ANY RUN
Interactive malware hunting service

General Info

File name emotet.doc
Full analysis
Verdict Malicious activity
Threats: Emotet

Emotet is one of the most dangerous trojans ever created. Over the course of its lifetime, it was upgraded to become a very destructive malware. It targets mostly corporate victims but even private users get infected in mass spam email campaigns.

Malware Trends Tracker More details

Analysis date 9/16/2019, 13:54:48
OS: Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Tags: macros | macros-on-open | emotet-doc | emotet | generated-doc | trojan | loader
Indicators:

MIME: application/vnd.openxmlformats-officedocument.wordprocessingml.document
File info: Microsoft Word 2007+
MD5 B92021CA10AED3046FC3BE5AC1C2A094
SHA1 0FB1AD5B53CDD09A7268C823EC796A6E623F086F
SHA256 C378387344E0A552DC065DE6BFA607FD26E0B5C569751C79FBF9C6F2E91C9807
SSDEEP 3072:/MSKNOK2ER/YR5DPQKAJNDU1CKBWN0PQJFWSQ:ZKOROKDPQZQQKMN0SCR

TAKE YOUR SECURITY TO THE NEXT LEVEL

- ✓ Realtime interaction
- ✓ Process monitoring
- ✓ Network tracking
- ✓ Inspect behavior graph
- ✓ IOC gathering

JOIN FREE!
with ANY.RUN Community Version

Behavior activities

Application was dropped or rewritten from another process
- easywindow.exe (PID: 2936)
- easywindow.exe (PID: 3872)
- 284.exe (PID: 3900)
- easywindow.exe (PID: 2820)
- 284.exe (PID: 2652)
- 284.exe (PID: 2604)
- 284.exe (PID: 3808)
- easywindow.exe (PID: 3560)

Downloads executable files from the Internet
- powershell.exe (PID: 2748)

EMOTET was detected
- easywindow.exe (PID: 3560)

Emotet process was detected
- 284.exe (PID: 2652)

Connects to CnC server
- easywindow.exe (PID: 3560)

Application launched itself
- easywindow.exe (PID: 2936)

Starts itself from another location
- 284.exe (PID: 2652)

Executable content was dropped or overwritten
- powershell.exe (PID: 2748)
- 284.exe (PID: 2652)

Creates files in the user directory
- powershell.exe (PID: 2748)

PowerShell script executed
- powershell.exe (PID: 2748)

Connects to server without host name
- easywindow.exe (PID: 3560)

Executed via WMI
- powershell.exe (PID: 2748)

Creates files in the user directory
- WINWORD.EXE (PID: 2848)

Reads Microsoft Office registry keys
- WINWORD.EXE (PID: 2848)

Static information

TRiD

.docm | Word Microsoft Office Open XML Format document (with Macro) (53.6%)
.docx | Word Microsoft Office Open XML Format document (24.2%)
.zip | Open Packaging Conventions container (18%)
.zip | ZIP compressed archive (4.1%)

EXIF

XML

AppVersion:	16
HyperlinksChanged:	No
SharedDoc:	No
CharactersWithSpaces:	445
LinksUpToDate:	No
Company:	*null*
ScaleCrop:	No
Paragraphs:	1
Lines:	3
DocSecurity:	None
Application:	Microsoft Office Word
Characters:	380
Words:	66
Pages:	1
TotalEditTime:	*null*
Template:	Normal.dotm
ModifyDate:	2019:09:16 12:22:00Z
CreateDate:	2019:09:16 12:22:00Z
RevisionNumber:	1
LastModifiedBy:	*null*
Keywords:	*null*

XMP

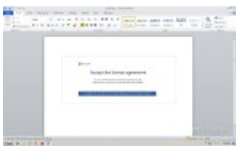
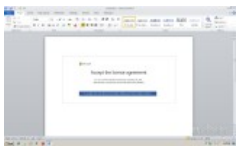
Description:	*null*
Creator:	*null*
Subject:	*null*
Title:	*null*

ZIP

ZipFileName:	[Content_Types].xml
ZipUncompressedSize:	3939
ZipCompressedSize:	524
ZipCRC:	0x247a0b47
ZipModifyDate:	1980:01:01 00:00:00
ZipCompression:	Deflated
ZipBitFlag:	0x0006
ZipRequiredVersion:	20

Video and screenshots

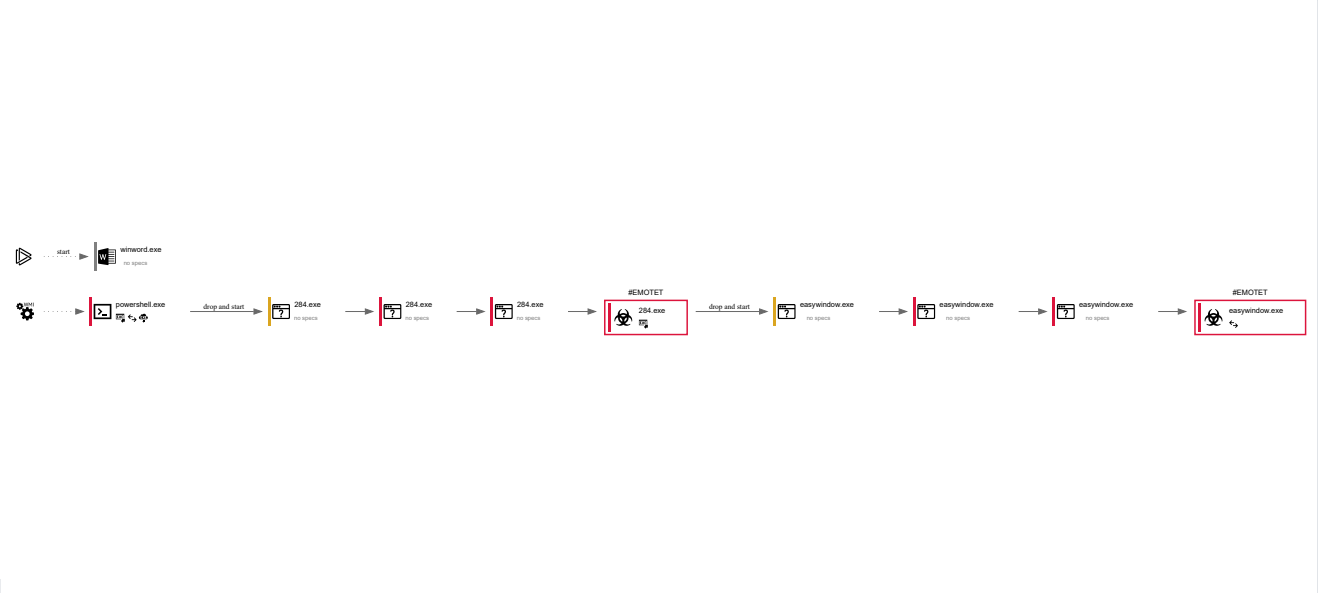


Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
44	10	7	2

Behavior graph



Registry activity

Total events	Read events	Write events	Delete events
2093	0	763	1

Modification events

PID	Process	Operation	Key	Name	Value
2848	WINWORD.EXE	delete key	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems		
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems	d`!	64602100200B0000010000000000000000000000
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages	1033	Off
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages	1033	On
2848	WINWORD.EXE	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000000000000F01FEC\Usage	WORDFiles	1328545822
2848	WINWORD.EXE	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000000000000F01FEC\Usage	ProductFiles	1328545936
2848	WINWORD.EXE	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000000000000F01FEC\Usage	ProductFiles	1328545937
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word	MTTT	200B00006E190A58966CD50100000000

