malwr

Flattr this!

Tags: None

Analysis

CATEGORY	STARTED	COMPLETED	DURATION
FILE	2015-11-12 08:03:52	2015-11-12 08:06:10	138 seconds

- **Error:** Analysis failed: 'ascii' codec can't encode characters in position 108-110: ordinal not in range(128)

File Details

FILE NAME	cb4f444c624a0ad569b63c1422d1c682
FILE SIZE	68064 bytes
FILE TYPE	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-
MD5	cb4f444c624a0ad569b63c1422d1c682
SHA1	89b28711270a891b0a04483ca8e2bb967def35bb
SHA256	df4e5f39bc5c819a0fbbd2d194a95ec239620b0e63c71752dfac00727d1
SHA512	b9c5dea334b8436e8062f722d80bf2c809a22cfc13df78ebecd710f7a1b8
CRC32	C2C3A782
SSDEEP	1536:w4lVqauhF/NXcLUv8OFal8JBXJeUCWRQL+TEfXZbg/FbfTI6tzrid:w4lV
YARA	None matched
	Download You need to login

Signatures

File has been identified by at least one AntiVirus on VirusTotal as malicious

Screenshots

Hosts

No hosts contacted.

Domains

No domains contacted.

Summary

- Files
- Registry Keys

- Mutexes

```
IDE#CdRomVBOX_CD-
ROM_____________________________1.0_____#42562d3231303037333036372020202020202(
{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
MountPointManager
STORAGE#Volume#1&30a96598&0&Signature32B832B7Offset7E00Length27F4DB200#
{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
C:\DOCUME~1
C:\Documents and Settings\User
C:\Documents and Settings\User\LOCALS~1
C:\Documents and Settings\User\Local Settings\Temp
C:\DOCUME~1\User\LOCALS~1\Temp\nsn1.tmp
C:\DOCUME~1\User\LOCALS~1\Temp\cb4f444c624a0ad569b63c1422d1c682.exe
C:\DOCUME~1\User\LOCALS~1\Temp\\xc3\x84\xc3\xab\xc3\xbf
\xc3\xae\xc3\xa7\xc3\xad\xc3\xa0\xc3\xaa\xc3\xae\xc3\xac\xc3\xab\xc3\xa5\xc3\
C:\DOCUME~1\User\LOCALS~1\Temp\nsh2.tmp
C:\DOCUME~1\User\LOCALS~1\Temp\nsh2.tmp\System.dll
C:\DOCUME~1\User\LOCALS~1\Temp
C:\DOCUME~1\User\LOCALS~1
C:\DOCUME~1\User
C:\DOCUME~1\User\LOCALS~1\Temp\nsh2.tmp\*.*
C:\DOCUME~1\User\LOCALS~1\Temp\nsh2.tmp\
C:\Program Files\Common Files\Microsoft Shared\office12\Cultures\office.odf
C:\WINDOWS\system32\msctfime.ime
C:\Program Files\Microsoft Office\Office12\WINWORD.EXE.config
C:\WINDOWS\Microsoft.NET\Framework\v2.0.0\mscorwks.dll
C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll
C:\Program Files\Common Files\Microsoft Shared\OFFICE11\msxml5.dll
C:\Documents and Settings\User\Application Data\Microsoft\Office\Word12.pip
C:\Program Files\Microsoft Office\Office12\ID_00030.DPC
C:\Program Files
C:\Program Files\Microsoft Office
C:\Program Files\Microsoft Office\Office12\Normal.dotm
C:\Documents and Settings\User\Application
Data\Microsoft\Templates\Normal.dotm
C:\Documents and Settings\User\Application
Data\Microsoft\Templates\~$Normal.dotm
C:\Documents and Settings
C:\Documents and Settings\User\Desktop
C:\Documents and Settings\User\Application Data
C:\Documents and Settings\User\Application Data\desktop.ini
C:\Documents and Settings\User\Application Data\Microsoft
C:\Documents and Settings\User\Application Data\Microsoft\Templates
C:\Documents and Settings\User\My Documents
C:\Documents and Settings\User\My Documents\desktop.ini
C:\Documents and Settings\All Users
C:\Documents and Settings\All Users\Documents
C:\Documents and Settings\All Users\Documents\desktop.ini
C:\Documents and Settings\All Users\Desktop
C:\WINDOWS\Registration\R000000000007.clb
PIPE\lsarpc
C:\Documents and Settings\User\Local Settings\Temporary Internet
Files\Content.Word\~WRS{8430D9FE-52B5-42D6-B135-C919A6B4A558}.tmp
C:\Documents and Settings\User\Local Settings\Application
Data\Microsoft\Office\Word.qat
C:\Documents and Settings\User\Local Settings\Application
Data\Microsoft\Schemas\MS Word_restart.xml
C:\Documents and Settings\User\Application Data\Microsoft\Word\STARTUP\*.*
C:\Program Files\Microsoft Office\Office12\STARTUP\*.*
C:\Program Files\Microsoft Office\Office12\id_00030.dpc
C:\Documents and Settings\User\Local Settings\Temp\\xc3\x84\xc3\xab\xc3\xbf
\xc3\xae\xc3\xa7\xc3\xad\xc3\xa0\xc3\xaa\xc3\xae\xc3\xac\xc3\xab\xc3\xa5\xc3\
C:\DOCUME~1\User\LOCALS~1\Temp\~DF7557.tmp
C:\DOCUME~1\User\LOCALS~1\Temp\~$\xc3\xbf
```

```
\xc3\xae\xc3\xa7\xc3\xad\xc3\xa0\xc3\xaa\xc3\xae\xc3\xac\xc3\xab\xc3\xa5\xc3\
C:\Documents and Settings\User\Local Settings\Temporary Internet
Files\Content.Word\~WRS{FA0F6E52-6AB4-4D7F-8A10-69C17CA4235C}.tmp
C:\Documents and Settings\User\Application Data\Microsoft\Office\review.rcd
C:\Documents and Settings\User\Application Data\Microsoft\Office\adhoc.rcd
C:\Documents and Settings\User\Local Settings
C:\Program Files\Microsoft Office\Office12\mssp3??.dll
C:\Documents and Settings\User\Application Data\Microsoft\Proof\mssp3??.dll
C:\Program Files\Common Files\Microsoft Shared\mssp3??.dll
C:\Program Files\Microsoft Office\Office12\mssp??32.dll
C:\Documents and Settings\User\Application Data\Microsoft\Proof\mssp??32.dll
C:\Program Files\Common Files\Microsoft Shared\mssp??32.dll
C:\Program Files\Microsoft Office\Office12\msp??32.dll
C:\Program Files\Microsoft Office\Office12\msgr2??.dll
C:\Documents and Settings\User\Application Data\Microsoft\Proof\msgr2??.dll
C:\Program Files\Common Files\Microsoft Shared\msgr2??.dll
C:\Program Files\Microsoft Office\Office12\msgr??32.dll
C:\Documents and Settings\User\Application Data\Microsoft\Proof\msgr??32.dll
C:\Program Files\Common Files\Microsoft Shared\msgr??32.dll
C:\Program Files\Microsoft Office\Office12\gram??32.dll
C:\Documents and Settings\User\Application Data\Microsoft\Proof\gram??32.dll
C:\Program Files\Common Files\Microsoft Shared\gram??32.dll
C:\Program Files\Microsoft Office\Office12\msth3??.dll
C:\Documents and Settings\User\Application Data\Microsoft\Proof\msth3??.dll
C:\Program Files\Common Files\Microsoft Shared\msth3??.dll
C:\Program Files\Microsoft Office\Office12\msth32.dll
C:\Documents and Settings\User\Application Data\Microsoft\Proof\msth32.dll
C:\Program Files\Common Files\Microsoft Shared\msth32.dll
C:\Program Files\Microsoft Office\Office12\msth??32.dll
C:\Documents and Settings\User\Application Data\Microsoft\Proof\msth??32.dll
C:\Program Files\Common Files\Microsoft Shared\msth??32.dll
C:\Program Files\Microsoft Office\Office12\msth232.dll
C:\Documents and Settings\User\Application Data\Microsoft\Proof\msth232.dll
C:\Program Files\Common Files\Microsoft Shared\msth232.dll
C:\Program Files\Microsoft Office\Office12\mshy3??.dll
C:\Documents and Settings\User\Application Data\Microsoft\Proof\mshy3??.dll
C:\Program Files\Common Files\Microsoft Shared\mshy3??.dll
C:\Program Files\Microsoft Office\Office12\hyph??32.dll
C:\Documents and Settings\User\Application Data\Microsoft\Proof\hyph??32.dll
C:\Program Files\Common Files\Microsoft Shared\hyph??32.dll
C:\Program Files\Microsoft Office\Office12\mshy32.dll
C:\Documents and Settings\User\Application Data\Microsoft\Proof\mshy32.dll
C:\Program Files\Common Files\Microsoft Shared\mshy32.dll
C:\Program Files\Microsoft Office\Office12\hyph32.dll
C:\Documents and Settings\User\Application Data\Microsoft\Proof\hyph32.dll
C:\Program Files\Common Files\Microsoft Shared\hyph32.dll
C:\Program Files\Microsoft Office\Office12\hhc32.dll
C:\Documents and Settings\User\Application Data\Microsoft\Proof\hhc32.dll
C:\Program Files\Common Files\Microsoft Shared\hhc32.dll
C:\Program Files\Microsoft Office\Office12\msdcsc32.dll
C:\Documents and Settings\User\Application Data\Microsoft\Proof\msdcsc32.dll
C:\Program Files\Common Files\Microsoft Shared\msdcsc32.dll
C:\Documents and Settings\User\Application Data\Microsoft\UProof\CUSTOM.DIC
C:\Program Files\Microsoft Office\Office12\msgr2RU.dll
C:\Documents and Settings\User\Application Data\Microsoft\Proof\msgr2RU.dll
C:\Program Files\Common Files\Microsoft Shared\msgr2RU.dll
C:\Program Files\Microsoft Office\Office12\msgrRU32.dll
C:\Documents and Settings\User\Application Data\Microsoft\Proof\msgrRU32.dll
C:\Program Files\Common Files\Microsoft Shared\msgrRU32.dll
C:\Program Files\Microsoft Office\Office12\gramRU32.dll
C:\Documents and Settings\User\Application Data\Microsoft\Proof\gramRU32.dll
C:\Program Files\Common Files\Microsoft Shared\gramRU32.dll
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explore
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibili
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibili
{20D04FE0-3AEA-1069-A2D8-08002B30309D}
HKEY_CLASSES_ROOT\CLSID\{20D04FE0-3AEA-1069-A2D8-
08002B30309D}\InProcServer32
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoi
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoi
{475c7950-e3d2-11e0-8d7a-806d6172696f}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoi
{475c7952-e3d2-11e0-8d7a-806d6172696f}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoi
{475c7952-e3d2-11e0-8d7a-806d6172696f}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoi
{475c7950-e3d2-11e0-8d7a-806d6172696f}\
HKEY_CLASSES_ROOT\Drive\shellex\FolderExtensions
HKEY_CLASSES_ROOT\Drive\shellex\FolderExtensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}
HKEY_CLASSES_ROOT\Directory
HKEY_CLASSES_ROOT\Directory\CurVer
HKEY_CLASSES_ROOT\Directory\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
HKEY_CLASSES_ROOT\Directory\\ShellEx\IconHandler
HKEY_CLASSES_ROOT\Directory\\Clsid
HKEY_CLASSES_ROOT\Folder
HKEY_CLASSES_ROOT\Folder\Clsid
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office Test\Special\Perf
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems
HKEY_CURRENT_USER\Software\Policies\Microsoft\Office
HKEY_CURRENT_USER\Software\Microsoft\Office\Common
HKEY_LOCAL_MACHINE\Software\Microsoft\SQMClient
HKEY_LOCAL_MACHINE\Software\Microsoft\Office\12.0\Common\ProductVersion
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Debug
HKEY_LOCAL_MACHINE\Software\Microsoft\Office\12.0\Common\LanguageResources
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\Ena
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale\Alternate
Sorts
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Language Groups
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\MUILanguages
HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Common\LanguageResc
HKEY_LOCAL_MACHINE\Software\Microsoft\Office\12.0\Common\LanguageResources\In
HKEY_CURRENT_USER\Software\Microsoft\Shared
HKEY_CURRENT_USER\Keyboard Layout\Substitutes
HKEY_LOCAL_MACHINE\Software\Microsoft\Office\BypassMigration
HKEY_LOCAL_MACHINE\Software\Microsoft\Office\OPWBypassMigration
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Migration\Office
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Migration\Word
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Office\12.0\User Settings\
HKEY_LOCAL_MACHINE\Software\Microsoft\Office\12.0\User Settings\
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\User Settings\
HKEY_LOCAL_MACHINE\Software\Microsoft\Office\12.0\User
Settings\\AccessDE_Core
HKEY_LOCAL_MACHINE\Software\Microsoft\Office\12.0\User Settings\\Access_Core
HKEY_LOCAL_MACHINE\Software\Microsoft\Office\12.0\User
Settings\\Ace_OdbcCurrentUser
HKEY_LOCAL_MACHINE\Software\Microsoft\Office\12.0\User Settings\\Excel_Core
HKEY_LOCAL_MACHINE\Software\Microsoft\Office\12.0\User Settings\\Excel_Intl
HKEY_LOCAL_MACHINE\Software\Microsoft\Office\12.0\User Settings\\Graph_Core
HKEY_LOCAL_MACHINE\Software\Microsoft\Office\12.0\User Settings\\Mso_Core
HKEY_LOCAL_MACHINE\Software\Microsoft\Office\12.0\User Settings\\Mso_CoreReg
```

