020996	Sandbox	178.33.163.154	6893
73.6434829235	Sandbox	178.33.163.155	6893
73.6435608864	Sandbox	178.33.163.156	6893
73.6436378956	Sandbox	178.33.163.157	6893
73.6437149048	Sandbox	178.33.163.158	6893
73.6437931061	Sandbox	178.33.163.159	6893
73.643871069	Sandbox	178.33.163.160	6893
73.6439490318	Sandbox	178.33.163.161	6893
73.6440351009	Sandbox	178.33.163.162	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
73.6441140175	Sandbox	178.33.163.163	6893
73.6441919804	Sandbox	178.33.163.164	6893
73.6442689896	Sandbox	178.33.163.165	6893
73.6443500519	Sandbox	178.33.163.166	6893
73.6444280148	Sandbox	178.33.163.167	6893
73.644505024	Sandbox	178.33.163.168	6893
73.6445829868	Sandbox	178.33.163.169	6893
73.6446609497	Sandbox	178.33.163.170	6893
73.6447389126	Sandbox	178.33.163.171	6893
73.6448159218	Sandbox	178.33.163.172	6893
73.6448938847	Sandbox	178.33.163.173	6893
73.6449708939	Sandbox	178.33.163.174	6893
73.6450490952	Sandbox	178.33.163.175	6893
73.645127058	Sandbox	178.33.163.176	6893
73.6452050209	Sandbox	178.33.163.177	6893
73.6452839375	Sandbox	178.33.163.178	6893
73.6453630924	Sandbox	178.33.163.179	6893
73.6454401016	Sandbox	178.33.163.180	6893
73.6455180645	Sandbox	178.33.163.181	6893
73.6456279755	Sandbox	178.33.163.182	6893
73.6457118988	Sandbox	178.33.163.183	6893
73.645802021	Sandbox	178.33.163.184	6893
73.6458890438	Sandbox	178.33.163.185	6893
73.6459739208	Sandbox	178.33.163.186	6893
73.6460590363	Sandbox	178.33.163.187	6893
73.6461439133	Sandbox	178.33.163.188	6893
73.646228075	Sandbox	178.33.163.189	6893
73.6463119984	Sandbox	178.33.163.190	6893
73.6463959217	Sandbox	178.33.163.191	6893
73.6464838982	Sandbox	178.33.163.192	6893
73.6465680599	Sandbox	178.33.163.193	6893
73.6466510296	Sandbox	178.33.163.194	6893
73.6467339993	Sandbox	178.33.163.195	6893
73.6468179226	Sandbox	178.33.163.196	6893
73.6469039917	Sandbox	178.33.163.197	6893
73.6469869614	Sandbox	178.33.163.198	6893
73.6470720768	Sandbox	178.33.163.199	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
73.6471560001	Sandbox	178.33.163.200	6893
73.6472389698	Sandbox	178.33.163.201	6893
73.6473219395	Sandbox	178.33.163.202	6893
73.6474049091	Sandbox	178.33.163.203	6893
73.6475560665	Sandbox	178.33.163.204	6893
73.6476500034	Sandbox	178.33.163.205	6893
73.6477329731	Sandbox	178.33.163.206	6893
73.6478168964	Sandbox	178.33.163.207	6893
73.6478989124	Sandbox	178.33.163.208	6893
73.6480250359	Sandbox	178.33.163.209	6893
73.6481208801	Sandbox	178.33.163.210	6893
73.6482439041	Sandbox	178.33.163.211	6893
73.6483299732	Sandbox	178.33.163.212	6893
73.6484138966	Sandbox	178.33.163.213	6893
73.6484980583	Sandbox	178.33.163.214	6893
73.6485829353	Sandbox	178.33.163.215	6893
73.6486649513	Sandbox	178.33.163.216	6893
73.648747921	Sandbox	178.33.163.217	6893
73.6488339901	Sandbox	178.33.163.218	6893
73.6489169598	Sandbox	178.33.163.219	6893
73.6489999294	Sandbox	178.33.163.220	6893
73.6490840912	Sandbox	178.33.163.221	6893
73.6491680145	Sandbox	178.33.163.222	6893
73.6492500305	Sandbox	178.33.163.223	6893
73.6493339539	Sandbox	178.33.163.224	6893
73.6494159698	Sandbox	178.33.163.225	6893
73.6494989395	Sandbox	178.33.163.226	6893
73.6495819092	Sandbox	178.33.163.227	6893
73.6496660709	Sandbox	178.33.163.228	6893
73.6497490406	Sandbox	178.33.163.229	6893
73.6498310566	Sandbox	178.33.163.230	6893
73.6499140263	Sandbox	178.33.163.231	6893
73.6499969959	Sandbox	178.33.163.232	6893
73.6500790119	Sandbox	178.33.163.233	6893
73.6501619816	Sandbox	178.33.163.234	6893
73.6502449512	Sandbox	178.33.163.235	6893
73.6503288746	Sandbox	178.33.163.236	6893

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
73.6504120827	Sandbox	178.33.163.237	6893
73.6504940987	Sandbox	178.33.163.238	6893
73.6505799294	Sandbox	178.33.163.239	6893
73.6506619453	Sandbox	178.33.163.240	6893
73.6507749557	Sandbox	178.33.163.241	6893
73.6508610249	Sandbox	178.33.163.242	6893
73.6509439945	Sandbox	178.33.163.243	6893
73.6510300636	Sandbox	178.33.163.244	6893
73.6511120796	Sandbox	178.33.163.245	6893
73.6511950493	Sandbox	178.33.163.246	6893
73.6512770653	Sandbox	178.33.163.247	6893
73.6513600349	Sandbox	178.33.163.248	6893
73.6514430046	Sandbox	178.33.163.249	6893
73.6515259743	Sandbox	178.33.163.250	6893
73.6516089439	Sandbox	178.33.163.251	6893
73.6516919136	Sandbox	178.33.163.252	6893
73.6517739296	Sandbox	178.33.163.253	6893
73.6518559456	Sandbox	178.33.163.254	6893
74.6977028847	Sandbox	178.33.163.255	6893
84.7037119865	Sandbox	224.0.0.252	5355
86.1696469784	Sandbox	224.0.0.252	5355
87.6901810169	Sandbox	8.8.4.4	53
88.2481839657	Sandbox	8.8.4.4	53
88.8608579636	Sandbox	8.8.4.4	53
90.1388599873	Sandbox	8.8.4.4	53
90.2551529408	Sandbox	8.8.4.4	53
90.2556400299	Sandbox	8.8.4.4	53
91.0401690006	Sandbox	8.8.4.4	53
91.1313209534	Sandbox	8.8.4.4	53
91.5202610493	Sandbox	8.8.4.4	53
91.6165618896	Sandbox	8.8.4.4	53
93.2618379593	Sandbox	8.8.4.4	53
130.151349068	Sandbox	8.8.4.4	53
132.034847021	Sandbox	8.8.4.4	53

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
D:_R_E_A_D___T_H_I_S___SIZ9T2UH_.Txt **C:\Users\User\AppData\Roaming\Microsoft\Outlook_R_E_A_D___T_H_I_S___0Y9M_.Txt**	**Type :** ASCII text, with CRLF line terminators **MD5 :** 1c85f3fba77c5644a17161fc914b11a8 **SHA-1 :** cd4e1b64656516a9145c4ab3445a72ee260042ca **SHA-256 :** 2c6a94c8cb01c436781b94deedf3b03c247d95e9 **SHA-512 :** bc0b5979f736b886c49aea399b5345bc964d390b **Size :** 1.36 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Outlook\RxPSr5YUl7.97bf	**Type :** Microsoft Outlook email folder (>=2003) **MD5 :** 56b7ec6297716c13a2930b621c1b3c3b **SHA-1 :** 97cb16312726562ff8fbc6afd0f341a4f8792fef **SHA-256 :** 99c94821874661d7c7ef6b3d80ad43910509298 **SHA-512 :** 86c389d5dd7bb71d4ec99d487f2fa757a0e850e6 **Size :** 271.78 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Outlook\U0zWeuumVq.97bf	**Type :** Composite Document File V2 Document, No summary info **MD5 :** c4d154e1c4bca0bfc68d092d2e30654b **SHA-1 :** a028cf89fce5a948da74d6feb9bc46d4cf26449a **SHA-256 :** 796a4009c4c5850eeb3d04dd2e3c2ed8dc5f0c8b **SHA-512 :** 89beeffe2d2157e2596cedeb991e004f1281f4c48 **Size :** 2.98 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Outlook\0g4yPMug6i.97bf	**Type :** XML document text **MD5 :** 87385958e283c062e59cbd7102fe24ba **SHA-1 :** 6dc5002b8cc7509b2f28ebfad57eecfa03971e33 **SHA-256 :** 7a93156072cda78e85c31ddf149429cdc4ac7417 **SHA-512 :** bdf70ffe9367dbaa5afee8472b5770ad784da4d5 **Size :** 3.447 Kilobytes.
C:\Users\User\AppData\Local\Temp\8902607b\40b9.Tmp	**Type :** ASCII text, with very long lines, with no line terminators **MD5 :** 56bebe2a3b89fa49a75796e577df1026 **SHA-1 :** 16f40f1a8961bbc295790ebc379f4cd92cda3be5 **SHA-256 :** 247704b2bf39d5f8d491a6b910168d7d0966a52 **SHA-512 :** 8530db7b51a719131512d2f72a5e19c73a0ea904 **Size :** 0.344 Kilobytes.
C:\Users\User\AppData\Local\Temp\8902607b\Cafe.Tmp	**Type :** b.out overlay separate pure segmented object file V3.0 86 Large Text Large Data **MD5 :** fb0f30181f7f4597752c8677b234ee32 **SHA-1 :** 6a1c808ddc3c75978202fedcda4e1af38bb4bbe6 **SHA-256 :** 6eb86bd7ca437beb2c4d61659edfe13607712c07 **SHA-512 :** 758c29a0f142fd829d5027b352594abcf67d5fa31 **Size :** 0.13 Kilobytes.
D:\CPbJPOO7nE.97bf	**Type :** data **MD5 :** d27721c778a037aae8afbf9af6db23dd **SHA-1 :** 6de5208d8999a7368be4395cae52a558eb003316 **SHA-256 :** 9b8667524ed96b50d41b8202dc986aa0391e227 **SHA-512 :** 94bff6fc9d981a6cb6e89ae189770c831a5ce218e **Size :** 6.989 Kilobytes.

FILE PATH	TYPE AND HASHES
D:_R_E_A_D___T_H_I_S___V5BE_.Hta **C:\Users\User\AppData\Roaming\Microsoft\Outlook_R_E_A_D___T_H_I_S___JN4MMCO_.Hta**	**Type :** HTML document, UTF-8 Unicode text, with very long lines, with CRLF line terminators **MD5 :** c54e894b3139f7eff2ca1b1e3906b86c **SHA-1 :** f07bc3e64a7925147f4ec5e56483b2dec3ef9f5e **SHA-256 :** 382e8187f6da6e032c178334e310c2a78075419b **SHA-512 :** 8d382a2cdeaec0038543ab6ed013ed1a2432ce47 **Size :** 77.335 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	2
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	0dddca0add163af6238f2b68bc25a88ada1f35d5
MD5:	cc52ba8f6f250704f6ed9139a242382f
First Seen Date:	2017-05-22 08:24:48.646232 (7 years ago)
Number Of Clients Seen:	5
Last Analysis Date:	2018-08-07 13:56:12.808825 (6 years ago)
Human Expert Analysis Date:	2020-12-06 13:50:28.374153 (3 years ago)
Human Expert Analysis Result:	Malware

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[]
Number Of Sections	4
Trid	[[41.0, u'Win32 Executable MS Visual C++ (generic)'], [36.3, u'Win64 Executable (generic)'], [8.6, u'Win32 Dynamic Link Library (generic)'], [5.9, u'Win32 Executable (generic)'], [2.6, u'OS/2 Executable (generic)']]
Compilation Time Stamp	0x59229958 [Mon May 22 07:55:04 2017 UTC]
CompanyName	IObit
Entry Point	0x454a40 (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	452608
Ssdeep	
Sha256	b076d68a304f781505c27fd7e6b2c7d1d247aa676f5fda360c86718ce0920712
Exifinfo	[]
Mime Type	application/x-dosexec
Imphash	fe97a329c0136b1755732853ef345541

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x5450e	0x54600	5.60898088057	47f65ab5880a617e4b17d686d29e0980
.rdata	0x56000	0x2248	0x2400	5.44278324885	01658a0edbe083c39e299d57aaf37960
.data	0x59000	0x71c	0x800	4.17726006954	e2e4624986edd8db71cc356ae5a1438f
.rsrc	0x5a000	0x17070	0x17200	5.85967888392	2f3c4406275f887d7075c80fb94156dd

PE Imports

- KERNEL32.dll
  - WriteFile
  - WideCharToMultiByte
  - WaitForSingleObject
  - VirtualFree
  - VirtualAlloc
  - VerifyVersionInfoW
  - UnhandledExceptionFilter
  - TlsSetValue
  - TlsGetValue
  - TlsFree