2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems	;a!	
3B612100200B0000040000000000000008C0000000100000084000003E0043003A005C00550073006500720073005C00610064006D0069006E005C0041007000700440061007400610 05C0052006F0061006D0069006E0067005C004D006900630072006F0073006F00660074005C00540065006D0070006C006100740065007300 5C004E006F0072006D0061006C002E0064006F0074006D00000000000000					
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap	UNCAsIntranet	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap	AutoDetect	1
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems	5b!	
35622100200B0000060000000100000006A000000020000005A000000040000006300 3A005C00750073006500720073005C00610064006D0069006E005C006100700070006400610 0740061005C006C006F00630061006C005C00740065006D0070005C0065006D006F007400650074002E0064006F006300000000000000					
2848	WINWORD.EXE	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000000000000F01FEC\Usage	ProductFiles	1328545938
2848	WINWORD.EXE	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000000000000F01FEC\Usage	ProductFiles	1328545939
2848	WINWORD.EXE	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109E60090400000000000F01FEC\Usage	TCWP5FilesIntl_1033	1328545793
2848	WINWORD.EXE	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109E60090400000000000F01FEC\Usage	TCWP6FilesIntl_1033	1328545793
2848	WINWORD.EXE	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109E60090400000000000F01FEC\Usage	TCWP5FilesIntl_1033	1328545794
2848	WINWORD.EXE	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109E60090400000000000F01FEC\Usage	TCWP6FilesIntl_1033	1328545794
2848	WINWORD.EXE	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109E60090400000000000F01FEC\Usage	TCWP5FilesIntl_1033	1328545795
2848	WINWORD.EXE	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109E60090400000000000F01FEC\Usage	TCWP6FilesIntl_1033	1328545795
2848	WINWORD.EXE	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000000000000F01FEC\Usage	VBAFiles	1328545796
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{04598FC4-866C-11CF-AB7C-00AA00C08FCF}		ICommandButton
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{79176FB3-B7F2-11CE-97EF-00AA006D2776}		ISpinbutton
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{5512D111-5CC6-11CF-8D67-00AA00BDCE1D}		IWHTMLSubmitButton
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{5512D115-5CC6-11CF-8D67-00AA00BDCE1D}		IWHTMLReset
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{5512D11B-5CC6-11CF-8D67-00AA00BDCE1D}		IWHTMLText
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{7B020EC1-AF6C-11CE-9F46-00AA00574A4F}		CommandButtonEvents
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{8BD21D42-EC42-11CE-9E0D-00AA006002F3}		MdcCheckBoxEvents
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{8BD21D62-EC42-11CE-9E0D-00AA006002F3}		MdcToggleButtonEvents
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{7B020EC7-AF6C-11CE-9F46-00AA00574A4F}		TabStripEvents
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{4C5992A5-6926-101B-9992-00000B65C6F9}		ImageEvents
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{47FF8FE0-6198-11CF-8CE8-00AA006CB389}		WHTMLControlEvents1

2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{47FF8FE2-6198-11CF-8CE8-00AA006CB389}		WHTMLControlEvents3
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{47FF8FE5-6198-11CF-8CE8-00AA006CB389}		WHTMLControlEvents6
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{47FF8FE8-6198-11CF-8CE8-00AA006CB389}		WHTMLControlEvents9
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{04598FC9-866C-11CF-AB7C-00AA00C08FCF}		IMultiPage
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\16A638	16A638	

04000000200B00002C00000043003A005C0055007300650072007300 5C00610064006D0069006E005C0041007000700044006100740061005C004C006F00630061
006C005C00540065006D0070005C0065006D006F007400650074002E0064006F0063000A00000065006D006F007400650074002E0064006F006300000000000100
0000000000052CBFB57966CD50138A6160038A616000000000DB040000000000000000000000000000000000000000000000000000000FFFFFFFF00000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000FFFFFFFF

2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Courier New	02070309020205020404
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	MS Mincho	02020609040205080304
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	MS Gothic	020B0609070205080204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Angsana New	02020603050405020304
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Sylfaen	010A0502050306030303
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	@BatangChe	02030609000101010101
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	DaunPenh	01010101010101010101
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Euphemia	020B0503040102020104
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	MingLiU-ExtB	02020500000000000000
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	MingLiU_HKSCS-ExtB	02020500000000000000
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	MS PGothic	020B0600070205080204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	@MS Mincho	02020609040205080304
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	SimSun-ExtB	02010609060101010101
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Aparajita	020B0604020202020204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Leelawadee	020B0502040204020203
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Vijaya	020B0604020202020204

2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Simplified Arabic Fixed	02070309020205020404
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	David	020E0502060401010101
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Miriam Fixed	020B0509050101010101
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	@FangSong	02010609060101010101
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	AngsanaUPC	02020603050405020304
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	DilleniaUPC	02020603050405020304
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	JasmineUPC	02020603050405020304
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	@DFKai-SB	03000509000000000000
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Comic Sans MS	030F0702030302020204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Franklin Gothic Medium	020B0603020102020204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Segoe Print	02000600000000000000
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	MT Extra	05050102010205020202
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Book Antiqua	02040602050305030304
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Arial Narrow	020B0606020202030204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Baskerville Old Face	02020602080505020303
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Bernard MT Condensed	02050806060905020404
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Brush Script MT	03060802040406070304
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Colonna MT	04020805060202030203
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Harlow Solid Italic	04030604020F02020D02
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Juice ITC	04040403040A02020202
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Lucida Calligraphy	03010101010101010101
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Mistral	03090702030407020403
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Old English Text MT	03040902040508030806
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Showcard Gothic	04020904020102020604
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Tempus Sans ITC	04020404030D07020202
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Wide Latin	020A0A07050505020404
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Rockwell Extra Bold	02060903040505020403
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Pristina	03060402040406080204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU	Max Display	25
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Palace Script MT	030303020206070C0B05

