ANY RUN
INTERACTIVE MALWARE ANALYSIS

General Info

File name:	0208_54741869750132.doc
Full analysis:	https://app.any.run/tasks/2a535f88-8c8f-4325-93a4-fae4895412a4
Verdict:	Malicious activity
Threats:	**Hancitor** Hancitor was created in 2014 to drop other malware on infected machines. It is also known as Tordal and Chanitor. This malware is available as a service which makes it accessible tools to criminals and contributes to the popularity of this virus. **Trojan** Trojans are a group of malicious programs distinguished by their ability to masquerade as benign software. Depending on their type, trojans possess a variety of capabilities, ranging from maintaining full remote control over the victim's machine to stealing data and files, as well as dropping other malware. At the same time, the main functionality of each trojan family can differ significantly depending on its type. The most common trojan infection chain starts with a phishing email.
Analysis date:	March 15, 2024 at 15:41:28
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Tags:	generated-doc maldoc-57 macros ole-embedded macros-on-open evasion hancitor trojan sinkhole
Indicators:	
MIME:	application/msword
File info:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1252, Author: MyPc, Template: 0802_20304783210485.dotm, Last Saved By: MyPc, Revision Number: 2, Name of Creating Application: Microsoft Office Word, Total Editing Time: 01:00, Create Time/Date: Mon Feb 8 13:07:00 2021, Last Saved Time/Date: Mon Feb 8 13:07:00 2021, Number of Pages: 1, Number of Words: 3, Number of Characters: 19, Security: 0
MD5:	7F6C623196D7E76C205B4FB898AD9BE6
SHA1:	408BB5B4E8AC34CE3B70BA54E00E9858CED885C0
SHA256:	3A5648F7DE99C4F87331C36983FC8ADCD667743569A19C8DAFDD5E8A33DE154D
SSDEEP:	24576:pA8N8rVgYpNGhCOndGCl/LSD7aq/Iq9Mz:x0JkCOo6Tf

Software environment set and analysis options

Launch configuration

Task duration:	60 seconds	**Heavy Evasion option:**	off	**Network geolocation:**	off
Additional time used:	none	**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 Acrobat Reader DC (20.013.20064)
- Adobe Flash Player 32 ActiveX (32.0.0.453)
- Adobe Flash Player 32 ActiveX (32.0.0.453)
- Adobe Flash Player 32 NPAPI (32.0.0.453)
- Adobe Flash Player 32 NPAPI (32.0.0.453)
- Adobe Flash Player 32 PPAPI (32.0.0.453)
- Adobe Flash Player 32 PPAPI (32.0.0.453)
- Adobe Refresh Manager (1.8.0)
- Adobe Refresh Manager (1.8.0)
- CCleaner (6.14)
- CCleaner (6.14)
- FileZilla 3.65.0 (3.65.0)
- FileZilla 3.65.0 (3.65.0)
- Google Chrome (109.0.5414.120)
- Google Chrome (109.0.5414.120)
- Google Update Helper (1.3.36.31)
- Google Update Helper (1.3.36.31)
- Java 8 Update 271 (8.0.2710.9)
- Java 8 Update 271 (8.0.2710.9)
- Java Auto Updater (2.8.271.9)
- Java Auto Updater (2.8.271.9)
- Microsoft .NET Framework 4.8 (4.8.03761)
- Microsoft .NET Framework 4.8 (4.8.03761)
- Microsoft .NET Framework 4.8 (4.8.03761)
- Microsoft .NET Framework 4.8 (4.8.03761)
- Microsoft Edge (109.0.1518.115)
- Microsoft Edge (109.0.1518.115)
- Microsoft Edge Update (1.3.175.29)
- Microsoft Edge Update (1.3.175.29)
- Microsoft Office Access MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Access MUI (English) 2010 (14.0.6029.1000)

- Microsoft Office Access MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Italian) 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 (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Korean) 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 (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Russian) 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 (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Access MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Access Setup Metadata MUI (English) 2010 (14.0.6029.1000)
- 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 (English) 2010 (14.0.6029.1000)
- Microsoft Office Excel MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Italian) 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 (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Korean) 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 (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Russian) 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 (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Excel MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Groove MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (German) 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 (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (Japanese) 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 (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (Portuguese (Brazil)) 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 (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (Spanish) 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 Groove MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office IME (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office IME (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office IME (Korean) 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 (French) 2010 (14.0.4763.1000)
- Microsoft Office InfoPath MUI (German) 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 (Italian) 2010 (14.0.4763.1000)
- Microsoft Office InfoPath MUI (Japanese) 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 (Korean) 2010 (14.0.4763.1000)
- Microsoft Office InfoPath MUI (Portuguese (Brazil)) 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 (Russian) 2010 (14.0.4763.1000)
- Microsoft Office InfoPath MUI (Spanish) 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 InfoPath MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Language Pack 2010 - French/Français (14.0.4763.1000)
- 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 - German/Deutsch (14.0.4763.1000)
- Microsoft Office Language Pack 2010 - Italian/Italiano (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 - Japanese/日本語 (14.0.4763.1000)
- Microsoft Office Language Pack 2010 - Korean/한국어 (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 - Portuguese/Português (Brasil) (14.0.4763.1000)
- Microsoft Office Language Pack 2010 - Russian/русский (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 - Spanish/Español (14.0.4763.1000)
- Microsoft Office Language Pack 2010 - Turkish/Türkçe (14.0.4763.1013)
- 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 (French) 2010 (14.0.4763.1000)
- Microsoft Office O MUI (German) 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 (Italian) 2010 (14.0.4763.1000)
- Microsoft Office O MUI (Japanese) 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 (Korean) 2010 (14.0.4763.1000)
- Microsoft Office O MUI (Portuguese (Brazil)) 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 (Russian) 2010 (14.0.4763.1000)
- Microsoft Office O MUI (Spanish) 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 O MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office OneNote MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office OneNote MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office OneNote MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office OneNote MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office OneNote MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office OneNote MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office OneNote MUI (Italian) 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 (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office OneNote MUI (Korean) 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 (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office OneNote MUI (Russian) 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 (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office OneNote MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office OneNote MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Outlook MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Outlook MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Outlook MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Outlook MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Outlook MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Outlook MUI (German) 2010 (14.0.4763.1000)