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Office\12.0\User Settings\\Mso_Intl
HKEY_LOCAL_MACHINE\Software\Microsoft\Office\12.0\User Settings\\outexum
HKEY_LOCAL_MACHINE\Software\Microsoft\Office\12.0\User
Settings\\Outlook_AutoDiscover
HKEY_LOCAL_MACHINE\Software\Microsoft\Office\12.0\User
Settings\\Outlook_Core
HKEY_LOCAL_MACHINE\Software\Microsoft\Office\12.0\User
Settings\\Outlook_Intl
HKEY_LOCAL_MACHINE\Software\Microsoft\Office\12.0\User
Settings\\PowerPoint_Core
HKEY_LOCAL_MACHINE\Software\Microsoft\Office\12.0\User
Settings\\PowerPoint_Intl
HKEY_LOCAL_MACHINE\Software\Microsoft\Office\12.0\User
Settings\\Sps_OutlookAddin
HKEY_LOCAL_MACHINE\Software\Microsoft\Office\12.0\User Settings\\Word_Core
HKEY_LOCAL_MACHINE\Software\Microsoft\Office\12.0\User Settings\\Word_Intl
HKEY_LOCAL_MACHINE\Software\Microsoft\Office\12.0\User
Settings\\XDocs_XMLEditVerbHandler
HKEY_LOCAL_MACHINE\Software\Microsoft\Office\12.0\User Settings\\{90120000-
0030-0000-0000-0000000FF1CE}
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\User Settings\\Access_Core
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\User
Settings\\Ace_OdbcCurrentUser
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\User Settings\\Excel_Core
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\User Settings\\Excel_Intl
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\User Settings\\Graph_Core
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\User Settings\\Mso_Core
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\User Settings\\Mso_CoreReg
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\User Settings\\Mso_Intl
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\User Settings\\outexum
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\User
Settings\\Outlook_AutoDiscover
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\User Settings\\Outlook_Core
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\User Settings\\Outlook_Intl
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\User
Settings\\PowerPoint_Core
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\User
Settings\\PowerPoint_Intl
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\User
Settings\\Sps_OutlookAddin
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\User Settings\\Word_Core
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\User Settings\\Word_Intl
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\User
Settings\\XDocs_XMLEditVerbHandler
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\User
Settings\\AccessDE_Core
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Options\Debug
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Options
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-21-1547161642-507921405-839522115-
1004\Components\D94C8360B8BB1DC41B1950E1F8237563
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\D94C8360B8BB1DC41B1950E1F8237563
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Manage
1-5-21-1547161642-507921405-839522115-
1004\Installer\Products\00002109030000000000000000F01FEC
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-
1004\Software\Microsoft\Installer\Products\00002109030000000000000000F01FEC
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\0000210903000000000000
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Products\00002109030000000000000000F01FEC\InstallProperties
HKEY_LOCAL_MACHINE\Software\Microsoft\Office\12.0\Registration
HKEY_LOCAL_MACHINE\Software\Microsoft\Office\12.0\Registration\{90120000-
0030-0000-0000-0000000FF1CE}
```

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Manage
1-5-21-1547161642-507921405-839522115-
1004\Installer\Features\00002109030000000000000000F01FEC
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-
1004\Software\Microsoft\Installer\Features\00002109030000000000000000F01FEC
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Features\0000210903000000000000
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Products\00002109030000000000000000F01FEC\Features
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\A5824C2FB557A5D43881763B7A07D05E
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\AD4E638E8714C454FA1AD399C0E81909
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\CAB7071E27686994093945B9EE85F69D
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\FE334C41ADDE81149944C1D33967043A
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\C89954FBD4FB47C449CE85E9F7E918FB
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\379E92CC2CB71D119A12000A9CE1A22A
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\748B2526ADAB4D3429253E7976AF041A
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\5120EEDE039486F42830D8D2552797F6
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\CCABF232126726445BC57F4CDE05C5EB
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\47155108894E68A409FDC1FC6E8DA2CB
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\9B271454ED4348B47B365F93ADEAC015
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\9D6BD49C8A516ED41BB0C0D31B0F52BC
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\4006F64980E4BACB0EF18C3B9B1A1EE8
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\1FA18F7974E099CD0AF18C3B9B1A1EE8
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\1FA18F7974E099CD0CF18C3B9B1A1EE8
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\1FA18F7974E099CD0BF18C3B9B1A1EE8
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\4006F64980E4BACB0DF18C3B9B1A1EE8
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\DA42BC89BF25F5BD0AF18C3B9B1A1EE8
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\DA42BC89BF25F5BD0CF18C3B9B1A1EE8
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\DA42BC89BF25F5BD0BF18C3B9B1A1EE8
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\82DE7549CF3F8CCB0DF18C3B9B1A1EE8
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\2A31EAB9FA7E3C6D0AF18C3B9B1A1EE8
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\2A31EAB9FA7E3C6D0CF18C3B9B1A1EE8
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\2A31EAB9FA7E3C6D0BF18C3B9B1A1EE8
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\B92D5049E11C93DB0DF18C3B9B1A1EE8
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\6EC3DF47D8A2C9E00AF18C3B9B1A1EE8
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\6EC3DF47D8A2C9E00CF18C3B9B1A1EE8
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\6EC3DF47D8A2C9E00BF18C3B9B1A1EE8
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa

```
1-5-18\Components\77AE531D63D456630DF18C3B9B1A1EE8
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\D94C8360B8BB1DC41B1950E0F8237563
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\2562336682C91B850AF18C3B9B1A1EE8
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\2562336682C91B850CF18C3B9B1A1EE8
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\6F949E36CB3004C50AF18C3B9B1A1EE8
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\6F949E36CB3004C50CF18C3B9B1A1EE8
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\9D6C7B862FD11C450AF18C3B9B1A1EE8
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\9D6C7B862FD11C450CF18C3B9B1A1EE8
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\F3D0372D14C348850AF18C3B9B1A1EE8
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\F3D0372D14C348850CF18C3B9B1A1EE8
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\11B564CAA807C694ABE73044DC90516B
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\E3F997A2790938844ACDF81020B32415
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\9C1D6229422D71045BFB2F8BCE017AA4
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\6C9A6F846E2818A47A408CAF13381C71
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\C733A8B34D26AF4458B43E09EFC2C77F
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\2227A34C816D4F94EB598446F9BD8B17
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\7AA6F3DBF3CE139469FE63D56E7AF446
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\F7CD01816C53D32438CF043106011676
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Products\00002109030000000000000000F01FEC\Usage
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Manage
1-5-21-1547161642-507921405-839522115-
1004\Installer\Components\1F5C93A1704E3E445ADD70E3090042AE
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-
1004\Software\Microsoft\Installer\Components\1F5C93A1704E3E445ADD70E3090042AE
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Components\1F5C93A1704E3E445ADD
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\General
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User
Shell Folders
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell
Folders
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common
HKEY_LOCAL_MACHINE\Software\Microsoft\Office\12.0\Common\Security
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-1004
Control Panel\International
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\FixedFormat
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\MailSettings
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing Tools\Spelling
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Outlook\Options\Calendar
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing Tools\1.0\Office
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing
Tools\HangulHanjaConv
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Options\Vpref
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Options\Vprsu
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Options\Vpreffuz
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Options\Assist
```

```
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing Tools
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\IMM
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-
1004\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers
HKEY_CURRENT_USER\SOFTWARE\Microsoft\CTF
HKEY_LOCAL_MACHINE\Software\Microsoft\CTF\SystemShared
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\D94C8360B8BB2DC41B1950E0F8237563
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Security
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\GELPrefs
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Research\Translation
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework
HKEY_CURRENT_USER\Software\Microsoft\.NETFramework\Policy\Upgrades
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\Policy\Upgrades
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\TypeLib\{F5078F18-C551-11D3-89B9-
0000F81FE221}\5.0\0\win32
HKEY_CURRENT_USER\Software\Microsoft\Office\8.0\Outlook
HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\
HKEY_LOCAL_MACHINE\Software\Microsoft\Office\12.0\Common\General
HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Word\DisabledCmdBar
HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Word\DisabledCmdBar
HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Word\DisabledShortc
HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Word\DisabledShortc
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Toolbars
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Manage
1-5-21-1547161642-507921405-839522115-
1004\Installer\Components\621EAA421190F8740A91708B57BE9969
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-
1004\Software\Microsoft\Installer\Components\621EAA421190F8740A91708B57BE9969
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Components\621EAA421190F8740A91
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\72550EAA4F7970143BF094E2F6C9164E
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\9B905EB838DBFEE4991CF8E66F518BBF
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\D94C8360B8BB1DC41B1950E2F8237563
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\2FAFA61ADBF18444690EDB85CAA39EB7
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\337E30A68012B5341B7A8ADE48F4064A
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-
1004\Software\Microsoft\Windows NT\CurrentVersion\Windows
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\OneNote\MDI writer
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Devices
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Messaging Subsystem
HKEY_CLASSES_ROOT\CLSID\{00020907-0000-0000-C000-000000000046}\LocalServer32
HKEY_CLASSES_ROOT\CLSID\{00020906-0000-0000-C000-000000000046}\LocalServer32
HKEY_CLASSES_ROOT\CLSID\{F4754C9B-64F5-4B40-8AF4-679732AC0607}\LocalServer32
HKEY_CLASSES_ROOT\Word.Document\CurVer
HKEY_CLASSES_ROOT\Component Categories\{56FFCC30-D398-11D0-B2AE-
00A0C908FA49}
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\TrustCenter
HKEY_LOCAL_MACHINE\Software\Microsoft\CTF\TIP
HKEY_CURRENT_USER\Software\Microsoft\CTF
HKEY_CURRENT_USER\Software\Microsoft\CTF\TIP
HKEY_CURRENT_USER\Software\Microsoft\CTF\TIP\{70FAF614-E0B1-11D3-8F5C-
00C04F9CF4AC}\LanguageProfile
HKEY_LOCAL_MACHINE\Software\Microsoft\CTF\TIP\{70FAF614-E0B1-11D3-8F5C-
00C04F9CF4AC}\LanguageProfile
HKEY_CURRENT_USER\Software\Microsoft\CTF\TIP\{78CB5B0E-26ED-4FCC-854C-
77E8F3D1AA80}\LanguageProfile
HKEY_LOCAL_MACHINE\Software\Microsoft\CTF\TIP\{78CB5B0E-26ED-4FCC-854C-
77E8F3D1AA80}\LanguageProfile
HKEY_CURRENT_USER\Software\Microsoft\CTF\TIP\{C1EE01F2-B3B6-4A6A-9DDD-
E988C088EC82}\LanguageProfile
```

```
HKEY_LOCAL_MACHINE\Software\Microsoft\CTF\TIP\{C1EE01F2-B3B6-4A6A-9DDD-
E988C088EC82}\LanguageProfile
HKEY_CURRENT_USER\Software\Microsoft\CTF\TIP\{DCBD6FA8-032F-11D3-B5B1-
00C04FC324A1}\LanguageProfile
HKEY_CURRENT_USER\Software\Microsoft\CTF\TIP\{DCBD6FA8-032F-11D3-B5B1-
00C04FC324A1}\LanguageProfile\0x00000409
HKEY_CURRENT_USER\Software\Microsoft\CTF\TIP\{DCBD6FA8-032F-11D3-B5B1-
00C04FC324A1}\LanguageProfile\0x00000409\{09EA4E4B-46CE-4469-B450-
0DE76A435BBB}
HKEY_LOCAL_MACHINE\Software\Microsoft\CTF\TIP\{DCBD6FA8-032F-11D3-B5B1-
00C04FC324A1}\LanguageProfile
HKEY_LOCAL_MACHINE\Software\Microsoft\CTF\TIP\{DCBD6FA8-032F-11D3-B5B1-
00C04FC324A1}\LanguageProfile\0x0000ffff
HKEY_LOCAL_MACHINE\Software\Microsoft\CTF\TIP\{DCBD6FA8-032F-11D3-B5B1-
00C04FC324A1}\LanguageProfile\0x0000ffff\{09EA4E4B-46CE-4469-B450-
0DE76A435BBB}
HKEY_CURRENT_USER\Software\Microsoft\CTF\TIP\{F89E9E58-BD2F-4008-9AC2-
0F816C09F4EE}\LanguageProfile
HKEY_LOCAL_MACHINE\Software\Microsoft\CTF\TIP\{F89E9E58-BD2F-4008-9AC2-
0F816C09F4EE}\LanguageProfile
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Toolbars\Settings
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\IME
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\ShipAsserts
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\StatusBar
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Open Find\Places
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Open Find
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibili
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\DrawAlerts\FTP Sites
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\User
Shell Folders
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell
Folders
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Security\FileOpenBlock
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Office\12.0\Common\Security
HKEY_LOCAL_MACHINE\Software\Microsoft\COM3
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-1004_Classes
HKEY_LOCAL_MACHINE\Software\Classes
\REGISTRY\USER
HKEY_LOCAL_MACHINE\Software\Classes\CLSID
CLSID\{88D969EC-8B8B-4C3D-859E-AF6CD158BE0F}
CLSID\{88D969EC-8B8B-4C3D-859E-AF6CD158BE0F}\TreatAs
\CLSID\{88D969EC-8B8B-4C3D-859E-AF6CD158BE0F}
\CLSID\{88D969EC-8B8B-4C3D-859E-AF6CD158BE0F}\InprocServer32
\CLSID\{88D969EC-8B8B-4C3D-859E-AF6CD158BE0F}\InprocServerX86
\CLSID\{88D969EC-8B8B-4C3D-859E-AF6CD158BE0F}\LocalServer32
\CLSID\{88D969EC-8B8B-4C3D-859E-AF6CD158BE0F}\InprocHandler32
\CLSID\{88D969EC-8B8B-4C3D-859E-AF6CD158BE0F}\InprocHandlerX86
\CLSID\{88D969EC-8B8B-4C3D-859E-AF6CD158BE0F}\LocalServer
HKEY_CLASSES_ROOT\CLSID\{88D969EC-8B8B-4C3D-859E-AF6CD158BE0F}
HKEY_CLASSES_ROOT\CLSID\{88D969EC-8B8B-4C3D-859E-AF6CD158BE0F}\TreatAs
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Office\12.0\Common\OpenXMLForm
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Publisher\Internet
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\PowerPoint\Internet
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer
HKEY_LOCAL_MACHINE\Software\Netscape\Netscape Navigator
HKEY_LOCAL_MACHINE\Software\Netscape\Netscape Navigator Gold
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Internet
HKEY_LOCAL_MACHINE\Software\Microsoft\Office\12.0\Common\Internet
HKEY_LOCAL_MACHINE\Software\Microsoft\Ole
HKEY_CLASSES_ROOT\AppID\WINWORD.EXE
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OLE
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\ComputerName
ActiveComputerName
CLSID\{88D969EF-F192-11D4-A65F-0040963251E5}
```