2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Lucida Sans	020B0602030504020204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Gloucester MT Extra Condensed	02030808020601010101
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Gill Sans MT	020B0502020104020203
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Franklin Gothic Medium Cond	020B0606030402020204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Eras Demi ITC	020B0805030504020804
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Edwardian Script ITC	030303020407070D0804
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Century Schoolbook	02040604050505020304
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Bookman Old Style	02050604050505020204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Blackadder ITC	04020505051007020D02
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	MS Reference Sans Serif	020B0604030504040204
2848	WINWORD.EXE	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00000000000F01FEC\Usage	SpellingAndGrammarFiles_3082	1328545833
2848	WINWORD.EXE	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00000000000F01FEC\Usage	SpellingAndGrammarFiles_3082	1328545834
2848	WINWORD.EXE	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00000000000F01FEC\Usage	SpellingAndGrammarFiles_1033	1328545854
2848	WINWORD.EXE	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400000000000F01FEC\Usage	SpellingAndGrammarFiles_1033	1328545854
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\ReviewCycle	ReviewToken	{FAA2A2CD-3F26-49FF-A8EA-D0F9692FAC7E}
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU	Max Display	25
2848	WINWORD.EXE	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400000000000F01FEC\Usage	SpellingAndGrammarFiles_1033	1328545856
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Licensing	019C826E445A4649A5B00BF08FCC4EEE	

0100000027000007B39303134303030302D303033442D303030302D303030302D303030303030304646314345 7D005A0000004F006600660069006300650020003 10034002C0020004F006600660069006300650050007 2006F006600650073007300690006F006E0061006C002D005200650074006100690006C002000650064006900 740069006F006E000000

2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\TypeLib\{5829F2E4-E9DA-42FC-BF4E-6519475DD7DB}\2.0\HELPDIR	C:\Users\admin\AppData\Local\Temp\Word8.0
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{82B02371-B5BC-11CF-810F-00A0C9030074}	IReturnBoolean
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{04598FC6-866C-11CF-AB7C-00AA00C08FCF}	IControl
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{29B86A70-F52E-11CE-9BCE-00AA00608E01}	IOptionFrame
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{04598FC1-866C-11CF-AB7C-00AA00C08FCF}	ILabelControl
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{8BD21D33-EC42-11CE-9E0D-00AA006002F3}	IMdcCombo
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{04598FC8-866C-11CF-AB7C-00AA00C08FCF}	_UserForm
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{5B9D8FC8-4A71-101B-97A6-00000B65C08B}	FormEvents
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{8BD21D13-EC42-11CE-9E0D-00AA006002F3}	IMdcText
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{8BD21D63-EC42-11CE-9E0D-00AA006002F3}	IMdcToggleButton

2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{A38BFFC3-A5A0-11CE-8107-00AA00611080}		Tab
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{04598FC2-866C-11CF-AB7C-00AA00C08FCF}		ITabStrip
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{5512D119-5CC6-11CF-8D67-00AA00BDCE1D}		IWHTMLOption
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{5512D123-5CC6-11CF-8D67-00AA00BDCE1D}		IWHTMLSelect
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{8BD21D12-EC42-11CE-9E0D-00AA006002F3}		MdcTextEvents
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{92E11A03-7358-11CE-80CB-00AA00611080}		Pages
2848	WINWORD.EXE	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400000000000F01FEC\Usage	SpellingAndGrammarFiles_1033	1328545860
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\TypeLib\{5829F2E4-E9DA-42FC-BF4E-6519475DD7DB}\2.0		Microsoft Forms 2.0 Object Library
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\TypeLib\{5829F2E4-E9DA-42FC-BF4E-6519475DD7DB}\2.0\FLAGS		6
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\TypeLib\{5829F2E4-E9DA-42FC-BF4E-6519475DD7DB}\2.0\0\win32		
C:\Users\admin\AppData\Local\Temp\Word8.0\MSForms.exd					
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{BEF6E003-A874-101A-8BBA-00AA00300CAB}		Font
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{EC72F590-F375-11CE-B9E8-00AA006B1A69}		IDataAutoWrapper
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{82B02370-B5BC-11CF-810F-00A0C9030074}		IReturnInteger
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{82B02372-B5BC-11CF-810F-00A0C9030074}		IReturnString
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{8A683C90-BA84-11CF-8110-00A0C9030074}		IReturnSingle
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{8BD21D43-EC42-11CE-9E0D-00AA006002F3}		IMdcCheckBox
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{04598FC3-866C-11CF-AB7C-00AA00C08FCF}		IScrollbar
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{944ACF93-A1E6-11CE-8104-00AA00611080}		Tabs
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{5512D11F-5CC6-11CF-8D67-00AA00BDCE1D}		IWHTMLPassword
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{978C9E22-D4B0-11CE-BF2D-00AA003F40D0}		LabelControlEvents
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{8BD21D22-EC42-11CE-9E0D-00AA006002F3}		MdcListEvents
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{8BD21D32-EC42-11CE-9E0D-00AA006002F3}		MdcComboEvents
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{8BD21D52-EC42-11CE-9E0D-00AA006002F3}		MdcOptionButtonEvents
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{7B020EC2-AF6C-11CE-9F46-00AA00574A4F}		ScrollbarEvents
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{79176FB2-B7F2-11CE-97EF-00AA006D2776}		SpinbuttonEvents
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{796ED650-5FE9-11CF-8D68-00AA00BDCE1D}		WHTMLControlEvents
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{47FF8FE1-6198-11CF-8CE8-00AA006CB389}		WHTMLControlEvents2
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{47FF8FE3-6198-11CF-8CE8-00AA006CB389}		WHTMLControlEvents4
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{47FF8FE4-6198-11CF-8CE8-00AA006CB389}		WHTMLControlEvents5

2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{47FF8FE6-6198-11CF-8CE8-00AA006CB389}		WHTMLControlEvents7
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{47FF8FE9-6198-11CF-8CE8-00AA006CB389}		WHTMLControlEvents10
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{7B020EC8-AF6C-11CE-9F46-00AA00574A4F}		MultiPageEvents
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{8A683C91-BA84-11CF-8110-00A0C9030074}		IReturnEffect
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{04598FC7-866C-11CF-AB7C-00AA00C08FCF}		Controls
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{9A4BBF53-4E46-101B-8BBD-00AA003E3B29}		ControlEvents
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{CF3F94A0-F546-11CE-9BCE-00AA00608E01}		OptionFrameEvents
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{8BD21D23-EC42-11CE-9E0D-00AA006002F3}		IMdcList
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{8BD21D53-EC42-11CE-9E0D-00AA006002F3}		IMdcOptionButton
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{4C599243-6926-101B-9992-00000B65C6F9}		IImage
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{5512D113-5CC6-11CF-8D67-00AA00BDCE1D}		IWHTMLImage
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{5512D117-5CC6-11CF-8D67-00AA00BDCE1D}		IWHTMLCheckbox
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{5512D11D-5CC6-11CF-8D67-00AA00BDCE1D}		IWHTMLHidden
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{5512D125-5CC6-11CF-8D67-00AA00BDCE1D}		IWHTMLTextArea
2848	WINWORD.EXE	write	HKEY_CLASSES_ROOT\Interface\{5CEF5613-713D-11CE-80C9-00AA00611080}		IPage
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	SimSun	02010600030101010101
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	SimHei	02010609060101010101
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Mangal	02040503050203030202
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Raavi	020B0502040204020203
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Tunga	020B0502040204020203
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Cambria Math	02040503050406030204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Tahoma	020B0604030504040204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	BatangChe	02030609000101010101
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	@Gungsuh	02030600000101010101
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	@GungsuhChe	02030609000101010101
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	DokChampa	020B0604020202020204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	@Gulim	020B0600000101010101
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Khmer UI	020B0502040204020203
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Lao UI	020B0502040204020203
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	@Malgun Gothic	020B0503020000020004