- Microsoft Office Outlook MUI (Italian) 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 (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Outlook MUI (Korean) 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 (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Outlook MUI (Russian) 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 (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Outlook MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Outlook MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office PowerPoint MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office PowerPoint MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office PowerPoint MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office PowerPoint MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office PowerPoint MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office PowerPoint MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office PowerPoint MUI (Italian) 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 (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office PowerPoint MUI (Korean) 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 (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office PowerPoint MUI (Russian) 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 (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office PowerPoint MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office PowerPoint MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Professional 2010 (14.0.6029.1000)
- Microsoft Office Professional 2010 (14.0.6029.1000)
- Microsoft Office Proof (Arabic) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Arabic) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Basque) 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 (Catalan) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Dutch) 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 (English) 2010 (14.0.6029.1000)
- Microsoft Office Proof (French) 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 (Galician) 2010 (14.0.4763.1000)
- Microsoft Office Proof (German) 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 (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Japanese) 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 (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Portuguese (Brazil)) 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 (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Spanish) 2010 (14.0.6029.1000)
- Microsoft Office Proof (Spanish) 2010 (14.0.6029.1000)
- Microsoft Office Proof (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Proof (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Proof (Ukrainian) 2010 (14.0.4763.1000)
- Microsoft Office Proof (Ukrainian) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (English) 2010 (14.0.6029.1000)
- Microsoft Office Proofing (English) 2010 (14.0.6029.1000)
- Microsoft Office Proofing (French) 2010 (14.0.4763.1000)

- Microsoft Office Proofing (French) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (German) 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 (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (Japanese) 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 (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (Portuguese (Brazil)) 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 (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Proofing (Spanish) 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 Proofing (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Publisher MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Publisher MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Publisher MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Publisher MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Publisher MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Publisher MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Publisher MUI (Italian) 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 (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Publisher MUI (Korean) 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 (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Publisher MUI (Russian) 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 (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Publisher MUI (Turkish) 2010 (14.0.4763.1013)
- 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 (French) 2010 (14.0.4763.1000)
- Microsoft Office SharePoint Designer MUI (German) 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 (Italian) 2010 (14.0.4763.1000)
- Microsoft Office SharePoint Designer MUI (Japanese) 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 (Korean) 2010 (14.0.4763.1000)
- Microsoft Office SharePoint Designer MUI (Portuguese (Brazil)) 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 (Russian) 2010 (14.0.4763.1000)
- Microsoft Office SharePoint Designer MUI (Spanish) 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 SharePoint Designer MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Shared MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Shared MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Shared MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Shared MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Shared MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Shared MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Shared MUI (Italian) 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 (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Shared MUI (Korean) 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 (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Shared MUI (Russian) 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 (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Shared MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Shared MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Shared Setup Metadata MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Shared Setup Metadata MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Single Image 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 (English) 2010 (14.0.6029.1000)
- Microsoft Office Word MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Italian) 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 (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Korean) 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 (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Russian) 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 (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Word MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Word MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office X MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (German) 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 (Italian) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Japanese) 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 (Korean) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Portuguese (Brazil)) 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 (Russian) 2010 (14.0.4763.1000)
- Microsoft Office X MUI (Spanish) 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 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++ 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++ 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 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 Additional Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2015-2022 Redistributable (x86) - 14.36.32532 (14.36.32532.0)
- Microsoft Visual C++ 2015-2022 Redistributable (x86) - 14.36.32532 (14.36.32532.0)
- Microsoft Visual C++ 2022 X86 Additional Runtime - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X86 Additional Runtime - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X86 Minimum Runtime - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X86 Minimum Runtime - 14.36.32532 (14.36.32532)
- Mozilla Firefox (x86 en-US) (115.0.2)
- Mozilla Firefox (x86 en-US) (115.0.2)
- Mozilla Maintenance Service (115.0.2)
- Mozilla Maintenance Service (115.0.2)
- Notepad++ (32-bit x86) (7.9.1)
- Notepad++ (32-bit x86) (7.9.1)
- PowerShell 7-x86 (7.2.11.0)
- PowerShell 7-x86 (7.2.11.0)
- Skype version 8.110 (8.110)

- Skype version 8.110 (8.110)
- Update for Microsoft .NET Framework 4.8 (KB4503575) (1)
- Update for Microsoft .NET Framework 4.8 (KB4503575) (1)
- VLC media player (3.0.11)
- VLC media player (3.0.11)
- WinRAR 5.91 (32-bit) (5.91.0)
- WinRAR 5.91 (32-bit) (5.91.0)

Behavior activities

MALICIOUS

Drops the executable file immediately after the start
- WINWORD.EXE (PID: 2124)

Executable content was dropped or overwritten
- WINWORD.EXE (PID: 2124)

HANCITOR has been detected (SURICATA)
- rundll32.exe (PID: 3276)

Unusual execution from MS Office
- WINWORD.EXE (PID: 2124)

Connects to the CnC server
- rundll32.exe (PID: 3276)

HANCITOR has been detected (YARA)
- rundll32.exe (PID: 3276)

Unusual connection from system programs
- rundll32.exe (PID: 3276)

SUSPICIOUS

Creates FileSystem object to access computer's file system (SCRIPT)
- WINWORD.EXE (PID: 2124)

Non-standard symbols in registry
- WINWORD.EXE (PID: 2124)

Reads the Internet Settings
- rundll32.exe (PID: 3276)

Uses RUNDLL32.EXE to load library
- WINWORD.EXE (PID: 2124)

Checks for external IP
- rundll32.exe (PID: 3276)

INFO

The process uses the downloaded file
- WINWORD.EXE (PID: 2124)

Checks proxy server information
- rundll32.exe (PID: 3276)

Malware configuration

Hancitor

(PID) Process	(3276) rundll32.exe
Hosts (3)	http://satursed.com/8/forum.php
	http://sameastar.ru/8/forum.php
	http://ludiesibut.ru/8/forum.php

Static information

TRiD

.doc | Microsoft Word document (34.5)

.doc | Microsoft Word document (old ver.) (20.5)