```
CLSID\{88D969EF-F192-11D4-A65F-0040963251E5}\TreatAs
\CLSID\{88D969EF-F192-11D4-A65F-0040963251E5}
\CLSID\{88D969EF-F192-11D4-A65F-0040963251E5}\InprocServer32
\CLSID\{88D969EF-F192-11D4-A65F-0040963251E5}\InprocServerX86
\CLSID\{88D969EF-F192-11D4-A65F-0040963251E5}\LocalServer32
\CLSID\{88D969EF-F192-11D4-A65F-0040963251E5}\InprocHandler32
\CLSID\{88D969EF-F192-11D4-A65F-0040963251E5}\InprocHandlerX86
\CLSID\{88D969EF-F192-11D4-A65F-0040963251E5}\LocalServer
HKEY_CLASSES_ROOT\CLSID\{88D969EF-F192-11D4-A65F-0040963251E5}
HKEY_CLASSES_ROOT\CLSID\{88D969EF-F192-11D4-A65F-0040963251E5}\TreatAs
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MOTIF\FlexUIAutomation
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Toolbars\Word
HKEY_LOCAL_MACHINE\Software\Microsoft\Office\Word\Addins
HKEY_CURRENT_USER\Software\Microsoft\Office\Word\Addins
HKEY_CURRENT_USER\Software\Microsoft\Office\Word\Addins\WordEEFonts.Connect
WordEEFonts.Connect\Clsid
HKEY_CLASSES_ROOT\WordEEFonts.Connect
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\UserInfo
HKEY_CURRENT_USER\Keyboard Layout\Toggle
HKEY_CURRENT_USER\SOFTWARE\Microsoft\CTF\LangBarAddIn\
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\LangBarAddIn\
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office Test\Special
HKEY_LOCAL_MACHINE\Software\Microsoft\Office\12.0\Common\InstallRoot
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Licensing
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Office\12.0\Common\General
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Registration
HKEY_LOCAL_MACHINE\Software\Microsoft\Shared\HTML
HKEY_LOCAL_MACHINE\Software\Microsoft\Shared\MHTML
HKEY_CLASSES_ROOT\.htm
HKEY_CLASSES_ROOT\htmlfile\shell
HKEY_CLASSES_ROOT\htmlfile\shell\edit\command
HKEY_CLASSES_ROOT\htmlfile\shell\print\command
HKEY_CLASSES_ROOT\CLSID\{42042206-2D85-11D3-8CFF-005004838597}\Version
HKEY_CLASSES_ROOT\CLSID\{42042206-2D85-11D3-8CFF-005004838597}\Version\12
HKEY_CLASSES_ROOT\.mht
HKEY_CLASSES_ROOT\mhtmlfile\shell
HKEY_CLASSES_ROOT\mhtmlfile\shell\edit\command
HKEY_CLASSES_ROOT\mhtmlfile\shell\print\command
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Outlook\Security
ActiveComputerName\Cursors
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\DisabledItem
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\DRM
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Files
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Send To OneNote 2007
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts
HKEY_CLASSES_ROOT\.dotm
HKEY_CLASSES_ROOT\Word.TemplateMacroEnabled.12
HKEY_CLASSES_ROOT\Word.TemplateMacroEnabled.12\CurVer
HKEY_CLASSES_ROOT\Word.TemplateMacroEnabled.12\
HKEY_CLASSES_ROOT\Word.TemplateMacroEnabled.12\\ShellEx\IconHandler
HKEY_CLASSES_ROOT\SystemFileAssociations\.dotm
HKEY_CLASSES_ROOT\SystemFileAssociations\.dotm\ShellEx\IconHandler
HKEY_CLASSES_ROOT\SystemFileAssociations\document
HKEY_CLASSES_ROOT\Word.TemplateMacroEnabled.12\\Clsid
HKEY_CLASSES_ROOT\CLSID\{8A624388-AA27-43E0-89F8-2A12BFF7BCCD}\Implemented
Categories\{00021490-0000-0000-C000-000000000046}
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\ReviewCycle
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Font Mapping
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Comdlg32
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts
HKEY_CLASSES_ROOT\.doc
HKEY_CLASSES_ROOT\Word.Document.8
```

```
HKEY_CLASSES_ROOT\Word.Document.8\CurVer
HKEY_CLASSES_ROOT\Word.Document.8\
HKEY_CLASSES_ROOT\Word.Document.8\\ShellEx\IconHandler
HKEY_CLASSES_ROOT\SystemFileAssociations\.doc
HKEY_CLASSES_ROOT\SystemFileAssociations\.doc\ShellEx\IconHandler
HKEY_CLASSES_ROOT\Word.Document.8\\Clsid
HKEY_CLASSES_ROOT\CLSID\{00020906-0000-0000-C000-000000000046}\Implemented
Categories\{00021490-0000-0000-C000-000000000046}
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Workflow\Cache
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Workflow\WorkgroupCache
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\DWS
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Security\Trusted
Locations
HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Common\Security\Tru
Locations
HKEY_CURRENT_USER\Environment
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\DocumentRecc
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\DocumentRecc
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Restore Workspace
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag
HKEY_CURRENT_USER\AppEvents\Schemes\Apps\Office97
CLSID\{7B8A2D94-0AC9-11D1-896C-00C04FB6BFC4}
CLSID\{7B8A2D94-0AC9-11D1-896C-00C04FB6BFC4}\TreatAs
\CLSID\{7B8A2D94-0AC9-11D1-896C-00C04FB6BFC4}
\CLSID\{7B8A2D94-0AC9-11D1-896C-00C04FB6BFC4}\InprocServer32
\CLSID\{7B8A2D94-0AC9-11D1-896C-00C04FB6BFC4}\InprocServerX86
\CLSID\{7B8A2D94-0AC9-11D1-896C-00C04FB6BFC4}\LocalServer32
\CLSID\{7B8A2D94-0AC9-11D1-896C-00C04FB6BFC4}\InprocHandler32
\CLSID\{7B8A2D94-0AC9-11D1-896C-00C04FB6BFC4}\InprocHandlerX86
\CLSID\{7B8A2D94-0AC9-11D1-896C-00C04FB6BFC4}\LocalServer
HKEY_CLASSES_ROOT\CLSID\{7B8A2D94-0AC9-11D1-896C-00C04FB6BFC4}
HKEY_CLASSES_ROOT\CLSID\{7B8A2D94-0AC9-11D1-896C-00C04FB6BFC4}\TreatAs
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\ZoneMap\
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings\ZoneMap\
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Interne
Settings\ZoneMap\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\ZoneMap\\Ranges\
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Interne
Settings
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet
Explorer\Main\FeatureControl
HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet
Explorer\Main\FeatureControl
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet
Explorer\Main\FeatureControl\FEATURE_VALIDATE_URLHOSTNAME
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\Proofing Tools\Proof Type
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing
Tools\1.0\Override
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Manage
1-5-21-1547161642-507921405-839522115-
1004\Installer\Components\A01FEFDE8C822B9408582AC21997CABB
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-
1004\Software\Microsoft\Installer\Components\A01FEFDE8C822B9408582AC21997CABB
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Components\A01FEFDE8C822B940858
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Manage
1-5-21-1547161642-507921405-839522115-
1004\Installer\Components\E9A16771B8AFC744D9BDB7B2BBBC15A1
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-
1004\Software\Microsoft\Installer\Components\E9A16771B8AFC744D9BDB7B2BBBC15A1
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Components\E9A16771B8AFC744D9BD
```

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Manage
1-5-21-1547161642-507921405-839522115-
1004\Installer\Features\00002109F100A0C00000000000F01FEC
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-
1004\Software\Microsoft\Installer\Features\00002109F100A0C00000000000F01FEC
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Features\00002109F100A0C000000(
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Products\00002109F100A0C00000000000F01FEC\Features
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\37B0B509FD9CC284A8E27AE607FE5270
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\45527C2C9B765B1428CF7E17324433CD
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\CF0CF973CF05E0743B9BF52D4870FB24
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\5E743E26CA007804580F1F5C5D683E88
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\BD64546253186C44DB392B0002A364FE
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\7C41BD7E28A59E247AD2B573BACB8677
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Manage
1-5-21-1547161642-507921405-839522115-
1004\Installer\Products\00002109F100A0C00000000000F01FEC
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-
1004\Software\Microsoft\Installer\Products\00002109F100A0C00000000000F01FEC
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\00002109F100A0C000000(
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Products\00002109F100A0C00000000000F01FEC\Usage
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Manage
1-5-21-1547161642-507921405-839522115-
1004\Installer\Components\6BFFEAF45FF36B342ADC37DE1B1FC241
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-
1004\Software\Microsoft\Installer\Components\6BFFEAF45FF36B342ADC37DE1B1FC241
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Components\6BFFEAF45FF36B342ADC
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Manage
1-5-21-1547161642-507921405-839522115-
1004\Installer\Features\00002109F10090400000000000F01FEC
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-
1004\Software\Microsoft\Installer\Features\00002109F10090400000000000F01FEC
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Features\00002109F100904000000(
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Products\00002109F10090400000000000F01FEC\Features
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\F97A7CF51C1B13C428CBD7B3DD106020
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\07B795E021151E34DBF8D2CB39429C69
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\FBFC0F36C55A64A439A747B668E50D4D
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\41F463C603D4CFE4290226B0966AFF87
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\0B812766B2315D14EB7B147A0DC96653
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\FF59970FE4207784CB006918B6A8400B
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Manage
1-5-21-1547161642-507921405-839522115-
1004\Installer\Products\00002109F10090400000000000F01FEC
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-
1004\Software\Microsoft\Installer\Products\00002109F10090400000000000F01FEC
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\00002109F100904000000(
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Products\00002109F10090400000000000F01FEC\Usage
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Manage
1-5-21-1547161642-507921405-839522115-
1004\Installer\Components\F3BE92CC2CB71D119A12000A9CE1A22A

HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-
1004\Software\Microsoft\Installer\Components\F3BE92CC2CB71D119A12000A9CE1A22A
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Components\F3BE92CC2CB71D119A12
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Manage
1-5-21-1547161642-507921405-839522115-
1004\Installer\Features\00002109F100C0400000000000F01FEC
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-
1004\Software\Microsoft\Installer\Features\00002109F100C0400000000000F01FEC
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Features\00002109F100C040000000
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Products\00002109F100C0400000000000F01FEC\Features
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\072FB27307B79A84981E90D9D7FD34F3
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\848E74D12EF64E04B87C08B37F9DFA31
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\28BA0E7878234D11C85300008F40C0E5
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\48BA0E7878234D11C85300008F40C0E5
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\89529A66F52EE824286E5D7280BF2B9C
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\5D5F721B7BEE8EC4DA5E526F139246D0
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Manage
1-5-21-1547161642-507921405-839522115-
1004\Installer\Products\00002109F100C0400000000000F01FEC
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-
1004\Software\Microsoft\Installer\Products\00002109F100C0400000000000F01FEC
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\00002109F100C040000000
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Products\00002109F100C0400000000000F01FEC\Usage
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Manage
1-5-21-1547161642-507921405-839522115-
1004\Installer\Components\D3BE92CC2CB71D119A12000A9CE1A22A
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-
1004\Software\Microsoft\Installer\Components\D3BE92CC2CB71D119A12000A9CE1A22A
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Components\D3BE92CC2CB71D119A12
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Manage
1-5-21-1547161642-507921405-839522115-
1004\Installer\Components\C18EB3B85D045C14AA95785DC1D767B1
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-
1004\Software\Microsoft\Installer\Components\C18EB3B85D045C14AA95785DC1D767B1
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Components\C18EB3B85D045C14AA95
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\Proofing Tools\Grammar
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\Proofing Tools\Language
Auto Detect
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\Proofing Tools\Formatting
Consistency Checker
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\Proofing Tools\Smart Tag
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Manage
1-5-21-1547161642-507921405-839522115-
1004\Installer\Components\34BE92CC2CB71D119A12000A9CE1A22A
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-
1004\Software\Microsoft\Installer\Components\34BE92CC2CB71D119A12000A9CE1A22A
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Components\34BE92CC2CB71D119A12
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\Proofing Tools\Thesaurus
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Manage
1-5-21-1547161642-507921405-839522115-
1004\Installer\Components\53BE92CC2CB71D119A12000A9CE1A22A
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-
1004\Software\Microsoft\Installer\Components\53BE92CC2CB71D119A12000A9CE1A22A
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Components\53BE92CC2CB71D119A12
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\Proofing
Tools\Hyphenation
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\Proofing