2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Microsoft JhengHei	020B0604030504040204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Microsoft YaHei	020B0503020204020204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	@MingLiU	02020509000000000000
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	MingLiU_HKSCS	02020500000000000000
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	PMingLiU-ExtB	02020500000000000000
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Mongolian Baiti	03000500000000000000
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	MS UI Gothic	020B0600070205080204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Shonar Bangla	020B0502040204020203
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Ebrima	02000000000000000000
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	MoolBoran	020B0100010101010101
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Arabic Typesetting	03020402040406030203
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Traditional Arabic	02020603050405020304
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Levenim MT	02010502060101010101
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Rod	02030509050101010101
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	KaiTi	02010609060101010101
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	BrowalliaUPC	020B0604020202020204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	FreesiaUPC	020B0604020202020204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	LilyUPC	020B0604020202020204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Wingdings	05000000000000000000
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	PMingLiU	02020500000000000000
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	MingLiU	02020509000000000000
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Gulim	020B0600000101010101
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Century	02040604050505020304
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Latha	020B0604020202020204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Shruti	020B0502040204020203
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Gautami	020B0502040204020203
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Estrangelo Edessa	03080600000000000000
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	@Batang	02030600000101010101
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Gungsuh	02030600000101010101
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	GulimChe	020B0609000101010101

2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	@Meiryo	020B0604030504040204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	@Meiryo UI	020B0604030504040204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Arial	020B0604020202020204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Symbol	05050102010706020507
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Batang	02030600000101010101
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Dotum	020B0600000101010101
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Cordia New	020B0304020202020204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Vrinda	020B0502040204020203
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Arial Unicode MS	020B0604020202020204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Marlett	0000000000000000000
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	GungsuhChe	02030609000101010101
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Vani	020B0502040204020203
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	@GulimChe	020B0609000101010101
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	@Dotum	020B0600000101010101
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	DotumChe	020B0609000101010101
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	@DotumChe	020B0609000101010101
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Impact	020B0806030902050204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Iskoola Pota	020B0502040204020203
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Kalinga	020B0502040204020203
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Kartika	02020503030404060203
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Lucida Console	020B0609040504020204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Malgun Gothic	020B0503020000020004
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Meiryo	020B0604030504040204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Meiryo UI	020B0604030504040204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Microsoft Himalaya	01010100010101010101
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	@Microsoft JhengHei	020B0604030504040204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	@Microsoft YaHei	020B0503020204020204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	@PMingLiU	02020500000000000000
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	@MingLiU-ExtB	02020500000000000000
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	@MingLiU_HKSCS-ExtB	02020500000000000000

2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	@MS PGothic	020B0600070205080204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	MS PMincho	02020600040205080304
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	@MS PMincho	02020600040205080304
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	MV Boli	02000500030200090000
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Microsoft New Tai Lue	020B0502040204020203
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Nyala	02000504070300020003
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Microsoft PhagsPa	020B0502040204020203
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Plantagenet Cherokee	02020602070100000000
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Segoe Script	020B0504020000000003
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Segoe UI	020B0502040204020203
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Segoe UI Semibold	020B0702040204020203
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Segoe UI Light	020B0502040204020203
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Segoe UI Symbol	020B0502040204020203
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	@SimSun-ExtB	02010609060101010101
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Microsoft Yi Baiti	03000500000000000000
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Gisha	020B0502040204020203
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Microsoft Uighur	02000000000000000000
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Andalus	02020603050405020304
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Sakkal Majalla	02000000000000000000
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	FrankRuehl	020E0503060101010101
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Narkisim	020E0502050101010101
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Arial Black	020B0A04020102020204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Corbel	020B0503020204020204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Palatino Linotype	02040502050505030304
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Webdings	05030102010509060703
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Wingdings 3	05040102010807070707
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	MS Outlook	05010100010000000000
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Algerian	04020705040A02060702
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Berlin Sans FB	020E0602020502020306
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Broadway	04040905080B02020502

2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Chiller	04020404031007020602
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Freestyle Script	030804020302050B0404
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Jokerman	04090605060D06020702
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Lucida Bright	02040602050505020304
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Magneto	04030805050802020D02
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Niagara Engraved	04020502070703030202
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Parchment	03040602040708040804
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Snap ITC	04040A07060A02020202
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Viner Hand ITC	03070502030502020203
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Tw Cen MT	020B0602020104020603
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Rockwell Condensed	02060603050405020104
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Perpetua Titling MT	02020502060505020804
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	OCR A Extended	02010509020102010303
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Imprint MT Shadow	04020605060303030202
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Gill Sans Ultra Bold Condensed	020B0A06020104020203
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Gill Sans MT Ext Condensed Bold	020B0902020104020203
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Eras Light ITC	020B0402030504020804
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Elephant	02020904090505020303
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Copperplate Gothic Bold	020E0705020206020404
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Bradley Hand ITC	03070402050302030203
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Bodoni MT	02070603080606020203
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Bookshelf Symbol 7	05010101010101010101
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Tw Cen MT Condensed Extra Bold	020B0803020202020204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	@MingLiU_HKSCS	02020500000000000000
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	@PMingLiU-ExtB	02020500000000000000
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	@MS Gothic	020B0609070205080204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	@MS UI Gothic	020B0600070205080204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	@SimSun	02010600030101010101
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	NSimSun	02010609030101010101
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	@NSimSun	02010609030101010101