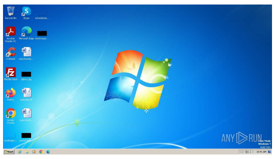
EXIF

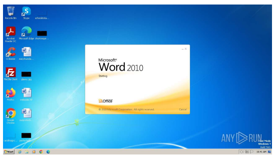
FlashPix

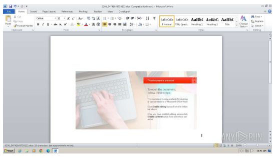
Lines:	1
Paragraphs:	1
Pages:	1
Characters:	19
Words:	3
TotalEditTime:	1 minute
RevisionNumber:	2
LastPrinted:	0000:00:00 00:00:00
CompObjUserType:	Microsoft Word 97-2003 Document
CompObjUserTypeLen:	32
HeadingPairs:	Title 1
TitleOfParts:	-
HyperlinksChanged:	No
SharedDoc:	No
LinksUpToDate:	No
ScaleCrop:	No
AppVersion:	16
CharCountWithSpaces:	21
Company:	-
CodePage:	Windows Latin 1 (Western European)
Security:	None
ModifyDate:	2021:02:08 13:07:00
CreateDate:	2021:02:08 13:07:00
Software:	Microsoft Office Word
LastModifiedBy:	MyPc

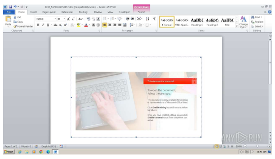
Template:	0802_20304783210485.dotm
Comments:	-
Keywords:	-
Author:	MyPc
Subject:	-
Title:	-
Word97:	No
System:	Windows
DocFlags:	Has picture, 1Table, ExtChar
LanguageCode:	English (US)
Identification:	Word 8.0

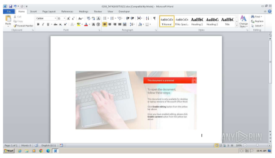
Video and screenshots







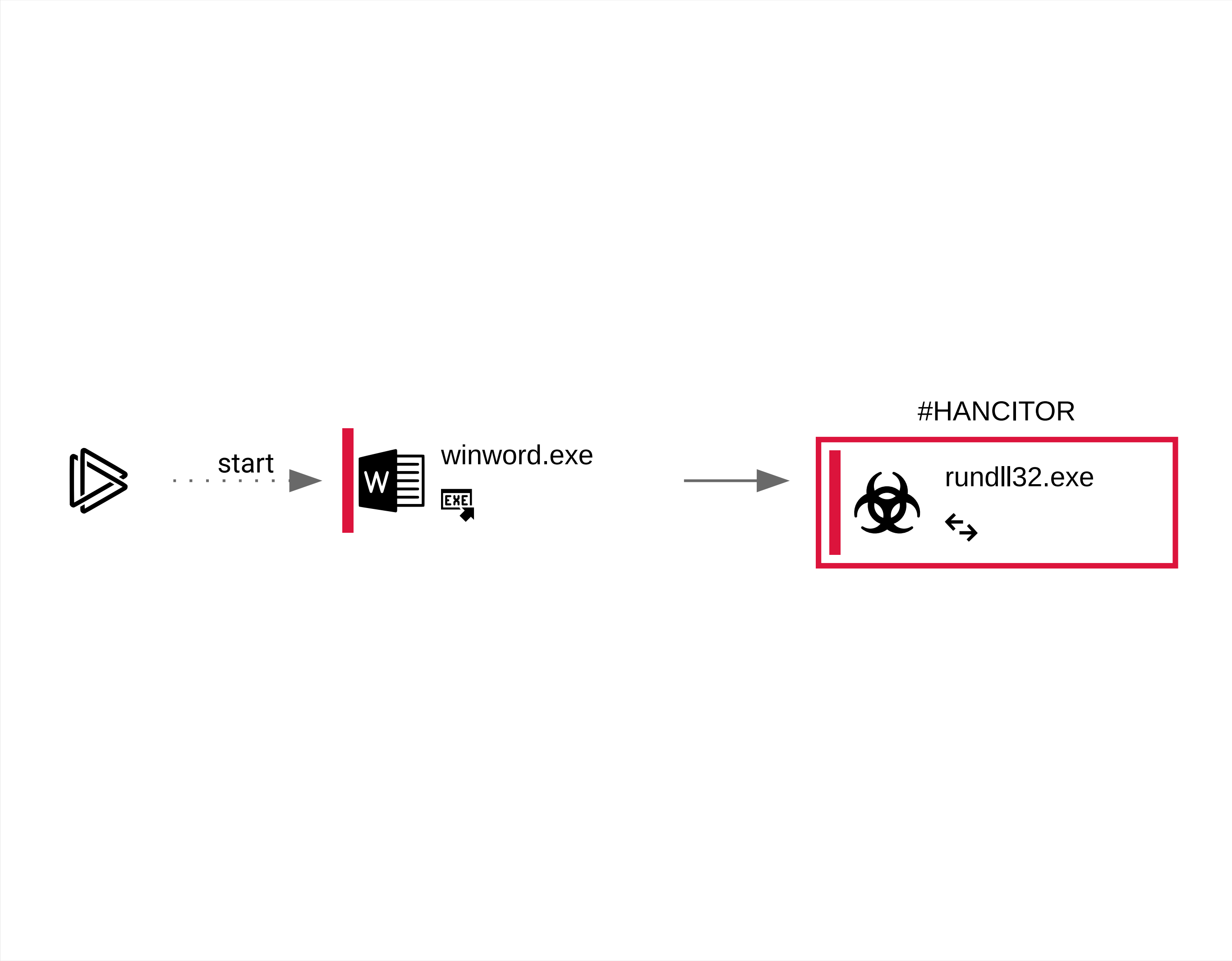




Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
39	2	2	0

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
2124	"C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /n "C:\Users\admin\AppData\Local\Temp\0208_54741869750132.doc"	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE	EXE	explorer.exe

Information

User: admin **Company:** Microsoft Corporation

Integrity Level: MEDIUM **Description:** Microsoft Word

Version: 14.0.6024.1000

3276 "C:\Windows\System32\rundll32.exe" C:\Users\admin\AppData\Roaming\Microsoft\Templates\W0rd.dll,UminslalIF0mt C:\Windows\System32\rundll32.exe WINWORD.EXE

Information

User: admin **Company:** Microsoft Corporation

Integrity Level: MEDIUM **Description:** Windows host process (Rundll32)

Version: 6.1.7600.16385 (win7_rtm.090713-1255)

Malware configuration Hancitor

Hancitor

(PID) Process	(3276) rundll32.exe
Hosts (3)	http://satursed.com/8/forum.php
	http://sameastar.ru/8/forum.php
	http://ludiesibut.ru/8/forum.php

Registry activity

Total events	Read events	Write events	Delete events
7 911	7 110	548	253

Modification events

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems
Operation: write **Name:** 0i
Value: 306920004C080000010000000000000000000000

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation: write **Name:** 1033
Value: Off