```
Tools\HangulHanjaConv
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\Proofing Tools\Dictionary
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Manage
1-5-21-1547161642-507921405-839522115-
1004\Installer\Components\F4BE92CC2CB71D119A12000A9CE1A22A
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-
1004\Software\Microsoft\Installer\Components\F4BE92CC2CB71D119A12000A9CE1A22A
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Components\F4BE92CC2CB71D119A12
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\Proofing Tools\Word Forms
HKEY_LOCAL_MACHINE\Software\Microsoft\Shared Tools Location
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\2447246F41EC398429FCD2997760A0F5
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing Tools\1.0\Custom
Dictionaries
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing Tools\1.0\Custom
Dictionaries\
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing
Tools\1.0\SpecialtyLexicons
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\PTWatson
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Manage
1-5-21-1547161642-507921405-839522115-
1004\Installer\Components\285E35716D00D104F994678A97F78A0A
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-
1004\Software\Microsoft\Installer\Components\285E35716D00D104F994678A97F78A0A
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Components\285E35716D00D104F994
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\Addres
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\Brandi
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\Connec
Manager
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\Direct
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\Direct
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\distor
py2.7
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\DXM_Ru
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\ENTERP
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\ENTERP
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\Fontcc
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\ICW
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\IDNMit
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\IE40
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\IE4Dat
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAK
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\IEData
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\Micros
.NET Framework 3.5
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\Mobile
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\Mozill
Firefox 6.0.2 (x86 en-US)
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\MPlaye
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\NetMee
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\NLSDow
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\Outloc
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\PCHeal
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\PIL-
py2.7
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\Schedu
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\WIC
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\Windov
XP Service Pack
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\XpsEPS
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{26A24AE4-039D-4CA4-87B4-2F83216027FF}
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
```

```
{2BA00471-0328-3743-93BD-FA813353A783}
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{2E295B5B-1AD4-4d36-97C2-A316084722CF}
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{2FC099BD-AC9B-33EB-809C-D332E1B27C40}
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{350C97B0-3D7C-4EE8-BAA9-00BCB3D54227}
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{4A03706F-666A-4037-7777-5F2748764D10}
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{4E3E9F50-0068-440B-BCD1-DB28AA667BA3}
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{5640C7C7-35CC-4D49-B084-496BE66E7E38}
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{664F4782-C761-4803-913B-6A7AF69D4B5D}
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{90120000-0010-0409-0000-0000000FF1CE}
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{90120000-0015-0409-0000-0000000FF1CE}
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{90120000-0016-0409-0000-0000000FF1CE}
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{90120000-0018-0409-0000-0000000FF1CE}
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{90120000-0019-0409-0000-0000000FF1CE}
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{90120000-001A-0409-0000-0000000FF1CE}
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{90120000-001B-0409-0000-0000000FF1CE}
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{90120000-001F-0409-0000-0000000FF1CE}
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{90120000-001F-040C-0000-0000000FF1CE}
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{90120000-001F-0C0A-0000-0000000FF1CE}
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{90120000-002C-0409-0000-0000000FF1CE}
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{90120000-0030-0000-0000-0000000FF1CE}
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{90120000-0044-0409-0000-0000000FF1CE}
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{90120000-006E-0409-0000-0000000FF1CE}
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{90120000-00A1-0409-0000-0000000FF1CE}
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{90120000-00BA-0409-0000-0000000FF1CE}
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{90120000-0114-0409-0000-0000000FF1CE}
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{90120000-0115-0409-0000-0000000FF1CE}
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{90120000-0117-0409-0000-0000000FF1CE}
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{AC76BA86-7AD7-1033-7B44-A94000000001}
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{B508B3F1-A24A-32C0-B310-85786919EF28}
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\
{D1AC5696-CC7E-34D7-89B3-4D09E7CF7D14}
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Manage
1-5-21-1547161642-507921405-839522115-
1004\Installer\Products\00002109E60090400000000000F01FEC
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-
1004\Software\Microsoft\Installer\Products\00002109E60090400000000000F01FEC
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\00002109E6009040000000
```

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Products\00002109E60090400000000000F01FEC\InstallProperties
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Manage
1-5-21-1547161642-507921405-839522115-
1004\Installer\Products\00002109511090400000000000F01FEC
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-
1004\Software\Microsoft\Installer\Products\00002109511090400000000000F01FEC
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\0000210951109040000000
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Products\00002109511090400000000000F01FEC\InstallProperties
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Manage
1-5-21-1547161642-507921405-839522115-
1004\Installer\Products\00002109610090400000000000F01FEC
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-
1004\Software\Microsoft\Installer\Products\00002109610090400000000000F01FEC
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\0000210961009040000000
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Products\00002109610090400000000000F01FEC\InstallProperties
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Manage
1-5-21-1547161642-507921405-839522115-
1004\Installer\Products\00002109A10090400000000000F01FEC
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-
1004\Software\Microsoft\Installer\Products\00002109A10090400000000000F01FEC
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\00002109A100904000000
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Products\00002109A10090400000000000F01FEC\InstallProperties
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Manage
1-5-21-1547161642-507921405-839522115-
1004\Installer\Products\00002109810090400000000000F01FEC
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-
1004\Software\Microsoft\Installer\Products\00002109810090400000000000F01FEC
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\0000210981009040000000
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Products\00002109810090400000000000F01FEC\InstallProperties
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Manage
1-5-21-1547161642-507921405-839522115-
1004\Installer\Products\00002109010090400000000000F01FEC
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-
1004\Software\Microsoft\Installer\Products\00002109010090400000000000F01FEC
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\0000210901009040000000
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Products\00002109010090400000000000F01FEC\InstallProperties
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Manage
1-5-21-1547161642-507921405-839522115-
1004\Installer\Products\00002109AB0090400000000000F01FEC
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-
1004\Software\Microsoft\Installer\Products\00002109AB0090400000000000F01FEC
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\00002109AB009040000000
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Products\00002109AB0090400000000000F01FEC\InstallProperties
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Manage
1-5-21-1547161642-507921405-839522115-
1004\Installer\Products\00002109411090400000000000F01FEC
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-
1004\Software\Microsoft\Installer\Products\00002109411090400000000000F01FEC
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\0000210941109040000000
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Products\00002109411090400000000000F01FEC\InstallProperties
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Manage
1-5-21-1547161642-507921405-839522115-
1004\Installer\Products\00002109440090400000000000F01FEC
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-
1004\Software\Microsoft\Installer\Products\00002109440090400000000000F01FEC
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\0000210944009040000000
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa

```
1-5-18\Products\00002109440090400000000000F01FEC\InstallProperties
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Products\00002109F100A0C00000000000F01FEC\InstallProperties
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Products\00002109F100C0400000000000F01FEC\InstallProperties
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Products\00002109F10090400000000000F01FEC\InstallProperties
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Manage
1-5-21-1547161642-507921405-839522115-
1004\Installer\Products\00002109C20090400000000000F01FEC
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-
1004\Software\Microsoft\Installer\Products\00002109C20090400000000000F01FEC
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\00002109C2009040000000(
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Products\00002109C20090400000000000F01FEC\InstallProperties
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Manage
1-5-21-1547161642-507921405-839522115-
1004\Installer\Products\00002109910090400000000000F01FEC
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-
1004\Software\Microsoft\Installer\Products\00002109910090400000000000F01FEC
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\0000210991009040000000(
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Products\00002109910090400000000000F01FEC\InstallProperties
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Manage
1-5-21-1547161642-507921405-839522115-
1004\Installer\Products\00002109B10090400000000000F01FEC
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-
1004\Software\Microsoft\Installer\Products\00002109B10090400000000000F01FEC
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\00002109B1009040000000(
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Products\00002109B10090400000000000F01FEC\InstallProperties
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Manage
1-5-21-1547161642-507921405-839522115-
1004\Installer\Products\00002109510090400000000000F01FEC
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-
1004\Software\Microsoft\Installer\Products\00002109510090400000000000F01FEC
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\0000210951009040000000(
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Products\00002109510090400000000000F01FEC\InstallProperties
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Manage
1-5-21-1547161642-507921405-839522115-
1004\Installer\Products\00002109711090400000000000F01FEC
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-
1004\Software\Microsoft\Installer\Products\00002109711090400000000000F01FEC
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\0000210971109040000000(
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Products\00002109711090400000000000F01FEC\InstallProperties
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Manage
1-5-21-1547161642-507921405-839522115-
1004\Installer\Products\000021091A0090400000000000F01FEC
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-
1004\Software\Microsoft\Installer\Products\000021091A0090400000000000F01FEC
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Products\000021091A009040000000(
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Products\000021091A0090400000000000F01FEC\InstallProperties
HKEY_LOCAL_MACHINE\Software\Microsoft\Office\12.0\Common\LanguageResources\Pa
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\Proofing
Tools\Grammar\1049\Normal
HKEY_LOCAL_MACHINE\Software\Microsoft\Shared Tools\Proofing Tools\Language
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserDa
1-5-18\Components\14355655CBD54D944A7518EDDF19EA2D
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Internet\Fonts
CTF.TimListCache.FMPDefaultS-1-5-21-1547161642-507921405-839522115-
1004MUTEX.DefaultS-1-5-21-1547161642-507921405-839522115-1004
Local\MU_ACBPIDS09_S-1-5-5-0-39993
```

```
MSCTF.Shared.MUTEX.EMF
Global\MTX_MSO_Formal1_S-1-5-21-1547161642-507921405-839522115-1004
Global\MTX_MSO_AdHoc1_S-1-5-21-1547161642-507921405-839522115-1004
```

- Static Analysis
- Strings
- Antivirus

PE Imphash

e160ef8e55bb9d162da4e266afd9eef3

Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	SIZE OF RAW DATA	ENTROPY
.text	0x00001000	0x00005a7c	0x00005c00	6.43021696145
.rdata	0x00007000	0x000011ce	0x00001200	5.23558258678
.data	0x00009000	0x0003d7d8	0x00000400	4.95741874714
.ndata	0x00047000	0x00052000	0x00000000	0.0
.rsrc	0x00099000	0x00000a18	0x00000c00	4.06510416606

Resources

NAME	OFFSET	SIZE	LANGUAGE	SUB-LANGUAGE
RT_ICON	0x00099190	0x000002e8	LANG_ENGLISH	SUBLANG_ENGLISH_
RT_DIALOG	0x00099698	0x00000060	LANG_ENGLISH	SUBLANG_ENGLISH_
RT_DIALOG	0x00099698	0x00000060	LANG_ENGLISH	SUBLANG_ENGLISH_
RT_DIALOG	0x00099698	0x00000060	LANG_ENGLISH	SUBLANG_ENGLISH_
RT_GROUP_ICON	0x000996f8	0x00000014	LANG_ENGLISH	SUBLANG_ENGLISH_
RT_MANIFEST	0x00099710	0x00000305	LANG_ENGLISH	SUBLANG_ENGLISH_

Imports

Library KERNEL32.dll:

- 0x407060 GetTickCount
- 0x407064 GetFullPathNameA
- 0x407068 MoveFileA
- 0x40706c SetCurrentDirectoryA
- 0x407070 GetFileAttributesA
- 0x407074 GetLastError
- 0x407078 CreateDirectoryA
- 0x40707c SetFileAttributesA
- 0x407080 SearchPathA
- 0x407084 GetShortPathNameA
- 0x407088 GetFileSize

- 0x40708c GetModuleFileNameA
- 0x407090 GetCurrentProcess
- 0x407094 CopyFileA
- 0x407098 ExitProcess
- 0x40709c SetEnvironmentVariableA
- 0x4070a0 GetWindowsDirectoryA
- 0x4070a4 GetTempPathA
- 0x4070a8 Sleep
- 0x4070ac CloseHandle
- 0x4070b0 LoadLibraryA
- 0x4070b4 lstrlenA
- 0x4070b8 lstrcpynA
- 0x4070bc GetDiskFreeSpaceA
- 0x4070c0 GlobalUnlock
- 0x4070c4 GlobalLock
- 0x4070c8 CreateThread
- 0x4070cc CreateProcessA
- 0x4070d0 RemoveDirectoryA
- 0x4070d4 CreateFileA
- 0x4070d8 GetTempFileNameA
- 0x4070dc ReadFile
- 0x4070e0 lstrcpyA
- 0x4070e4 lstrcatA
- 0x4070e8 GetSystemDirectoryA
- 0x4070ec GetVersion
- 0x4070f0 GetProcAddress
- 0x4070f4 GlobalAlloc
- 0x4070f8 CompareFileTime
- 0x4070fc SetFileTime
- 0x407100 ExpandEnvironmentStringsA
- 0x407104 lstrcmpiA
- 0x407108 lstrcmpA
- 0x40710c WaitForSingleObject
- 0x407110 GlobalFree
- 0x407114 GetExitCodeProcess
- 0x407118 GetModuleHandleA
- 0x40711c SetErrorMode
- 0x407120 GetCommandLineA
- 0x407124 LoadLibraryExA
- 0x407128 FindFirstFileA
- 0x40712c FindNextFileA
- 0x407130 DeleteFileA
- 0x407134 SetFilePointer
- 0x407138 WriteFile
- 0x40713c FindClose
- 0x407140 WritePrivateProfileStringA
- 0x407144 MultiByteToWideChar
- 0x407148 MulDiv
- 0x40714c GetPrivateProfileStringA
- 0x407150 FreeLibrary

Library USER32.dll:

- 0x407174 CreateWindowExA
- 0x407178 EndDialog
- 0x40717c ScreenToClient
- 0x407180 GetWindowRect
- 0x407184 EnableMenuItem
- 0x407188 GetSystemMenu

- 0x40718c SetClassLongA
- 0x407190 IsWindowEnabled
- 0x407194 SetWindowPos
- 0x407198 GetSysColor
- 0x40719c GetWindowLongA
- 0x4071a0 SetCursor
- 0x4071a4 LoadCursorA
- 0x4071a8 CheckDlgButton
- 0x4071ac GetMessagePos
- 0x4071b0 LoadBitmapA
- 0x4071b4 CallWindowProcA
- 0x4071b8 IsWindowVisible
- 0x4071bc CloseClipboard
- 0x4071c0 GetDC
- 0x4071c4 SystemParametersInfoA
- 0x4071c8 RegisterClassA
- 0x4071cc TrackPopupMenu
- 0x4071d0 AppendMenuA
- 0x4071d4 CreatePopupMenu
- 0x4071d8 GetSystemMetrics
- 0x4071dc SetDlgItemTextA
- 0x4071e0 GetDlgItemTextA
- 0x4071e4 MessageBoxIndirectA
- 0x4071e8 CharPrevA
- 0x4071ec DispatchMessageA
- 0x4071f0 PeekMessageA
- 0x4071f4 ReleaseDC
- 0x4071f8 EnableWindow
- 0x4071fc InvalidateRect
- 0x407200 SendMessageA
- 0x407204 DefWindowProcA
- 0x407208 BeginPaint
- 0x40720c GetClientRect
- 0x407210 FillRect
- 0x407214 DrawTextA
- 0x407218 GetClassInfoA
- 0x40721c DialogBoxParamA
- 0x407220 CharNextA
- 0x407224 ExitWindowsEx
- 0x407228 DestroyWindow
- 0x40722c CreateDialogParamA
- 0x407230 SetTimer
- 0x407234 GetDlgItem
- 0x407238 wsprintfA
- 0x40723c SetForegroundWindow
- 0x407240 ShowWindow
- 0x407244 IsWindow
- 0x407248 LoadImageA
- 0x40724c SetWindowLongA
- 0x407250 SetClipboardData
- 0x407254 EmptyClipboard
- 0x407258 OpenClipboard
- 0x40725c EndPaint
- 0x407260 PostQuitMessage
- 0x407264 FindWindowExA
- 0x407268 SendMessageTimeoutA
- 0x40726c SetWindowTextA

Library GDI32.dll:
- 0x40703c SelectObject
- 0x407040 SetBkMode
- 0x407044 CreateFontIndirectA
- 0x407048 SetTextColor
- 0x40704c DeleteObject
- 0x407050 GetDeviceCaps
- 0x407054 CreateBrushIndirect
- 0x407058 SetBkColor

Library SHELL32.dll:
- 0x407158 SHGetSpecialFolderLocation
- 0x40715c SHGetPathFromIDListA
- 0x407160 SHBrowseForFolderA
- 0x407164 SHGetFileInfoA
- 0x407168 ShellExecuteA
- 0x40716c SHFileOperationA

Library ADVAPI32.dll:
- 0x407000 RegCloseKey
- 0x407004 RegOpenKeyExA
- 0x407008 RegDeleteKeyA
- 0x40700c RegDeleteValueA
- 0x407010 RegEnumValueA
- 0x407014 RegCreateKeyExA
- 0x407018 RegSetValueExA
- 0x40701c RegQueryValueExA
- 0x407020 RegEnumKeyA

Library COMCTL32.dll:
- 0x407028 ImageList_Create
- 0x40702c ImageList_AddMasked
- 0x407030 ImageList_Destroy
- 0x407034 None

Library ole32.dll:
- 0x407284 CoCreateInstance
- 0x407288 CoTaskMemFree
- 0x40728c OleInitialize
- 0x407290 OleUninitialize

Library VERSION.dll:
- 0x407274 GetFileVersionInfoSizeA
- 0x407278 GetFileVersionInfoA
- 0x40727c VerQueryValueA