2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Microsoft Tai Le	020B0502040204020203
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Microsoft Sans Serif	020B0604020202020204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Kokila	020B0604020202020204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Utsaah	020B0604020202020204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Simplified Arabic	02020603050405020304
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Aharoni	02010803020104030203
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Miriam	020B0502050101010101
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	FangSong	02010609060101010101
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	@KaiTi	02010609060101010101
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	CordiaUPC	020B0304020202020204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	IrisUPC	020B0604020202020204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	DFKai-SB	03000509000000000000
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Candara	020E0502030303020204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Constantia	02030602050306030303
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Georgia	02040502050405020303
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Verdana	020B0604030504040204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Wingdings 2	05020102010507070707
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Haettenschweiler	020B0706040902060204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Monotype Corsiva	03010101010201010101
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Bell MT	02020503060305020303
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Britannic Bold	020B0903060703020204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Californian FB	0207040306080B030204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Cooper Black	0208090404030B020404
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Harrington	04040505050A02020702
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Kristen ITC	03050502040202030202
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Lucida Fax	02060602050505020204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Matura MT Script Capitals	03020802060602070202
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Niagara Solid	04020502070702020202
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Playbill	040506030A0602020202
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Stencil	040409050D0802020404

2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Vivaldi	03020602050506090804
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Tw Cen MT Condensed	020B0606020104020203
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Rockwell	02060603020205020403
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Perpetua	02020502060401020303
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Maiandra GD	020E0502030308020204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Goudy Stout	0202090407030B020401
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Gill Sans Ultra Bold	020B0A02020104020203
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Gigi	04040504061007020D02
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Franklin Gothic Heavy	020B0903020102020204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Franklin Gothic Demi	020B0703020102020204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Forte	03060902040502070203
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Eras Medium ITC	020B0602030504020804
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Engravers MT	02090707080505020304
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Copperplate Gothic Light	020E0507020206020404
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Calisto MT	02040603050505030304
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Bodoni MT Black	02070A03080606020203
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Agency FB	020B0503020202020204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Berlin Sans FB Demi	020E0802020502020306
2848	WINWORD.EXE	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400000000000F01FEC\Usage	SpellingAndGrammarFiles_1036	1328545833
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	@SimHei	02010609060101010101
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Browallia New	020B0604020202020204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	EucrosiaUPC	02020603050405020304
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	KodchiangUPC	02020603050405020304
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Lucida Sans Unicode	020B0602030504020204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Consolas	020B0609020204030204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Gabriola	04040605051002020D02
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Trebuchet MS	020B0603020202020204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	@Arial Unicode MS	020B0604020202020204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Century Gothic	020B0502020202020204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Garamond	02020404030301010803

2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Bauhaus 93	04030905020B02020C02
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Bodoni MT Poster Compressed	02070706080601050204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Centaur	02030504050205020304
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Footlight MT Light	0204060206030A020304
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	High Tower Text	02040502050506030303
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Kunstler Script	030304020206070D0D06
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Lucida Handwriting	03010101010101010101
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Modern No. 20	02070704070505020303
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Onyx	04050602080702020203
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Poor Richard	02080502050505020702
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Ravie	04040805050809020602
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Informal Roman	030604020304060B0204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Vladimir Script	03050402040407070305
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Script MT Bold	03040602040607080904
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Rage Italic	03070502040507070304
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Papyrus	03070502060502030205
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Lucida Sans Typewriter	020B0509030504030204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Goudy Old Style	02020502050305020303
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Gill Sans MT Condensed	020B0506020104020203
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	French Script MT	03020402040607040605
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Franklin Gothic Demi Cond	020B0706030402020204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Franklin Gothic Book	020B0503020102020204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Felix Titling	04060505060202020A04
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Eras Bold ITC	020B0907030504020204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Curlz MT	04040404050702020202
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Castellar	020A0402060406010301
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Bodoni MT Condensed	02070606080606020203
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Arial Rounded MT Bold	020F0704030504030204
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	MS Reference Specialty	05000500000000000000
2848	WINWORD.EXE	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400000000000F01FEC\Usage	SpellingAndGrammarFiles_1036	1328545834

2848	WINWORD.EXE	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400000000000F01FEC\Usage	SpellingAndGrammarFiles_1033	1328545855
2848	WINWORD.EXE	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C000000000000F01FEC\Usage	SpellingAndGrammarFiles_3082	1328545835
2848	WINWORD.EXE	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C000000000000F01FEC\Usage	SpellingAndGrammarFiles_3082	1328545836
2848	WINWORD.EXE	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400000000000F01FEC\Usage	SpellingAndGrammarFiles_1036	1328545836
2848	WINWORD.EXE	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400000000000F01FEC\Usage	SpellingAndGrammarFiles_1033	1328545857
2848	WINWORD.EXE	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400000000000F01FEC\Usage	SpellingAndGrammarFiles_1036	1328545835
2848	WINWORD.EXE	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400000000000F01FEC\Usage	SpellingAndGrammarFiles_1033	1328545859
2848	WINWORD.EXE	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400000000000F01FEC\Usage	SpellingAndGrammarFiles_1033	1328545858
2848	WINWORD.EXE	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400000000000F01FEC\Usage	SpellingAndGrammarFiles_1033	1328545861
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	@Batang	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	@DFKai-SB	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	@FangSong	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	@Gulim	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	@GungsuhChe	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	@KaiTi	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	@Meiryo UI	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	@Microsoft YaHei	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	@MingLiU_HKSCS	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	@MingLiU_HKSCS-ExtB	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	@MingLiU-ExtB	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	@MS Mincho	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	@NSimSun	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	@PMingLiU	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	@SimHei	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	@SimSun	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Aharoni	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Algerian	0

2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Angsana New	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Aparajita	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Arabic Typesetting	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Arial Black	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Arial Unicode MS	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	BatangChe	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Berlin Sans FB Demi	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Bernard MT Condensed	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Bodoni MT	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Bodoni MT Black	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Book Antiqua	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Britannic Bold	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Broadway	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	BrowalliaUPC	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Calibri	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Californian FB	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Castellar	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Centaur	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Century Schoolbook	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Colonna MT	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Constantia	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Cooper Black	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Corbel	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Courier	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Courier New	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	DaunPenh	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	DFKai-SB	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	DilleniaUPC	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Dotum	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	DotumChe	0

2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Elephant	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Engravers MT	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Eras Bold ITC	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Eras Demi ITC	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Estrangelo Edessa	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	EucrosiaUPC	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	FangSong	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Felix Titling	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Fixedsys	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Footlight MT Light	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Forte	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	@Arial Unicode MS	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	@BatangChe	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	@Dotum	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	@DotumChe	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	@GulimChe	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	@Gungsuh	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	@Malgun Gothic	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	@Meiryo	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	@Microsoft JhengHei	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	@MingLiU	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	@MS Gothic	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	@MS PGothic	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	@MS PMincho	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	@MS UI Gothic	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	@PMingLiU-ExtB	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Franklin Gothic Book	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Franklin Gothic Demi	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Franklin Gothic Demi Cond	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Franklin Gothic Heavy	0

