Virtual Analyzer Report



Submission Context

Logged	2021-05-27 11:33:12
Submitter	Manual Submission
Туре	Office Word 2007 document

Analysis Overview

Overall risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.					
Detections	TROJ_FRS.VSNW19E21					
Exploited vulnerabilities	•					
Analyzed objects	Office Word 2007 document 1 - Quote 2405987021.docx F1A0ABB5F96C21F8A799E4F65C4216BD968C29B7					

Analysis Environments

	W7	W10	CentOS w Docker
Anti-security, self-preservation			
Autostart or other system reconfiguration			
Deception, social engineering			
File drop, download, sharing, or replication		✓	
Hijack, redirection, or data theft	~		
Malformed, defective, or with known malware traits	~	~	~
Process, service, or memory object change		~	
Rootkit, cloaking			
Suspicious network or messaging activity	~	~	

W7

Environment-specific risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.				
Detections	TROJ_FRS.VSNW19E21				
Exploited vulnerabilities					
Network connection	Custom				

▼ Object 1 - Quote 2405987021.docx (Office Word 2007 document)

File name	Quote 2405987021.docx
File type	Office Word 2007 document
SHA-1	F1A0ABB5F96C21F8A799E4F65C4216BD968C29B7
SHA-256	5274C7FEA16B84E327D5AF683B6EF0C3E1FE1649B6CEA88399E029ED5DEEEE 6F
MD5	992ACD038FD49F200BD5510C029E74B1
Size	10356 byte(s)

Risk Level	High risk
Detection	TROJ_FRS.VSNW19E21
Exploited vulnerabilities	-
Threat Characteristics	Hijack, redirection, or data theft (1) Malformed, defective, or with known malware traits (1) Suspicious network or messaging activity (14)

Process Graph





MITRE ATT&CK™ Framework Tactics and Techniques 🕜

Tactics	Techniques	Notable Threat Characteristics
Discovery	Network Share Discovery	Characteristics: 1
Command and Control	Commonly Used Port	Characteristics: 1, 2 Characteristics: 1, 2, 3
	Standard Application Layer Protocol	Characteristics: 1, 2 Characteristics: 1, 2, 3

© ATT&CK™ is a trademark of The MITRE Corporation.

▼ Notable Threat Characteristics

▼ Hijack, redirection, or data theft (1)

Characteristic	Significance	Details
Executes commands or uses API to obtain system information	•	Process ID: 2344 Info: Enums share folder from API result

▼ Malformed, defective, or with known malware traits (1)

Characteristic	Significance	Details
Detected as known malware	•••	Source: ATSE Detection Name: TROJ_FRS.VSNW19E21 Engine Version: 12.500.1008 Malware Pattern Version: 16.743.92

▼ Suspicious network or messaging activity (14)

Characteristic	Significance	Details
Attempts to connect to suspicious host		198.46.132.185
Attempts to connect to malicious URL		URL: http://198.46.132.185/ Threat Name: LOW-REPUTATION-URL_BLOCKED-LIST.SCORE.WRS
Attempts to connect to suspicious URL		http://198.46.132.185/dashboard/
Attempts to connect to suspicious URL		http://198.46.132.185/
Attempts to connect to suspicious URL		http://198.46.132.185/
Attempts to connect to malicious URL		URL: http://198.46.132.185/
Connects to remote URL or IP address	•••	Connection: 198.46.132.185:80 Content: GET /wbk HTTP/1.1\r\nAccept: */"\n\u00fcUser-Agent: Mozilla/4.0 [compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .N ET4.0C; .NET4.0E; MSOffice 12]\r\nAccept-Encoding: gzip, deflate\r\nHost: 198.46.132.185\r\nhoconnection: Keep-Alive\r\n\r\nhoconnection: Keep-Alive\r\n\r\nhoconnection: Keep-Alive\r\nhoconnection: Keep-Alive\r\
Connects to remote URL or IP address	•	Connection: 198.46.132.185:80 Content: OPTIONS /
Connects to remote URL or IP address		http://198.46.132.185/wbk
Connects to remote URL or IP address		http://198.46.132.185/
Listens on port		0.0.0.0:49168
Listens on port		127.0.0.1:62203
Listens on port		0.0.0.0:49166
Queries DNS server		198.46.132.185

▼ Network Destinations

IP Address	Port	Location	Risk Level	Threat	Accessed By
198.46.132.185	80	-	-	-	Quote 2405987021.docx

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
198.46.132.185	-	53	-	-	-	Quote 2405987021.docx

URL	Site Category	Risk Level	Threat	Accessed By
http://198.46.132.185/	Disease Vector	High	LOW-REPUTATION-URL_BLOCKED-LIST.SCO RE.WRS	Quote 2405987021.docx
http://198.46.132.185/dashboard/	Untested	-	-	Quote 2405987021.docx
http://198.46.132.185/	Untested	-	-	Quote 2405987021.docx
http://198.46.132.185/	Untested	-	-	Quote 2405987021.docx
http://198.46.132.185/wb	Malware Accomplice	High	EXPLOIT_MSOFFICE.WRS	Quote 2405987021.docx