    - TlsAlloc
    - Thread32Next
    - TerminateProcess
    - Sleep
    - SetUnhandledExceptionFilter
    - SetLocalTime
    - SetLastError
    - SetHandleCount
    - SetConsoleScreenBufferSize
    - RtlUnwind
    - RaiseException
    - QueryPerformanceCounter
    - MultiByteToWideChar
    - LocalFree
    - LoadLibraryA
    - LeaveCriticalSection
    - LCMapStringW
    - LCMapStringA
    - IsValidCodePage
    - IsDebuggerPresent
    - InterlockedIncrement
    - InterlockedDecrement
    - InitializeCriticalSectionAndSpinCount
    - HeapSize
    - HeapReAlloc
    - HeapFree
    - HeapCreate
    - GetVersionExA
    - GetTickCount
    - GetTempPathA
    - GetSystemTimeAsFileTime
    - GetStringTypeW
    - GetStringTypeA
    - GetStdHandle
    - GetStartupInfoA
    - GetProcAddress
    - GetOEMCP
    - GetModuleHandleW
    - GetModuleHandleA
    - GetModuleFileNameA
    - GetLocaleInfoA
    - GetLastError
    - GetFileType
    - GetEnvironmentStringsW
    - GetEnvironmentStrings
    - GetCurrentThreadId
    - GetCurrentProcessId
    - GetCurrentProcess
    - GetCommandLineA
    - GetCommMask
    - GetCPInfo
    - BeginUpdateResourceA
    - GetACP
    - FreeEnvironmentStringsW
    - FreeEnvironmentStringsA
    - FormatMessageA
    - FindNextFileA
    - FindFirstFileA
    - FindClose
    - ExitProcess
    - EnumLanguageGroupLocalesA
    - EnterCriticalSection
    - DeleteCriticalSection
    - CloseHandle
    - HeapAlloc
- USER32.dll
    - GetProcessWindowStation
    - IsIconic
    - EndMenu
    - GetOpenClipboardWindow
    - GetClipboardSequenceNumber
    - GetCaretBlinkTime
    - IsWindow
    - CharUpperA
    - GetActiveWindow

- PaintDesktop
- GetWindowDC
- IsCharAlphaNumericA
- GetDesktopWindow
- CloseDesktop
- GetKeyboardLayout
- GetInputState
- IsWindowVisible
- GetMenuContextHelpId
- GetLastActivePopup
- CloseClipboard
- LoadCursorFromFileA
- CharLowerW
- IsCharAlphaNumericW
- DestroyCursor
- VkKeyScanA
- VkKeyScanW
- GetQueueStatus
- GetSysColor
- GetWindowTextLengthW
- IsGUIThread
- CharLowerA
- GetDialogBaseUnits
- IsCharLowerA
- ShowCaret
- GetKeyState
- GetMessageExtraInfo
- GetTopWindow
- CharNextA
- IsCharAlphaA
- DestroyIcon
- UserHandleGrantAccess
- TranslateMessage
- TranslateMDISysAccel
- ToAscii
- SystemParametersInfoW
- ShowWindow
- SetWindowTextW
- SetWindowPos
- IsWindowEnabled
- SetTimer
- SetScrollInfo
- SetMenuContextHelpId
- SetForegroundWindow
- SetDlgItemTextW
- SetClipboardViewer
- SendMessageW
- SendMessageTimeoutA
- SendDlgItemMessageW
- ReplyMessage
- RegisterClipboardFormatA
- RegisterClassExA
- PostQuitMessage
- PostMessageW
- OpenIcon
- MonitorFromRect
- MessageBoxW
- MessageBoxA
- LoadStringW
- LoadKeyboardLayoutW
- LoadImageW
- LoadBitmapW
- KillTimer
- IsCharUpperW
- HiliteMenuItem
- GetWindowLongW
- GetSystemMetrics
- GetSysColorBrush
- GetScrollPos
- GetMonitorInfoW
- GetMessageW
- GetMenuItemRect
- GetInputDesktop
- GetDlgItem
- GetDlgCtrlID

- GetClientRect
- FindWindowW
- EnumWindowStationsA
- EndDialog
- DispatchMessageW
- DestroyWindow
- DefWindowProcW
- CreateWindowExW
- CreateMenu
- CreateIconIndirect
- GetMenu
- LoadCursorFromFileW
- WindowFromDC
- GetCursor
- CallWindowProcW
- ChangeDisplaySettingsExW
- CharNextW
- CloseWindow
- CopyIcon
- SetWindowLongW
- GetThreadDesktop
- CreateIconFromResourceEx
- CreateIcon
- CreateDialogIndirectParamW
- IsMenu

- GDI32.dll
  - GdiPlayJournal
  - GdiPlayPrivatePageEMF
  - GdiSetBatchLimit
  - GetCharABCWidthsFloatW
  - GetCharABCWidthsW
  - GetCurrentPositionEx
  - GetDeviceCaps
  - GetEnhMetaFileW
  - GetFontData
  - GetGlyphIndicesA
  - GetTextExtentExPointWPri
  - GetWinMetaFileBits
  - ModifyWorldTransform
  - NamedEscape
  - PathToRegion
  - PolyDraw
  - ScaleViewportExtEx
  - SetDIBColorTable
  - SetMetaRgn
  - SetPolyFillMode
  - SetROP2
  - SetTextAlign
  - UpdateColors
  - GetSystemPaletteUse
  - CreateMetaFileW
  - FlattenPath
  - GdiEntry8
  - BeginPath
  - CreatePatternBrush
  - GetTextCharacterExtra
  - CancelDC
  - GdiGetBatchLimit
  - GetColorSpace
  - EndPath
  - EndPage
  - SaveDC
  - SwapBuffers
  - CloseMetaFile
  - GetDCPenColor
  - AbortDoc
  - GetTextCharset
  - GdiFlush
  - FillPath
  - CloseFigure
  - GetTextAlign
  - GetMapMode
  - GetBkMode
  - GetStretchBltMode
  - CreateMetaFileA

    - FillRgn
    - EngTextOut
    - EngPaint
    - EngFillPath
    - GdiDeleteSpoolFileHandle
    - GdiConvertBrush
    - GdiAlphaBlend
    - FontIsLinked
    - DeleteEnhMetaFile
    - FloodFill
    - EngDeleteSurface
    - EngCreatePalette
    - EngCreateDeviceSurface
    - DeleteObject
    - AbortPath
    - CreateFontA
    - CreateCompatibleDC
    - CreateColorSpaceW
    - CopyEnhMetaFileA
    - CloseEnhMetaFile
    - AngleArc
    - AddFontResourceExW
    - EndDoc
- ADVAPI32.dll
    - RegSetValueExA
    - CryptReleaseContext
    - RegCloseKey
    - RegCreateKeyExW
    - RegDeleteKeyW
    - RegDeleteValueA
    - RegOpenKeyExA
    - RegQueryValueExA
    - RegSetValueExW
    - RegQueryValueExW
    - RegOpenKeyW
    - CryptGetHashParam
    - CryptDestroyHash
    - CryptCreateHash
    - CryptAcquireContextW
    - CryptHashData
- SHELL32.dll
    - SHGetFolderPathW
    - CommandLineToArgvW
    - ShellExecuteExA
- ole32.dll
    - CoUninitialize
    - CoCreateInstance
    - CoInitialize
- SHLWAPI.dll
    - StrCmpNA
    - StrStrA
- COMCTL32.dll
    - CreateStatusWindowW
    - ImageList_Create
    - ImageList_Destroy
    - InitCommonControlsEx
    - ImageList_AddMasked
- msvcrt.dll
    - wcslen
    - _XcptFilter
    - __dllonexit
    - __p__commode
    - __p__fmode
    - __set_app_type
    - __setusermatherr
    - __wgetmainargs
    - _adjust_fdiv
    - _c_exit
    - _cexit
    - _controlfp
    - _except_handler3
    - _exit
    - _initterm
    - _onexit
    - _purecall

- _snwprintf
- _wcmdln
- _wcsicmp
- _wcsnicmp
- exit
- wcscat
- wcscmp
- wcscpy

- IMM32.dll
  - ImmDisableIME

PE Resources

{u'lang': u'LANG_NEUTRAL', u'name': u'MAD', u'offset': 370864, u'sha256': u'a22abdb37c6ee8509574c60d5ed0b01bccc3501969b76b5ba4d50ff11597c0d9', u'type': u'data', u'size': 20}

{u'lang': u'LANG_NEUTRAL', u'name': u'MAD', u'offset': 370888, u'sha256': u'57a48b81b376f6b172e6493a0c152b3cc4af2848ba29379b3011951d299da01a', u'type': u'data', u'size': 20812}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_BITMAP', u'offset': 391704, u'sha256': u'79b57981370a365630c38347a72faae39178f2a966f3255f86d4d1093b680dbc', u'type': u'dBase IV DBT, block length 4096, next free block index 40, next free block 0, next used block 0', u'size': 4136}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_BITMAP', u'offset': 395840, u'sha256': u'3a77f0b86773d8e38579de4dde3e4653bdcb511c8356d0da3f308d2bc4058d85', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1064}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_BITMAP', u'offset': 396904, u'sha256': u'8508136dfa1d6d0c5f83ac380e3135a082ac51c1569169334fd1cf77e88b47eb', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1064}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_BITMAP', u'offset': 397968, u'sha256': u'6e02c6e2d9e4d7b1ee9e9447ad9092ade890923991299620fa3ecb6576e0b80c', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1064}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_BITMAP', u'offset': 399032, u'sha256': u'ade53dffb0f3cdfef249a1dba71227bd8f61102aa2860f07e11b268aeadfafdf', u'type': u'dBase IV DBT, block length 4096, next free block index 40, next free block 0, next used block 0', u'size': 4136}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_BITMAP', u'offset': 403168, u'sha256': u'fc1664a227956d727418bfbef2aa7c93aca65b135f04e42378411424ebae5f11', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1064}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_BITMAP', u'offset': 404232, u'sha256': u'c62165726722a9bf988f39ac1aa95366766c2af4eff9f25fc662d4548c440bcd', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1064}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_BITMAP', u'offset': 405296, u'sha256': u'fb7edb68625e48b2265ee382e1e56eddda1c0d2d8a7cd0da7663d892d29b7da2', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1064}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_BITMAP', u'offset': 406360, u'sha256': u'4e97f521449f95b5e0b395db0eb8b87d92e66a76948bb267431cdee3cf24a8a0', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1064}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_BITMAP', u'offset': 407424, u'sha256': u'f060483634c2e364d9cc6cd256a8b5adbdd4cbcf1ae890da65274915c4d5ab2a', u'type': u'dBase IV DBT, block length 4096, next free block index 40, next free block 0, next used block 0', u'size': 4136}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_BITMAP', u'offset': 411560, u'sha256': u'30ad678fa5f9840550fa060ca4fa2599849c0ced2839daac9b0a3c7f7e92cf80', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1064}

{u'lang': u'LANG_CHINESE', u'name': u'RT_ICON', u'offset': 451496, u'sha256': u'a94f3eae5b9ad7fc0c9ad2b74ca775f72505adb104eb20d413b35ba88b98cb6c', u'type': u'data', u'size': 2217}

{u'lang': u'LANG_CHINESE', u'name': u'RT_ICON', u'offset': 453720, u'sha256': u'da0359262ac75d0afbb3de3aa7713c631509fc1e96ee431db25d54ce683dfc19', u'type': u'data', u'size': 1736}

{u'lang': u'LANG_CHINESE', u'name': u'RT_ICON', u'offset': 455456, u'sha256': u'a37c109e095c6e08e243c3ee9ddc729f376470374de52c2f721a241753e621c2', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1384}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 458664, u'sha256': u'ca1a224b0a01ec8fa7f0c2b3f7081fdd76c0ac9f60bed5a2d695d6414c2daf60', u'type': u'data', u'size': 582}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 459248, u'sha256': u'b0468f892ac62fb3d94cdb4c9359ca8fb20f75fa3f85658506c18c780ec41feb', u'type': u'data', u'size': 880}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 460128, u'sha256': u'6a65302c89c7ba229f1b21b3daa3b991c648234cc5c027a1492220c2f2370f09', u'type': u'data', u'size': 266}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 460400, u'sha256': u'c6ec1e31e5a3b39db364ef98b5f44727eb821481518601e0d62a61a597231363', u'type': u'data', u'size': 204}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 460608, u'sha256': u'd73479e1eaa6a8f97c82b597e2184dc24167b1663d17924f550b35c684c46124', u'type': u'data', u'size': 566}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 461176, u'sha256': u'6b96d88f3182ca0a51213c6378b452178c3d17ab9eb99516f862f306a1efe878', u'type': u'data', u'size': 980}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 462160, u'sha256': u'cb7dedaebad394640a5aa87950b89368a2e4fe11941b75717de27701890865c8', u'type': u'data', u'size': 796}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_RCDATA', u'offset': 412624, u'sha256': u'677245e2a6b2eb5495b4965b8c26025a4b26e8b8c21a825f658cb390b493b9a0', u'type': u'data', u'size': 33512}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_RCDATA', u'offset': 446136, u'sha256': u'88d14cc6638af8a0836f6d868dfab60df92907a2d7becaefbbd7e007acb75610', u'type': u'Sendmail frozen configuration ', u'size': 16}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_RCDATA', u'offset': 446152, u'sha256': u'7897c32507b4982280a72489c545de7228061dab0be4f3a903bc45f6d3411e89', u'type': u'data', u'size': 580}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_RCDATA', u'offset': 446736, u'sha256': u'7ff0b5c1677be36127872446d06f9b2cfd44792e07f2e0b32691751291c5d793', u'type': u"Delphi compiled form 'TMadExcept'", u'size': 2680}