2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Franklin Gothic Medium	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Franklin Gothic Medium Cond	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	FrankRuehl	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	FreesiaUPC	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Freestyle Script	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	French Script MT	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Gabriola	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Garamond	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Gautami	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Georgia	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Gigi	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Gill Sans MT	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Gill Sans MT Condensed	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Gill Sans MT Ext Condensed Bold	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Gill Sans Ultra Bold	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Gill Sans Ultra Bold Condensed	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Gisha	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Gloucester MT Extra Condensed	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Goudy Old Style	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Goudy Stout	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Gulim	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	GulimChe	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Gungsuh	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	GungsuhChe	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Haettenschweiler	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Harlow Solid Italic	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Harrington	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	High Tower Text	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Impact	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Imprint MT Shadow	0

2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Informal Roman	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	IrisUPC	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Iskoola Pota	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	JasmineUPC	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Jokerman	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Juice ITC	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	@SimSun-ExtB	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Agency FB	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Andalus	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	AngsanaUPC	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Arial	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Arial Narrow	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Arial Rounded MT Bold	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Baskerville Old Face	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Batang	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Bauhaus 93	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Bell MT	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Berlin Sans FB	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Blackadder ITC	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Bodoni MT Condensed	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Bodoni MT Poster Compressed	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Bookman Old Style	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Bookshelf Symbol 7	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Bradley Hand ITC	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Browallia New	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Brush Script MT	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Calisto MT	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Cambria	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Cambria Math	1
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Candara	0

2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Century	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Century Gothic	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Chiller	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Comic Sans MS	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Consolas	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Copperplate Gothic Bold	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Copperplate Gothic Light	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Cordia New	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	CordiaUPC	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Curlz MT	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	David	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	DokChampa	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Ebrima	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Edwardian Script ITC	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Eras Light ITC	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Eras Medium ITC	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Kalinga	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Kartika	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Khmer UI	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	KodchiangUPC	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Kokila	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Kristen ITC	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Kunstler Script	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Lao UI	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Latha	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Leelawadee	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Levenim MT	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	LilyUPC	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Lucida Bright	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Lucida Calligraphy	0

2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Lucida Console	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Lucida Fax	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Lucida Handwriting	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Lucida Sans	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Lucida Sans Typewriter	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Lucida Sans Unicode	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Magneto	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Maiandra GD	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Malgun Gothic	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Mangal	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Marlett	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Matura MT Script Capitals	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Meiryo	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Meiryo UI	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Microsoft Himalaya	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Microsoft JhengHei	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Microsoft New Tai Lue	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Microsoft PhagsPa	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Microsoft Sans Serif	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Microsoft Tai Le	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Microsoft Uighur	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Microsoft YaHei	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Microsoft Yi Baiti	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	MingLiU	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	MingLiU_HKSCS	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	MingLiU_HKSCS-ExtB	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	MingLiU-ExtB	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Miriam	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Miriam Fixed	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Mistral	0

2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Modern No. 20	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Mongolian Baiti	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Monotype Corsiva	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	MoolBoran	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	MS Gothic	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	MS Mincho	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	MS Outlook	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	MS PGothic	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	MS PMincho	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	MS Reference Sans Serif	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	MS Reference Specialty	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	MS Sans Serif	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	MS Serif	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	MS UI Gothic	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	MT Extra	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	MV Boli	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Narkisim	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Niagara Engraved	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Niagara Solid	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	NSimSun	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Nyala	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	OCR A Extended	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Old English Text MT	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Onyx	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Palace Script MT	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Palatino Linotype	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Papyrus	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Parchment	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Perpetua	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Perpetua Titling MT	0

2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Plantagenet Cherokee	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Playbill	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	PMingLiU	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	PMingLiU-ExtB	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Poor Richard	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Pristina	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Raavi	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Rage Italic	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Ravie	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Rockwell	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Rockwell Condensed	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Rockwell Extra Bold	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Rod	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Sakkal Majalla	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Script MT Bold	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Segoe Print	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Segoe Script	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Segoe UI	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Segoe UI Light	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Segoe UI Semibold	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Segoe UI Symbol	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Shonar Bangla	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Showcard Gothic	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Shruti	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	SimHei	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Simplified Arabic	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Simplified Arabic Fixed	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	SimSun	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	SimSun-ExtB	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Small Fonts	0

2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Snap ITC	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Stencil	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Sylfaen	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Symbol	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	System	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Tahoma	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Tempus Sans ITC	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Terminal	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Times New Roman	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Traditional Arabic	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Trebuchet MS	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Tunga	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Tw Cen MT	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Tw Cen MT Condensed	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Tw Cen MT Condensed Extra Bold	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Utsaah	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Vani	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Verdana	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Vijaya	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Viner Hand ITC	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Vivaldi	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Vladimir Script	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Vrinda	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Webdings	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Wide Latin	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Wingdings	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Wingdings 2	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Wingdings 3	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	KaiTi	0
2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Euphemia	0

2848	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Security\Trusted Documents	LastPurgeTime	26144036
2748	powershell.exe	write	HKEY_CLASSES_ROOT\Local Settings\MuiCache\72\52C64B7E	LanguageList	en-US
2748	powershell.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASAPI32	MaxFileSize	1048576
2748	powershell.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASMANCS	FileTracingMask	4294901760
2748	powershell.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASAPI32	EnableFileTracing	0
2748	powershell.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASAPI32	FileDirectory	%windir%\tracing
2748	powershell.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASMANCS	ConsoleTracingMask	4294901760
2748	powershell.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASMANCS	EnableFileTracing	0
2748	powershell.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASMANCS	MaxFileSize	1048576
2748	powershell.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASAPI32	EnableConsoleTracing	0
2748	powershell.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASAPI32	FileTracingMask	4294901760
2748	powershell.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASAPI32	ConsoleTracingMask	4294901760
2748	powershell.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASMANCS	EnableConsoleTracing	0
2748	powershell.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASMANCS	FileDirectory	%windir%\tracing
2748	powershell.exe	write	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap	AutoDetect	1
2748	powershell.exe	write	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap	UNCAsIntranet	0
3560	easywindow.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\easywindow_RASAPI32	FileTracingMask	4294901760
3560	easywindow.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\easywindow_RASAPI32	FileDirectory	%windir%\tracing
3560	easywindow.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\easywindow_RASMANCS	MaxFileSize	1048576
3560	easywindow.exe	write	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings	ProxyEnable	0
3560	easywindow.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\easywindow_RASAPI32	EnableConsoleTracing	0
3560	easywindow.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\easywindow_RASAPI32	MaxFileSize	1048576
3560	easywindow.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\easywindow_RASMANCS	EnableConsoleTracing	0
3560	easywindow.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\easywindow_RASMANCS	FileTracingMask	4294901760
3560	easywindow.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\easywindow_RASMANCS	ConsoleTracingMask	4294901760
3560	easywindow.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\easywindow_RASMANCS	FileDirectory	%windir%\tracing
3560	easywindow.exe	write	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	SavedLegacySettings	

