ANY RUN
INTERACTIVE MALWARE ANALYSIS

General Info

File name:	test.html
Full analysis:	https://app.any.run/tasks/95932f01-54cc-4704-9ce5-099df5c6315e
Verdict:	Malicious activity
Analysis date:	March 15, 2024 at 15:59:17
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Tags:	maldoc-57
Indicators:	
MIME:	text/html
File info:	HTML document, ASCII text, with very long lines (64950)
MD5:	81F1BAD1F8F01C561E83204F40F19A76
SHA1:	945ACA28ADCBAAED1CA8C2666693D336DA57D25D
SHA256:	858AAC988E85075348F32E4750F17BF5C16E579FFF258D3DEF9F23563E89372D
SSDEEP:	24576:jZHTcRqtm3eZ1diSQsyOWciO1vBFeNnTuppTct6DH6cBfiAK3I9Z:RZmORzQsyOlWBFeNnTuLTVacgAK6

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 known malicious document
- chrome.exe (PID: 120)
- WINWORD.EXE (PID: 3620)

SUSPICIOUS

Non-standard symbols in registry
- WINWORD.EXE (PID: 3620)

Application launched itself
- WINWORD.EXE (PID: 3620)

INFO

The process uses the downloaded file
- chrome.exe (PID: 1544)
- WINWORD.EXE (PID: 3620)

Reads Microsoft Office registry keys
- chrome.exe (PID: 120)

Application launched itself
- chrome.exe (PID: 120)

Malware configuration

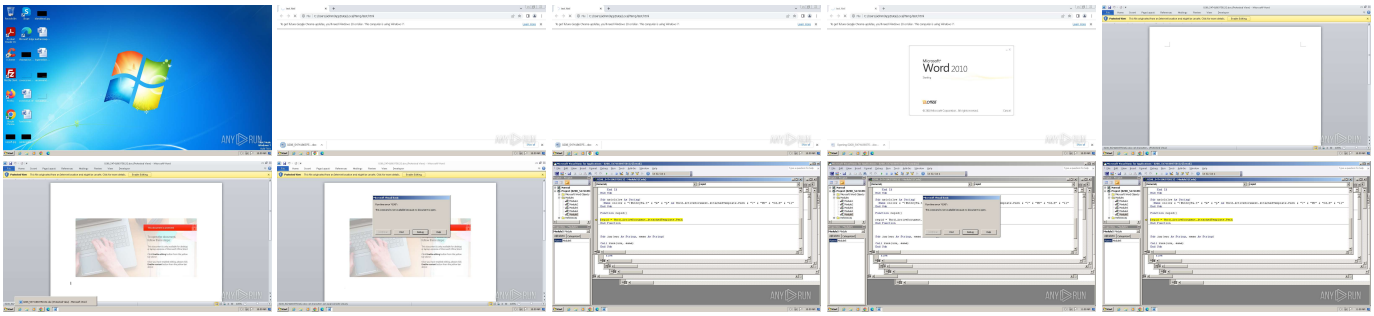
No Malware configuration.

Static information

TRiD

.html | HyperText Markup Language (100)

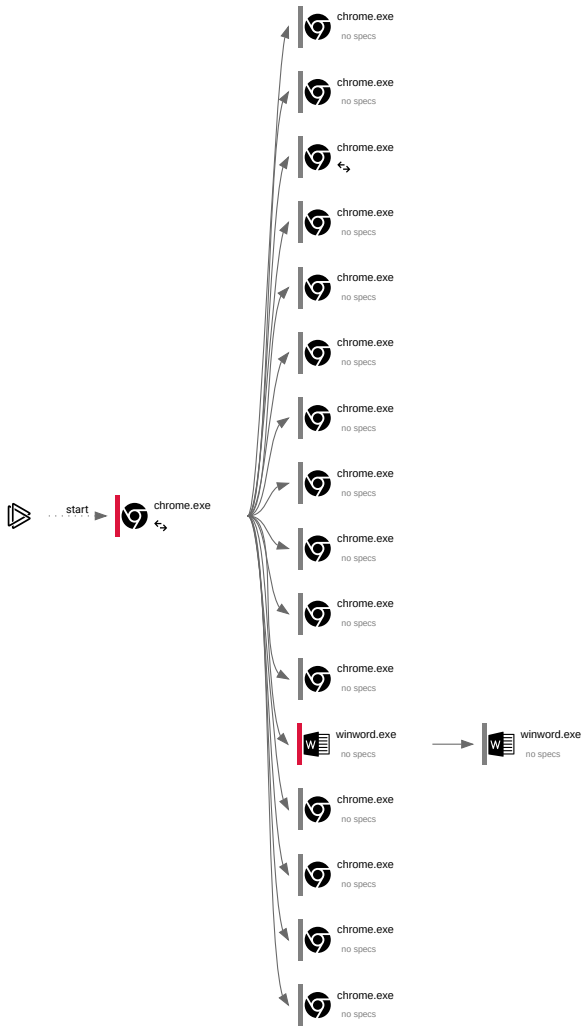
Video and screenshots



Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
54	18	2	0

Behavior graph



Specs description

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

Process information

PID	CMD	Path	Indicators	Parent process
120	"C:\Program Files\Google\Chrome\Application\chrome.exe" "C:\Users\admin\AppData\Local\Temp\test.html"	C:\Program Files\Google\Chrome\Application\chrome.exe		explorer.exe

Information

User:	admin	**Company:**	Google LLC
Integrity Level:	MEDIUM	**Description:**	Google Chrome
Version:	109.0.5414.120		

2124	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=crashpad-handler "--user-data-dir=C:\Users\admin\AppData\Local\Google\Chrome\User Data" /prefetch:7 --monitor-self-annotation=ptype=crashpad-handler "--database=C:\Users\admin\AppData\Local\Google\Chrome\User Data\Crashpad" --url=https://clients2.google.com/cr/report --annotation=channel= --annotation=plat=Win32 --annotation=prod=Chrome --annotation=ver=109.0.5414.120 --initial-client-data=0xc8,0xcc,0xd0,0x9c,0xd4,0x6bcd8b38,0x6bcd8b48,0x6bcd8b54	C:\Program Files\Google\Chrome\Application\chrome.exe	—	chrome.exe

Information

User:	admin	**Company:**	Google LLC
Integrity Level:	MEDIUM	**Description:**	Google Chrome
Version:	109.0.5414.120		

2208	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=gpu-process --gpu-preferences=UAAAAAAAAADgAAAYAAAAAAAAAAAAAAAAAABgAAAAAAAAwAAAAAAAAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEgAAAAAAAAASAAAAAAAAAAAYAAAAAgAAABAAAAAAAAAAGAAAAAAAAAAAQAAAAAAAAAAAAAAAOAAAAEAAAAAAAAABAAAADgAAAAgAAAAAAAAACAAAAAAAAAA= --mojo-platform-channel-handle=1112 --field-trial-handle=1144,i,2532196339168984491,11293414647763908868, 131072 /prefetch:2	C:\Program Files\Google\Chrome\Application\chrome.exe	—	chrome.exe

Information

User:	admin	**Company:**	Google LLC
Integrity Level:	LOW	**Description:**	Google Chrome
Exit code:	0	**Version:**	109.0.5414.120

2672	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --disable-quic --mojo-platform-channel-handle=1332 --field-trial-handle=1144,i,2532196339168984491,11293414647763908868, 131072 /prefetch:8	C:\Program Files\Google\Chrome\Application\chrome.exe	↪	chrome.exe

Information

User:	admin	**Company:**	Google LLC
Integrity Level:	MEDIUM	**Description:**	Google Chrome
Version:	109.0.5414.120		

956	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=storage.mojom.StorageService --lang=en-US --service-sandbox-type=service --disable-quic --mojo-platform-channel-handle=1536 --field-trial-handle=1144,i,2532196339168984491,11293414647763908868, 131072 /prefetch:8	C:\Program Files\Google\Chrome\Application\chrome.exe	—	chrome.exe

Information

User:	admin	**Company:**	Google LLC
Integrity Level:	LOW	**Description:**	Google Chrome
Version:	109.0.5414.120		