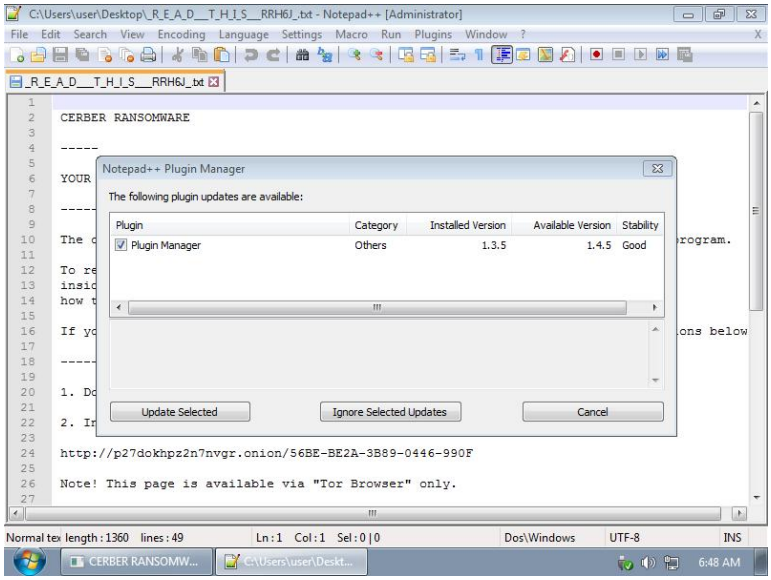
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_RCDATA', u'offset': 449416, u'sha256':

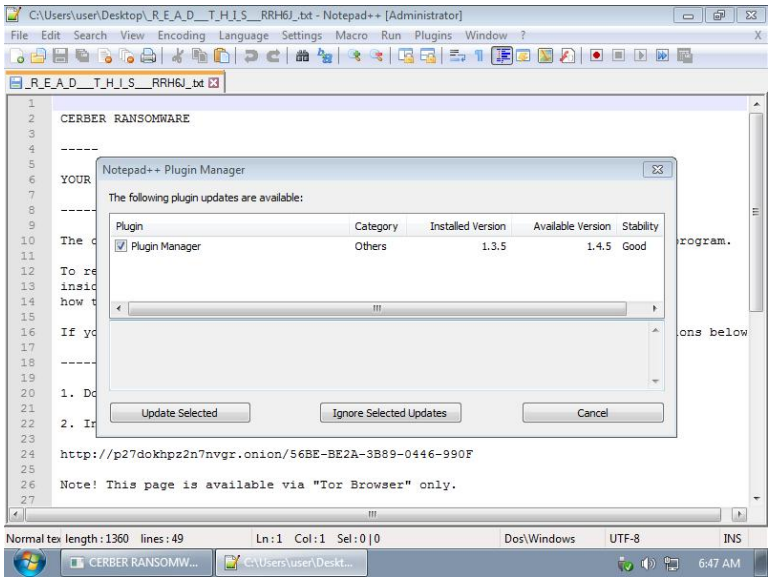
u'6535aff16f7dbc6e9de5441e7d8c37c05b5561ca3513320737191080688 6e460', u'type': u"Delphi compiled form 'TMEContactForm'", u'size': 846}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_RCDATA', u'offset': 450264, u'sha256': u'3ac3b9b5ce96065d66e43a39cfd94a2537f1fe814b207a91e98809233c08788f', u'type': u"Delphi compiled form 'TMEDetailsForm'", u'size': 552}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_RCDATA', u'offset': 450816, u'sha256': u'59969b70b6bc055a7e1bc5e8162e9689972d3c76af959d22ded3bdad37088810', u'type': u"Delphi compiled form 'TMEScrShotForm'", u'size': 675}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_RCDATA', u'offset': 457096, u'sha256': u'57c2e5664a7397eab29502b4a13024d8aa81ab6c54037d808030bc994bd05cce', u'type': u'exported SGML document, ASCII text, with CRLF line terminators', u'size': 1564}
{u'lang': u'LANG_CHINESE', u'name': u'RT_GROUP_ICON', u'offset': 456840, u'sha256': u'881824ef0c1b86bc95fee30f24eba14ed0728264013fdb13e44bca0c935e6028', u'type': u'MS Windows icon resource - 3 icons, 32x32', u'size': 48}
{u'lang': u'LANG_DUTCH', u'name': u'RT_VERSION', u'offset': 456888, u'sha256': u'a613afcf7d6ca3984e9e15e00b78bc91aa9e1a9c2587686553dfb2b24005922f', u'type': u'data', u'size': 202}

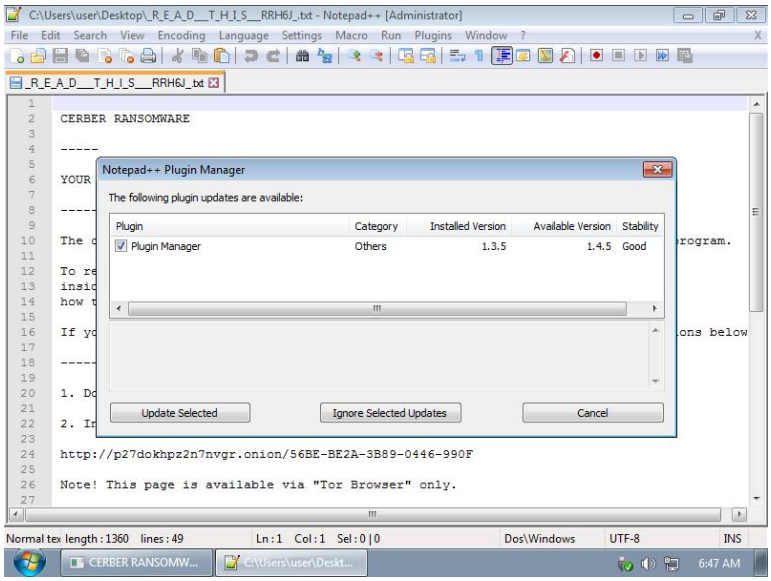
CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS

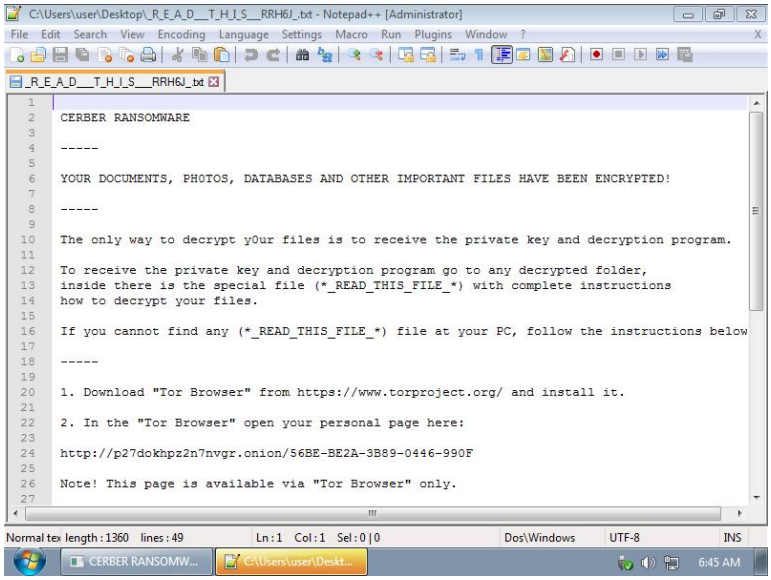





C:\Users\user\Desktop_R_E_A_D___T_H_I_S___RRH6J_.txt - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
_R_E_A_D___T_H_I_S___RRH6J_.txt
CERBER RANSOMWARE

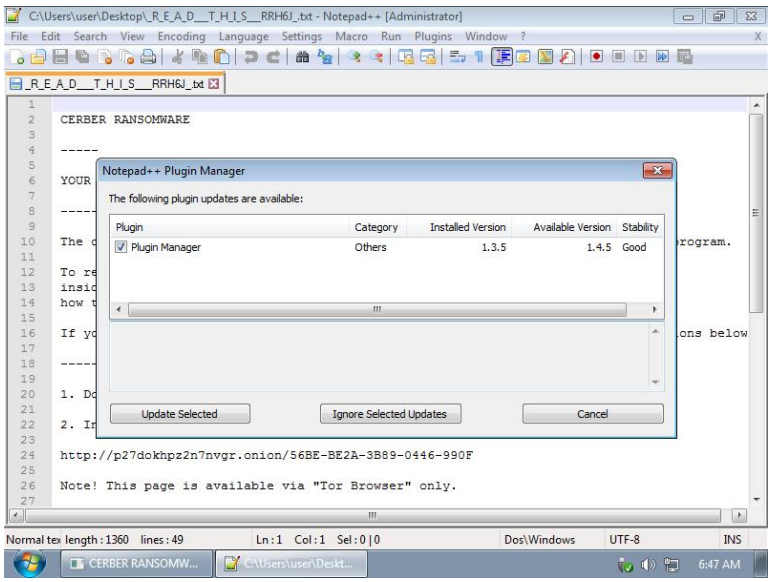
YOUR

The
To re
insid
how t
If yo
-----
1. Do
2. In
http://p27dokhpz2n7nvgr.onion/56BE-BE2A-3B89-0446-990F
Note! This page is available via "Tor Browser" only.
Notepad++ Plugin Manager
The following plugin updates are available:
Plugin
Category
Installed Version
Available Version
Stability
Plugin Manager
Others
1.3.5
1.4.5
Good
Update Selected
Ignore Selected Updates
Cancel
Normal tex length : 1360 lines : 49
Ln : 1 Col : 1 Sel : 0 | 0
Dos\Windows
UTF-8
INS
CERBER RANSOMW...
6:47 AM


C:\Users\user\Desktop_R_E_A_D___T_H_I_S___RRH6J_.txt - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
_R_E_A_D___T_H_I_S___RRH6J_.txt
CERBER RANSOMWARE

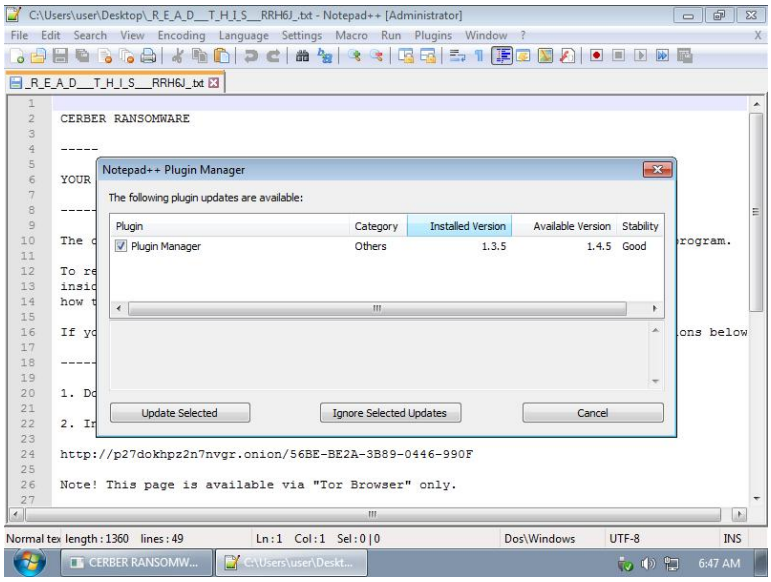
YOUR DOCUMENTS, PHOTOS, DATABASES AND OTHER IMPORTANT FILES HAVE BEEN ENCRYPTED!

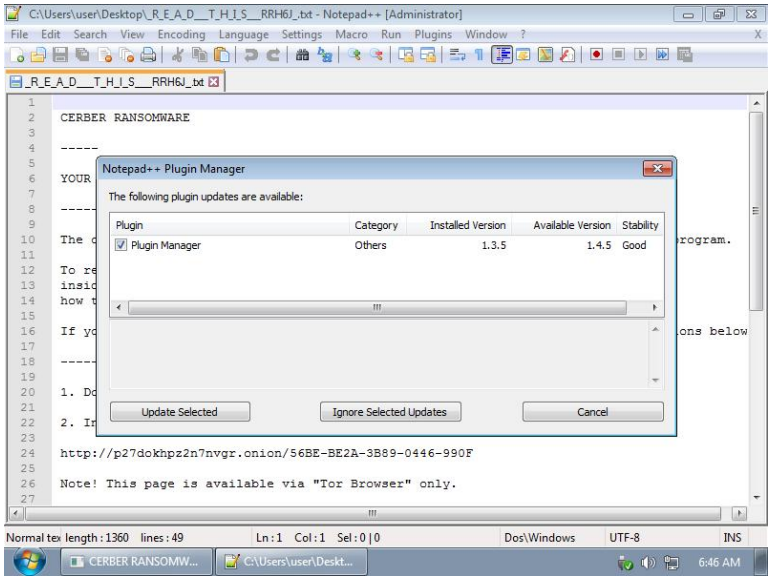
The only way to decrypt yOur files is to receive the private key and decryption program.
To receive the private key and decryption program go to any decrypted folder,
inside there is the special file (*_READ_THIS_FILE_*) with complete instructions
how to decrypt your files.
If you cannot find any (*_READ_THIS_FILE_*) file at your PC, follow the instructions below
-----
1. Download "Tor Browser" from https://www.torproject.org/ and install it.
2. In the "Tor Browser" open your personal page here:
http://p27dokhpz2n7nvgr.onion/56BE-BE2A-3B89-0446-990F
Note! This page is available via "Tor Browser" only.
Normal tex length : 1360 lines : 49
Ln : 1 Col : 1 Sel : 0 | 0
Dos\Windows
UTF-8
INS
CERBER RANSOMW...
6:45 AM