46000000920000000100000000000000000000000000000000000000000000C0E333BBEAB1D301000000000000000000000000020000001700000000000000FE8
0000000000007D6CB050D9C573F70B0000000000000006D00330032005C004D00530049004D004700330032002E0064006C000100000004AA400014AA40000400
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000002000000C0A80164000000000
00000000000000000000000000000000800000000000000805D3F0098374000000800000200000000000006000000020600400000B8A940000200000088020000060040
000B8A9400004000000F8010000B284000088B64000B84B400043003A000000000000000000000000000000000000000000

3560	easywindow.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\easywindow_RASAPI32	EnableFileTracing	0

3560	easywindow.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\easywindow_RASAPI32	ConsoleTracingMask	4294901760
3560	easywindow.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\easywindow_RASMANCS	EnableFileTracing	0

Files activity

Executable files	Suspicious files	Text files	Unknown types
2	10	0	27

Dropped files

PID	Process	Filename	Type
2748	powershell.exe	C:\Users\admin\284.exe **MD5:** F1AB1FA6D2B93AE55B448B96733FF195 **SHA256:** 045C4AB485BD45781234451AF0EAE62F23ABCEAE375D5434CFF3	executable
2652	284.exe	C:\Users\admin\AppData\Local\easywindow\easywindow.exe **MD5:** F1AB1FA6D2B93AE55B448B96733FF195 **SHA256:** 045C4AB485BD45781234451AF0EAE62F23ABCEAE375D5434CFF3	executable
2848	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2BA4EDDC.wmf **MD5:** — **SHA256:** —	—
2604	284.exe	C:\Users\admin\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-1302019708-1500728564-335382590-1000\0f5007522459c86e95ffcc62f32308f1_90059c37-1320-41a4-b58d-2b75a9850d2f **MD5:** C1B696D9ABC26385E13BFB7CD438FE1A **SHA256:** 889B017CB8DB5481BCEA02A193E6CB069ACF11DF4415BBC452F	binary
2936	easywindow.exe	C:\Users\admin\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-1302019708-1500728564-335382590-1000\0f5007522459c86e95ffcc62f32308f1_90059c37-1320-41a4-b58d-2b75a9850d2f **MD5:** 1328F7A33E1FA72FCD4DAA8B77376704 **SHA256:** EFA08BD25F464B24861CB35489AB01896A95B1B4B69E7E099AF8E	binary
3900	284.exe	C:\Users\admin\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-1302019708-1500728564-335382590-1000\0f5007522459c86e95ffcc62f32308f1_90059c37-1320-41a4-b58d-2b75a9850d2f **MD5:** C1B696D9ABC26385E13BFB7CD438FE1A **SHA256:** 889B017CB8DB5481BCEA02A193E6CB069ACF11DF4415BBC452F	binary
2748	powershell.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms **MD5:** 0F2CAD9746414ABA31294C3B560FCFD5 **SHA256:** 19AD383DED364BB44DED7C7CF00EB6254E5E98D696632944F6B	binary
2848	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B1454633.wmf **MD5:** FEA8B79F65B72D34A60353CD7225A45A **SHA256:** 21AEF6E2AADE6340C2B6E9325E657C279F257CC4CAFAD55828D	wmf
2848	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4230347A.wmf **MD5:** 26303F4E5F76EFB7713E44DE8DAE7B94 **SHA256:** 74356BB34A244D2FED5537F92AF76E30CDAD6BCC680373F6054E	wmf
2748	powershell.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF16a7fc.TMP **MD5:** 0F2CAD9746414ABA31294C3B560FCFD5 **SHA256:** 19AD383DED364BB44DED7C7CF00EB6254E5E98D696632944F6B	binary
2848	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\8CA6528C.wmf **MD5:** 4F9995F7AF668BA7D2877827B278A59B **SHA256:** C2D861E85128F3AFACE3AA557A96B35D051E9BC861CBA7947668	wmf
2748	powershell.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\JS1CJ636SR8QS76NMA2K.temp **MD5:** — **SHA256:** —	—
2848	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7901F91D.wmf **MD5:** 39FBBE649E8141EE9D0AFC8B267411B2 **SHA256:** 10D1D217FA622EC6D2CD3E10FD634E7909FA069A6472AB31CBCF	wmf
2848	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\8BFD4CF7.wmf **MD5:** CB95456695CE399EDC42BE6273510082 **SHA256:** 39954FC84774769A433E45EDCCA0DF975434B3AB697FE72B5AED	wmf
3872	easywindow.exe	C:\Users\admin\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-1302019708-1500728564-335382590-1000\0f5007522459c86e95ffcc62f32308f1_90059c37-1320-41a4-b58d-2b75a9850d2f **MD5:** 1328F7A33E1FA72FCD4DAA8B77376704 **SHA256:** EFA08BD25F464B24861CB35489AB01896A95B1B4B69E7E099AF8E	binary
2848	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\37A0C94E.wmf	wmf