```
!This program cannot be run in DOS mode.
iRichu
`.rdata
@.data
.ndata
SQSSSPW
v#VhB+@
Instu`
softuW
NulluN
D$(Ph,
D$,SPS
Vj%SSS
D$$+D$
D$,+D$$P
u49-lgD
PPPPPP
<v"Ph
RichEdit
```

```
RichEdit20A
RichEd32
RichEd20
.DEFAULT\Control Panel\International
Control Panel\Desktop\ResourceLocale
Software\Microsoft\Windows\CurrentVersion
\Microsoft\Internet Explorer\Quick Launch
MulDiv
DeleteFileA
FindFirstFileA
FindNextFileA
FindClose
SetFilePointer
WriteFile
GetPrivateProfileStringA
WritePrivateProfileStringA
MultiByteToWideChar
FreeLibrary
LoadLibraryExA
GetModuleHandleA
GetExitCodeProcess
WaitForSingleObject
GlobalAlloc
GlobalFree
ExpandEnvironmentStringsA
lstrcmpA
lstrcmpiA
CloseHandle
SetFileTime
CompareFileTime
SearchPathA
GetShortPathNameA
GetFullPathNameA
MoveFileA
SetCurrentDirectoryA
GetFileAttributesA
GetLastError
CreateDirectoryA
SetFileAttributesA
GetTickCount
GetFileSize
GetModuleFileNameA
GetCurrentProcess
CopyFileA
ExitProcess
SetEnvironmentVariableA
GetWindowsDirectoryA
GetTempPathA
GetCommandLineA
SetErrorMode
LoadLibraryA
lstrlenA
lstrcpynA
GetDiskFreeSpaceA
GlobalUnlock
GlobalLock
CreateThread
CreateProcessA
RemoveDirectoryA
CreateFileA
GetTempFileNameA
ReadFile
lstrcpyA
lstrcatA
GetSystemDirectoryA
```

```
GetVersion
GetProcAddress
KERNEL32.dll
EndPaint
DrawTextA
FillRect
GetClientRect
BeginPaint
DefWindowProcA
SendMessageA
InvalidateRect
EnableWindow
ReleaseDC
LoadImageA
SetWindowLongA
GetDlgItem
IsWindow
FindWindowExA
SendMessageTimeoutA
wsprintfA
ShowWindow
SetForegroundWindow
PostQuitMessage
SetWindowTextA
SetTimer
CreateDialogParamA
DestroyWindow
ExitWindowsEx
CharNextA
DialogBoxParamA
GetClassInfoA
CreateWindowExA
SystemParametersInfoA
RegisterClassA
EndDialog
ScreenToClient
GetWindowRect
EnableMenuItem
GetSystemMenu
SetClassLongA
IsWindowEnabled
SetWindowPos
GetSysColor
GetWindowLongA
SetCursor
LoadCursorA
CheckDlgButton
GetMessagePos
LoadBitmapA
CallWindowProcA
IsWindowVisible
CloseClipboard
SetClipboardData
EmptyClipboard
OpenClipboard
TrackPopupMenu
AppendMenuA
CreatePopupMenu
GetSystemMetrics
SetDlgItemTextA
GetDlgItemTextA
MessageBoxIndirectA
CharPrevA
DispatchMessageA
PeekMessageA
```

```
USER32.dll
SelectObject
SetTextColor
SetBkMode
CreateFontIndirectA
CreateBrushIndirect
DeleteObject
GetDeviceCaps
SetBkColor
GDI32.dll
SHFileOperationA
ShellExecuteA
SHGetFileInfoA
SHBrowseForFolderA
SHGetPathFromIDListA
SHGetSpecialFolderLocation
SHELL32.dll
RegEnumValueA
RegEnumKeyA
RegQueryValueExA
RegSetValueExA
RegCreateKeyExA
RegCloseKey
RegDeleteValueA
RegDeleteKeyA
RegOpenKeyExA
ADVAPI32.dll
ImageList_Destroy
ImageList_AddMasked
ImageList_Create
COMCTL32.dll
CoCreateInstance
OleUninitialize
OleInitialize
CoTaskMemFree
ole32.dll
VerQueryValueA
GetFileVersionInfoA
GetFileVersionInfoSizeA
VERSION.dll
verifying installer: %d%%
Installer integrity check has failed. Common causes include
incomplete download and damaged media. Contact the
installer's author to obtain a new copy.
More information at:
http://nsis.sf.net/NSIS_Error
Error launching installer
... %d%%
SeShutdownPrivilege
~nsu.tmp
NSIS Error
Error writing temporary file. Make sure your temp folder is valid.
%u.%u%s%s
SHGetFolderPathA
SHFOLDER
SHAutoComplete
SHLWAPI
InitiateShutdownA
AdjustTokenPrivileges
LookupPrivilegeValueA
OpenProcessToken
RegDeleteKeyExA
ADVAPI32
GetUserDefaultUILanguage
MoveFileExA
```

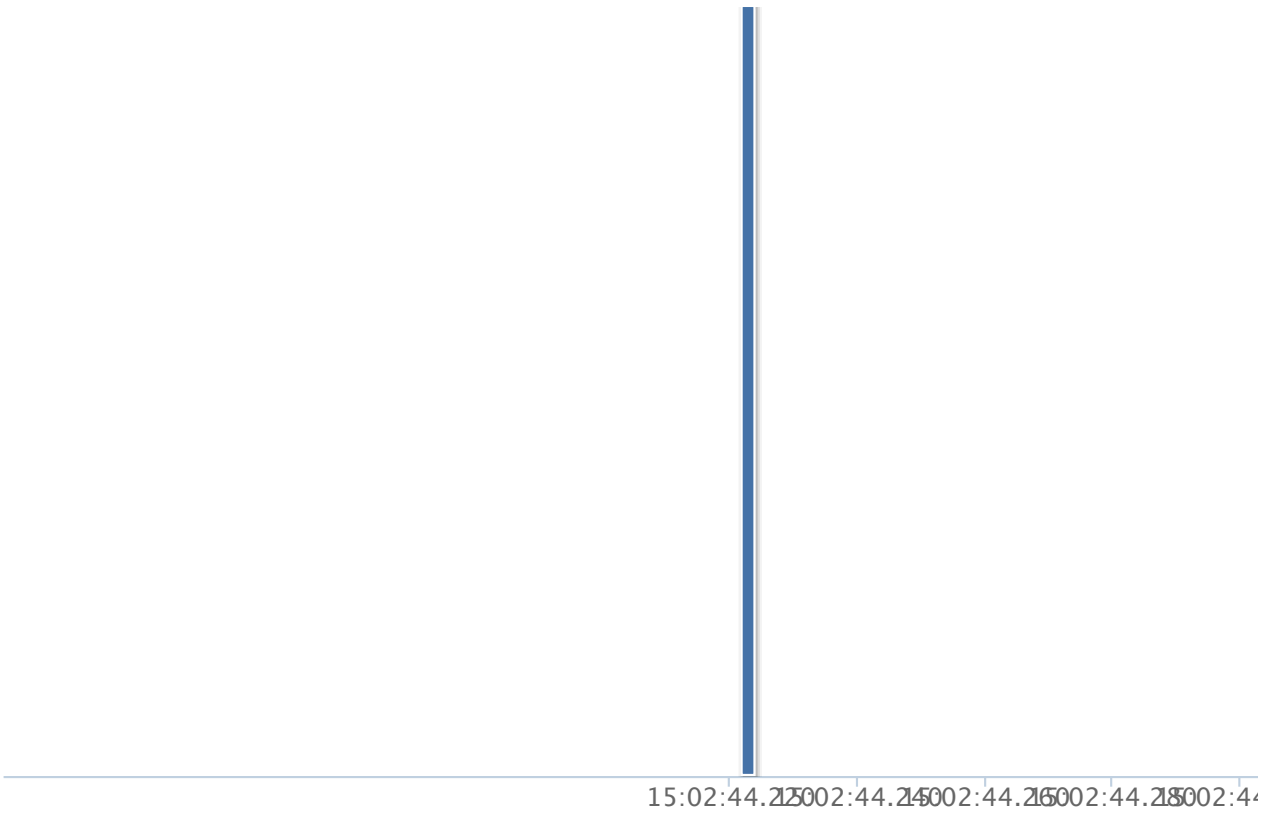
```
GetDiskFreeSpaceExA
KERNEL32
[Rename]
*?|<>/":
wwwwwwwxp
wwwwwwww
<?xml version="1.0" encoding="UTF-8" standalone="yes"?><assembly
xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
<assemblyIdentity version="1.0.0.0" processorArchitecture="*"
name="Nullsoft.NSIS.exehead" type="win32"/><description>Nullsoft Install
System v3.0b1</description><trustInfo xmlns="urn:schemas-microsoft-
com:asm.v3"><security><requestedPrivileges><requestedExecutionLevel
level="asInvoker" uiAccess="false"/></requestedPrivileges></security>
</trustInfo><compatibility xmlns="urn:schemas-microsoft-
com:compatibility.v1"><application><supportedOS Id="{1f676c76-80e1-4239-
95bb-83d0f6d0da78}"/><supportedOS Id="{4a2f28e3-53b9-4441-ba9c-
d69d4a4a6e38}"/><supportedOS Id="{35138b9a-5d96-4fbd-8e2d-a2440225f93a}"/>
</application></compatibility></assembly>
NullsoftInst$G
ln~lOrj.P
F}H6C=
DC$J#;2
A.>fc0
RP"$]d
X>+M!
rDAoZI:
WT]9|-
}Z%97#,-
m$vo.:xXE
|)LP\B
*~kHy54
^a}$;FD
uAVGMM!
Bq?0%k
Tjjc"5
|L^<^
@8udA;}
w8i3^;
r$PoWIA
)pvTBMl
8{YqCj~
&OuYdy
^sMZ$j
,bPTKL
oJlD[,V4g
;*Xv$_.
bKh!JnW@
635L+pL
|R"*?O
K8$ZJC
*~kHy54
[Qfh2V7:
)g0+Z!
Ms?-jWc
YV?xpt
Nv=OOeb
Um6"\-
LFm&\z
RIGby%
yQ;:~;
5U63F#
fL7;)E
kYT881
CfhfzZq
B1k%7
```