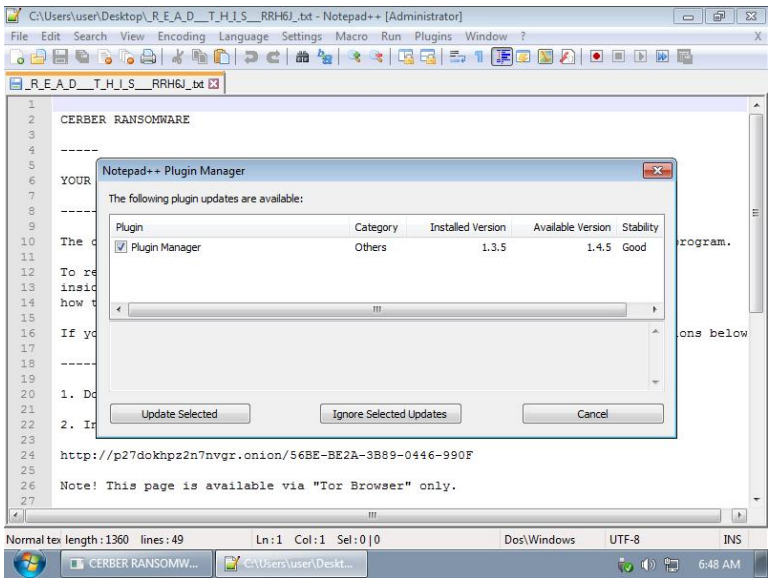

C:\Users\user\Desktop_R_E_A_D___T_H_I_S___RRH6J_.txt - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
_R_E_A_D___T_H_I_S___RRH6J_.txt
CERBER RANSOMWARE

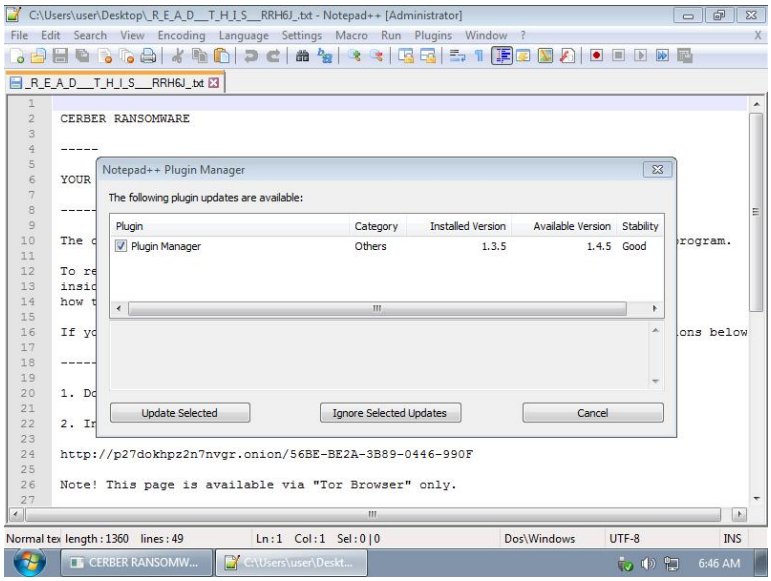
YOUR

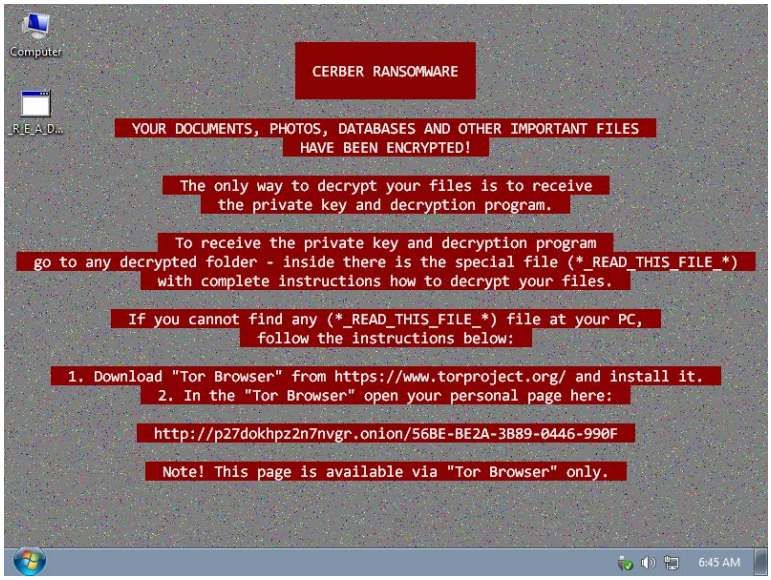
The
To re
insid
how t
If yo
-----
1. Do
2. In
http://p27dokhpz2n7nvgr.onion/56BE-BE2A-3B89-0446-990F
Note! This page is available via "Tor Browser" only.
Notepad++ Plugin Manager
The following plugin updates are available:
Plugin
Category
Installed Version
Available Version
Stability
Plugin Manager
Others
1.3.5
1.4.5
Good
Update Selected
Ignore Selected Updates
Cancel
Normal tex length : 1360 lines : 49
Ln : 1 Col : 1 Sel : 0 | 0
Dos\Windows
UTF-8
INS
CERBER RANSOMW...
6:47 AM

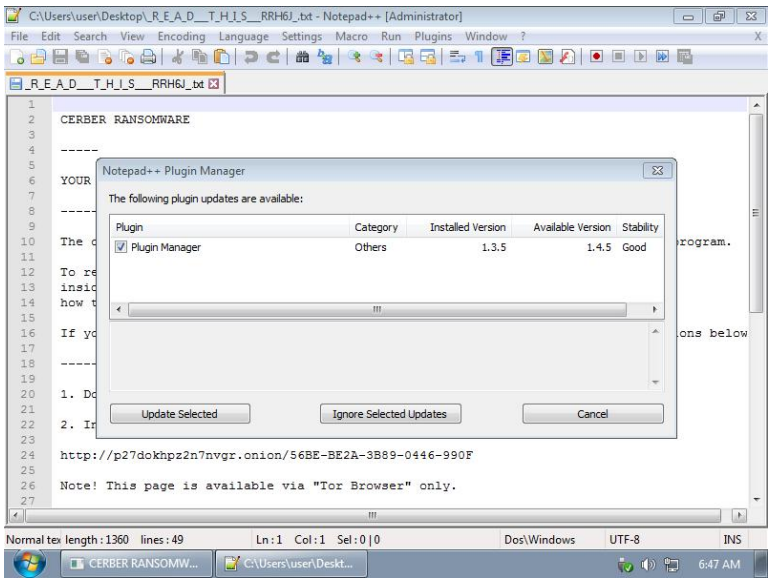

C:\Users\user\Desktop_R_E_A_D___T_H_I_S___RRH6J_.txt - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
_R_E_A_D___T_H_I_S___RRH6J_.txt
CERBER RANSOMWARE
Notepad++ Plugin Manager
The following plugin updates are available:
Plugin
Category
Installed Version
Available Version
Stability
Plugin Manager
Others
1.3.5
1.4.5
Good
Update Selected
Ignore Selected Updates
Cancel
http://p27dokhpz2n7nvgr.onion/56BE-BE2A-3B89-0446-990F
Note! This page is available via "Tor Browser" only.
Normal tex length : 1360 lines : 49
Ln : 1 Col : 1 Sel : 0 | 0
Dos\Windows
UTF-8
INS
6:47 AM

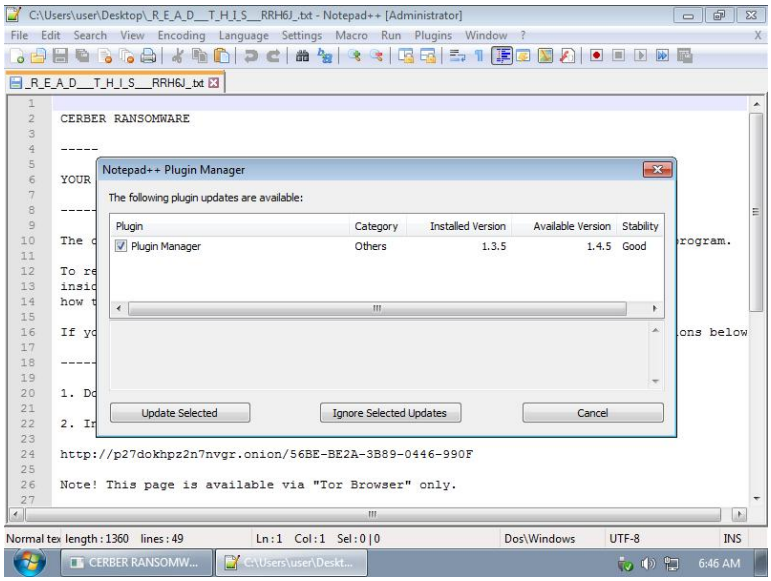

C:\Users\user\Desktop_R_E_A_D___T_H_I_S___RRH6J_.txt - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
_R_E_A_D___T_H_I_S___RRH6J_.txt
CERBER RANSOMWARE
Notepad++ Plugin Manager
The following plugin updates are available:
Plugin
Category
Installed Version
Available Version
Stability
Plugin Manager
Others
1.3.5
1.4.5
Good
Update Selected
Ignore Selected Updates
Cancel
http://p27dokhpz2n7nvgr.onion/56BE-BE2A-3B89-0446-990F
Note! This page is available via "Tor Browser" only.
Normal tex length : 1360 lines : 49
Ln : 1 Col : 1 Sel : 0 | 0
Dos\Windows
UTF-8
INS
6:46 AM

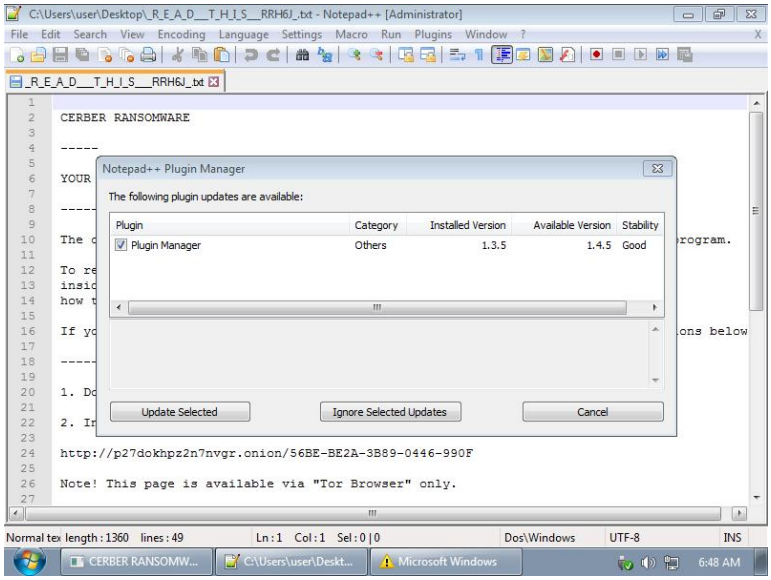

C:\Users\user\Desktop_R_E_A_D___T_H_I_S___RRH6J_.txt - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
_R_E_A_D___T_H_I_S___RRH6J_.txt
CERBER RANSOMWARE
Notepad++ Plugin Manager
The following plugin updates are available:
Plugin
Category
Installed Version
Available Version
Stability
Plugin Manager
Others
1.3.5
1.4.5
Good
Update Selected
Ignore Selected Updates
Cancel
http://p27dokhpz2n7nvgr.onion/56BE-BE2A-3B89-0446-990F
Note! This page is available via "Tor Browser" only.
Normal tex length : 1360 lines : 49
Ln : 1 Col : 1 Sel : 0 | 0
Dos\Windows
UTF-8
INS
6:48 AM

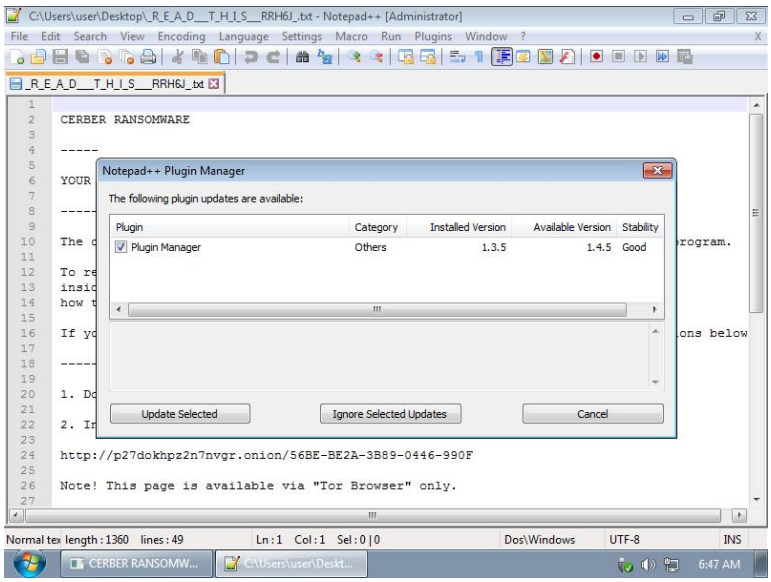

C:\Users\user\Desktop_R_E_A_D___T_H_I_S___RRH6J_.txt - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
_R_E_A_D___T_H_I_S___RRH6J_.txt
CERBER RANSOMWARE
YOUR
Notepad++ Plugin Manager
The following plugin updates are available:
Plugin
Category
Installed Version
Available Version
Stability
Plugin Manager
Others
1.3.5
1.4.5
Good
Update Selected
Ignore Selected Updates
Cancel
http://p27dokhpz2n7nvgr.onion/56BE-BE2A-3B89-0446-990F
Note! This page is available via "Tor Browser" only.
Normal tex length : 1360 lines : 49
Ln : 1 Col : 1 Sel : 0 | 0
Dos\Windows
UTF-8
INS
6:46 AM