3068	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --first-renderer-process --lang=en-US --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=6 --mojo-platform-channel-handle=2120 --field-trial-handle=1144,i,2532196339168984491,11293414647763908868, 131072 /prefetch:1	C:\Program Files\Google\Chrome\Application\chrome.exe	—	chrome.exe

Information

User:	admin	**Company:**	Google LLC
Integrity Level:	LOW	**Description:**	Google Chrome
Exit code:	0	**Version:**	109.0.5414.120

2000	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --lang=en-US --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=5 --mojo-platform-channel-handle=2136 --field-trial-handle=1144,i,2532196339168984491,11293414647763908868, 131072 /prefetch:1	C:\Program Files\Google\Chrome\Application\chrome.exe	—	chrome.exe

Information

User:	admin	**Company:**	Google LLC
Integrity Level:	LOW	**Description:**	Google Chrome
Exit code:	0	**Version:**	109.0.5414.120

2804	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=gpu-process --gpu-preferences=UAAAAAAAAADgAAAYAAAAAAAAAAAAAAAAAABgAAAAAAAAwAAAAAAAAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEgAAAAAAAAASAAAAAAAAAAAYAAAAAgAAABAAAAAAAAAAGAAAAAAAAAAAQAAAAAAAAAAAAAAAOAAAAEAAAAAAAAABAAAADgAAAAgAAAAAAAAACAAAAAAAAAA= --use-gl=angle --use-angle=swiftshader-webgl --mojo-platform-channel-handle=1304 --field-trial-handle=1144,i,2532196339168984491,11293414647763908868, 131072 /prefetch:2	C:\Program Files\Google\Chrome\Application\chrome.exe	—	chrome.exe

Information

User:	admin	**Company:**	Google LLC
Integrity Level:	LOW	**Description:**	Google Chrome
Version:	109.0.5414.120		

2112	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --disable-gpu-compositing --lang=en-US --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=8 --mojo-platform-channel-handle=1480 --field-trial-handle=1144,i,2532196339168984491,11293414647763908868, 131072 /prefetch:1	C:\Program Files\Google\Chrome\Application\chrome.exe	–	chrome.exe

Information

User:	admin	**Company:**	Google LLC
Integrity Level:	LOW	**Description:**	Google Chrome
Version:	109.0.5414.120		

3984	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=chrome.mojom.DocumentAnalysisService --lang=en-US --service-sandbox-type=service --disable-quic --mojo-platform-channel-handle=3600 --field-trial-handle=1144,i,2532196339168984491,11293414647763908868, 131072 /prefetch:8	C:\Program Files\Google\Chrome\Application\chrome.exe	–	chrome.exe

Information

User:	admin	**Company:**	Google LLC
Integrity Level:	LOW	**Description:**	Google Chrome
Exit code:	0	**Version:**	109.0.5414.120

1544	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=quarantine.mojom.Quarantine --lang=en-US --service-sandbox-type=none --disable-quic --mojo-platform-channel-handle=4104 --field-trial-handle=1144,i,2532196339168984491,11293414647763908868, 131072 /prefetch:8	C:\Program Files\Google\Chrome\Application\chrome.exe	–	chrome.exe

Information

User:	admin	**Company:**	Google LLC
Integrity Level:	MEDIUM	**Description:**	Google Chrome
Exit code:	0	**Version:**	109.0.5414.120

2620	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=chrome.mojom.UtilWin --lang=en-US --service-sandbox-type=none --disable-quic --mojo-platform-channel-handle=4412 --field-trial-handle=1144,i,2532196339168984491,11293414647763908868, 131072 /prefetch:8	C:\Program Files\Google\Chrome\Application\chrome.exe	–	chrome.exe

Information

User:	admin	**Company:**	Google LLC
Integrity Level:	MEDIUM	**Description:**	Google Chrome
Exit code:	0	**Version:**	109.0.5414.120

3620	"C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /n "C:\Users\admin\Downloads\0208_54741869750132.doc"	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE	–	chrome.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Microsoft Word
Version:	14.0.6024.1000		

552	"C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Embedding	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE	–	WINWORD.EXE

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	LOW	**Description:**	Microsoft Word
Version:	14.0.6024.1000		

2956	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --disable-gpu-compositing --lang=en-US --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=12 --mojo-platform-channel-handle=3140 --field-trial-handle=1144,i,2532196339168984491,11293414647763908868, 131072 /prefetch:1	C:\Program Files\Google\Chrome\Application\chrome.exe	–	chrome.exe

Information

User:	admin	**Company:**	Google LLC
Integrity Level:	LOW	**Description:**	Google Chrome
Exit code:	0	**Version:**	109.0.5414.120

3112	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --disable-gpu-compositing --lang=en-US --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=13 --mojo-platform-channel-handle=2324 --field-trial-handle=1144,i,2532196339168984491,11293414647763908868, 131072 /prefetch:1	C:\Program Files\Google\Chrome\Application\chrome.exe	—	chrome.exe

Information

User:	admin	**Company:**	Google LLC
Integrity Level:	LOW	**Description:**	Google Chrome
Exit code:	0	**Version:**	109.0.5414.120

584	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --disable-gpu-compositing --lang=en-US --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=14 --mojo-platform-channel-handle=1976 --field-trial-handle=1144,i,2532196339168984491,11293414647763908868, 131072 /prefetch:1	C:\Program Files\Google\Chrome\Application\chrome.exe	—	chrome.exe

Information

User:	admin	**Company:**	Google LLC
Integrity Level:	LOW	**Description:**	Google Chrome
Version:	109.0.5414.120		

2740	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --disable-gpu-compositing --lang=en-US --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=15 --mojo-platform-channel-handle=2272 --field-trial-handle=1144,i,2532196339168984491,11293414647763908868, 131072 /prefetch:1	C:\Program Files\Google\Chrome\Application\chrome.exe	—	chrome.exe

Information

User:	admin	**Company:**	Google LLC
Integrity Level:	LOW	**Description:**	Google Chrome
Version:	109.0.5414.120		

Registry activity

Total events	Read events	Write events	Delete events
15 240	14 491	541	208

Modification events

(PID) Process:	(120) chrome.exe	**Key:**	HKEY_CURRENT_USER\Software\Google\Chrome\BLBeacon
Operation:	write	**Name:**	failed_count
Value:	0		

(PID) Process:	(120) chrome.exe	**Key:**	HKEY_CURRENT_USER\Software\Google\Chrome\BLBeacon
Operation:	write	**Name:**	state
Value:	2		

(PID) Process:	(120) chrome.exe	**Key:**	HKEY_CURRENT_USER\Software\Google\Chrome\ThirdParty
Operation:	write	**Name:**	StatusCodes
Value:			

(PID) Process:	(120) chrome.exe	**Key:**	HKEY_CURRENT_USER\Software\Google\Chrome\ThirdParty
Operation:	write	**Name:**	StatusCodes
Value:	01000000		

(PID) Process:	(120) chrome.exe	**Key:**	HKEY_CURRENT_USER\Software\Google\Chrome\BLBeacon
Operation:	write	**Name:**	state
Value:	1		

(PID) Process:	(120) chrome.exe	**Key:**	HKEY_CURRENT_USER\Software\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation:	write	**Name:**	dr
Value:	1		

(PID) Process:	(120) chrome.exe	**Key:**	HKEY_CURRENT_USER\Software\Google\Chrome\StabilityMetrics
Operation:	write	**Name:**	user_experience_metrics.stability.exited_cleanly
Value:	0		

(PID) Process:	(120) chrome.exe	**Key:**	HKEY_CURRENT_USER\Software\Google\Chrome
Operation:	write	**Name:**	UsageStatsInSample
Value:	0		

(PID) Process:	(120) chrome.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\Google\Update\ClientStateMedium\{8A69D345-D564-463C-AFF1-A69D9E530F96}
Operation:	write	**Name:**	usagestats

Value: 0

(PID) Process: (120) chrome.exe **Key:** HKEY_CURRENT_USER\Software\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation: write **Name:** metricsid
Value:

(PID) Process: (120) chrome.exe **Key:** HKEY_CURRENT_USER\Software\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation: write **Name:** metricsid_installdate
Value: 0

(PID) Process: (120) chrome.exe **Key:** HKEY_CURRENT_USER\Software\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation: write **Name:** metricsid_enableddate
Value: 0

(PID) Process: (120) chrome.exe **Key:** HKEY_CURRENT_USER\Software\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation: write **Name:** lastrun
Value: 13354973969434500

(PID) Process: (1544) chrome.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** ProxyBypass
Value: 1

(PID) Process: (1544) chrome.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** IntranetName
Value: 1

(PID) Process: (1544) chrome.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** UNCAsIntranet
Value: 1

(PID) Process: (1544) chrome.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** AutoDetect
Value: 0

(PID) Process: (1544) chrome.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Discardable\PostSetup\Component Categories\{56FFCC30-D398-11D0-B2AE-00A0C908FA49}\Enum
Operation: write **Name:** Implementing
Value: 1C000000010000000E807030005000F000A003B002500D500010000001E768127E028094199FEB9D127C57AFE

(PID) Process: (1544) chrome.exe **Key:** HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Discardable\PostSetup\Component Categories\{56FFCC30-D398-11D0-B2AE-00A0C908FA49}\Enum
Operation: write **Name:** Implementing
Value: 1C000000010000000E807030005000F000A003B002500DB00010000001E768127E028094199FEB9D127C57AFE

(PID) Process: (2620) chrome.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\182\52C64B7E
Operation: write **Name:** LanguageList
Value: en-US

(PID) Process: (120) chrome.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: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems
Operation: write **Name:** h¨;
Value: 687F3B00240E0000010000000000000000000000

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation: write **Name:** 1033
Value: Off

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation: write **Name:** 1041
Value: Off

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation: write **Name:** 1046
Value: Off

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation: write **Name:** 1036
Value: Off

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation: write **Name:** 1031
Value: Off

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation: write **Name:** 1040
Value: Off

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation:	write	**Name:**	1049
Value:	Off		
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation:	write	**Name:**	3082
Value:	Off		
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation:	write	**Name:**	1042
Value:	Off		
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation:	write	**Name:**	1055
Value:	Off		
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation:	write	**Name:**	1033
Value:	On		
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation:	write	**Name:**	1041
Value:	On		
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation:	write	**Name:**	1042
Value:	On		
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation:	write	**Name:**	1046
Value:	On		
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation:	write	**Name:**	1036
Value:	On		
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation:	write	**Name:**	1031
Value:	On		
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation:	write	**Name:**	1040
Value:	On		
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation:	write	**Name:**	1049
Value:	On		
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation:	write	**Name:**	3082
Value:	On		
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation:	write	**Name:**	1055
Value:	On		
(PID) Process:	(3620) 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:	(3620) 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:	(3620) 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:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word
Operation:	write	**Name:**	MTTT
Value:	240E00008E0D91E2C776DA0100000000		
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LCCache\Themes\1033
Operation:	delete value	**Name:**	NextUpdate
Value:			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LCCache\WordDocParts\1033

Operation: delete value **Name:** NextUpdate
Value:

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LCCache\SmartArt\1033
Operation: delete value **Name:** NextUpdate
Value:

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems
Operation: write **Name:** !`;
Value: 21603B00240E0000040000000000000008C0000000100000084000003E0043003A005C00550073006500720073005C00610064006D0069006E005C00410070007000440061007400610 05C0052006F0061006D0069006E0067005C004D006900630072006F0073006F00660074005C00540065006D0070006C006100740065007300 5C004E006F0072006D0061006C002E0064006F0074006D00000000000000

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems
Operation: delete value **Name:** !`;
Value: 怡;ף

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems
Operation: write **Name:** ~`;
Value: 7E603B00240E0000020000000000000008E000000010000005000000032000000630003A005C00700072006F006700720061007E0031005C006D006900630072006F0073007E0031005C006F00660066006900630065003100340005C00670065006E006B006F002E0064006C006C0000006D006900630072006F0073006F006600740020007700 6F00720064002000D0C6E0ACC0C9200094CD00AC200030AEA5B20000

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems
Operation: delete value **Name:** ~`;
Value: 恺;ף

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems
Operation: write **Name:** (b;
Value: 28623B00240E0000060000000100000072000000020000006200000004000000630003A005C00750073006500720073005C00610064006D0069006E005C0064006F0077006E006C006F006100640073005C00300032003000380 05F00350034003700340031003800360039003700350030003100330032002E0064006F006300000000000000

(PID) Process: (3620) 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: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Max Display
Value: ♀

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: write **Name:** Max Display
Value: 25

(PID) Process: (3620) 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: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: write **Name:** Item 1
Value: [F00000000][T01DA76C7E36FB7D0][O00000000]*C:\Users\admin\Downloads\

(PID) Process: (3620) 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: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: write **Name:** Item 2
Value: [F00000000][T01D56F995041B2E0][O00000000]*C:\Users\admin\Documents\

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 3
Value:

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 4
Value:

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 5
Value:

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 6
Value:

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation: delete value **Name:** Item 7
Value:

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU

Operation:	delete value	**Name:**	Item 8
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation:	delete value	**Name:**	Item 9
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation:	delete value	**Name:**	Item 10
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation:	delete value	**Name:**	Item 11
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation:	delete value	**Name:**	Item 12
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation:	delete value	**Name:**	Item 13
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation:	delete value	**Name:**	Item 14
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation:	delete value	**Name:**	Item 15
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation:	delete value	**Name:**	Item 16
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation:	delete value	**Name:**	Item 17
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation:	delete value	**Name:**	Item 18
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation:	delete value	**Name:**	Item 19
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation:	delete value	**Name:**	Item 20
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation:	delete value	**Name:**	Item 21
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation:	delete value	**Name:**	Item 22
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation:	delete value	**Name:**	Item 23
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation:	delete value	**Name:**	Item 24
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation:	delete value	**Name:**	Item 25
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation:	delete value	**Name:**	Item 26
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation:	delete value	**Name:**	Item 27
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU

Operation:	delete value	**Name:**	Item 28
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation:	delete value	**Name:**	Item 29
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation:	delete value	**Name:**	Item 30
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation:	delete value	**Name:**	Item 31
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation:	delete value	**Name:**	Item 32
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation:	delete value	**Name:**	Item 33
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation:	delete value	**Name:**	Item 34
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation:	delete value	**Name:**	Item 35
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation:	delete value	**Name:**	Item 36
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation:	delete value	**Name:**	Item 37
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation:	delete value	**Name:**	Item 38
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation:	delete value	**Name:**	Item 39
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation:	delete value	**Name:**	Item 40
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation:	delete value	**Name:**	Item 41
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation:	delete value	**Name:**	Item 42
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation:	delete value	**Name:**	Item 43
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation:	delete value	**Name:**	Item 44
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation:	delete value	**Name:**	Item 45
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation:	delete value	**Name:**	Item 46
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation:	delete value	**Name:**	Item 47
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU

Operation:	delete value	**Name:**	Item 48
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation:	delete value	**Name:**	Item 49
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU
Operation:	delete value	**Name:**	Item 50
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint
Operation:	delete value	**Name:**	Site 1
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint
Operation:	delete value	**Name:**	Site 2
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint
Operation:	delete value	**Name:**	Site 3
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint
Operation:	delete value	**Name:**	Site 4
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint
Operation:	delete value	**Name:**	Site 5
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint
Operation:	delete value	**Name:**	Site 6
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint
Operation:	delete value	**Name:**	Site 7
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint
Operation:	delete value	**Name:**	Site 8
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint
Operation:	delete value	**Name:**	Site 9
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint
Operation:	delete value	**Name:**	Site 10
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint
Operation:	delete value	**Name:**	Site 11
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint
Operation:	delete value	**Name:**	Site 12
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint
Operation:	delete value	**Name:**	Site 13
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint
Operation:	delete value	**Name:**	Site 14
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint
Operation:	delete value	**Name:**	Site 15
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint
Operation:	delete value	**Name:**	Site 16
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint
Operation:	delete value	**Name:**	Site 17
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint

Operation: delete value **Name:** Site 18
Value:

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint
Operation: delete value **Name:** Site 19
Value:

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint
Operation: delete value **Name:** Site 20
Value:

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Max Display
Value: ♀

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: write **Name:** Max Display
Value: 25

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 1
Value: [F00000000][T01D66807373FC580][O00000000]*C:\Users\admin\Desktop\loginmedicine.rtf

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: write **Name:** Item 1
Value: [F00000000][T01DA76C7E37005F0][O00000000]*C:\Users\admin\Downloads\0208_54741869750132.doc

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 2
Value: [F00000000][T01D73F7DF4F63100][O00000000]*C:\Users\admin\Desktop\functionwest.rtf

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: write **Name:** Item 2
Value: [F00000000][T01D66807373FC580][O00000000]*C:\Users\admin\Desktop\loginmedicine.rtf

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 3
Value: [F00000000][T01D54AFDCD618200][O00000000]*C:\Users\admin\Desktop\eventstrue.rtf

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: write **Name:** Item 3
Value: [F00000000][T01D73F7DF4F63100][O00000000]*C:\Users\admin\Desktop\functionwest.rtf

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 4
Value: [F00000000][T01D35686078B4000][O00000000]*C:\Users\admin\Desktop\leathercompany.rtf

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: write **Name:** Item 4
Value: [F00000000][T01D54AFDCD618200][O00000000]*C:\Users\admin\Desktop\eventstrue.rtf

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 5
Value: [F00000000][T01D29B55E2E55C80][O00000000]*C:\Users\admin\Documents\demembership.rtf

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: write **Name:** Item 5
Value: [F00000000][T01D35686078B4000][O00000000]*C:\Users\admin\Desktop\leathercompany.rtf

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 6
Value: [F00000000][T01D63EBB245C8680][O00000000]*C:\Users\admin\Documents\multiplepatient.rtf

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: write **Name:** Item 6
Value: [F00000000][T01D29B55E2E55C80][O00000000]*C:\Users\admin\Documents\demembership.rtf

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 7
Value: [F00000000][T01D303BD8225B200][O00000000]*C:\Users\admin\Documents\youngpass.rtf

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: write **Name:** Item 7
Value: [F00000000][T01D63EBB245C8680][O00000000]*C:\Users\admin\Documents\multiplepatient.rtf

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 8
Value: [F00000000][T01D3DB343FE8AF00][O00000000]*C:\Users\admin\Documents\daysrobert.rtf

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU

Operation: write **Name:** Item 8
Value: [F00000000][T01D303BD8225B200][O00000000]*C:\Users\admin\Documents\youngpass.rtf

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 9
Value: [F00000000][T01D9B21DFB899A00][O00000000]*C:\Users\admin\Documents\camerasstatistics.rtf

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: write **Name:** Item 9
Value: [F00000000][T01D3DB343FE8AF00][O00000000]*C:\Users\admin\Documents\daysrobert.rtf

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 10
Value: [F00000000][T01D7BD9DD3CA0480][O00000000]*C:\Users\admin\Documents\articlesstates.rtf

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: write **Name:** Item 10
Value: [F00000000][T01D9B21DFB899A00][O00000000]*C:\Users\admin\Documents\camerasstatistics.rtf

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 11
Value: [F00000000][T01D395A9F5723480][O00000000]*C:\Users\admin\Documents\southquite.rtf

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: write **Name:** Item 11
Value: [F00000000][T01D7BD9DD3CA0480][O00000000]*C:\Users\admin\Documents\articlesstates.rtf

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 12
Value:

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: write **Name:** Item 12
Value: [F00000000][T01D395A9F5723480][O00000000]*C:\Users\admin\Documents\southquite.rtf

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 13
Value:

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 14
Value:

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 15
Value:

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 16
Value:

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 17
Value:

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 18
Value:

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 19
Value:

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 20
Value:

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 21
Value:

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 22
Value:

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 23
Value:

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU

Operation:	delete value	**Name:**	Item 24
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation:	delete value	**Name:**	Item 25
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation:	delete value	**Name:**	Item 26
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation:	delete value	**Name:**	Item 27
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation:	delete value	**Name:**	Item 28
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation:	delete value	**Name:**	Item 29
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation:	delete value	**Name:**	Item 30
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation:	delete value	**Name:**	Item 31
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation:	delete value	**Name:**	Item 32
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation:	delete value	**Name:**	Item 33
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation:	delete value	**Name:**	Item 34
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation:	delete value	**Name:**	Item 35
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation:	delete value	**Name:**	Item 36
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation:	delete value	**Name:**	Item 37
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation:	delete value	**Name:**	Item 38
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation:	delete value	**Name:**	Item 39
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation:	delete value	**Name:**	Item 40
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation:	delete value	**Name:**	Item 41
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation:	delete value	**Name:**	Item 42
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation:	delete value	**Name:**	Item 43
Value:			

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU

Operation: delete value **Name:** Item 44
Value:

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 45
Value:

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 46
Value:

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 47
Value:

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 48
Value:

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 49
Value:

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 50
Value:

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 1
Value: [F00000000][T01DA76C7E37005F0][O00000000]*C:\Users\admin\Downloads\0208_54741869750132.doc

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 2
Value: [F00000000][T01D66807373FC580][O00000000]*C:\Users\admin\Desktop\loginmedicine.rtf

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 3
Value: [F00000000][T01D73F7DF4F63100][O00000000]*C:\Users\admin\Desktop\functionwest.rtf

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 4
Value: [F00000000][T01D54AFDCD618200][O00000000]*C:\Users\admin\Desktop\eventstrue.rtf

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 5
Value: [F00000000][T01D35686078B4000][O00000000]*C:\Users\admin\Desktop\leathercompany.rtf

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 6
Value: [F00000000][T01D29B55E2E55C80][O00000000]*C:\Users\admin\Documents\demembership.rtf

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 7
Value: [F00000000][T01D63EBB245C8680][O00000000]*C:\Users\admin\Documents\multiplepatient.rtf

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 8
Value: [F00000000][T01D303BD8225B200][O00000000]*C:\Users\admin\Documents\youngpass.rtf

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 9
Value: [F00000000][T01D3DB343FE8AF00][O00000000]*C:\Users\admin\Documents\daysrobert.rtf

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 10
Value: [F00000000][T01D9B21DFB899A00][O00000000]*C:\Users\admin\Documents\camerasstatistics.rtf

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 11
Value: [F00000000][T01D7BD9DD3CA0480][O00000000]*C:\Users\admin\Documents\articlesstates.rtf

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\File MRU
Operation: delete value **Name:** Item 12
Value: [F00000000][T01D395A9F5723480][O00000000]*C:\Users\admin\Documents\southquite.rtf

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\18683B
Operation: write **Name:** 18683B
Value: 04000000240E0000300000043003A005C005500730065007200730005C00610064006D0069006E005C0044006F0077006E006C006F006100640073005C003000320030003800 5F0035003400370034003100380036003900370035003000310033003200 2E0064006F006300000000000100010000000000694FF8DEC776DA013B6818003B68180000000000DB040000000000000000000000000000000000000000000000000000000000000000FFFFFFFF0000000000000

00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000FFFFFFFF

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems
Operation: delete value **Name:** (b;
Value: 戬;ŋ

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems
Operation: delete value **Name:** h¨;
Value: 罨;ŋ

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems
Operation: delete key **Name:** (default)
Value:

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems
Operation: write **Name:** id;
Value: 69643B00240E0000020000000000000008E00000001000000500000003200000063003A005C00700072006F006700720061007E0031005C006D006900630072006F0073007E0031005C006F00
66006600690063006500310034005C00670065006E006B006F002E0064006C006C0000006D006900630072006F0073006F0066007400200077006F00720064002000D0C6E0ACC0C9200094C
D00AC200030AEA5B20000