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation: write **Name:** 1041
Value: Off

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation: write **Name:** 1046
Value: Off

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation: write **Name:** 1036
Value: Off

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation: write **Name:** 1031
Value: Off

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation: write **Name:** 1040
Value: Off

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation: write **Name:** 1049
Value: Off

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation: write **Name:** 3082
Value: Off

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation: write **Name:** 1042
Value: Off

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation: write **Name:** 1055
Value: Off

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation: write **Name:** 1033
Value: On

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages

Operation: write **Name:** 1041
Value: On

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation: write **Name:** 1042
Value: On

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation: write **Name:** 1046
Value: On

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation: write **Name:** 1036
Value: On

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation: write **Name:** 1031
Value: On

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation: write **Name:** 1040
Value: On

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation: write **Name:** 1049
Value: On

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation: write **Name:** 3082
Value: On

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation: write **Name:** 1055
Value: On

(PID) Process: (2124) 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: (2124) 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: (2124) 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: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word
Operation: write **Name:** MTTT
Value: 4C080000BA82B75CC576DA0100000000

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LCCache\Themes\1033
Operation: delete value **Name:** NextUpdate
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LCCache\WordDocParts\1033
Operation: delete value **Name:** NextUpdate
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LCCache\SmartArt\1033
Operation: delete value **Name:** NextUpdate
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems
Operation: write **Name:** *j
Value: 2A6A20004C08000004000000000000008C000000010000000840000003E0043003A005C0055007300650072007300C00610064006D0069006E005C0041007000700044006100740061005C0052006F0061006D0069006E0067005C004D006900630072006F0073006F00660074005C00540065006D0070006C006100740065007300C004E006F0072006D0061006C002E0064006F0074006D00000000000000

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems
Operation: delete value **Name:** *j
Value: 横 ﺷ

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems
Operation: write **Name:** 'j
Value: 276A20004C0800000200000000000008E000000010000005000000032000000063003A005C00700072006F006700720061007E0031005C006D006900630072006F0073007E0031005C006F0066006600690063006500310034005C00670065006E006B006F002E0064006C006C0000006D006900630072006F0073006F006600740020077006F00720064002000D0C6E0ACC0C9200094CD00AC200030AEA5B20000

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems
Operation: delete value **Name:** 'j
Value: 椵 ᓴ

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** ProxyBypass
Value: 1

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** IntranetName
Value: 1

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** UNCAsIntranet
Value: 1

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** AutoDetect
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems
Operation: write **Name:** !k
Value: 216B20004C08000000600000000100000084000000002000000074000000004000000063003A005C00750073006500720073005C00610064006D0069006E005C0061007000700064006100740061005C006C006F00630061006C005C00740065006D0070005C0030003200300038005F0035003400370034003100380036003900370035003000310033003200 2E0064006F006300000000000000000

(PID) Process: (2124) 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: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Max Display
Value: ♀

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: write **Name:** Max Display
Value: 25

(PID) Process: (2124) 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: (2124) 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: (2124) 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: (2124) 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: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 3
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 4
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 5
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 6
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 7
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 8
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 9

Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 10
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 11
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 12
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 13
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 14
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 15
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 16
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 17
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 18
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 19
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 20
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 21
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 22
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 23
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 24
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 25
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 26
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 27
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 28
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 29

Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 30
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 31
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 32
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 33
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 34
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 35
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 36
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 37
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 38
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 39
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 40
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 41
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 42
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 43
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 44
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 45
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 46
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 47
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 48
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 49

Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 50
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint
Operation: delete value **Name:** Site 1
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint
Operation: delete value **Name:** Site 2
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint
Operation: delete value **Name:** Site 3
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint
Operation: delete value **Name:** Site 4
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint
Operation: delete value **Name:** Site 5
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint
Operation: delete value **Name:** Site 6
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint
Operation: delete value **Name:** Site 7
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint
Operation: delete value **Name:** Site 8
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint
Operation: delete value **Name:** Site 9
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint
Operation: delete value **Name:** Site 10
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint
Operation: delete value **Name:** Site 11
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint
Operation: delete value **Name:** Site 12
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint
Operation: delete value **Name:** Site 13
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint
Operation: delete value **Name:** Site 14
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint
Operation: delete value **Name:** Site 15
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint
Operation: delete value **Name:** Site 16
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint
Operation: delete value **Name:** Site 17
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint
Operation: delete value **Name:** Site 18
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint
Operation: delete value **Name:** Site 19

Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint
Operation: delete value **Name:** Site 20
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Max Display
Value: ♀

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: write **Name:** Max Display
Value: 25

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 1
Value: [F00000000][T01D3793B5EF69F80][O00000000]*C:\Users\admin\Desktop\easyfoundation.rtf

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: write **Name:** Item 1
Value: [F00000000][T01D3793B5EF69F80][O00000000]*C:\Users\admin\Desktop\easyfoundation.rtf

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 2
Value: [F00000000][T01D5972F96F53000][O00000000]*C:\Users\admin\Desktop\indiaside.rtf

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: write **Name:** Item 2
Value: [F00000000][T01D5972F96F53000][O00000000]*C:\Users\admin\Desktop\indiaside.rtf

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 3
Value: [F00000000][T01D8A21A0AE5D280][O00000000]*C:\Users\admin\Desktop\ourprotection.rtf

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: write **Name:** Item 3
Value: [F00000000][T01D8A21A0AE5D280][O00000000]*C:\Users\admin\Desktop\ourprotection.rtf

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 4
Value: [F00000000][T01D52189BCE05F00][O00000000]*C:\Users\admin\Documents\fnaked.rtf

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: write **Name:** Item 4
Value: [F00000000][T01D52189BCE05F00][O00000000]*C:\Users\admin\Documents\fnaked.rtf

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 5
Value: [F00000000][T01D73F7DF4F63100][O00000000]*C:\Users\admin\Documents\estcompleted.rtf

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: write **Name:** Item 5
Value: [F00000000][T01D73F7DF4F63100][O00000000]*C:\Users\admin\Documents\estcompleted.rtf

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 6
Value: [F00000000][T01D27F0F49D96F00][O00000000]*C:\Users\admin\Documents\andpa.rtf

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: write **Name:** Item 6
Value: [F00000000][T01D27F0F49D96F00][O00000000]*C:\Users\admin\Documents\andpa.rtf

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 7
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 8
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 9
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 10
Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 11