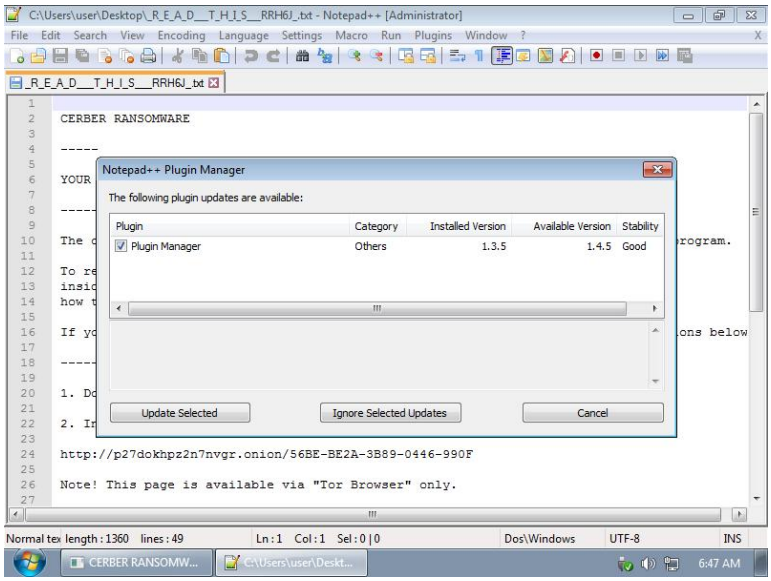

Computer
_R_E_A_D...
CERBER RANSOMWARE
YOUR DOCUMENTS, PHOTOS, DATABASES AND OTHER IMPORTANT FILES HAVE BEEN ENCRYPTED!
The only way to decrypt your files is to receive the private key and decryption program.
To receive the private key and decryption program go to any decrypted folder - inside there is the special file (*_READ_THIS_FILE_*) with complete instructions how to decrypt your files.
If you cannot find any (*_READ_THIS_FILE_*) file at your PC, follow the instructions below:
1. Download "Tor Browser" from https://www.torproject.org/ and install it.
2. In the "Tor Browser" open your personal page here:
http://p27dokhpz2n7nvgr.onion/56BE-BE2A-3B89-0446-990F
Note! This page is available via "Tor Browser" only.
6:45 AM

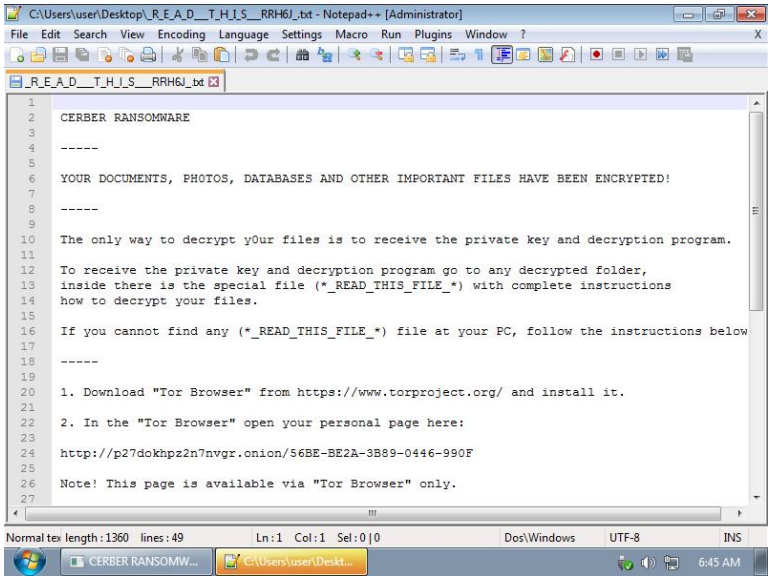

C:\Users\user\Desktop_R_E_A_D___T_H_I_S___RRH6J_.txt - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
_R_E_A_D___T_H_I_S___RRH6J_.txt
CERBER RANSOMWARE
YOUR
Notepad++ Plugin Manager
The following plugin updates are available:
Plugin
Category
Installed Version
Available Version
Stability
Plugin Manager
Others
1.3.5
1.4.5
Good
Update Selected
Ignore Selected Updates
Cancel
http://p27dokhpz2n7nvgr.onion/56BE-BE2A-3B89-0446-990F
Note! This page is available via "Tor Browser" only.
Normal tex length : 1360 lines : 49
Ln : 1 Col : 1 Sel : 0 | 0
Dos\Windows
UTF-8
INS
6:47 AM

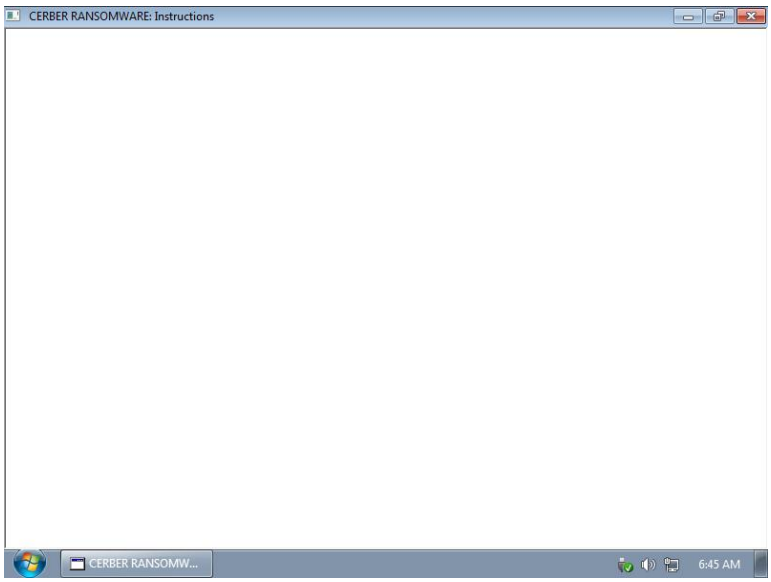

C:\Users\user\Desktop_R_E_A_D___T_H_I_S___RRH6J_.txt - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
_R_E_A_D___T_H_I_S___RRH6J_.txt
CERBER RANSOMWARE
Notepad++ Plugin Manager
The following plugin updates are available:
Plugin
Category
Installed Version
Available Version
Stability
Plugin Manager
Others
1.3.5
1.4.5
Good
Update Selected
Ignore Selected Updates
Cancel
http://p27dokhpz2n7nvgr.onion/56BE-BE2A-3B89-0446-990F
Note! This page is available via "Tor Browser" only.
Normal tex length : 1360 lines : 49
Ln : 1 Col : 1 Sel : 0 | 0
Dos\Windows
UTF-8
INS
6:46 AM

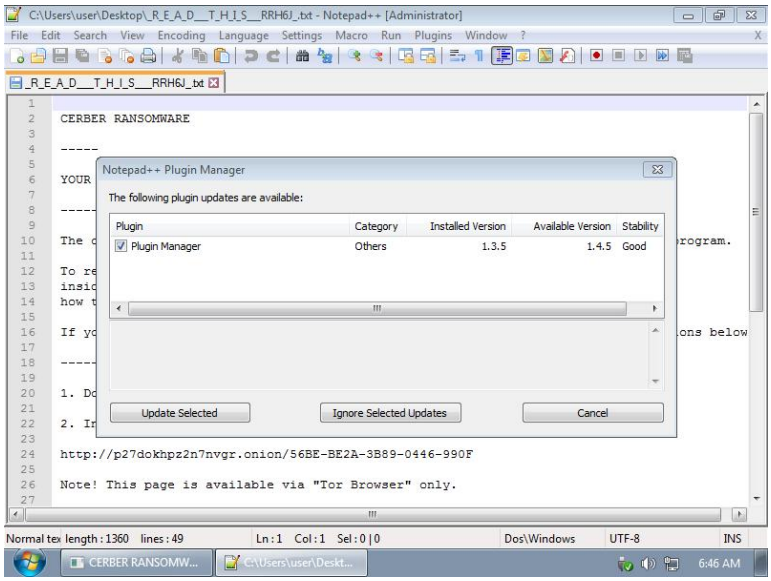

C:\Users\user\Desktop_R_E_A_D___T_H_I_S___RRH6J_.txt - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
_R_E_A_D___T_H_I_S___RRH6J_.txt
CERBER RANSOMWARE
Notepad++ Plugin Manager
The following plugin updates are available:
Plugin
Category
Installed Version
Available Version
Stability
Plugin Manager
Others
1.3.5
1.4.5
Good
Update Selected
Ignore Selected Updates
Cancel
http://p27dokhpz2n7nvgr.onion/56BE-BE2A-3B89-0446-990F
Note! This page is available via "Tor Browser" only.
Normal tex length : 1360 lines : 49
Ln : 1 Col : 1 Sel : 0 | 0
Dos\Windows
UTF-8
INS
6:48 AM

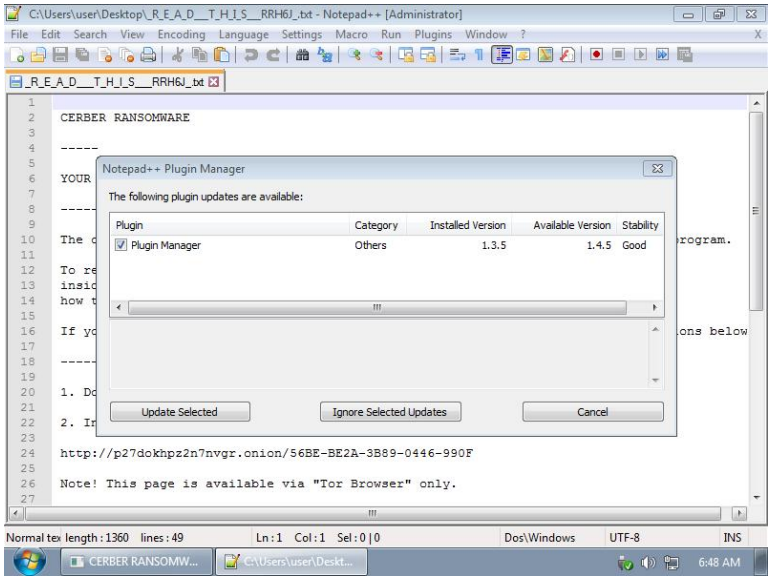

C:\Users\user\Desktop_R_E_A_D___T_H_I_S___RRH6J_.txt - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
_R_E_A_D___T_H_I_S___RRH6J_.txt
CERBER RANSOMWARE
Notepad++ Plugin Manager
The following plugin updates are available:
Plugin
Category
Installed Version
Available Version
Stability
Plugin Manager
Others
1.3.5
1.4.5
Good
Update Selected
Ignore Selected Updates
Cancel
http://p27dokhpz2n7nvgr.onion/56BE-BE2A-3B89-0446-990F
Note! This page is available via "Tor Browser" only.
Normal tex length : 1360 lines : 49
Ln : 1 Col : 1 Sel : 0 | 0
Dos\Windows
UTF-8
INS
6:47 AM

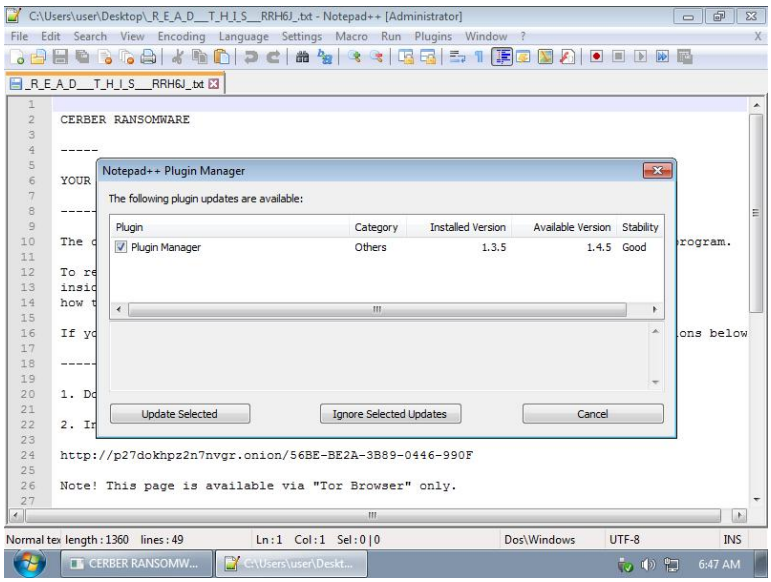

C:\Users\user\Desktop_R_E_A_D___T_H_I_S___RRH6J_.txt - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
_R_E_A_D___T_H_I_S___RRH6J_.txt
CERBER RANSOMWARE
Notepad++ Plugin Manager
The following plugin updates are available:
Plugin
Category
Installed Version
Available Version
Stability
Plugin Manager
Others
1.3.5
1.4.5
Good
Update Selected
Ignore Selected Updates
Cancel
http://p27dokhpz2n7nvgr.onion/56BE-BE2A-3B89-0446-990F
Note! This page is available via "Tor Browser" only.
Normal tex length : 1360 lines : 49
Ln : 1 Col : 1 Sel : 0 | 0
Dos\Windows
UTF-8
INS
6:47 AM