```
+|=yR@
y)"u$%
-09>:R
3qU\O^t
Western Cape1
Durbanville1
Thawte1
Thawte Certification10
Thawte Timestamping CA0
121221000000Z
201230235959Z0^1
Symantec Corporation100.
'Symantec Time Stamping Services CA - G20
http://ocsp.thawte.com0
.http://crl.thawte.com/ThawteTimestampingCA.crl0
TimeStamp-2048-10
Symantec Corporation100.
'Symantec Time Stamping Services CA - G20
121018000000Z
201229235959Z0b1
Symantec Corporation1402
+Symantec Time Stamping Services Signer - G40
http://ts-ocsp.ws.symantec.com07
+http://ts-aia.ws.symantec.com/tss-ca-g2.cer0<
+http://ts-crl.ws.symantec.com/tss-ca-g2.crl0(
TimeStamp-2048-20
n-4I'+k
Greater Manchester1
Salford1
COMODO CA Limited1#0!
COMODO RSA Code Signing CA0
150113000000Z
160113235959Z0
1071401
Moscow1
Moscow1301
*12/1, str.1, Pom 15, 17, ul.Krasnoprudnaya1
RADIANT, OOO1
RADIANT, OOO0
https://secure.comodo.net/CPS0C
2http://crl.comodoca.com/COMODORSACodeSigningCA.crl0t
2http://crt.comodoca.com/COMODORSACodeSigningCA.crt0$
http://ocsp.comodoca.com0
AddTrust AB1&0$
AddTrust External TTP Network1"0
AddTrust External CA Root0
000530104838Z
2005301048382Z0
Greater Manchester1
Salford1
COMODO CA Limited1+0)
"COMODO RSA Certification Authority0
HCgNr*
3http://crl.usertrust.com/AddTrustExternalCARoot.crl05
http://ocsp.usertrust.com0
Greater Manchester1
Salford1
COMODO CA Limited1+0)
"COMODO RSA Certification Authority0
130509000000Z
2805082359592Z0}1
Greater Manchester1
Salford1
COMODO CA Limited1#0!
COMODO RSA Code Signing CA0
```