Value:

(PID) Process: (2124) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value Name: Item 12
Value:

(PID) Process: (2124) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value Name: Item 13
Value:

(PID) Process: (2124) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value Name: Item 14
Value:

(PID) Process: (2124) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value Name: Item 15
Value:

(PID) Process: (2124) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value Name: Item 16
Value:

(PID) Process: (2124) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value Name: Item 17
Value:

(PID) Process: (2124) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value Name: Item 18
Value:

(PID) Process: (2124) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value Name: Item 19
Value:

(PID) Process: (2124) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value Name: Item 20
Value:

(PID) Process: (2124) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value Name: Item 21
Value:

(PID) Process: (2124) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value Name: Item 22
Value:

(PID) Process: (2124) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value Name: Item 23
Value:

(PID) Process: (2124) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value Name: Item 24
Value:

(PID) Process: (2124) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value Name: Item 25
Value:

(PID) Process: (2124) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value Name: Item 26
Value:

(PID) Process: (2124) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value Name: Item 27
Value:

(PID) Process: (2124) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value Name: Item 28
Value:

(PID) Process: (2124) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value Name: Item 29
Value:

(PID) Process: (2124) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value Name: Item 30
Value:

(PID) Process: (2124) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value Name: Item 31

Value:			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation:	delete value	**Name:**	Item 32
Value:			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation:	delete value	**Name:**	Item 33
Value:			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation:	delete value	**Name:**	Item 34
Value:			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation:	delete value	**Name:**	Item 35
Value:			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation:	delete value	**Name:**	Item 36
Value:			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation:	delete value	**Name:**	Item 37
Value:			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation:	delete value	**Name:**	Item 38
Value:			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation:	delete value	**Name:**	Item 39
Value:			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation:	delete value	**Name:**	Item 40
Value:			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation:	delete value	**Name:**	Item 41
Value:			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation:	delete value	**Name:**	Item 42
Value:			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation:	delete value	**Name:**	Item 43
Value:			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation:	delete value	**Name:**	Item 44
Value:			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation:	delete value	**Name:**	Item 45
Value:			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation:	delete value	**Name:**	Item 46
Value:			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation:	delete value	**Name:**	Item 47
Value:			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation:	delete value	**Name:**	Item 48
Value:			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation:	delete value	**Name:**	Item 49
Value:			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation:	delete value	**Name:**	Item 50
Value:			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\18240E
Operation:	write	**Name:**	18240E

Value:

```
040000004C0800003900000043003A005C0055007300650072 0073005C00610064006D0069006E005C0041007000700044006100740061005C004C006F00630061006C005C00540065006D0
070005C0030003200300038005F00350034003700340031003800360039003700350030003100330032002E0064006F00630017000000300032003000 38005F00350034003700340031003800
360039003700350030003100330032002E0064006F0063000000000000010000000000000003C23775CC576DA010E2418000E2418000000000000DB040000000000000000000000000000000
000000000000000FFFFFFFF00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000FF
FFFFFF
```

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems

Operation: delete value **Name:** !k

Value: 次 ᔑ

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems

Operation: delete value **Name:** 0i

Value: 椰 ᔑ

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems

Operation: delete key **Name:** (default)

Value:

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems

Operation: write **Name:** rm

Value: 726D20004C08000002000000000000008E000000010000005000000032000000063003A005C00700072006F006700720061007E0031005C006D00690063072006F0073007E0031005C006F00660066006900630065003100034005C00670065006E006B006F002E0064006C006C0000006D006900630072006F0073006F0066007400200077006F00720064002000D0C6E0ACC0C9200094CD00AC200030AEA5B20000

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems

Operation: delete value **Name:** rm

Value: 浲 ᔑ

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems

Operation: write **Name:** 1n

Value: 316E20004C08000002000000000000008E000000010000005000000032000000063003A005C00700072006F006700720061007E0031005C006D00690063072006F0073007E0031005C006F00660066006900630065003100034005C00670065006E006B006F002E0064006C006C0000006D006900630072006F0073006F0066007400200077006F00720064002000D0C6E0ACC0C9200094CD00AC200030AEA5B20000

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems

Operation: delete value **Name:** 1n

Value: 湱 ᔑ

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100A0C00000000000F01FEC\Usage

Operation: write **Name:** SpellingAndGrammarFiles_3082

Value:

(PID) Process: (2124) 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: (2124) WINWORD.EXE **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F100904000000000000F01FEC\Usage

Operation: write **Name:** SpellingAndGrammarFiles_1033

Value:

(PID) Process: (2124) 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: (2124) 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: (2124) 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: (2124) 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: (2124) 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: (2124) 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: (2124) 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: (2124) 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: (2124) 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: (2124) 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: (2124) 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: (2124) 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: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems

Operation: write **Name:** .n

Value: 2E6E20004C0800000200000000000000008E000000010000005000000032000000630003A005C00700072006F006700720061007E0031005C006D006900630072006F0073007E0031005C006F00
66006600690063006500310034005C00670065006E006B006F002E0064006C006C0000006D006900630072006F0073006F00660074002000770006F00720064002000D0C6E0ACC0C9200094C
D00AC200030AEA5B20000

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems

Operation: delete value **Name:** .n

Value: 湤 ы

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems

Operation: write **Name:** >n

Value: 3E6E20004C0800000200000000000000008E000000010000005000000032000000630003A005C00700072006F006700720061007E0031005C006D006900630072006F0073007E0031005C006F00
66006600690063006500310034005C00670065006E006B006F002E0064006C006C0000006D006900630072006F0073006F00660074002000770006F00720064002000D0C6E0ACC0C9200094C
D00AC200030AEA5B20000

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems

Operation: delete value **Name:** >n

Value: 渾 ы

(PID) Process: (3276) rundll32.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings

Operation: write **Name:** ProxyEnable

Value: 0

(PID) Process: (3276) rundll32.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings

Operation: delete value **Name:** ProxyServer

Value:

(PID) Process: (3276) rundll32.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings

Operation: delete value **Name:** ProxyOverride

Value:

(PID) Process: (3276) rundll32.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings

Operation: delete value **Name:** AutoConfigURL

Value:

(PID) Process: (3276) rundll32.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings

Operation: delete value **Name:** AutoDetect

Value:

(PID) Process: (3276) rundll32.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections

Operation: write **Name:** SavedLegacySettings

Value: 460000005C0100000900000000000000000000000000000000040000000000000000C0E333BBEAB1D3010000000000000000000000000000000001000000020000000C0A8016B0000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000

(PID) Process:	(3276) rundll32.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{FCC67766-6201-4AD1-A6B8-2F4553C93D47}
Operation:	write	Name:	WpadDecisionReason
Value:	1		

(PID) Process:	(3276) rundll32.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{FCC67766-6201-4AD1-A6B8-2F4553C93D47}
Operation:	write	Name:	WpadDecisionTime
Value:	3060F95DC576DA01		

(PID) Process:	(3276) rundll32.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{FCC67766-6201-4AD1-A6B8-2F4553C93D47}
Operation:	write	Name:	WpadDecision
Value:	0		

(PID) Process:	(3276) rundll32.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{FCC67766-6201-4AD1-A6B8-2F4553C93D47}
Operation:	write	Name:	WpadNetworkName
Value:	Network 3		

(PID) Process:	(3276) rundll32.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{FCC67766-6201-4AD1-A6B8-2F4553C93D47}
Operation:	delete value	Name:	WpadDetectedUrl
Value:			

(PID) Process:	(3276) rundll32.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:	(3276) rundll32.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\52-54-00-36-3e-ff
Operation:	write	Name:	WpadDecisionTime
Value:	3060F95DC576DA01		

(PID) Process:	(3276) rundll32.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:	(3276) rundll32.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:	(3276) rundll32.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
Operation:	write	Name:	CachePrefix
Value:			

(PID) Process:	(3276) rundll32.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
Operation:	write	Name:	CachePrefix
Value:	Cookie:		

(PID) Process:	(3276) rundll32.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
Operation:	write	Name:	CachePrefix
Value:	Visited:		

(PID) Process:	(2124) WINWORD.EXE	Key:	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Licensing
Operation:	write	Name:	019C826E445A4649A5B00BF08FCC4EEE
Value:	01000000270000007B39303134303030302D303033442D303030302D303030302D303030303030303046463143457D005A0000004F006600660069006300650020003100340002C0020004F0066006600690063006500500072006F0066006500730073069006F006E0061006C002D0052006500740061069006C0020006500640069007400069006F006E000000		

(PID) Process:	(2124) WINWORD.EXE	Key:	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word
Operation:	delete value	Name:	FontInfoCacheW
Value:	`		

(PID) Process:	(2124) WINWORD.EXE	Key:	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	Name:	@Ami R
Value:	0		

(PID) Process:	(2124) WINWORD.EXE	Key:	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	Name:	@Arial Unicode MS
Value:	0		

(PID) Process:	(2124) WINWORD.EXE	Key:	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	Name:	@Batang
Value:	0		

(PID) Process:	(2124) WINWORD.EXE	Key:	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	Name:	@BatangChe
Value:	0		

(PID) Process:	(2124) WINWORD.EXE	Key:	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	Name:	@DFKai-SB
Value:	0		

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @Dotum
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @DotumChe
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @Expo M
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @FangSong
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @Gulim
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @GulimChe
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @Gungsuh
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @GungsuhChe
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @Headline R
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @HGGothicE
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @HGGothicM
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @HGGyoshotai
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @HGKyokashotai
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @HGMaruGothicMPRO
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @HGMinchoB
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @HGMinchoE
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @HGPGothicE
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @HGPGothicM
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @HGPGyoshotai
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @HGPKyokashotai
Value: 0

(PID) Process: (2124) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write Name: @HGPMinchoB
Value: 0

(PID) Process: (2124) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write Name: @HGPMinchoE
Value: 0

(PID) Process: (2124) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write Name: @HGPSoeiKakugothicUB
Value: 0

(PID) Process: (2124) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write Name: @HGPSoeiKakupoptai
Value: 0

(PID) Process: (2124) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write Name: @HGPSoeiPresenceEB
Value: 0

(PID) Process: (2124) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write Name: @HGSeikaishotaiPRO
Value: 0

(PID) Process: (2124) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write Name: @HGSGothicE
Value: 0

(PID) Process: (2124) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write Name: @HGSGothicM
Value: 0

(PID) Process: (2124) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write Name: @HGSGyoshotai
Value: 0

(PID) Process: (2124) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write Name: @HGSKyokashotai
Value: 0

(PID) Process: (2124) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write Name: @HGSMinchoB
Value: 0

(PID) Process: (2124) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write Name: @HGSMinchoE
Value: 0

(PID) Process: (2124) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write Name: @HGSoeiKakugothicUB
Value: 0

(PID) Process: (2124) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write Name: @HGSoeiKakupoptai
Value: 0

(PID) Process: (2124) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write Name: @HGSoeiPresenceEB
Value: 0

(PID) Process: (2124) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write Name: @HGSSoeiKakugothicUB
Value: 0

(PID) Process: (2124) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write Name: @HGSSoeiKakupoptai
Value: 0

(PID) Process: (2124) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write Name: @HGSSoeiPresenceEB
Value: 0

(PID) Process: (2124) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write Name: @HYGothic-Extra
Value: 0

(PID) Process: (2124) WINWORD.EXE Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write Name: @HYGothic-Medium
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @HYGraphic-Medium
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @HYGungSo-Bold
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @HYHeadLine-Medium
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @HYMyeongJo-Extra
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @HYPMokGak-Bold
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @HYPost-Light
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @HYPost-Medium
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @HYShortSamul-Medium
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @HYSinMyeongJo-Medium
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @KaiTi
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @Magic R
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @Malgun Gothic
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @Meiryo
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @Meiryo UI
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @Microsoft JhengHei
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @Microsoft YaHei
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @MingLiU
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @MingLiU_HKSCS
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @MingLiU_HKSCS-ExtB
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @MingLiU-ExtB
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @MoeumT R
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @MS Gothic
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @MS Mincho
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @MS PGothic
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @MS PMincho
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @MS UI Gothic
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @New Gulim
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @NSimSun
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @PMingLiU
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @PMingLiU-ExtB
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @Pyunji R
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @SimHei
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @SimSun
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @SimSun-ExtB
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @Yet R
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Agency FB
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Aharoni
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Algerian
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Ami R
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Andalus
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Angsana New
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** AngsanaUPC
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Aparajita
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Arabic Typesetting
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Arial
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Arial Black
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Arial Narrow
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Arial Rounded MT Bold
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Arial Unicode MS
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Baskerville Old Face
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Batang
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** BatangChe
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Bauhaus 93
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Bell MT
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Berlin Sans FB
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Berlin Sans FB Demi
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Bernard MT Condensed
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Blackadder ITC
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Bodoni MT
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Bodoni MT Black
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Bodoni MT Condensed
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Bodoni MT Poster Compressed
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Book Antiqua
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Bookman Old Style
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Bookshelf Symbol 7
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Bradley Hand ITC
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Britannic Bold
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Broadway
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Browallia New
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** BrowalliaUPC
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Brush Script MT
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Calibri
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Calibri Light
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Californian FB
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Calisto MT
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Cambria
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Cambria Math
Value: 1