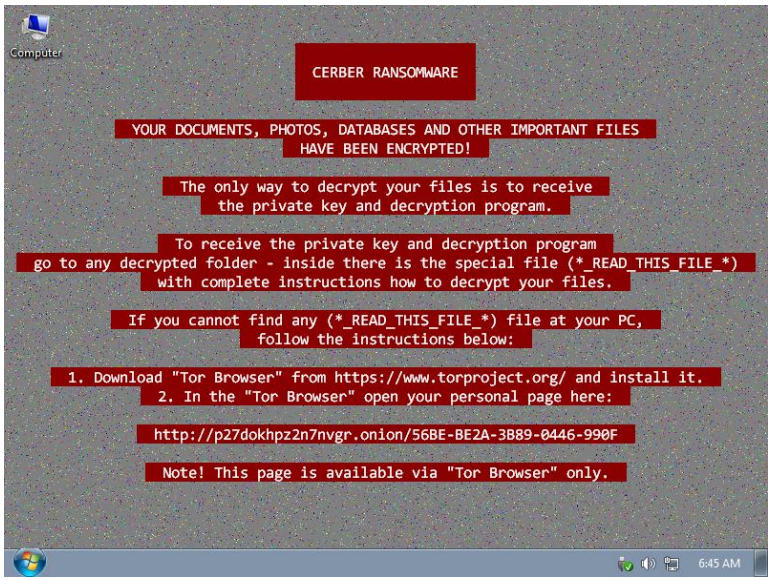

C:\Users\user\Desktop_R_E_A_D___T_H_I_S___RRH6J_.txt - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
_R_E_A_D___T_H_I_S___RRH6J_.txt
CERBER RANSOMWARE
YOUR DOCUMENTS, PHOTOS, DATABASES AND OTHER IMPORTANT FILES HAVE BEEN ENCRYPTED!
The only way to decrypt yOur files is to receive the private key and decryption program.
To receive the private key and decryption program go to any decrypted folder,
inside there is the special file (*_READ_THIS_FILE_*) with complete instructions
how to decrypt your files.
If you cannot find any (*_READ_THIS_FILE_*) file at your PC, follow the instructions below
1. Download "Tor Browser" from https://www.torproject.org/ and install it.
2. In the "Tor Browser" open your personal page here:
http://p27dokhpz2n7nvgr.onion/56BE-BE2A-3B89-0446-990F
Note! This page is available via "Tor Browser" only.
Normal tex length : 1360 lines : 49
Ln : 1 Col : 1 Sel : 0 | 0
Dos\Windows
UTF-8
INS
6:45 AM

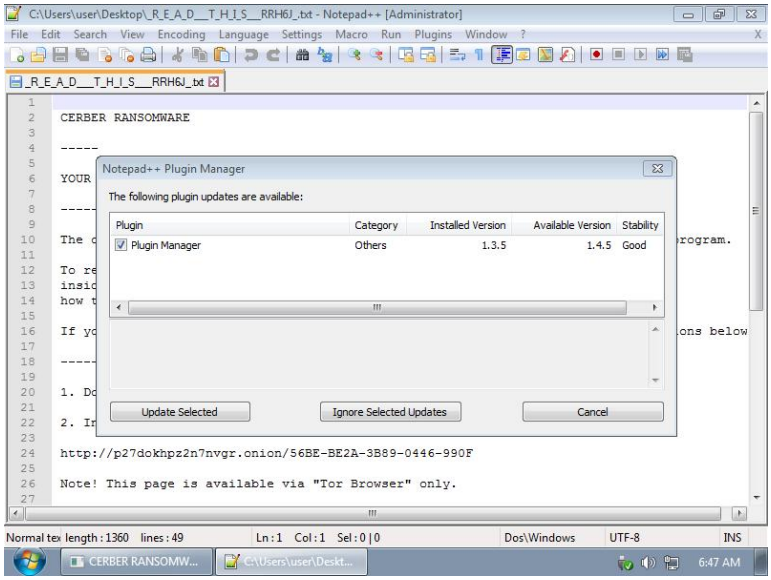

CERBER RANSOMWARE: Instructions
6:45 AM


C:\Users\user\Desktop_R_E_A_D___T_H_I_S___RRH6J_.txt - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
_R_E_A_D___T_H_I_S___RRH6J_.txt
CERBER RANSOMWARE
Notepad++ Plugin Manager
The following plugin updates are available:
Plugin
Category
Installed Version
Available Version
Stability
Plugin Manager
Others
1.3.5
1.4.5
Good
Update Selected
Ignore Selected Updates
Cancel
http://p27dokhpz2n7nvgr.onion/56BE-BE2A-3B89-0446-990F
Note! This page is available via "Tor Browser" only.
Normal tex length : 1360 lines : 49
Ln : 1 Col : 1 Sel : 0 | 0
Dos\Windows
UTF-8
INS
6:46 AM

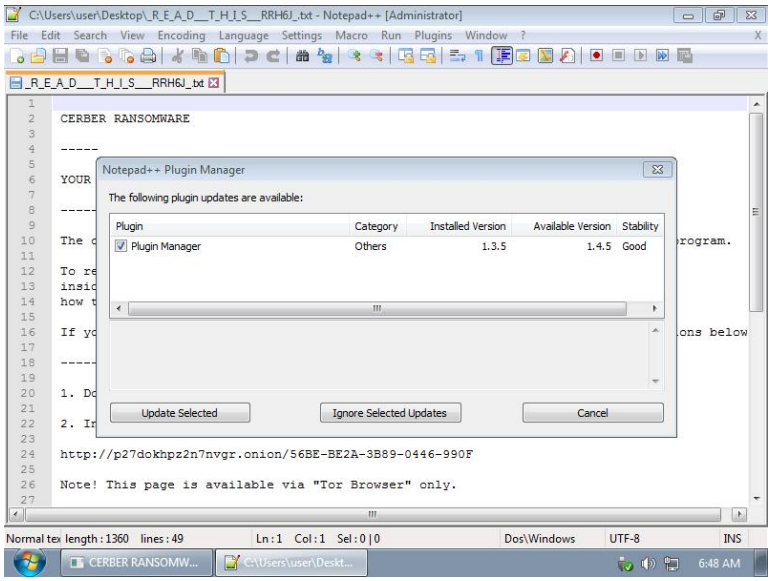

C:\Users\user\Desktop_R_E_A_D___T_H_I_S___RRH6J_.txt - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
_R_E_A_D___T_H_I_S___RRH6J_.txt
CERBER RANSOMWARE
Notepad++ Plugin Manager
The following plugin updates are available:
Plugin
Category
Installed Version
Available Version
Stability
Plugin Manager
Others
1.3.5
1.4.5
Good
Update Selected
Ignore Selected Updates
Cancel
http://p27dokhpz2n7nvgr.onion/56BE-BE2A-3B89-0446-990F
Note! This page is available via "Tor Browser" only.
Normal tex length : 1360 lines : 49
Ln : 1 Col : 1 Sel : 0 | 0
Dos\Windows
UTF-8
INS
6:48 AM

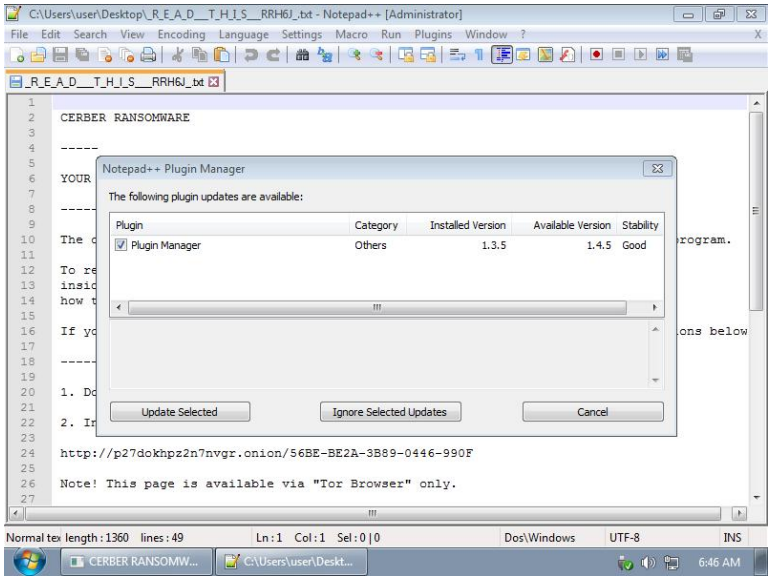

C:\Users\user\Desktop_R_E_A_D___T_H_I_S___RRH6J_.txt - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
_R_E_A_D___T_H_I_S___RRH6J_.txt
CERBER RANSOMWARE
Notepad++ Plugin Manager
The following plugin updates are available:
Plugin
Category
Installed Version
Available Version
Stability
Plugin Manager
Others
1.3.5
1.4.5
Good
Update Selected
Ignore Selected Updates
Cancel
http://p27dokhpz2n7nvgr.onion/56BE-BE2A-3B89-0446-990F
Note! This page is available via "Tor Browser" only.
Normal tex length : 1360 lines : 49
Ln : 1 Col : 1 Sel : 0 | 0
Dos\Windows
UTF-8
INS
6:47 AM

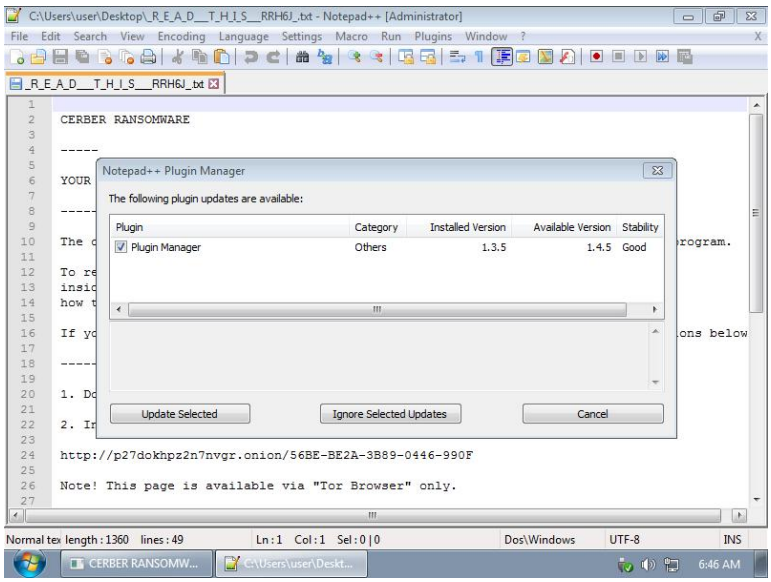

Computer
CERBER RANSOMWARE
YOUR DOCUMENTS, PHOTOS, DATABASES AND OTHER IMPORTANT FILES HAVE BEEN ENCRYPTED!
The only way to decrypt your files is to receive the private key and decryption program.
To receive the private key and decryption program go to any decrypted folder - inside there is the special file (*_READ_THIS_FILE_*) with complete instructions how to decrypt your files.
If you cannot find any (*_READ_THIS_FILE_*) file at your PC, follow the instructions below:
1. Download "Tor Browser" from https://www.torproject.org/ and install it.
2. In the "Tor Browser" open your personal page here:
http://p27dokhpz2n7nvgr.onion/56BE-BE2A-3B89-0446-990F
Note! This page is available via "Tor Browser" only.
6:45 AM

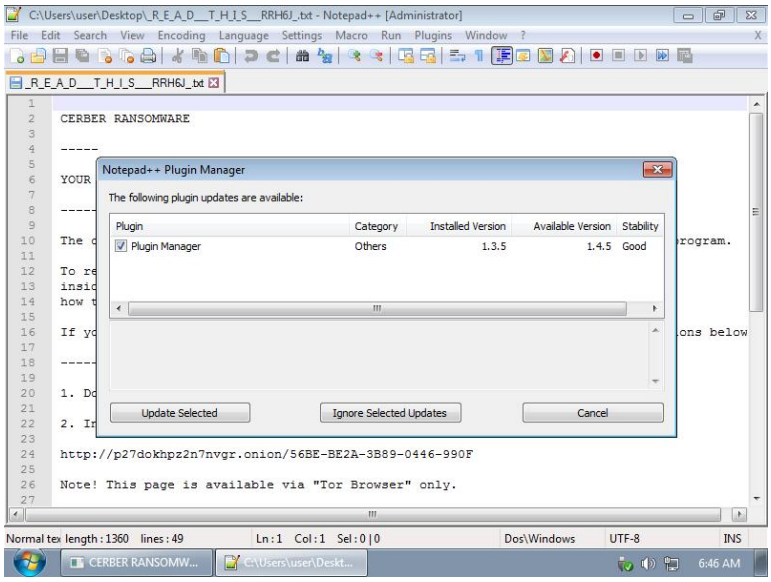

C:\Users\user\Desktop_R_E_A_D___T_H_I_S___RRH6J_.txt - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
_R_E_A_D___T_H_I_S___RRH6J_.txt
CERBER RANSOMWARE
Notepad++ Plugin Manager
The following plugin updates are available:
Plugin
Category
Installed Version
Available Version
Stability
Plugin Manager
Others
1.3.5
1.4.5
Good
Update Selected
Ignore Selected Updates
Cancel
http://p27dokhpz2n7nvgr.onion/56BE-BE2A-3B89-0446-990F
Note! This page is available via "Tor Browser" only.
Normal tex length : 1360 lines : 49
Ln : 1 Col : 1 Sel : 0 | 0
Dos\Windows
UTF-8
INS
CERBER RANSOMW...
6:47 AM