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems
Operation: delete value **Name:** id;
Value: 摩;ŋ

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Licensing
Operation: write **Name:** 019C826E445A4649A5B00BF08FCC4EEE
Value: 01000000270000007B393031343030302D303033442D303030302D303030302D303030303030303046463143457D005A0000004F00660066006900630065002000310034002C0020004F0066
006600690063006500500072006F00660065007300730069006F006E0061006C002D00520065007400610069006C002000650064006900740069006F006E000000

(PID) Process: (3620) 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: (3620) 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: (3620) WINWORD.EXE **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109F10090400000000000F01FEC\Usage
Operation: write **Name:** SpellingAndGrammarFiles_1033
Value:

(PID) Process: (3620) 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: (3620) 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: (3620) 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: (3620) 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: (3620) 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: (3620) 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: (3620) 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: (3620) 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: (3620) 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: (3620) 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: (3620) 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: (3620) 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: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems
Operation: write **Name:** k ;
Value: 6B203B00240E00000600000001000000720000000200000062000000040000000063003A005C0075007300650072007300 5C00610064006D0069006E005C0064006F0077006E006C006F006100
640073005C0030003200300038005F003500340037003400310038003600390037003500300031003300 32002E0064006F0063000000000000000

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\188578
Operation: write **Name:** 188578
Value: 04000000240E00003000000043003A005C00550073006500720073005C00610064006D0069006E005C0044006F0077006E006C006F00610064 0073005C0030003200300038005F0035003400
37003400310038003600390037003500300031003300 32002E0064006F006300170000003000320030003800 5F0035003400370034003100380036003900370035003000310033003200 2E006
4006F00630000000000000100000000000000694FF8DEC776DA01788518007885180000000000DB040000000000000000000000000000000000000000000000000FFFFFFFF0000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000FFFFFFFF

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems
Operation: delete value **Name:** k ;
Value: ;ꞃ

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word
Operation: delete value **Name:** FontInfoCacheW
Value: `

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @Ami R
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @Arial Unicode MS
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @Batang
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @BatangChe
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @DFKai-SB
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** @Dotum

Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@DotumChe
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@Expo M
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@FangSong
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@Gulim
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@GulimChe
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@Gungsuh
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@GungsuhChe
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@Headline R
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HGGothicE
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HGGothicM
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HGGyoshotai
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HGKyokashotai
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HGMaruGothicMPRO
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HGMinchoB
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HGMinchoE
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HGPGothicE
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HGPGothicM
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HGPGyoshotai
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HGPKyokashotai
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HGPMinchoB

Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HGPMinchoE
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HGPSoeiKakugothicUB
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HGPSoeiKakupoptai
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HGPSoeiPresenceEB
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HGSeikaishotaiPRO
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HGSGothicE
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HGSGothicM
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HGSGyoshotai
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HGSKyokashotai
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HGSMinchoB
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HGSMinchoE
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HGSoeiKakugothicUB
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HGSoeiKakupoptai
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HGSoeiPresenceEB
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HGSSoeiKakugothicUB
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HGSSoeiKakupoptai
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HGSSoeiPresenceEB
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HYGothic-Extra
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HYGothic-Medium
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HYGraphic-Medium

Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HYGungSo-Bold
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HYHeadLine-Medium
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HYMyeongJo-Extra
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HYPMokGak-Bold
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HYPost-Light
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HYPost-Medium
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HYShortSamul-Medium
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@HYSinMyeongJo-Medium
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@KaiTi
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@Magic R
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@Malgun Gothic
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@Meiryo
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@Meiryo UI
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@Microsoft JhengHei
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@Microsoft YaHei
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@MingLiU
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@MingLiU_HKSCS
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@MingLiU_HKSCS-ExtB
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@MingLiU-ExtB
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@MoeumT R

Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@MS Gothic
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@MS Mincho
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@MS PGothic
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@MS PMincho
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@MS UI Gothic
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@New Gulim
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@NSimSun
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@PMingLiU
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@PMingLiU-ExtB
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@Pyunji R
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@SimHei
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@SimSun
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@SimSun-ExtB
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	@Yet R
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Agency FB
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Aharoni
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Algerian
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Ami R
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Andalus
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Angsana New

Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** AngsanaUPC
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Aparajita
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Arabic Typesetting
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Arial
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Arial Black
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Arial Narrow
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Arial Rounded MT Bold
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Arial Unicode MS
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Baskerville Old Face
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Batang
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** BatangChe
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Bauhaus 93
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Bell MT
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Berlin Sans FB
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Berlin Sans FB Demi
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Bernard MT Condensed
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Blackadder ITC
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Bodoni MT
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Bodoni MT Black
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Bodoni MT Condensed

Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Bodoni MT Poster Compressed
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Book Antiqua
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Bookman Old Style
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Bookshelf Symbol 7
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Bradley Hand ITC
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Britannic Bold
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Broadway
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Browallia New
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	BrowalliaUPC
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Brush Script MT
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Calibri
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Calibri Light
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Californian FB
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Calisto MT
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Cambria
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Cambria Math
Value: 1			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Candara
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Castellar
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Centaur
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Century

Value: 0

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Century Gothic
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Century Schoolbook
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Chiller
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Colonna MT
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Comic Sans MS
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Consolas
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Constantia
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Cooper Black
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Copperplate Gothic Bold
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Copperplate Gothic Light
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Corbel
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Cordia New
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	CordiaUPC
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Courier
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Courier New
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Curlz MT
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	DaunPenh
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	David
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	DFKai-SB
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	DilleniaUPC

Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	DokChampa
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Dotum
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	DotumChe
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Ebrima
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Edwardian Script ITC
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Elephant
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Engravers MT
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Eras Bold ITC
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Eras Demi ITC
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Eras Light ITC
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Eras Medium ITC
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Estrangelo Edessa
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	EucrosiaUPC
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Euphemia
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Expo M
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	FangSong
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Felix Titling
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Fixedsys
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Footlight MT Light
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Forte

Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Franklin Gothic Book
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Franklin Gothic Demi
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Franklin Gothic Demi Cond
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Franklin Gothic Heavy
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Franklin Gothic Medium
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Franklin Gothic Medium Cond
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** FrankRuehl
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** FreesiaUPC
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Freestyle Script
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** French Script MT
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Gabriola
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Garamond
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Gautami
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Georgia
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Gigi
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Gill Sans MT
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Gill Sans MT Condensed
Value: 0

(PID) Process: (3620) 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: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Gill Sans Ultra Bold
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Gill Sans Ultra Bold Condensed

Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Gisha
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Gloucester MT Extra Condensed
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Goudy Old Style
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Goudy Stout
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Gulim
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** GulimChe
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Gungsuh
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** GungsuhChe
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Haettenschweiler
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Harlow Solid Italic
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Harrington
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Headline R
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGGothicE
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGGothicM
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGGyoshotai
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGKyokashotai
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGMaruGothicMPRO
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGMinchoB
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGMinchoE
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGPGothicE

Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGPGothicM
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGPGyoshotai
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGPKyokashotai
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGPMinchoB
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGPMinchoE
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGPSoeiKakugothicUB
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGPSoeiKakupoptai
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGPSoeiPresenceEB
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGSeikaishotaiPRO
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGSGothicE
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGSGothicM
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGSGyoshotai
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGSKyokashotai
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGSMinchoB
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGSMinchoE
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGSoeiKakugothicUB
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGSoeiKakupoptai
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGSoeiPresenceEB
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGSSoeiKakugothicUB
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** HGSSoeiKakupoptai

Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	HGSSoeiPresenceEB
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	High Tower Text
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	HYGothic-Extra
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	HYGothic-Medium
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	HYGraphic-Medium
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	HYGungSo-Bold
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	HYHeadLine-Medium
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	HYMyeongJo-Extra
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	HYPMokGak-Bold
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	HYPost-Light
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	HYPost-Medium
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	HYShortSamul-Medium
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	HYSinMyeongJo-Medium
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Impact
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Imprint MT Shadow
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Informal Roman
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	IrisUPC
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Iskoola Pota
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	JasmineUPC
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Jokerman

Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Juice ITC
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	KaiTi
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Kalinga
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Kartika
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Khmer UI
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	KodchiangUPC
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Kokila
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Kristen ITC
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Kunstler Script
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Lao UI
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Latha
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Leelawadee
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Levenim MT
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	LilyUPC
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Lucida Bright
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Lucida Calligraphy
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Lucida Console
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Lucida Fax
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Lucida Handwriting
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Lucida Sans

Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Lucida Sans Typewriter
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Lucida Sans Unicode
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Magic R
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Magneto
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Maiandra GD
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Malgun Gothic
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Mangal
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Marlett
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Matura MT Script Capitals
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Meiryo
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Meiryo UI
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Microsoft Himalaya
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Microsoft JhengHei
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Microsoft New Tai Lue
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Microsoft PhagsPa
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Microsoft Sans Serif
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Microsoft Tai Le
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Microsoft Uighur
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Microsoft YaHei
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Microsoft Yi Baiti

Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** MingLiU
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** MingLiU_HKSCS
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** MingLiU_HKSCS-ExtB
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** MingLiU-ExtB
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Miriam
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Miriam Fixed
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Mistral
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Modern No. 20
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** MoeumT R
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Mongolian Baiti
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Monotype Corsiva
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** MoolBoran
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** MS Gothic
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** MS Mincho
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** MS Outlook
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** MS PGothic
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** MS PMincho
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** MS Reference Sans Serif
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** MS Reference Specialty
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** MS Sans Serif

Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** MS Serif
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** MS UI Gothic
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** MT Extra
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** MV Boli
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Narkisim
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** New Gulim
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Niagara Engraved
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Niagara Solid
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** NSimSun
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Nyala
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** OCR A Extended
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** OCRB
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Old English Text MT
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Onyx
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Palace Script MT
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Palatino Linotype
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Papyrus
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Parchment
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Perpetua
Value: 0

(PID) Process: (3620) WINWORD.EXE **Key:** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation: write **Name:** Perpetua Titling MT

Value: 0

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Plantagenet Cherokee
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Playbill
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	PMingLiU
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	PMingLiU-ExtB
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Poor Richard
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Pristina
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Pyunji R
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Raavi
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Rage Italic
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Ravie
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Rockwell
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Rockwell Condensed
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Rockwell Extra Bold
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Rod
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Sakkal Majalla
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Script MT Bold
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Segoe Print
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Segoe Script
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Segoe UI
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Segoe UI Light

Value: 0

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Segoe UI Semibold
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Segoe UI Symbol
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Shonar Bangla
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Showcard Gothic
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Shruti
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	SimHei
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Simplified Arabic
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Simplified Arabic Fixed
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	SimSun
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	SimSun-ExtB
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Small Fonts
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Snap ITC
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Stencil
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Sylfaen
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Symbol
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	System
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Tahoma
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Tempus Sans ITC
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Terminal
Value:	0		

(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Times New Roman

Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Traditional Arabic
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Trebuchet MS
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Tunga
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Tw Cen MT
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Tw Cen MT Condensed
Value: 0			
(PID) Process:	(3620) 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:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Utsaah
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Vani
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Verdana
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Vijaya
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Viner Hand ITC
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Vivaldi
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Vladimir Script
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Vrinda
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Webdings
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Wide Latin
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Wingdings
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Wingdings 2
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Wingdings 3
Value: 0			
(PID) Process:	(3620) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\MathFonts
Operation:	write	**Name:**	Yet R

Value: 0

Files activity

Executable files	Suspicious files	Text files	Unknown types
0	24	32	9

Dropped files

PID	Process	Filename	Type
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\commerce_subscription_db\LOG.old~RF182a95.TMP MD5: — SHA256: —	—
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\commerce_subscription_db\LOG.old MD5: — SHA256: —	—
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG.old~RF182ab4.TMP MD5: ADB669AB4CD1C63883C64FB0DBA2C7DA SHA256: 18BFF89047EC5B122573D089B3DC7A7DD14A5A7A515B2D8141584B41E723253F	text
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\coupon_db\LOG.old~RF182d74.TMP MD5: — SHA256: —	—
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\coupon_db\LOG.old MD5: — SHA256: —	—
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Variations MD5: 961E3604F228B0D10541EBF921500C86 SHA256: F7B24F2EB3D5EB0550527490395D2F61C3D2FE74BB9CB345197DAD81B58B5FED	binary
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG.old~RF182bfd.TMP MD5: C383FD120B14BB0E98E99C1BCC9B43F6 SHA256: 56A3A5EACBD28BEE1CF8C1D0052321A5C27EE858BEF7B2FA1DE20806A0823CC1	text
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG.old MD5: AD0DB8476493577A67FA94A162B646C4 SHA256: 304FB5B4FD83D4A9FF1EF4CF20232A1783169C148297BFE37ED24A1D22A74F2B	text
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Last Version MD5: 9F941EA08DBDCA2EB3CFA1DBBBA6F5DC SHA256: 127F71DF0D2AD895D4F293E62284D85971AE047CA15F90B87BF6335898B0B655	text
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat MD5: 9C016064A1F864C8140915D77CF3389A SHA256: 0E7265D4A8C16223538EDD8CD620B8820611C74538E420A88E333BE7F62AC787	binary
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\LOG.old~RF183294.TMP MD5: — SHA256: —	—
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\LOG.old MD5: — SHA256: —	—
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\LOG.old MD5: 4755704EAEB72509F8E78594142D80D6 SHA256: 52D45B3A4947B8B5B8C48F83F83BA6758CFB7C4434FC574124378F5B01E15999	text
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG.old~RF182a95.TMP MD5: 05CF4C3C5148DA6355D3561A9EAA5E8A SHA256: 8D720243F6876898E4F197C8867C4CEE69F1C7335C55B8A29C120B1028D93E41	text
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG.old MD5: ECD3386BCC950E73B86EB128A5F57622 SHA256: C9A068EAFBC587EDFC89392F64DDD350EEB96C5CF195CDB030BAB8F6DD33833B	text
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG.old MD5: 4E2B7997F4C3647F8D1ADA88339BBBA5 SHA256: C33226C460208AA10537A23CB5128FD887DCBAA335C7DC8BFFBE08A607CCFDF5	text
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG.old MD5: 65239F35CB63C76EA1F59EF64F7AAFF4 SHA256: 252EF82CC03FDE4BEF13CF81CD1AC5CE45854212D1A7359035E7A5D6BEDBE229	text
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\optimization_guide_hint_cache_store\LOG.old~RF1847e1.TMP MD5: — SHA256: —	—
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\optimization_guide_hint_cache_store\LOG.old MD5: — SHA256: —	—
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\optimization_guide_model_metadata_store\LOG.old~RF1847e1.TMP MD5: — SHA256: —	—
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\optimization_guide_model_metadata_store\LOG.old MD5: — SHA256: —	—
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG.old~RF1847e1.TMP MD5: — SHA256: —	—
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG.old MD5: — SHA256: —	—
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Segmentation Platform\SegmentInfoDB\LOG.old~RF1848bc.TMP MD5: — SHA256: —	—
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Segmentation Platform\SegmentInfoDB\LOG.old	—