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Candara
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Castellar
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Centaur
Value: 0

(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Century
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Century Gothic
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Century Schoolbook
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Chiller
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Colonna MT
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Comic Sans MS
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Consolas
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Constantia
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Cooper Black
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Copperplate Gothic Bold
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Copperplate Gothic Light
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Corbel
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Cordia New
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	CordiaUPC
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Courier
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Courier New
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Curlz MT
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	DaunPenh
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	David
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	DFKai-SB
Value: 0			

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** DilleniaUPC
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** DokChampa
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Dotum
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** DotumChe
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Ebrima
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Edwardian Script ITC
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Elephant
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Engravers MT
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Eras Bold ITC
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Eras Demi ITC
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Eras Light ITC
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Eras Medium ITC
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Estrangelo Edessa
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** EucrosiaUPC
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Euphemia
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Expo M
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** FangSong
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Felix Titling
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Fixedsys
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Footlight MT Light
Value: 0

(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Forte
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Franklin Gothic Book
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Franklin Gothic Demi
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Franklin Gothic Demi Cond
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Franklin Gothic Heavy
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Franklin Gothic Medium
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Franklin Gothic Medium Cond
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	FrankRuehl
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	FreesiaUPC
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Freestyle Script
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	French Script MT
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Gabriola
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Garamond
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Gautami
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Georgia
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Gigi
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Gill Sans MT
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Gill Sans MT Condensed
Value: 0			
(PID) Process:	(2124) 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:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Gill Sans Ultra Bold
Value: 0			

(PID) Process:	Operation:	Value:	Key:	Name:
(2124) WINWORD.EXE	write	0	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Gill Sans Ultra Bold Condensed
(2124) WINWORD.EXE	write	0	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Gisha
(2124) WINWORD.EXE	write	0	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Gloucester MT Extra Condensed
(2124) WINWORD.EXE	write	0	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Goudy Old Style
(2124) WINWORD.EXE	write	0	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Goudy Stout
(2124) WINWORD.EXE	write	0	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Gulim
(2124) WINWORD.EXE	write	0	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	GulimChe
(2124) WINWORD.EXE	write	0	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Gungsuh
(2124) WINWORD.EXE	write	0	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	GungsuhChe
(2124) WINWORD.EXE	write	0	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Haettenschweiler
(2124) WINWORD.EXE	write	0	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Harlow Solid Italic
(2124) WINWORD.EXE	write	0	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Harrington
(2124) WINWORD.EXE	write	0	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	Headline R
(2124) WINWORD.EXE	write	0	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	HGGothicE
(2124) WINWORD.EXE	write	0	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	HGGothicM
(2124) WINWORD.EXE	write	0	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	HGGyoshotai
(2124) WINWORD.EXE	write	0	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	HGKyokashotai
(2124) WINWORD.EXE	write	0	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	HGMaruGothicMPRO
(2124) WINWORD.EXE	write	0	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	HGMinchoB
(2124) WINWORD.EXE	write	0	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts	HGMinchoE

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGPGothicE
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGPGothicM
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGPGyoshotai
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGPKyokashotai
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGPMinchoB
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGPMinchoE
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGPSoeiKakugothicUB
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGPSoeiKakupoptai
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGPSoeiPresenceEB
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGSeikaishotaiPRO
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGSGothicE
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGSGothicM
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGSGyoshotai
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGSKyokashotai
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGSMinchoB
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGSMinchoE
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGSoeiKakugothicUB
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGSoeiKakupoptai
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGSoeiPresenceEB
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGSSoeiKakugothicUB
Value: 0

(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	HGSSoeiKakupoptai
Value:	0		
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	HGSSoeiPresenceEB
Value:	0		
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	High Tower Text
Value:	0		
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	HYGothic-Extra
Value:	0		
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	HYGothic-Medium
Value:	0		
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	HYGraphic-Medium
Value:	0		
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	HYGungSo-Bold
Value:	0		
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	HYHeadLine-Medium
Value:	0		
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	HYMyeongJo-Extra
Value:	0		
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	HYPMokGak-Bold
Value:	0		
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	HYPost-Light
Value:	0		
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	HYPost-Medium
Value:	0		
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	HYShortSamul-Medium
Value:	0		
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	HYSinMyeongJo-Medium
Value:	0		
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Impact
Value:	0		
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Imprint MT Shadow
Value:	0		
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Informal Roman
Value:	0		
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	IrisUPC
Value:	0		
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Iskoola Pota
Value:	0		
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	JasmineUPC
Value:	0		

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Jokerman
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Juice ITC
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** KaiTi
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Kalinga
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Kartika
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Khmer UI
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** KodchiangUPC
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Kokila
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Kristen ITC
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Kunstler Script
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Lao UI
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Latha
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Leelawadee
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Levenim MT
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** LilyUPC
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Lucida Bright
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Lucida Calligraphy
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Lucida Console
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Lucida Fax
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Lucida Handwriting
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Lucida Sans
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Lucida Sans Typewriter
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Lucida Sans Unicode
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Magic R
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Magneto
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Maiandra GD
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Malgun Gothic
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Mangal
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Marlett
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Matura MT Script Capitals
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Meiryo
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Meiryo UI
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Microsoft Himalaya
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Microsoft JhengHei
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Microsoft New Tai Lue
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Microsoft PhagsPa
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Microsoft Sans Serif
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Microsoft Tai Le
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Microsoft Uighur
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Microsoft YaHei
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Microsoft Yi Baiti
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** MingLiU
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** MingLiU_HKSCS
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** MingLiU_HKSCS-ExtB
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** MingLiU-ExtB
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Miriam
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Miriam Fixed
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Mistral
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Modern No. 20
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** MoeumT R
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Mongolian Baiti
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Monotype Corsiva
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** MoolBoran
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** MS Gothic
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** MS Mincho
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** MS Outlook
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** MS PGothic
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** MS PMincho
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** MS Reference Sans Serif
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** MS Reference Specialty
Value: 0