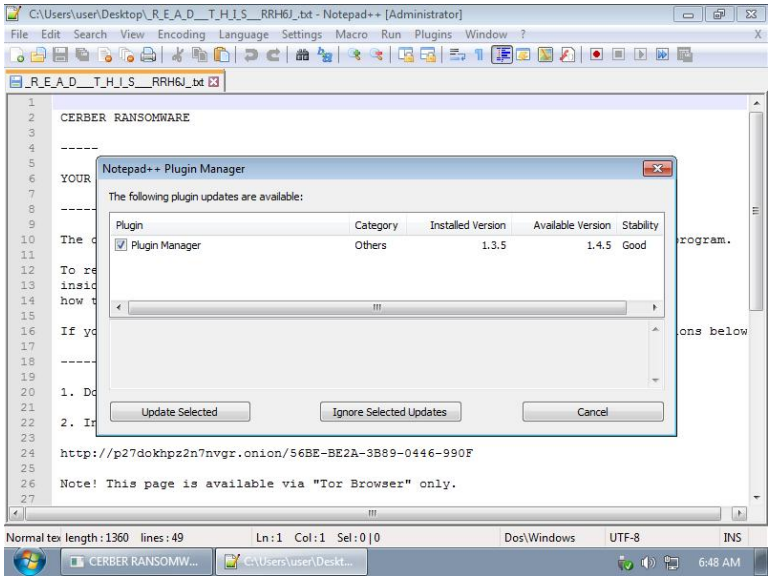

Computer
6:44 AM

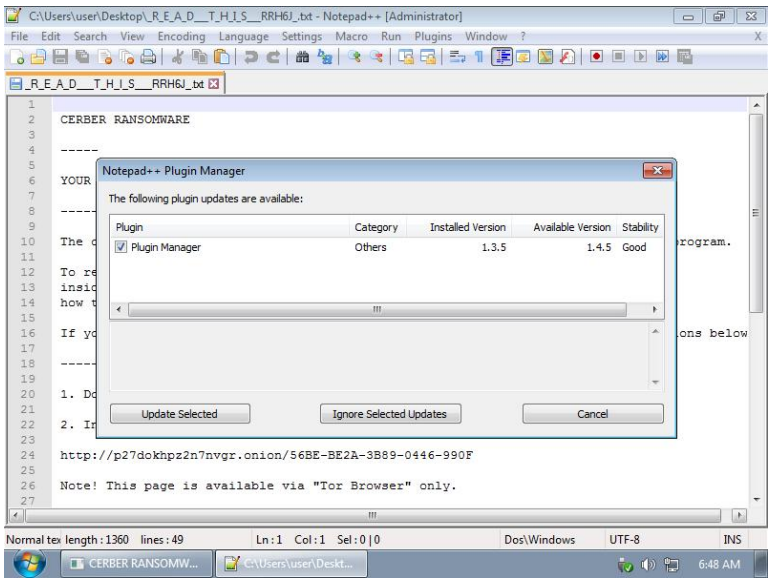

C:\Users\user\Desktop_R_E_A_D___T_H_I_S___RRH6J_.txt - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
_R_E_A_D___T_H_I_S___RRH6J_.txt
CERBER RANSOMWARE
Notepad++ Plugin Manager
The following plugin updates are available:
Plugin
Category
Installed Version
Available Version
Stability
Plugin Manager
Others
1.3.5
1.4.5
Good
Update Selected
Ignore Selected Updates
Cancel
http://p27dokhpz2n7nvgr.onion/56BE-BE2A-3B89-0446-990F
Note! This page is available via "Tor Browser" only.
Normal tex length : 1360 lines : 49
Ln : 1 Col : 1 Sel : 0 | 0
Dos\Windows
UTF-8
INS
CERBER RANSOMW...
C:\Users\user\Deskt...
6:48 AM

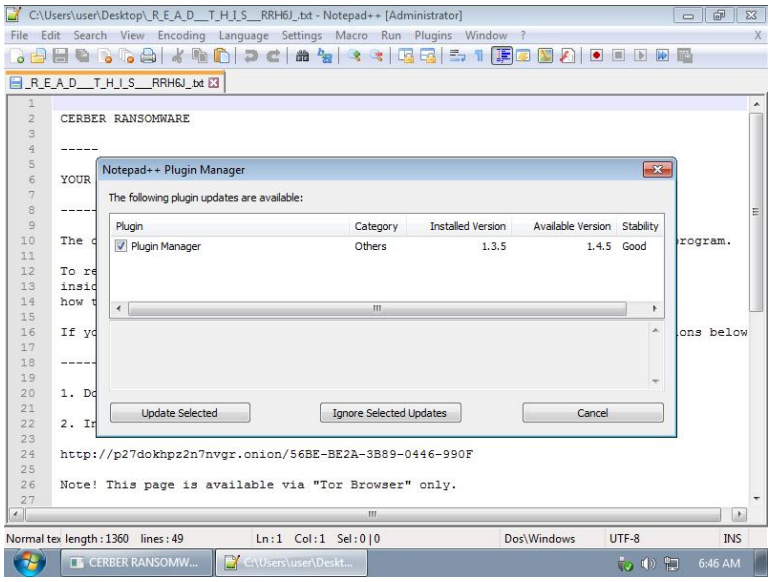

C:\Users\user\Desktop_R_E_A_D___T_H_I_S___RRH6J_.txt - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
_R_E_A_D___T_H_I_S___RRH6J_.txt
CERBER RANSOMWARE
Notepad++ Plugin Manager
The following plugin updates are available:
Plugin
Category
Installed Version
Available Version
Stability
Plugin Manager
Others
1.3.5
1.4.5
Good
Update Selected
Ignore Selected Updates
Cancel
http://p27dokhpz2n7nvgr.onion/56BE-BE2A-3B89-0446-990F
Note! This page is available via "Tor Browser" only.
Normal tex length : 1360 lines : 49
Ln : 1 Col : 1 Sel : 0 | 0
Dos\Windows
UTF-8
INS
CERBER RANSOMW...
C:\Users\user\Deskt...
6:46 AM

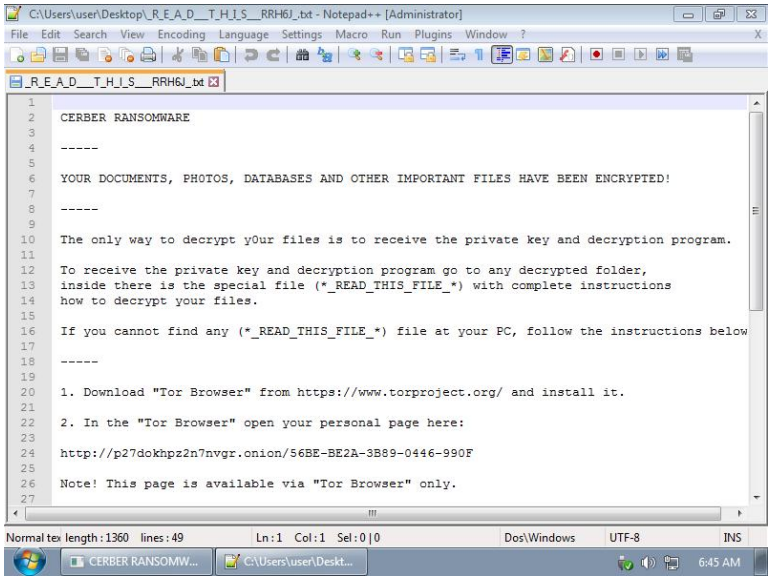

C:\Users\user\Desktop_R_E_A_D___T_H_I_S___RRH6J_.txt - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
_R_E_A_D___T_H_I_S___RRH6J_.txt
CERBER RANSOMWARE
Notepad++ Plugin Manager
The following plugin updates are available:
Plugin
Category
Installed Version
Available Version
Stability
Plugin Manager
Others
1.3.5
1.4.5
Good
Update Selected
Ignore Selected Updates
Cancel
http://p27dokhpz2n7nvgr.onion/56BE-BE2A-3B89-0446-990F
Note! This page is available via "Tor Browser" only.
Normal tex length : 1360 lines : 49
Ln : 1 Col : 1 Sel : 0 | 0
Dos\Windows
UTF-8
INS
CERBER RANSOMW...
C:\Users\user\Deskt...
6:46 AM

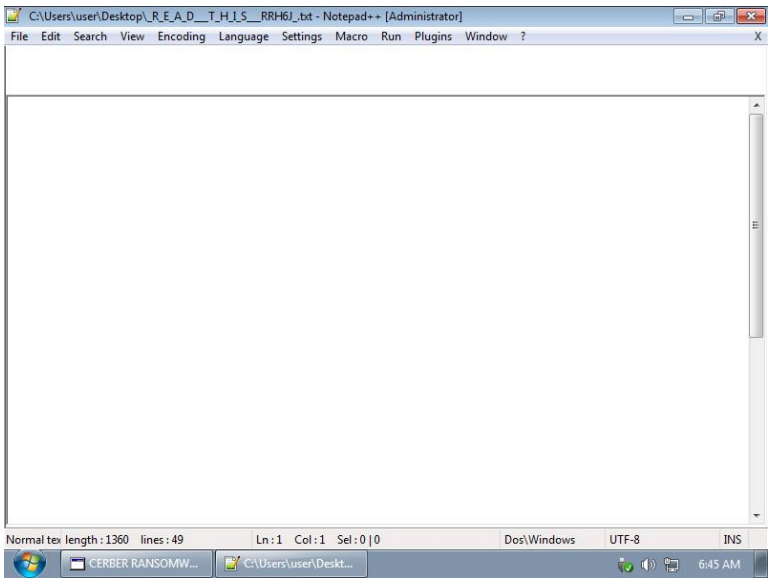

C:\Users\user\Desktop_R_E_A_D___T_H_I_S___RRH6J_.txt - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
_R_E_A_D___T_H_I_S___RRH6J_.txt
CERBER RANSOMWARE
Notepad++ Plugin Manager
The following plugin updates are available:
Plugin
Category
Installed Version
Available Version
Stability
Plugin Manager
Others
1.3.5
1.4.5
Good
Update Selected
Ignore Selected Updates
Cancel
http://p27dokhpz2n7nvgr.onion/56BE-BE2A-3B89-0446-990F
Note! This page is available via "Tor Browser" only.
Normal tex length : 1360 lines : 49
Ln : 1 Col : 1 Sel : 0 | 0
Dos\Windows
UTF-8
INS
6:46 AM

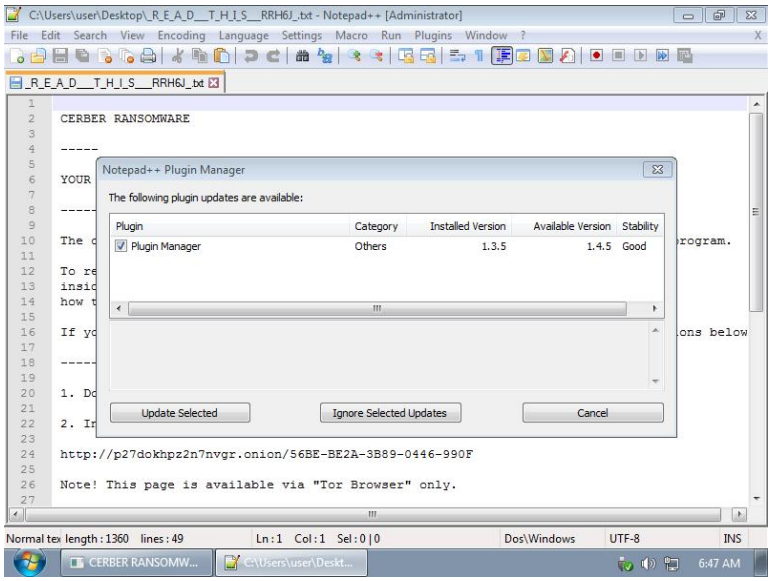

C:\Users\user\Desktop_R_E_A_D___T_H_I_S___RRH6J_.txt - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
_R_E_A_D___T_H_I_S___RRH6J_.txt
CERBER RANSOMWARE
Notepad++ Plugin Manager
The following plugin updates are available:
Plugin
Category
Installed Version
Available Version
Stability
Plugin Manager
Others
1.3.5
1.4.5
Good
Update Selected
Ignore Selected Updates
Cancel
http://p27dokhpz2n7nvgr.onion/56BE-BE2A-3B89-0446-990F
Note! This page is available via "Tor Browser" only.
Normal tex length : 1360 lines : 49
Ln : 1 Col : 1 Sel : 0 | 0
Dos\Windows
UTF-8
INS
6:48 AM


C:\Users\user\Desktop_R_E_A_D___T_H_I_S___RRH6J_.txt - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
_R_E_A_D___T_H_I_S___RRH6J_.txt
CERBER RANSOMWARE
Notepad++ Plugin Manager
The following plugin updates are available:
Plugin
Category
Installed Version
Available Version
Stability
Plugin Manager
Others
1.3.5
1.4.5
Good
Update Selected
Ignore Selected Updates
Cancel
http://p27dokhpz2n7nvgr.onion/56BE-BE2A-3B89-0446-990F
Note! This page is available via "Tor Browser" only.
Normal tex length : 1360 lines : 49
Ln : 1 Col : 1 Sel : 0 | 0
Dos\Windows
UTF-8
INS
6:48 AM