		MD5: — SHA256: —	
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG.old MD5: E53573A93829681410D5E7DBB1B61C78 SHA256: A82D28F2C1E22A2AE0ABC5F5AF0CC8EE7AD913BAB3A0BF84CE6D8D23F67E06A3	text
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG.old~RF1848bc.TMP MD5: — SHA256: —	—
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG.old MD5: — SHA256: —	—
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Segmentation Platform\SignalDB\LOG.old~RF1848bc.TMP MD5: — SHA256: —	—
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Segmentation Platform\SignalDB\LOG.old MD5: — SHA256: —	—
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old~RF1848bc.TMP MD5: — SHA256: —	—
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old MD5: — SHA256: —	—
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Segmentation Platform\SignalStorageConfigDB\LOG.old~RF1848cc.TMP MD5: — SHA256: —	—
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Segmentation Platform\SignalStorageConfigDB\LOG.old MD5: — SHA256: —	—
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG.old~RF1848fa.TMP MD5: — SHA256: —	—
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG.old MD5: — SHA256: —	—
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG.old~RF182d06.TMP MD5: 0272AD43ECEA4DC6C694BE6D918B5BA7 SHA256: 530F5A3F46B293038FEBEF2035CFA622F05B202363ABFAF9E40E105BD1472432	text
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG.old~RF182c89.TMP MD5: B36B68CE4A71A5BFAF89A4D1CC07893F SHA256: 6422CC04455EF100D67FD9F299AACFEF3BA4F77D0FA1D2440D89E7D1CF65EBBC	text
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG.old MD5: BF244CDEBD39A0D20444C1578C0200BE SHA256: CC7E247D7764DA50D4137E894838F918281D4915FE0823B4FC0CB763BF582F4D	text
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Download Service\EntryDB\LOG.old~RF184c08.TMP MD5: — SHA256: —	—
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Download Service\EntryDB\LOG.old MD5: — SHA256: —	—
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG.old~RF182c6a.TMP MD5: C5B082BC8EA6A9BD1DC6782C00A79605 SHA256: 6168A9E585264DE05DEE1B67427B1BC277F1B83B9297184EFACC5D3BB061ABDE	text
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\LOG.old~RF182c99.TMP MD5: 8593E82FF8753DC10267243C51E8A91B SHA256: FE9EE2D77D9EB5CBA707EDBCB7F1ABAA83418CDB66D66835B4B9A1B6CC5CC34F	text
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\31a550fc-2478-4e71-aa78-772d21a4a937.tmp MD5: 5058F1AF8388633F609CADB75A75DC9D SHA256: CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8	binary
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG.old~RF182c89.TMP MD5: F5B58F0B08202C8D6DE12514994A84BF SHA256: F5BA8809B6A3920A11CF31E7F6A1DEC46EF4F4339D6158967CCB1405409D1241	text
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG.old MD5: 358570F689377CE6838812643E03734B SHA256: 5B41FCC2E1A843AEAB9437B06E27B798870FF10D86A51B163BF48862BCD32590	text
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Last Browser MD5: DE9EF0C5BCC012A3A1131988DEE272D8 SHA256: 3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590	binary
3620	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\CVR6368.tmp.cvr MD5: — SHA256: —	—
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG.old~RF1847e1.TMP MD5: 6126A211B4F0AD6FBF434239A32A8932 SHA256: C48146DF152679DBB76FDB0B0892C1552DC96623FD93CC581D81266543480FA3	text
120	chrome.exe	C:\Users\admin\Downloads\Unconfirmed 320077.crdownload MD5: 7F6C623196D7E76C205B4FB898AD9BE6 SHA256: 3A5648F7DE99C4F87331C36983FC8ADCD667743569A19C8DAFDD5E8A33DE154D	document
3620	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\~$Normal.dotm MD5: BF269E930A5D35C7C0632B29858E4380 SHA256: BFC3DD2327A5E205DDE5A59DB46171BC1AFD3123E1EBFFF70A1B7445DB4BD499	pgc
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\ShaderCache\data_1 MD5: 1AB83CB324C9E98607E990B594B972B5 SHA256: 72D65DF10DF9FF251010EA7380CE39B9A0D5F47DF72464B86373C19ADA327112	binary
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\DawnCache\data_1 MD5: CB9461DB7811B5875919AE63EDB0D6A4 SHA256: 7B502111749EE28DE08C66BF503D15721D66F006414E449C206543E6265A96FC	binary
120	chrome.exe	C:\Users\admin\Downloads\0208_54741869750132.doc MD5: 7F6C623196D7E76C205B4FB898AD9BE6 SHA256: 3A5648F7DE99C4F87331C36983FC8ADCD667743569A19C8DAFDD5E8A33DE154D	document

120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG.old **MD5:** 865C413CDAAFB0E6CF263FF321291451 **SHA256:** CE54C4F6A5858D3029A62DAC96EBEFB5469321809CD8DDDBE40388D729534B35	text
1544	chrome.exe	C:\Users\admin\Downloads\0208_54741869750132.doc:Zone.Identifier **MD5:** FBCCF14D504B7B2DBCB5A5BDA75BD93B **SHA256:** EACD09517CE90D34BA562171D15AC40D302F0E691B439F91BE1B6406E25F5913	text
552	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\OICE_3A7BA3FA-85CB-402B-BA87-FE9130259FBB.0\D752A1F8.emf **MD5:** A08286784C9F2B367F405D02EECA6D49 **SHA256:** 91EC41F1FBBB6769B0F1D9062384CAFD742AF6B2E0FC790B60FF24E1E9BFE2E3	binary
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\428f58fd-7901-40ac-b13d-73d456c05ca2.tmp **MD5:** 3093FEE1A093B5B8DB30170F93883657 **SHA256:** 7FC658BE733CB0D482DC98F17022063AC266E82DEA083E74C778E7990A6FA437	binary
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Local State **MD5:** B408F029E8AB388DAE4A6C0F1EDB160B **SHA256:** 637A51F2A645EE11F3A140B91CCF63D6174908E4D8CFA78D842AFF03B9DB5AA8	binary
120	chrome.exe	C:\Users\admin\Downloads\b774c109-672b-43e7-9a72-058b917234c3.tmp **MD5:** 7F6C623196D7E76C205B4FB898AD9BE6 **SHA256:** 3A5648F7DE99C4F87331C36983FC8ADCD667743569A19C8DAFDD5E8A33DE154D	document
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Preferences **MD5:** 2D8A8148BADC3001711AEC3CFB9CD943 **SHA256:** 73E44D82064D1B9B0859D92F30F644E74E550C6120151ABA27B06E26621E7EEC	text
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\DownloadMetadata~RF18623f.TMP **MD5:** 3093FEE1A093B5B8DB30170F93883657 **SHA256:** 7FC658BE733CB0D482DC98F17022063AC266E82DEA083E74C778E7990A6FA437	binary
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\a53d5f64-96cc-4da1-8883-a6c6b1c5f901.tmp **MD5:** 9EF4A2CD9A091D7FE87EB265419B4CE2 **SHA256:** 65F3887EDA62D942909162FB67A41EE91299677B93B3AF77E2AF1217505503D4	binary
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\GPUCache\data_1 **MD5:** AD5AF099A5E1FF32705CFABBE2CC2BDA **SHA256:** C64D288683F37FFEE7B3E2880F8FF9265945834A23C29C8E9B968D32E3993709	binary
3620	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\OICE_3A7BA3FA-85CB-402B-BA87-FE9130259FBB.0\777D2630.doc **MD5:** 7F6C623196D7E76C205B4FB898AD9BE6 **SHA256:** 3A5648F7DE99C4F87331C36983FC8ADCD667743569A19C8DAFDD5E8A33DE154D	document
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\DownloadMetadata **MD5:** 3093FEE1A093B5B8DB30170F93883657 **SHA256:** 7FC658BE733CB0D482DC98F17022063AC266E82DEA083E74C778E7990A6FA437	binary
3620	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Office\Recent\0208_54741869750132.doc.LNK **MD5:** 92EEF4B89A3151F21B16B4E90FE7A69D **SHA256:** 636E19C2E5C5E25EDA23DF420D660080CE42DBC7C1C4E4099FE59FB95137A221	lnk
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\34e14612-1942-4cde-a5c1-5c79a4b03741.tmp **MD5:** B408F029E8AB388DAE4A6C0F1EDB160B **SHA256:** 637A51F2A645EE11F3A140B91CCF63D6174908E4D8CFA78D842AFF03B9DB5AA8	text
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\5873ba35-7167-45a9-b588-b973b1cacc5a.tmp **MD5:** 2D8A8148BADC3001711AEC3CFB9CD943 **SHA256:** 73E44D82064D1B9B0859D92F30F644E74E550C6120151ABA27B06E26621E7EEC	text
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\1a2c430c-247e-4987-bbf1-8c5976882f22.tmp **MD5:** 3433CCF3E03FC35B634CD0627833B0AD **SHA256:** F7D5893372EDAA08377CB270A99842A9C758B447B7B57C52A7B1158C0C202E6D	flc
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Download Service\Files\Unconfirmed 621626.crdownload **MD5:** — **SHA256:** —	—
3620	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A9421071.emf **MD5:** A08286784C9F2B367F405D02EECA6D49 **SHA256:** 91EC41F1FBBB6769B0F1D9062384CAFD742AF6B2E0FC790B60FF24E1E9BFE2E3	emf
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Local State~RF185138.TMP **MD5:** F2E71943E090CC493F0A98C5DC82007B **SHA256:** 16DB96A8355207E3B7D600F34690B5032A498B3520570645CD07E7F312832162	text
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Preferences~RF185186.TMP **MD5:** E1723B49AA8DC57F042D0CDFA2EDF18C **SHA256:** A7D3B6DFCEF88821AF78D1489C3E9B67573CF263B7B2089F37C432DA37214255	text
3620	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Office\Recent\index.dat **MD5:** 78302251E65E1335A5448AE7470603E6 **SHA256:** 19EF91CAD5F923F8EA17113CF65572592B545F6AFC4E29842875E47F8B54665C	ini
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Preferences~RF188af5.TMP **MD5:** 2D8A8148BADC3001711AEC3CFB9CD943 **SHA256:** 73E44D82064D1B9B0859D92F30F644E74E550C6120151ABA27B06E26621E7EEC	text
3620	WINWORD.EXE	C:\Users\admin\Downloads\~$08_54741869750132.doc **MD5:** CAE01A3B8B464FF7CADAF195D8F69D9A **SHA256:** 4C989956258ABA3F1CAB959BCBB96A7E7EB837EE7CD2DEDBBF88B9C44BA69249	binary
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Module Info Cache **MD5:** 814C997B974FCCC11A767BB21116B780 **SHA256:** 38BE48BFE92C429B690BC7B7A44CE45170F4C0B182C3D501E6E0E55F6B0F5FB0	binary
3620	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\OICE_3A7BA3FA-85CB-402B-BA87-FE9130259FBB.0\777D2630.doc:Zone.Identifier:$DATA **MD5:** FBCCF14D504B7B2DBCB5A5BDA75BD93B **SHA256:** EACD09517CE90D34BA562171D15AC40D302F0E691B439F91BE1B6406E25F5913	text
2672	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Network\5f2f0703-00bd-41d9-b657-7e5925994463.tmp **MD5:** 456DB8B36872BB2A27AB1BA89A938F7C **SHA256:** FC1730A20CC4953CA6762EEFA3F24FF57177573C9D849F3F37E7CF61573FFC9B	binary
3620	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\OICE_3A7BA3FA-85CB-402B-BA87-FE9130259FBB.0\mso67DD.tmp **MD5:** 965EAC13421205F6F69D1EDBB414B7C5 **SHA256:** 18B0E753CCF28985680339F60438A23F0619D6314234C8802D69686A971FA8EA	compressed
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\94b97a70-96f5-4a02-901c-ce43d90ede6e.tmp **MD5:** 0AD429802103DD46803ECB7629A52EFB **SHA256:** F6F81536A58479E276E721DD5F19C2E85A05752D02C79DFCDDC1696D813AD42D	text
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Module Info Cache~RF1889cc.TMP	binary