(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	MS Sans Serif
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	MS Serif
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	MS UI Gothic
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	MT Extra
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	MV Boli
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Narkisim
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	New Gulim
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Niagara Engraved
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Niagara Solid
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	NSimSun
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Nyala
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	OCR A Extended
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	OCRB
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Old English Text MT
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Onyx
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Palace Script MT
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Palatino Linotype
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Papyrus
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Parchment
Value: 0			
(PID) Process:	(2124) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Perpetua
Value: 0			

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Perpetua Titling MT
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Plantagenet Cherokee
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Playbill
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** PMingLiU
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** PMingLiU-ExtB
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Poor Richard
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Pristina
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Pyunji R
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Raavi
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Rage Italic
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Ravie
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Rockwell
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Rockwell Condensed
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Rockwell Extra Bold
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Rod
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Sakkal Majalla
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Script MT Bold
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Segoe Print
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Segoe Script
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Segoe UI
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Segoe UI Light
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Segoe UI Semibold
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Segoe UI Symbol
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Shonar Bangla
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Showcard Gothic
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Shruti
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** SimHei
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Simplified Arabic
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Simplified Arabic Fixed
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** SimSun
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** SimSun-ExtB
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Small Fonts
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Snap ITC
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Stencil
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Sylfaen
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Symbol
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** System
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Tahoma
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Tempus Sans ITC
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Terminal
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Times New Roman
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Traditional Arabic
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Trebuchet MS
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Tunga
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Tw Cen MT
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Tw Cen MT Condensed
Value: 0

(PID) Process: (2124) 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: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Utsaah
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Vani
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Verdana
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Vijaya
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Viner Hand ITC
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Vivaldi
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Vladimir Script
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Vrinda
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Webdings
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Wide Latin
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Wingdings
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Wingdings 2
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Wingdings 3
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Yet R
Value: 0

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems
Operation: write **Name:** I3
Value: 6C3320004C080000020000000000000008E000000010000005000000003200000063003A005C00700072006F006700720061007E0031005C006D00690063007200 6F0073007E0031005C006F006600660069006300650031003400 5C00670065006E006B006F002E0064006C006C0000006D006900630072006F0073006F0066007400200077006F00720064002000D0C6E0ACC0C9200094CD00AC200030AEA5B20000

(PID) Process: (2124) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems
Operation: delete value **Name:** I3
Value: 20点 ⩊

Files activity

Executable files	Suspicious files	Text files	Unknown types
2	1	1	2

Dropped files

PID	Process	Filename	Type
2124	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\CVR2110.tmp.cvr **MD5:** — **SHA256:** —	—
2124	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4497D6B6.emf **MD5:** A08286784C9F2B367F405D02EECA6D49 **SHA256:** 91EC41F1FBBB6769B0F1D9062384CAFD742AF6B2E0FC790B60FF24E1E9BFE2E3	emf
2124	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\Wh102yYa.tmp:Zone.Identifier **MD5:** FBCCF14D504B7B2DBCB5A5BDA75BD93B **SHA256:** EACD09517CE90D34BA562171D15AC40D302F0E691B439F91BE1B6406E25F5913	text
2124	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\~$Normal.dotm **MD5:** 280D2B65A6285DCE35099F1721B7999D **SHA256:** 9C481BFD497634B56792F1F82F7323677D76F0ECD94EC28D527714D4DEF38B52	pgc
2124	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\W0rd.dll **MD5:** 70B2822E6CF4AB4CDE9808B0DBA3A9DD **SHA256:** 0D7AA23A72D22DCF47F8723C58D101B3B113CBC79DD407A6FAC0E65D67076EA1	executable
2124	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\Wh102yYa.tmp **MD5:** 70B2822E6CF4AB4CDE9808B0DBA3A9DD **SHA256:** 0D7AA23A72D22DCF47F8723C58D101B3B113CBC79DD407A6FAC0E65D67076EA1	executable
2124	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\~$08_54741869750132.doc **MD5:** 0F4CD5E63B53E134FC987D180E28FA04 **SHA256:** CB7B20290717C1EEFA9D1A3D04F02FD7CDBFE2BACD85360502EFA31DE07208EB	pgc

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
2	6	13	0

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
3276	rundll32.exe	POST	200	34.126.189.157:80	http://satursed.com/8/forum.php	unknown	—	—	unknown
3276	rundll32.exe	GET	200	104.26.12.205:80	http://api.ipify.org/	unknown	text	12 b	unknown

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
4	System	192.168.100.255:137	—	—	—	whitelisted
4	System	192.168.100.255:138	—	—	—	whitelisted
—	—	224.0.0.252:5355	—	—	—	unknown
1080	svchost.exe	224.0.0.252:5355	—	—	—	unknown
3276	rundll32.exe	104.26.12.205:80	api.ipify.org	CLOUDFLARENET	US	unknown
3276	rundll32.exe	34.126.189.157:80	satursed.com	GOOGLE-CLOUD-PLATFORM	SG	unknown

DNS requests

Domain	IP	Reputation
api.ipify.org	104.26.12.205 104.26.13.205 172.67.74.152	shared
satursed.com	34.126.189.157	unknown
sameastar.ru	—	unknown
dns.msftncsi.com	131.107.255.255	shared
ludiesibut.ru	—	unknown

Threats

PID	Process	Class	Message
1080	svchost.exe	Misc activity	ET INFO External IP Lookup Domain (ipify .org) in DNS Lookup
3276	rundll32.exe	Device Retrieving External IP Address Detected	ET POLICY External IP Lookup api.ipify.org
3276	rundll32.exe	Device Retrieving External IP Address Detected	POLICY [ANY.RUN] External IP Lookup by HTTP (api .ipify .org)
3276	rundll32.exe	Malware Command and Control Activity Detected	ET MALWARE Tordal/Hancitor/Chanitor Checkin
3276	rundll32.exe	A Network Trojan was detected	ET MALWARE Possible Compromised Host AnubisNetworks Sinkhole Cookie Value Snkz
3276	rundll32.exe	A Network Trojan was detected	ET MALWARE Possible Compromised Host AnubisNetworks Sinkhole Cookie Value btst

Debug output strings

No debug info

ANY.RUN
INTERACTIVE MALWARE ANALYSIS

Interactive malware hunting service ANY.RUN