C:\Users\user\Desktop_R_E_A_D___T_H_I_S___RRH6J_.txt - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
_R_E_A_D___T_H_I_S___RRH6J_.txt
CERBER RANSOMWARE
Notepad++ Plugin Manager
The following plugin updates are available:
Plugin
Category
Installed Version
Available Version
Stability
Plugin Manager
Others
1.3.5
1.4.5
Good
Update Selected
Ignore Selected Updates
Cancel
http://p27dokhpz2n7nvgr.onion/56BE-BE2A-3B89-0446-990F
Note! This page is available via "Tor Browser" only.
Normal tex length : 1360 lines : 49
Ln : 1 Col : 1 Sel : 0 | 0
Dos\Windows
UTF-8
INS
6:46 AM

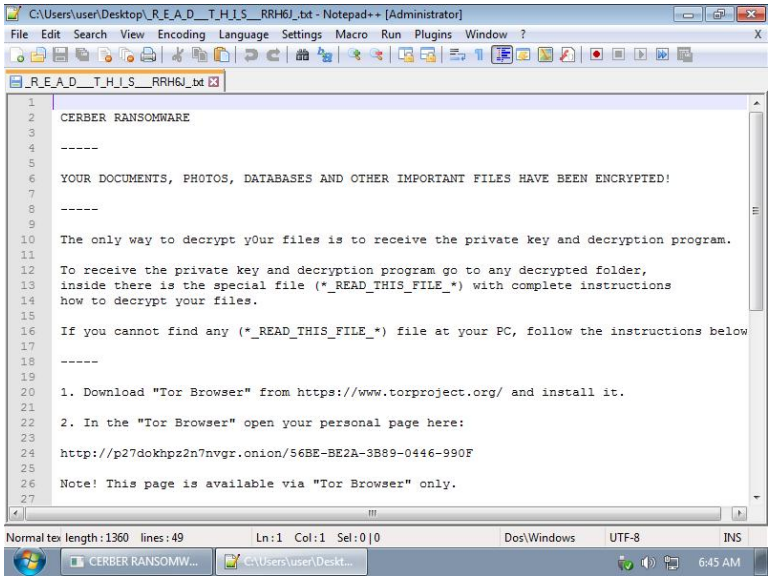

C:\Users\user\Desktop_R_E_A_D___T_H_I_S___RRH6J_.txt - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
_R_E_A_D___T_H_I_S___RRH6J_.txt
CERBER RANSOMWARE
YOUR DOCUMENTS, PHOTOS, DATABASES AND OTHER IMPORTANT FILES HAVE BEEN ENCRYPTED!
The only way to decrypt yOur files is to receive the private key and decryption program.
To receive the private key and decryption program go to any decrypted folder,
inside there is the special file (*_READ_THIS_FILE_*) with complete instructions
how to decrypt your files.
If you cannot find any (*_READ_THIS_FILE_*) file at your PC, follow the instructions below
1. Download "Tor Browser" from https://www.torproject.org/ and install it.
2. In the "Tor Browser" open your personal page here:
http://p27dokhpz2n7nvgr.onion/56BE-BE2A-3B89-0446-990F
Note! This page is available via "Tor Browser" only.
Normal tex length : 1360 lines : 49
Ln : 1 Col : 1 Sel : 0 | 0
Dos\Windows
UTF-8
INS
6:45 AM


C:\Users\user\Desktop_R_E_A_D___T_H_I_S___RRH6J_.txt - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
Normal tex length : 1360 lines : 49
Ln : 1 Col : 1 Sel : 0 | 0
Dos\Windows
UTF-8
INS
6:45 AM


C:\Users\user\Desktop_R_E_A_D___T_H_I_S___RRH6J_.txt - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
_R_E_A_D___T_H_I_S___RRH6J_.txt
CERBER RANSOMWARE

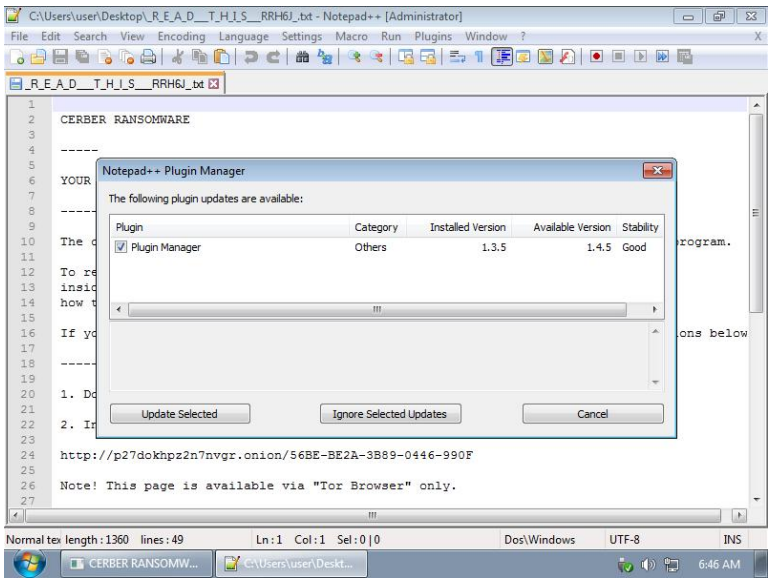
YOUR

The
To re
insid
how t
If yo
-----
1. Do
2. In
http://p27dokhpz2n7nvgr.onion/56BE-BE2A-3B89-0446-990F
Note! This page is available via "Tor Browser" only.
Notepad++ Plugin Manager
The following plugin updates are available:
Plugin
Category
Installed Version
Available Version
Stability
Plugin Manager
Others
1.3.5
1.4.5
Good
Update Selected
Ignore Selected Updates
Cancel
Normal tex length : 1360 lines : 49
Ln : 1 Col : 1 Sel : 0 | 0
Dos\Windows
UTF-8
INS
6:47 AM


C:\Users\user\Desktop_R_E_A_D___T_H_I_S___RRH6J_.txt - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
_R_E_A_D___T_H_I_S___RRH6J_.txt
CERBER RANSOMWARE

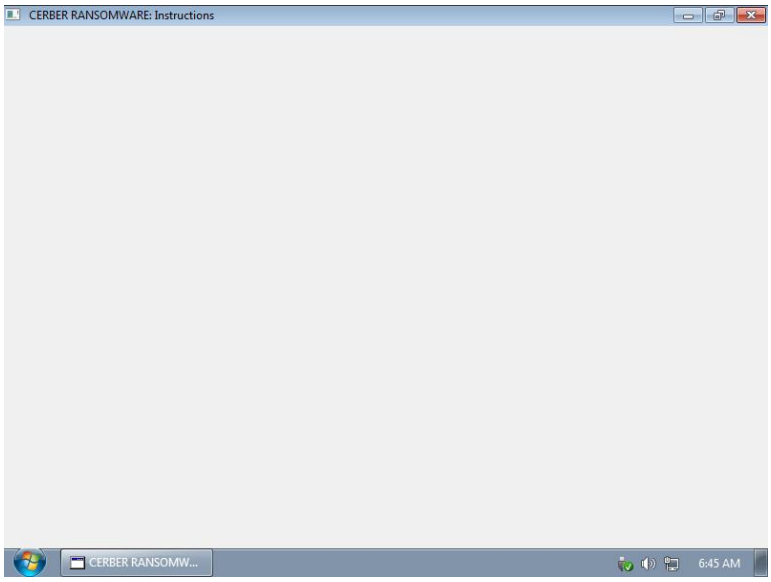
YOUR DOCUMENTS, PHOTOS, DATABASES AND OTHER IMPORTANT FILES HAVE BEEN ENCRYPTED!

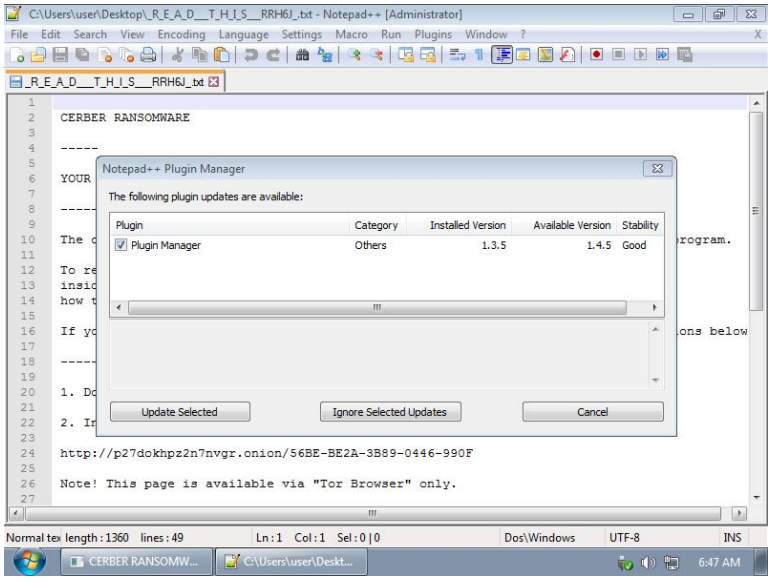
The only way to decrypt yOur files is to receive the private key and decryption program.
To receive the private key and decryption program go to any decrypted folder,
inside there is the special file (*_READ_THIS_FILE_*) with complete instructions
how to decrypt your files.
If you cannot find any (*_READ_THIS_FILE_*) file at your PC, follow the instructions below
-----
1. Download "Tor Browser" from https://www.torproject.org/ and install it.
2. In the "Tor Browser" open your personal page here:
http://p27dokhpz2n7nvgr.onion/56BE-BE2A-3B89-0446-990F
Note! This page is available via "Tor Browser" only.
Normal tex length : 1360 lines : 49
Ln : 1 Col : 1 Sel : 0 | 0
Dos\Windows
UTF-8
INS
6:45 AM

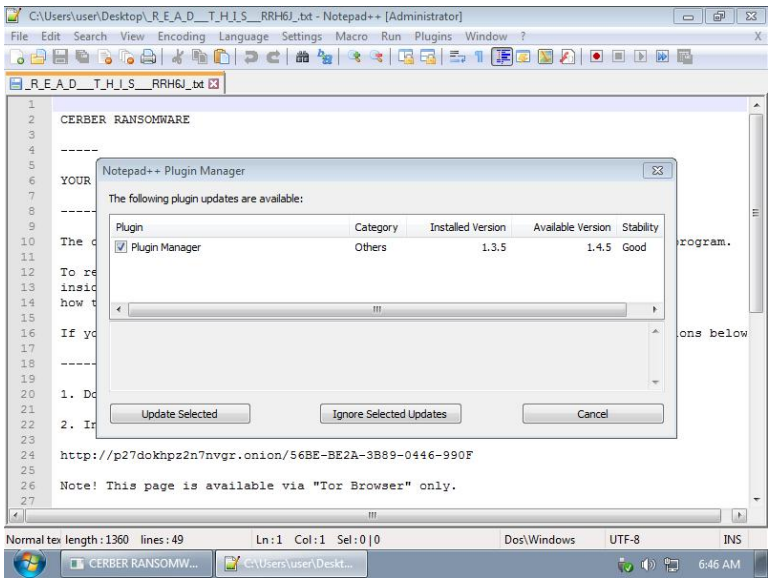

C:\Users\user\Desktop_R_E_A_D___T_H_I_S___RRH6J_.txt - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
_R_E_A_D___T_H_I_S___RRH6J_.txt
CERBER RANSOMWARE

YOUR

The
To re
insid
how t
If yo
-----
1. Do
2. In
http://p27dokhpz2n7nvgr.onion/56BE-BE2A-3B89-0446-990F
Note! This page is available via "Tor Browser" only.
Notepad++ Plugin Manager
The following plugin updates are available:
Plugin
Category
Installed Version
Available Version
Stability
Plugin Manager
Others
1.3.5
1.4.5
Good
Update Selected
Ignore Selected Updates
Cancel
Normal tex length : 1360 lines : 49
Ln : 1 Col : 1 Sel : 0 | 0
Dos\Windows
UTF-8
INS
6:46 AM


CERBER RANSOMWARE: Instructions
CERBER RANSOMW...
6:45 AM


C:\Users\user\Desktop_R_E_A_D___T_H_I_S___RRH6J_.txt - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
_R_E_A_D___T_H_I_S___RRH6J_.txt
CERBER RANSOMWARE
Notepad++ Plugin Manager
The following plugin updates are available:
Plugin
Category
Installed Version
Available Version
Stability
Plugin Manager
Others
1.3.5
1.4.5
Good
Update Selected
Ignore Selected Updates
Cancel
http://p27dokhpz2n7nvgr.onion/56BE-BE2A-3B89-0446-990F
Note! This page is available via "Tor Browser" only.
Normal tex length : 1360 lines : 49
Ln : 1 Col : 1 Sel : 0 | 0
Dos\Windows
UTF-8
INS
CERBER RANSOMW...
C:\Users\user\Deskt...
6:47 AM


C:\Users\user\Desktop_R_E_A_D___T_H_I_S___RRH6J_.txt - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
_R_E_A_D___T_H_I_S___RRH6J_.txt
CERBER RANSOMWARE
Notepad++ Plugin Manager
The following plugin updates are available:
Plugin
Category
Installed Version
Available Version
Stability
Plugin Manager
Others
1.3.5
1.4.5
Good
Update Selected
Ignore Selected Updates
Cancel
http://p27dokhpz2n7nvgr.onion/56BE-BE2A-3B89-0446-990F
Note! This page is available via "Tor Browser" only.
Normal tex length : 1360 lines : 49
Ln : 1 Col : 1 Sel : 0 | 0
Dos\Windows
UTF-8
INS
CERBER RANSOMW...
C:\Users\user\Deskt...
6:46 AM