```
;http://crl.comodoca.com/COMODORSACertificationAuthority.crl0q
/http://crt.comodoca.com/COMODORSAAddTrustCA.crt0$
http://ocsp.comodoca.com0
SN20s
Greater Manchester1
Salford1
COMODO CA Limited1#0!
COMODO RSA Code Signing CA
n-4I'+k
Symantec Corporation100.
'Symantec Time Stamping Services CA - G2
151022215430Z0#
U1oAaoq;Bt.V2
MS Shell Dlg
MS Shell Dlg
msctls_progress32
SysListView32
MS Shell Dlg
<<<Obsolete>>
NGeneric Host Process for Win32 Service
```

ANTIVIRUS	SIGNATURE
MicroWorld-eScan	Clean
nProtect	Clean
CMC	Clean
CAT-QuickHeal	Clean
ALYac	Clean
Malwarebytes	Clean
VIPRE	Trojan.Win32.Generic!BT
SUPERAntiSpyware	Clean
K7AntiVirus	Trojan-Downloader (004c57d21)
Alibaba	Clean
K7GW	Trojan-Downloader (004c57d21)
TheHacker	Clean
NANO-Antivirus	Trojan.Nsis.Agent.dtckhe
F-Prot	Clean
Symantec	Suspicious.Cloud.9
ByteHero	Clean
TrendMicro-HouseCall	Clean
Avast	Clean
ClamAV	Clean
Kaspersky	Clean
BitDefender	Clean
Agnitum	Clean
ViRobot	Clean
Rising	Clean
Sophos	Troj/Buhtra-A
Comodo	Clean
F-Secure	Clean
DrWeb	BackDoor.RatPack
Zillya	Worm.VBNA.Win32.262468
TrendMicro	Clean
McAfee-GW-Edition	Artemis
Emsisoft	Clean

Cyren	Clean
Jiangmin	Clean
Avira	BDS/Backdoor.A.7226
Antiy-AVL	Clean
Microsoft	Clean
Arcabit	Clean
AegisLab	Clean
GData	Clean
AhnLab-V3	PUP/Win32.Agent
McAfee	Artemis!CB4F444C624A
AVware	Trojan.Win32.Generic!BT
VBA32	Clean
Baidu-International	Trojan.NSIS.Agent.NTY
Zoner	Clean
ESET-NOD32	NSIS/TrojanDownloader.Agent.NSU
Tencent	Win32.Backdoor.Backdoor.Szbr
Ikarus	Clean
Fortinet	Clean
AVG	Dropper.Generic_c.APZT
Panda	Clean
Qihoo-360	HEUR/QVM42.1.Malware.Gen



- X-axis by: event
- Y-axis by: category

- cb4f444c624a0ad569b63c1422d1c682.exe 1592
  - WINWORD.EXE 580

- cb4f444c624a0ad569b63c1422d1c682.exe
- WINWORD.EXE

cb4f444c624a0ad569b63c1422d1c682.exe, PID: 1592, Parent PID: 1796

- 1
- 2
- 3
- ...
- 5

network filesystem registry process services synchronization

TIME	API	
2015-11-11 23:02:44,233	LdrGetDllHandle	ModuleHandle: 0x00000000 FileName: C:\WINDOWS\system32\rpcss.dl
2015-11-11 23:02:44,233	DeviceIoControl	DeviceHandle: 0x00000044 OutBuffer: \xf2\x07\xfc\xbc\x12gW\x9dU\ IoControlCode: 3735560 InBuffer: \x960\xeak\xe9\xda\x0b \xc3\x7f\xd5<\x7f\xbf\x13\x94o\\x12\x8
2015-11-11 23:02:44,233	DeviceIoControl	DeviceHandle: 0x00000044 OutBuffer: X\xabX\xbd\x03=*\xda^k\xe8\x IoControlCode: 3735560 InBuffer: \x960\xeak\xe9\xda\x0b \xc3\x7f\xd5<\x7f\xbf\xc6\xa2\x1c\x82\

2015-11-11 23:02:44,233	DeviceIoControl	DeviceHandle: 0x00000044 OutBuffer: \xad\xa35B<\xfe\xf4 \x7f\xb3 IoControlCode: 3735560 InBuffer: \x960\xeak\xe9\xda\x0b \xc3\x7f\xd5<\x7f\xbf\xc6\xa2\x1c\x82\
2015-11-11 23:02:44,233	DeviceIoControl	DeviceHandle: 0x00000044 OutBuffer: %o\x8d\xba~y$#$\xb5\xa1\xd3\ IoControlCode: 3735560 InBuffer: \x960\xeak\xe9\xda\x0b \xc3\x7f\xd5<\x7f\xbf\xc6\xa2\x1c\x82\
2015-11-11 23:02:44,233	DeviceIoControl	DeviceHandle: 0x00000044 OutBuffer: \x91$L\x8a\xfe(\xf4\xb7]J\xf IoControlCode: 3735560 InBuffer: \x960\xeak\xe9\xda\x0b \xc3\x7f\xd5<\x7f\xbf\xc6\xa2\x1c\x82\
2015-11-11 23:02:44,233	DeviceIoControl	DeviceHandle: 0x00000044 OutBuffer: \x8dr\xb9\xf3\xab\x10\x1a,\x IoControlCode: 3735560 InBuffer: \x960\xeak\xe9\xda\x0b \xc3\x7f\xd5<\x7f\xbf\xc6\xa2\x1c\x82\
2015-11-11 23:02:44,233	DeviceIoControl	DeviceHandle: 0x00000044 OutBuffer: \x15Y JVp~\x8fe\xd2x\x1b\x7f IoControlCode: 3735560 InBuffer: \x960\xeak\xe9\xda\x0b \xc3\x7f\xd5<\x7f\xbf\xc6\xa2\x1c\x82\
2015-11-11 23:02:44,233	LdrLoadDll	Flags: 1242952 BaseAddress: 0x5ad70000 FileName: C:\WINDOWS\system32\uxtheme.
2015-11-11 23:02:44,233	IsDebuggerPresent	
2015-11-11 23:02:44,233	LdrLoadDll	Flags: 1242772 BaseAddress: 0x5ad70000 FileName: uxtheme.dll
2015-11-11 23:02:44,233	GetSystemMetrics	SystemMetricIndex: 31
2015-11-11 23:02:44,233	ZwMapViewOfSection	SectionOffset: 0x0012f57c SectionHandle: 0x00000088 ProcessHandle: 0xffffffff BaseAddress: 0x00b80000
2015-11-11 23:02:44,233	GetSystemMetrics	SystemMetricIndex: 31
2015-11-11 23:02:44,233	LdrLoadDll	Flags: 1242956 BaseAddress: 0x74720000 FileName: C:\WINDOWS\system32\MSCTF.dl
2015-11-11 23:02:44,233	NtCreateMutant	Handle: 0x000000ac InitialOwner: 0 MutexName: CTF.TimListCache.FMPDefau
2015-11-11 23:02:44,243	NtOpenSection	DesiredAccess: 0x000f001f ObjectAttributes: C:\ntdll SectionHandle: 0x000000b0
2015-11-11 23:02:44,243	ZwMapViewOfSection	SectionOffset: 0x0012f278 SectionHandle: 0x000000b0 ProcessHandle: 0xffffffff BaseAddress: 0x00bd0000

2015-11-11 23:02:44,243	SetWindowsHookExA	ProcedureAddress: 0x747307c3 HookIdentifier: 2 ModuleAddress: 0x74720000 ThreadId: 452
2015-11-11 23:02:44,243	SetWindowsHookExA	ProcedureAddress: 0x747304cd HookIdentifier: 7 ModuleAddress: 0x74720000 ThreadId: 452
2015-11-11 23:02:44,243	LdrGetDllHandle	ModuleHandle: 0x00000000 FileName: SHFOLDER
2015-11-11 23:02:44,243	LdrLoadDll	Flags: 1244616 BaseAddress: 0x76780000 FileName: SHFOLDER
2015-11-11 23:02:44,243	LdrGetProcedureAddress	Ordinal: 0 FunctionName: SHGetFolderPathA FunctionAddress: 0x7678145d ModuleHandle: 0x76780000
2015-11-11 23:02:44,243	LdrLoadDll	Flags: 1242028 BaseAddress: 0x774e0000 FileName: ole32.dll
2015-11-11 23:02:44,243	LdrGetProcedureAddress	Ordinal: 0 FunctionName: CreateBindCtx FunctionAddress: 0x774fe54c ModuleHandle: 0x774e0000
2015-11-11 23:02:44,243	RegOpenKeyExW	Handle: 0x00000000 Registry: 0x80000002 SubKey: Software\Microsoft\Windows\Cur
2015-11-11 23:02:44,243	RegOpenKeyExW	Handle: 0x000000b4 Registry: 0x80000001 SubKey: Software\Microsoft\Windows\Cur
2015-11-11 23:02:44,243	RegQueryValueExW	Handle: 0x000000b4 DataLength: 4 ValueName: NoNetHood Type: 1241524
2015-11-11 23:02:44,243	RegCloseKey	Handle: 0x000000b4
2015-11-11 23:02:44,243	RegOpenKeyExW	Handle: 0x00000000 Registry: 0x80000002 SubKey: Software\Microsoft\Windows\Cur
2015-11-11 23:02:44,243	RegOpenKeyExW	Handle: 0x000000b4 Registry: 0x80000001 SubKey: Software\Microsoft\Windows\Cur
2015-11-11 23:02:44,243	RegQueryValueExW	Handle: 0x000000b4 DataLength: 4 ValueName: NoPropertiesMyComputer Type: 1241524
2015-11-11 23:02:44,243	RegCloseKey	Handle: 0x000000b4
2015-11-11 23:02:44,243	RegOpenKeyExW	Handle: 0x00000000 Registry: 0x80000002 SubKey: Software\Microsoft\Windows\Cur
2015-11-11 23:02:44,243	RegOpenKeyExW	Handle: 0x000000b4 Registry: 0x80000001 SubKey: Software\Microsoft\Windows\Cur

2015-11-11 23:02:44,243	RegQueryValueExW	Handle: 0x000000b4 DataLength: 4 ValueName: NoInternetIcon Type: 1241524
2015-11-11 23:02:44,243	RegCloseKey	Handle: 0x000000b4
2015-11-11 23:02:44,243	RegOpenKeyExA	Handle: 0x00000000 Registry: 0x80000002 SubKey: SOFTWARE\Microsoft\Windows\Cur
2015-11-11 23:02:44,243	LdrGetProcedureAddress	Ordinal: 236 FunctionName: FunctionAddress: 0x773e1798 ModuleHandle: 0x773d0000
2015-11-11 23:02:44,243	LdrGetDllHandle	ModuleHandle: 0x774e0000 FileName: OLE32.DLL
2015-11-11 23:02:44,243	LdrGetProcedureAddress	Ordinal: 0 FunctionName: CoGetMalloc FunctionAddress: 0x774fdd08 ModuleHandle: 0x774e0000
2015-11-11 23:02:44,243	RegOpenKeyExW	Handle: 0x00000000 Registry: 0x80000002 SubKey: Software\Microsoft\Windows\Cur
2015-11-11 23:02:44,243	RegOpenKeyExW	Handle: 0x000000b4 Registry: 0x80000001 SubKey: Software\Microsoft\Windows\Cur
2015-11-11 23:02:44,243	RegQueryValueExW	Handle: 0x000000b4 DataLength: 4 ValueName: NoCommonGroups Type: 1241524
2015-11-11 23:02:44,243	RegCloseKey	Handle: 0x000000b4
2015-11-11 23:02:44,243	RegOpenKeyExA	Handle: 0x00000000 Registry: 0x80000002 SubKey: SOFTWARE\Microsoft\Windows\Cur
2015-11-11 23:02:44,243	RegOpenKeyExW	Handle: 0x00000000 Registry: 0x80000002 SubKey: Software\Microsoft\Windows\Cur
2015-11-11 23:02:44,243	RegOpenKeyExW	Handle: 0x000000b4 Registry: 0x80000001 SubKey: Software\Microsoft\Windows\Cur
2015-11-11 23:02:44,243	RegQueryValueExW	Handle: 0x000000b4 DataLength: 4 ValueName: NoControlPanel Type: 1239876
2015-11-11 23:02:44,243	RegCloseKey	Handle: 0x000000b4
2015-11-11 23:02:44,243	RegOpenKeyExW	Handle: 0x00000000 Registry: 0x80000002 SubKey: Software\Microsoft\Windows\Cur
2015-11-11 23:02:44,243	RegOpenKeyExW	Handle: 0x000000b4 Registry: 0x80000001 SubKey: Software\Microsoft\Windows\Cur
		Handle: 0x000000b4

2015-11-11 23:02:44,243	RegQueryValueExW	DataLength: 4 ValueName: NoSetFolders Type: 1239876
2015-11-11 23:02:44,243	RegCloseKey	Handle: 0x000000b4
2015-11-11 23:02:44,243	RegOpenKeyExA	Handle: 0x000000be Registry: 0x80000000 SubKey: CLSID\{20D04FE0-3AEA-1069-A2D8
2015-11-11 23:02:44,243	RegQueryValueExW	Handle: 0x000000be Data: %\x00S\x00y\x00s\x00t\x00e\x00m\ ValueName:
2015-11-11 23:02:44,243	LdrLoadDll	Flags: 1240456 BaseAddress: 0x7c9c0000 FileName: C:\WINDOWS\system32\SHELL32.
2015-11-11 23:02:44,243	RegCloseKey	Handle: 0x000000be
2015-11-11 23:02:44,243	LdrGetProcedureAddress	Ordinal: 328 FunctionName: FunctionAddress: 0x773e1559 ModuleHandle: 0x773d0000
2015-11-11 23:02:44,243	LdrLoadDll	Flags: 1241248 BaseAddress: 0x77920000 FileName: SETUPAPI.dll
2015-11-11 23:02:44,243	LdrGetProcedureAddress	Ordinal: 0 FunctionName: CM_Get_Device_Interfac FunctionAddress: 0x77929025 ModuleHandle: 0x77920000
2015-11-11 23:02:44,243	LookupPrivilegeValueW	SystemName: PrivilegeName: SeLoadDriverPrivilege
2015-11-11 23:02:44,243	LookupPrivilegeValueW	SystemName: PrivilegeName: SeUndockPrivilege
2015-11-11 23:02:44,243	LdrGetProcedureAddress	Ordinal: 0 FunctionName: CM_Get_Device_Interfac FunctionAddress: 0x7792a15c ModuleHandle: 0x77920000
2015-11-11 23:02:44,243	NtOpenFile	ShareAccess: 3 FileName: IDE#CdRomVBOX_CD-ROM_____ DesiredAccess: 0x00100080 FileHandle: 0x000000e8
2015-11-11 23:02:44,243	DeviceIoControl	DeviceHandle: 0x000000e8 OutBuffer: \x1c\x00\\x00D\x00e\x00v\x0(IoControlCode: 5046280 InBuffer:
2015-11-11 23:02:44,243	NtQueryInformationFile	FileHandle: 0xffffffff FileInformation: \x00\x00\x00\x00\x84\xe
2015-11-11 23:02:44,243	NtCreateFile	ShareAccess: 3 FileName: MountPointManager DesiredAccess: 0x00100080 CreateDisposition: 1 FileHandle: 0x000000e8
2015-11-11 23:02:44,243	DeviceIoControl	DeviceHandle: 0x000000e8 OutBuffer: \xea\x01\x00\x00\x02\x00\x0(IoControlCode: 7143432 InBuffer: \x00\x00\x00\x00\x00\x00\x00\x

2015-11-11 23:02:44,243	DeviceIoControl	DeviceHandle: 0x000000e8 OutBuffer: \xea\x01\x00\x00\x02\x00\x0 IoControlCode: 7143432 InBuffer: \x00\x00\x00\x00\x00\x00\x00\x
2015-11-11 23:02:44,243	RegOpenKeyExW	Handle: 0x000000e8 Registry: 0x80000001 SubKey: Software\Microsoft\Windows\Cur
2015-11-11 23:02:44,243	RegOpenKeyExW	Handle: 0x000000ec Registry: 0x000000e8 SubKey: {475c7950-e3d2-11e0-8d7a-806d6
2015-11-11 23:02:44,243	RegCloseKey	Handle: 0x000000e8
2015-11-11 23:02:44,243	RegQueryValueExW	Handle: 0x000000ec Data: ValueName: Data
2015-11-11 23:02:44,243	RegCloseKey	Handle: 0x000000ec
2015-11-11 23:02:44,243	RegOpenKeyExW	Handle: 0x000000ec Registry: 0x80000001 SubKey: Software\Microsoft\Windows\Cur
2015-11-11 23:02:44,243	RegOpenKeyExW	Handle: 0x000000e8 Registry: 0x000000ec SubKey: {475c7950-e3d2-11e0-8d7a-806d6
2015-11-11 23:02:44,243	RegCloseKey	Handle: 0x000000ec
2015-11-11 23:02:44,243	RegQueryValueExW	Handle: 0x000000e8 Data: 1 ValueName: Generation
2015-11-11 23:02:44,243	RegCloseKey	Handle: 0x000000e8
2015-11-11 23:02:44,243	LdrGetProcedureAddress	Ordinal: 334 FunctionName: FunctionAddress: 0x773e0f5a ModuleHandle: 0x773d0000
2015-11-11 23:02:44,243	NtOpenFile	ShareAccess: 3 FileName: STORAGE#Volume#1&30a96598&0& DesiredAccess: 0x00100080 FileHandle: 0x000000e8
2015-11-11 23:02:44,243	DeviceIoControl	DeviceHandle: 0x000000e8 OutBuffer: .\x00\\x00D\x00e\x00v\x00i\x IoControlCode: 5046280 InBuffer:
2015-11-11 23:02:44,243	NtQueryInformationFile	FileHandle: 0xffffffff FileInformation: \x00\x00\x00\x00\x84\xe
2015-11-11 23:02:44,243	NtCreateFile	ShareAccess: 3 FileName: MountPointManager DesiredAccess: 0x00100080 CreateDisposition: 1 FileHandle: 0x000000e8
2015-11-11 23:02:44,243	DeviceIoControl	DeviceHandle: 0x000000e8 OutBuffer: \xee\x00\x00\x00\x02\x00\x0 IoControlCode: 7143432 InBuffer: \x00\x00\x00\x00\x00\x00\x00\x

2015-11-11 23:02:44,243	DeviceIoControl	DeviceHandle: 0x000000e8 OutBuffer: \xee\x00\x00\x00\x02\x00\x0 IoControlCode: 7143432 InBuffer: \x00\x00\x00\x00\x00\x00\x00\x
2015-11-11 23:02:44,243	RegOpenKeyExW	Handle: 0x000000e8 Registry: 0x80000001 SubKey: Software\Microsoft\Windows\Cur
2015-11-11 23:02:44,243	RegOpenKeyExW	Handle: 0x000000ec Registry: 0x000000e8 SubKey: {475c7952-e3d2-11e0-8d7a-806d6
2015-11-11 23:02:44,243	RegCloseKey	Handle: 0x000000e8
2015-11-11 23:02:44,243	RegQueryValueExW	Handle: 0x000000ec Data: ValueName: Data
2015-11-11 23:02:44,243	RegCloseKey	Handle: 0x000000ec
2015-11-11 23:02:44,243	RegOpenKeyExW	Handle: 0x000000ec Registry: 0x80000001 SubKey: Software\Microsoft\Windows\Cur
2015-11-11 23:02:44,243	RegOpenKeyExW	Handle: 0x000000e8 Registry: 0x000000ec SubKey: {475c7952-e3d2-11e0-8d7a-806d6
2015-11-11 23:02:44,243	RegCloseKey	Handle: 0x000000ec
2015-11-11 23:02:44,243	RegQueryValueExW	Handle: 0x000000e8 Data: 1 ValueName: Generation
2015-11-11 23:02:44,243	RegCloseKey	Handle: 0x000000e8