		MD5: A0A9B21FF4A34C64B991156A31A37AF5 **SHA256:** 29C8467DB18B2E8C485481DE78557C30404C274E7EA96CC358E8	
2848	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C866F936.wmf	—
		MD5: — **SHA256:** —	
2848	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7AA30AE8.wmf	—
		MD5: — **SHA256:** —	
2848	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E1957C4A.wmf	—
		MD5: — **SHA256:** —	
2848	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9D4D6041.wmf	wmf
		MD5: DA3C527530C77C1CA6132A12B41A0BCD **SHA256:** 553DF00E84F0EBCDC6F75A478D1732F7DEB32AEC087260B0B6D	
2848	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3FFED7B.wmf	wmf
		MD5: B7628193D7CF5A8672BBB90B9CB521C2 **SHA256:** 627FDDEFBAFEE73D5EFFD5160FEEC4BA195BCDE4A5EB019255	
2848	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5DA11140.wmf	wmf
		MD5: 47AFB50730F68901F48ED75DA817B7C2 **SHA256:** 5DD6A19CEEC84DAF240F7A7FF4FDC0619AEFF2AE3D64DA4B113	
2848	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\BB62EB25.wmf	wmf
		MD5: 5C9CC5DAE65C75AE121A3B785495E81E **SHA256:** 19F6A0188E80CF603364992E1DF87FE048013F2D3FAC99FC7FF91	
2848	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E453AEE2.wmf	wmf
		MD5: BDD0E44EFF8B2799A39FC75415CABFF6 **SHA256:** 68CCFD4905A24F7C542AAB67D50A3E25BF8EE673DC51DD7F946	
2848	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\~$emotet.doc	pgc
		MD5: 3D7A31ABBF01BFFDA350A12A72AF25D8 **SHA256:** 0EC215C7CCD69EC62B5F7983F4C52A45AFB4C9B06158133A1EE	
2848	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A68ACC1E.wmf	—
		MD5: — **SHA256:** —	
2848	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FC106F90.wmf	—
		MD5: — **SHA256:** —	
2848	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AAF73CB2.wmf	—
		MD5: — **SHA256:** —	
2848	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A293C404.wmf	—
		MD5: — **SHA256:** —	
2848	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\8063E206.wmf	—
		MD5: — **SHA256:** —	
2848	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\79A7DF38.wmf	—
		MD5: — **SHA256:** —	
2848	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\27C6901A.wmf	—
		MD5: — **SHA256:** —	
2848	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\8ACC2BBF.dat	wmf
		MD5: 38166337CE725C22B495ECAC8091BFBE **SHA256:** A440C62F0FA60F48B7D8E3DC3D9742BC2C3B1A854B68A017A6BE	
2848	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2756CBC3.dat	wmf
		MD5: F57A731751D6C07D989297189945DC22 **SHA256:** 48299988FF9C5D05502D33EC09A5D85E3CEAEE33254D3793C3DE	
2848	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4147FDC9.dat	wmf
		MD5: 579D464CECAA3CD6692B15E2E425C20C **SHA256:** B4EBF29AD33B0C328AFFA79132BB181DE0404686638343B8388CE	
2848	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B14E5187.dat	wmf
		MD5: 3B32B9F267CF31F99CB4F7C57DEE9065 **SHA256:** 99C45945420336B5DC994F243AA59F8075DEF1B35EED3B05EA70	
2848	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\28A1BC2D.dat	wmf
		MD5: D9050D476C53C087C432424D18BEE35A **SHA256:** 3F9823F2D24C3FC12B7253EC6BBBA9C6D26B3BE8C559F7B92DF	
2848	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\Word8.0\MSForms.exd	tlb
		MD5: 20512E0268129AC16E90F077D9CBC946 **SHA256:** 37980821C91E93AC4C58A0D1C873F83CF3622075CED132D902D1	
2848	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1E1F010B.dat	wmf
		MD5: 6226781EE2D60A4D68B56699B7815ABB **SHA256:** B253BEDFD4FC10977A663F47D6FA0D1CE9AFD6F79E238732FD6A	
2848	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\45FE8C35.dat	wmf
		MD5: B968160E32B2FBEBB3FF6C55F5B4885B **SHA256:** 7CF4AE188785F7C0E5E4A1D5BDAC0B52BC65D3AA46513022A9E	

2848	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6D04752C.wmf **MD5:** — **SHA256:** —	—
2848	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\CVR9C64.tmp.cvr **MD5:** — **SHA256:** —	—
2848	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3E590A51.dat **MD5:** 23EE1904F10A3641361F163E000DFF66 **SHA256:** 58D13515C530476E847D64718305B845B4110F87C88C7761BA9A05	wmf
2848	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3509AD53.dat **MD5:** C1F138C3F19B5545D60B3B5D4C2BA4FC **SHA256:** 80C4552EC9FED881E1806AA55368D3428832F52157AB8D92E7FB5	wmf
2848	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\DCEEA5D9.dat **MD5:** B2B55276284D41BAA290155CB55A94E2 **SHA256:** C08D5EC45948BDE7FBA129C2BD1A6BF2816015DA7BC0B8BC76D	wmf
2848	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\63B6DE4F.dat **MD5:** 35428803E94ECDFA6A957382868444DA **SHA256:** 73B03956B8DD27BFD4F7A828A7654456D6952E4C75AA03CF3F505	wmf
2848	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C1357B3D.dat **MD5:** 48D1B152FC6F014B9C45DBB5A7941F4D **SHA256:** 61CBDA84CEB5254E134CB6F59EA9D73812B48EF380298D53AEE6	wmf
2848	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\~$Normal.dotm **MD5:** 62F2DA178DD59EBA6B61EE250E55F925 **SHA256:** 8CF938206B83D51659082A32A71F3A9F077217F5A2E07A98541350	pgc
2848	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7577E298.wmf **MD5:** 42B0F97E9825449206338C874697BAAB **SHA256:** 84C95F3B3B0D356E85A9701D04B4F4CDFD29D28573141A5B0148I	wmf

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
5	5	1	18

HTTP requests

2748	powershell.exe	GET	200	104.27.132.137:80	http://blockchainjoblist.com/wp-admin/014080/	US	executable	477 Kb	malicious
3560	easywindow.exe	POST	—	181.188.149.134:80	http://181.188.149.134/raster/img/ringin/	BO	text —	491 b —	malicious
3560	easywindow.exe	POST	—	203.130.0.67:80	http://203.130.0.67/rtm/devices/	PK	text —	464 b —	malicious
3560	easywindow.exe	POST	—	5.67.96.120:8080	http://5.67.96.120:8080/prov/walk/	GB	text —	478 b —	malicious
3560	easywindow.exe	POST	—	143.0.245.169:8080	http://143.0.245.169:8080/schema/cone/nsip/merge/	AR	text —	482 b —	malicious

Connections

2748	powershell.exe	104.27.132.137:80	Cloudflare Inc	US	shared
3560	easywindow.exe	181.188.149.134:80	Telefónica Celular de Bolivia S.A.	BO	malicious
3560	easywindow.exe	203.130.0.67:80	Supernet Limited Transit Autonomous System Number	PK	malicious
3560	easywindow.exe	5.67.96.120:8080	Sky UK Limited	GB	malicious
3560	easywindow.exe	143.0.245.169:8080	COTELCAM	AR	malicious

DNS requests

blockchainjoblist.com	104.27.132.137 104.27.133.137	malicious

Threats

2748	powershell.exe	Potential Corporate Privacy Violation	ET POLICY PE EXE or DLL Windows file download HTTP
2748	powershell.exe	A Network Trojan was detected	AV INFO Suspicious EXE download from WordPress folder
2748	powershell.exe	Potentially Bad Traffic	ET INFO Executable Retrieved With Minimal HTTP Headers - Potential Second Stage Download
2748	powershell.exe	Misc activity	ET INFO EXE - Served Attached HTTP
3560	easywindow.exe	A Network Trojan was detected	AV TROJAN W32/Emotet CnC Checkin (Apr 2019)
3560	easywindow.exe	A Network Trojan was detected	MALWARE [PTsecurity] Feodo/Emotet
3560	easywindow.exe	A Network Trojan was detected	ET CNC Feodo Tracker Reported CnC Server group 15
3560	easywindow.exe	A Network Trojan was detected	MALWARE [PTsecurity] Feodo/Emotet
3560	easywindow.exe	A Network Trojan was detected	ET CNC Feodo Tracker Reported CnC Server group 20
3560	easywindow.exe	A Network Trojan was detected	MALWARE [PTsecurity] Feodo/Emotet
3560	easywindow.exe	A Network Trojan was detected	ET CNC Feodo Tracker Reported CnC Server group 3

Debug output strings

No debug info.

ANY RUN Interactive malware hunting service ANY.RUN
© 2017-2021 ANY.RUN LLC. ALL RIGHTS RESERVED