		MD5: C9DA9D9A7F661D9131D9F25FA11970B2 SHA256: 743DD558BEEC28B1B4EB0E158F15F9DBF327A4620F60BC2EA43ECF4523582776	
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\trusted_vault.pb MD5: 3433CCF3E03FC35B634CD0627833B0AD SHA256: F7D5893372EDAA08377CB270A99842A9C758B447B7B57C52A7B1158C0C202E6D	flc
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\485631fe-6e11-4e20-ac6a-34ed9f093f81.tmp MD5: 814C997B974FCCC11A767BB21116B780 SHA256: 38BE48BFE92C429B690BC7B7A44CE45170F4C0B182C3D501E6E0E55F6B0F5FB0	binary
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\trusted_vault.pb~RF1884fa.TMP MD5: 3433CCF3E03FC35B634CD0627833B0AD SHA256: F7D5893372EDAA08377CB270A99842A9C758B447B7B57C52A7B1158C0C202E6D	flc
2672	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Network\TransportSecurity~RF18abfa.TMP MD5: D1590A0D940AD28FB8935856182C05B6 SHA256: 228C92AAF9C3A45F9F66B78535FE63B49585017396B4B480B0D3A1998E99FE10	text
2672	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Network\TransportSecurity MD5: 456DB8B36872BB2A27AB1BA89A938F7C SHA256: FC1730A20CC4953CA6762EEFA3F24FF57177573C9D849F3F37E7CF61573FFC9B	binary
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\dc64835f-abe6-4919-8b0a-5c20c13d56a9.tmp MD5: DB546EECB90D5E0D6CCC72122EBF642F SHA256: 88F32775B9AD015796B6B42DACE914084A2C0090A7E46AF58F31761CCDC19673	binary
120	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Preferences~RF18c704.TMP MD5: 0AD429802103DD46803ECB7629A52EFB SHA256: F6F81536A58479E276E721DD5F19C2E85A05752D02C79DFCDDC1696D813AD42D	text

Network activity

HTTP(S) requests: 1
TCP/UDP connections: 30
DNS requests: 18
Threats: 0

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
2672	chrome.exe	GET	204	142.250.185.67:80	http://www.gstatic.com/generate_204	unknown	–	–	unknown

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
–	–	224.0.0.252:5355	–	–	–	unknown
4	System	192.168.100.255:137	–	–	–	whitelisted
4	System	192.168.100.255:138	–	–	–	whitelisted
1080	svchost.exe	224.0.0.252:5355	–	–	–	unknown
120	chrome.exe	239.255.255.250:1900	–	–	–	unknown
2672	chrome.exe	172.217.16.195:443	clientservices.googleapis.com	GOOGLE	US	whitelisted
2672	chrome.exe	74.125.71.84:443	accounts.google.com	GOOGLE	US	unknown
2672	chrome.exe	49.13.77.253:443	key.xn--nvigators-key-if2g.com	Hetzner Online GmbH	DE	unknown
2672	chrome.exe	142.250.185.132:443	www.google.com	GOOGLE	US	whitelisted
2672	chrome.exe	142.250.185.227:443	update.googleapis.com	GOOGLE	US	whitelisted
120	chrome.exe	224.0.0.251:5353	–	–	–	unknown
2672	chrome.exe	142.250.185.174:443	sb-ssl.google.com	GOOGLE	US	whitelisted
2672	chrome.exe	142.250.186.42:443	optimizationguide-pa.googleapis.com	GOOGLE	US	whitelisted
2672	chrome.exe	142.250.185.67:80	www.gstatic.com	GOOGLE	US	whitelisted
2672	chrome.exe	142.250.185.74:443	optimizationguide-pa.googleapis.com	GOOGLE	US	whitelisted

DNS requests

Domain	IP	Reputation
clientservices.googleapis.com	172.217.16.195	whitelisted
accounts.google.com	74.125.71.84	shared
key.xn--nvigators-key-if2g.com	49.13.77.253	unknown

www.google.com	142.250.185.132	whitelisted
update.googleapis.com	142.250.185.227	whitelisted
sb-ssl.google.com	142.250.185.174	whitelisted
optimizationguide-pa.googleapis.com	142.250.186.42 142.250.186.74 216.58.206.74 142.250.185.106 172.217.16.202 142.250.185.202 142.250.184.234 142.250.185.74 142.250.181.234 142.250.185.170 142.250.185.138 142.250.185.234 142.250.184.202 142.250.186.170 142.250.186.106 172.217.18.10	whitelisted
www.gstatic.com	142.250.185.67	whitelisted
www.googleapis.com	142.250.185.74 142.250.185.138 216.58.212.170 142.250.185.170 172.217.16.138 216.58.206.74 142.250.184.202 142.250.185.234 142.250.185.106 142.250.74.202 142.250.185.202 142.250.186.42 142.250.186.74 142.250.181.234 172.217.18.106 172.217.23.106	whitelisted

Threats

No threats detected

Debug output strings

No debug info