2015-11-11 23:02:44,243	LdrGetProcedureAddress	Ordinal: 332 FunctionName: FunctionAddress: 0x773e0df4 ModuleHandle: 0x773d0000
2015-11-11 23:02:44,243	NtQueryInformationFile	FileHandle: 0xffffffff FileInformation:
2015-11-11 23:02:44,243	NtCreateFile	ShareAccess: 3 FileName: MountPointManager DesiredAccess: 0x00100080 CreateDisposition: 1 FileHandle: 0x000000e8

- 1
- 2
- 3
- ...
- 5

WINWORD.EXE, PID: 580, Parent PID: 1592

- 1
- 2
- 3
- ...
- 82

network filesystem registry process services synchronization

TIME	API	ARG
2015-11-11 23:02:44,453	LdrGetDllHandle	ModuleHandle: `0x7c800000` FileName: `KERNEL32.DLL`
2015-11-11 23:02:44,453	LdrGetProcedureAddress	Ordinal: `0` FunctionName: `DecodePointer` FunctionAddress: `0x7c913405` ModuleHandle: `0x7c800000`
2015-11-11 23:02:44,453	LdrGetDllHandle	ModuleHandle: `0x7c800000` FileName: `KERNEL32.DLL`
2015-11-11 23:02:44,453	LdrGetProcedureAddress	Ordinal: `0` FunctionName: `DecodePointer` FunctionAddress: `0x7c913405` ModuleHandle: `0x7c800000`
2015-11-11 23:02:44,453	LdrGetDllHandle	ModuleHandle: `0x7c800000` FileName: `KERNEL32.DLL`
2015-11-11 23:02:44,453	LdrGetProcedureAddress	Ordinal: `0` FunctionName: `EncodePointer` FunctionAddress: `0x7c9133df` ModuleHandle: `0x7c800000`
2015-11-11 23:02:44,463	LdrGetProcedureAddress	Ordinal: `0` FunctionName: `DecodePointer` FunctionAddress: `0x7c913405` ModuleHandle: `0x7c800000`
2015-11-11 23:02:44,463	LdrGetDllHandle	ModuleHandle: `0x7c800000` FileName: `KERNEL32.DLL`
2015-11-11 23:02:44,463	LdrGetProcedureAddress	Ordinal: `0` FunctionName: `DecodePointer` FunctionAddress: `0x7c913405` ModuleHandle: `0x7c800000`
2015-11-11 23:02:44,463	LdrGetDllHandle	ModuleHandle: `0x7c800000` FileName: `KERNEL32.DLL`
2015-11-11 23:02:44,463	LdrGetProcedureAddress	Ordinal: `0` FunctionName: `DecodePointer` FunctionAddress: `0x7c913405` ModuleHandle: `0x7c800000`
2015-11-11 23:02:44,463	LdrGetDllHandle	ModuleHandle: `0x7c800000` FileName: `KERNEL32.DLL`
2015-11-11 23:02:44,463	LdrGetProcedureAddress	Ordinal: `0` FunctionName: `EncodePointer` FunctionAddress: `0x7c9133df` ModuleHandle: `0x7c800000`
2015-11-11 23:02:44,463	LdrGetProcedureAddress	Ordinal: `0` FunctionName: `DecodePointer` FunctionAddress: `0x7c913405` ModuleHandle: `0x7c800000`
2015-11-11 23:02:44,463	LdrGetDllHandle	ModuleHandle: `0x7c800000` FileName: `kernel32.dll`
2015-11-11 23:02:44,463	LdrGetProcedureAddress	Ordinal: `0` FunctionName: `HeapSetInformation` FunctionAddress: `0x7c839481` ModuleHandle: `0x7c800000`

2015-11-11 23:02:44,463	VirtualProtectEx	Protection: 0x00000040 ProcessHandle: 0xffffffff Address: 0x30001634 Size: 0x00000004
2015-11-11 23:02:44,463	VirtualProtectEx	Protection: 0x00000020 ProcessHandle: 0xffffffff Address: 0x30001634 Size: 0x00000004
2015-11-11 23:02:44,473	LdrLoadDll	Flags: 1244912 BaseAddress: 0x31240000 FileName: wwlib.dll
2015-11-11 23:02:44,473	LdrGetProcedureAddress	Ordinal: 0 FunctionName: FMain FunctionAddress: 0x31244562 ModuleHandle: 0x31240000
2015-11-11 23:02:44,473	LdrGetProcedureAddress	Ordinal: 0 FunctionName: wdCommandDispatch FunctionAddress: 0x31621275 ModuleHandle: 0x31240000
2015-11-11 23:02:44,473	LdrGetProcedureAddress	Ordinal: 0 FunctionName: wdGetApplicationObject FunctionAddress: 0x315c1c06 ModuleHandle: 0x31240000
2015-11-11 23:02:44,473	RegOpenKeyExW	Handle: 0x000000a0 Registry: 0x80000002 SubKey: Software\Microsoft\Windows\Cur
2015-11-11 23:02:44,473	RegQueryValueExW	Handle: 0x000000a0 Data: C\x00:\x00\\x00P\x00r\x00o\x00g\ \x00F\x00i\x00l\x00e\x00s\x00\\x00C\x0 \x00F\x00i\x00l\x00e\x00s\x00\x00\x00 ValueName: CommonFilesDir
2015-11-11 23:02:44,473	RegCloseKey	Handle: 0x000000a0
2015-11-11 23:02:44,483	LdrLoadDll	Flags: 1242908 BaseAddress: 0x32600000 FileName: C:\Program Files\Common File
2015-11-11 23:02:44,483	LdrLoadDll	Flags: 1243328 BaseAddress: 0x32600000 FileName: MSO.dll
2015-11-11 23:02:44,483	LdrGetProcedureAddress	Ordinal: 8512 FunctionName: FunctionAddress: 0x32604ac0 ModuleHandle: 0x32600000
2015-11-11 23:02:44,483	RegOpenKeyExA	Handle: 0x00000000 Registry: 0x80000001 SubKey: SOFTWARE\Microsoft\Office Test
2015-11-11 23:02:44,483	LdrGetProcedureAddress	Ordinal: 6877 FunctionName: FunctionAddress: 0x32605108 ModuleHandle: 0x32600000
2015-11-11 23:02:44,483	LdrGetProcedureAddress	Ordinal: 9552 FunctionName: FunctionAddress: 0x32604a53 ModuleHandle: 0x32600000

2015-11-11 23:02:44,483	LdrLoadDll	Flags: 1243424 BaseAddress: 0x32600000 FileName: mso.dll
2015-11-11 23:02:44,483	VirtualProtectEx	Protection: 0x00000040 ProcessHandle: 0xffffffff Address: 0x7c8449fd Size: 0x00000005
2015-11-11 23:02:44,483	VirtualProtectEx	Protection: 0x00000020 ProcessHandle: 0xffffffff Address: 0x7c8449fd Size: 0x00000005
2015-11-11 23:02:44,483	LdrGetProcedureAddress	Ordinal: 597 FunctionName: FunctionAddress: 0x326065de ModuleHandle: 0x32600000
2015-11-11 23:02:44,483	LdrGetProcedureAddress	Ordinal: 1332 FunctionName: FunctionAddress: 0x32605f04 ModuleHandle: 0x32600000
2015-11-11 23:02:44,483	LdrGetProcedureAddress	Ordinal: 2352 FunctionName: FunctionAddress: 0x32604c4e ModuleHandle: 0x32600000
2015-11-11 23:02:44,483	RegOpenKeyExA	Handle: 0x00000000 Registry: 0x80000001 SubKey: Software\Microsoft\Office\12.0
2015-11-11 23:02:44,483	RegCreateKeyExA	Handle: 0x000000bc Access: 131103 Registry: 0x80000001 Class: SubKey: Software\Microsoft\Office\12.0
2015-11-11 23:02:44,483	RegQueryValueExA	Handle: 0x000000bc DataLength: 0 ValueName: ct> Type: 188
2015-11-11 23:02:44,483	RegSetValueExA	Handle: 0x000000bc Buffer: ValueName: ct> Type: 3
2015-11-11 23:02:44,483	RegCloseKey	Handle: 0x000000bc
2015-11-11 23:02:44,483	RegOpenKeyExA	Handle: 0x00000000 Registry: 0x80000001 SubKey: Software\Policies\Microsoft\Of
2015-11-11 23:02:44,483	RegOpenKeyExW	Handle: 0x000000bc Registry: 0x80000001 SubKey: Software\Microsoft\Office\Comm
2015-11-11 23:02:44,483	RegQueryValueExW	Handle: 0x000000bc DataLength: 4 ValueName: QMStrMax Type: 1243232
2015-11-11 23:02:44,483	RegOpenKeyExW	Handle: 0x000000c0 Registry: 0x80000002 SubKey: Software\Microsoft\SQMClient

2015-11-11 23:02:44,483	RegQueryValueExW	Handle: 0x000000c0 DataLength: 0 ValueName: CorporateSQMURL Type: 0
2015-11-11 23:02:44,483	RegQueryValueExW	Handle: 0x000000bc DataLength: 4 ValueName: QMStudyID Type: 1243188
2015-11-11 23:02:44,483	RegQueryValueExW	Handle: 0x000000bc DataLength: 4 ValueName: QMPersNum Type: 1243192
2015-11-11 23:02:44,483	RegOpenKeyExW	Handle: 0x000000c4 Registry: 0x80000002 SubKey: Software\Microsoft\Office\12.0
2015-11-11 23:02:44,483	RegQueryValueExW	Handle: 0x000000c4 Data: 1\x002\x00.\x000\x00.\x004\x005\x001\x ValueName: LastProduct
2015-11-11 23:02:44,483	LdrGetProcedureAddress	Ordinal: 1813 FunctionName: FunctionAddress: 0x32604be5 ModuleHandle: 0x32600000
2015-11-11 23:02:44,483	LdrGetProcedureAddress	Ordinal: 1608 FunctionName: FunctionAddress: 0x3260661f ModuleHandle: 0x32600000
2015-11-11 23:02:44,483	RegOpenKeyExW	Handle: 0x00000000 Registry: 0x80000001 SubKey: Software\Microsoft\Office\12.0
2015-11-11 23:02:44,483	LdrGetProcedureAddress	Ordinal: 1379 FunctionName: FunctionAddress: 0x32606da1 ModuleHandle: 0x32600000
2015-11-11 23:02:44,483	LdrGetDllHandle	ModuleHandle: 0x00000000 FileName: C:\Program Files\Common File Shared\office12\Cultures\office.odf
2015-11-11 23:02:44,483	NtCreateFile	ShareAccess: 5 FileName: C:\Program Files\Common File Shared\office12\Cultures\office.odf DesiredAccess: 0x80100080 CreateDisposition: 1 FileHandle: 0x000000cc
2015-11-11 23:02:44,483	NtCreateSection	ObjectAttributes: DesiredAccess: 0x000f0005 SectionHandle: 0x000000c8 FileHandle: 0x000000cc
2015-11-11 23:02:44,483	ZwMapViewOfSection	SectionOffset: 0x0012f208 SectionHandle: 0x000000c8 ProcessHandle: 0xffffffff BaseAddress: 0x00bf0000
2015-11-11 23:02:44,483	RegOpenKeyExW	Handle: 0x000000c8 Registry: 0x80000002

		SubKey: Software\Microsoft\Office\12.0
2015-11-11 23:02:44,483	RegQueryValueExW	Handle: 0x000000c8 Data: 1033 ValueName: SKULanguage
2015-11-11 23:02:44,483	RegOpenKeyExW	Handle: 0x000000cc Registry: 0x80000001 SubKey: Software\Microsoft\Office\12.0\Common\
2015-11-11 23:02:44,483	RegEnumValueW	Index: 0 Handle: 0x000000cc Data: O\x00n\x00\x00\x00 ValueName: 1033
2015-11-11 23:02:44,483	RegCreateKeyExW	Handle: 0x000000d0 Access: 131103 Registry: 0x80000001 Class: SubKey: Software\Microsoft\Office\12.0\Common\
2015-11-11 23:02:44,483	RegSetValueExW	Handle: 0x000000d0 Buffer: O\x00f\x00f\x00\x00\x00 ValueName: 1033 Type: 1
2015-11-11 23:02:44,483	RegCloseKey	Handle: 0x000000d0
2015-11-11 23:02:44,493	RegEnumValueW	Index: 1 Handle: 0x000000cc DataLength: 64 ValueName: 1033 Type: 1236152
2015-11-11 23:02:44,493	RegCloseKey	Handle: 0x000000cc
2015-11-11 23:02:44,493	RegOpenKeyExW	Handle: 0x000000cc Registry: 0x80000001 SubKey: Software\Microsoft\Office\12.0
2015-11-11 23:02:44,493	RegQueryValueExW	Handle: 0x000000cc Data: 1033 ValueName: InstallLanguage
2015-11-11 23:02:44,493	NtOpenKey	DesiredAccess: 131097 KeyHandle: 0x000000d0 ObjectAttributes: \Registry\Machine\System\CurrentContro
2015-11-11 23:02:44,493	NtOpenKey	DesiredAccess: 131097 KeyHandle: 0x000000d4 ObjectAttributes: \Registry\Machine\System\CurrentContro
2015-11-11 23:02:44,493	NtOpenKey	DesiredAccess: 131097 KeyHandle: 0x000000d8 ObjectAttributes: \Registry\Machine\System\CurrentContro
2015-11-11 23:02:44,493	NtEnumerateValueKey	Index: 0 KeyHandle: 0x000000d0 KeyValueInformationClass: 1
2015-11-11	NtEnumerateValueKey	Index: 1 KeyHandle: 0x000000d0

23:02:44,493		KeyValueInformationClass: 1
2015-11-11 23:02:44,493	NtEnumerateValueKey	Index: 2 KeyHandle: 0x000000d0 KeyValueInformationClass: 1
2015-11-11 23:02:44,493	NtEnumerateValueKey	Index: 3 KeyHandle: 0x000000d0 KeyValueInformationClass: 1
2015-11-11 23:02:44,493	NtEnumerateValueKey	Index: 4 KeyHandle: 0x000000d0 KeyValueInformationClass: 1
2015-11-11 23:02:44,493	NtEnumerateValueKey	Index: 5 KeyHandle: 0x000000d0 KeyValueInformationClass: 1
2015-11-11 23:02:44,493	NtEnumerateValueKey	Index: 6 KeyHandle: 0x000000d0 KeyValueInformationClass: 1
2015-11-11 23:02:44,493	NtEnumerateValueKey	Index: 7 KeyHandle: 0x000000d0 KeyValueInformationClass: 1
2015-11-11 23:02:44,493	NtEnumerateValueKey	Index: 8 KeyHandle: 0x000000d0 KeyValueInformationClass: 1
2015-11-11 23:02:44,493	NtEnumerateValueKey	Index: 9 KeyHandle: 0x000000d0 KeyValueInformationClass: 1
2015-11-11 23:02:44,493	NtEnumerateValueKey	Index: 10 KeyHandle: 0x000000d0 KeyValueInformationClass: 1
2015-11-11 23:02:44,493	NtEnumerateValueKey	Index: 11 KeyHandle: 0x000000d0 KeyValueInformationClass: 1
2015-11-11 23:02:44,493	NtEnumerateValueKey	Index: 12 KeyHandle: 0x000000d0 KeyValueInformationClass: 1
2015-11-11 23:02:44,493	NtEnumerateValueKey	Index: 13 KeyHandle: 0x000000d0 KeyValueInformationClass: 1
2015-11-11 23:02:44,493	NtEnumerateValueKey	Index: 14 KeyHandle: 0x000000d0 KeyValueInformationClass: 1
2015-11-11 23:02:44,493	NtEnumerateValueKey	Index: 15 KeyHandle: 0x000000d0 KeyValueInformationClass: 1
2015-11-11 23:02:44,493	NtEnumerateValueKey	Index: 16 KeyHandle: 0x000000d0 KeyValueInformationClass: 1
2015-11-11 23:02:44,493	NtEnumerateValueKey	Index: 17 KeyHandle: 0x000000d0 KeyValueInformationClass: 1
2015-11-11 23:02:44,493	NtEnumerateValueKey	Index: 18 KeyHandle: 0x000000d0 KeyValueInformationClass: 1

2015-11-11 23:02:44,493	NtEnumerateValueKey	Index: 19 KeyHandle: 0x000000d0 KeyValueInformationClass: 1
2015-11-11 23:02:44,493	NtEnumerateValueKey	Index: 20 KeyHandle: 0x000000d0 KeyValueInformationClass: 1
2015-11-11 23:02:44,493	NtEnumerateValueKey	Index: 21 KeyHandle: 0x000000d0 KeyValueInformationClass: 1
2015-11-11 23:02:44,493	NtEnumerateValueKey	Index: 22 KeyHandle: 0x000000d0 KeyValueInformationClass: 1
2015-11-11 23:02:44,493	NtEnumerateValueKey	Index: 23 KeyHandle: 0x000000d0 KeyValueInformationClass: 1
2015-11-11 23:02:44,493	NtEnumerateValueKey	Index: 24 KeyHandle: 0x000000d0 KeyValueInformationClass: 1
2015-11-11 23:02:44,493	NtEnumerateValueKey	Index: 25 KeyHandle: 0x000000d0 KeyValueInformationClass: 1
2015-11-11 23:02:44,493	NtEnumerateValueKey	Index: 26 KeyHandle: 0x000000d0 KeyValueInformationClass: 1

- 1
- 2
- 3
- ...
- 82

- Domains (0)
- Hosts (0)
- HTTP (0)
- IRC (0)
- SMTP (0)

Domains

No domains contacted.

Hosts

No hosts contacted.

HTTP Requests

No HTTP requests performed.

IRC Traffic

No IRC traffic.

SMTP Requests

No SMTP requests performed.

FILE NAME	System.dll
FILE SIZE	11264 bytes
FILE TYPE	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	a436db0c473a087eb61ff5c53c34ba27
SHA1	65ea67e424e75f5065132b539c8b2eda88aa0506
SHA256	75ed40311875312617d6711baed0be29fcaee71031ca27a8d308a72b15
CRC32	C8485E15
SSDEEP	192:aVL7iZJX76BisO7+UZEw+Rl59pV8ghsVJ39dx8T:d7NsOpZsfLMJ39e
YARA	None matched

FILE NAME	nsn1.tmp
FILE SIZE	0 bytes
FILE TYPE	empty
MD5	d41d8cd98f00b204e9800998ecf8427e
SHA1	da39a3ee5e6b4b0d3255bfef95601890afd80709
SHA256	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852
CRC32	00000000
SSDEEP	3::
YARA	None matched

Bummer! No comments yet.

You have to login to comment.

Back to the top