▼ Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
Quote 2405987021.docx.LNK	No risk	-	-	-	1075	EFD3DF790F574BA577833E0042AC55153C 3C609C
WTYOSLM.LNK	No risk	-	-	-	893	0A1F7E216EC547C4EA2E974F21A289B5F7 C6CBBC
~WRS{2996D4FC-2228-4BDA-B0 59-CCB031414187}.tmp	No risk	-	-	-	1024	A62F70A7B17863E69759A6720E75FC80E12 B46E6
~\$ote 2405987021.docx	No risk	-	-	-	162	4C1AF666FEE715DCFE2BCD97E19269F386 31AB91
Word12.pip	No risk	-	-	-	1684	FC59411B10AF108AE0F1448C7A78DCA0A2 A901B3
~\$Normal.dotm	No risk	-	-	-	162	2950A41A9DA587E8D14B3E23B7B847C104 372EC8
~WRS{5F4688C0-F6C9-4AFE-8A 95-4D912406C8B3}.tmp	No risk	-	-	-	1024	DBB111419C704F116EFA8E72471DD83E86 E49677
index.dat	No risk	-	-	-	160	CEEFAE28EDADD431CF2B81C45A7476A71 CF391C9

▼ Suspicious Objects

Туре	Object	Risk Level
URL	http://198.46.132.185:80/	Medium
URL	http://198.46.132.185;80/dashboard/	Medium
File (SHA1)	F1A0ABB5F96C21F8A799E4F65C4216BD968C29B7	High
URL	http://198.46.132.185:80/wbk	High
URL	http://198.46.132.185:80/	Medium
URL	http://198.46.132.185:80/	High

▼ Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Attempts to connect to suspicious host 198.46.132.185		
Detection	Threat Characteristic: Attempts to connect to malicious URL URL: http://198.46.132.185// Threat Name: LOW-REPUTATION-URL BLOCKED-LIST.SCORE.WRS		
Detection	Threat Characteristic: Attempts to connect to suspicious URL http://198.46.132.185/dashboard/		
Detection	Threat Characteristic: Attempts to connect to suspicious URL http://198.46.132.185/		
Detection	Threat Characteristic: Attempts to connect to suspicious URL http://198.46.132.185/		
Detection	Threat Characteristic: Attempts to connect to malicious URL URL: http://198.46.132.185/wbk Threat Name: EXPLOIT_MSOFFICE.WRS		
Detection	Threat Characteristic: Detected as known malware Source: ATSE Detection Name: TROJ_FRS.VSNW19E21 Engine Version: 12.500.1008 Malware Pattern Version: 16.743.92		
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\ Value: None		2344
Add Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\Startup\tems\ Value: None		2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\6s% Value: None		2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\0000210903000000000000000000000000000000		2344
Write Registry Key	CÜJSage\WORDFiles Value: 52bb0008 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00002109030000000000000000000F0FE		2344
Write Registry Key	C.Usage\ProductFiles Value: 52bb0008 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000021090300000000000000000F01FE		2344
Call Filesystem API	CUsage\ProductFiles Value: 52bb0009 API Name: CopyFileExW Args: (%ALLUSERSPROFILE%Microsoft\OFFICE\DATA\OPA12.BAK, %ALLUSERSPROFILE%Microsoft\OFFICE\DATA\Opa12.d		2344
san i nooyotom / u i	at, 0, 0, 0, 1) Return: 0		2011
Vrite Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\MTTT Value: None		2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\0000210903000000000000000000000000000000		2344
Vrite Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\Startup\tems\'x% Value: None		2344
Add File	Path: %APPDATA%Microsoft\Templates\~\$Normal.dotm Type: VSDT_COM_DOS		2344
Vrite File	Path: %APPDATA%\Microsoft\Templates\~\$Normal.dotm Type: VSDT_COM_DOS		2344
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\`x% Value: None		2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\Startupltems\}\% Value: None		2344
Call Internet Helper API	API Name: InternetOpenW Args: (Microsoft Office Protocol Discovery, 0, , , 0) Return: cc0004		2344
Call System API	API Name: DnsQueryExW Args: (198.46.132.185, 1, 50000000) Return: 0		2344
Detection	Threat Characteristic: Queries DNS server 198.46.132.185		
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, 198.46.132.185, 80, , , 3, 0, 0) Return: cc0008		2344
Call Internet Helper API	API Name: HttpOpenRequestW Args: (cc0008, OPTIONS, /, HTTP/1.1, , 0, -2141124608, 0) Return: cc000c		2344
Detection	Threat Characteristic: Connects to remote URL or IP address http://198.46.132.185/		
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASAPI32\ Value: None		2344
Vrite Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASAPI32\EnableFileTracing Value: 0		2344
Vrite Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASAPI32\EnableConsoleTracing Value: 0		2344
Vrite Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASAP\32\FileTracingMask Value: ffff0000		2344
Vrite Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASAP\32\ConsoleTracing\Mask Value: ffff0000		2344
Vrite Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASAPI32\MaxFileSize Value: 100000		2344
Vrite Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASAPI32\FileDirectory Value: %windir%\tracing		2344
Call Service API	API Name: OpenServiceW Args: (265dcc8, Sens, 4) Return: 26d2188		2344
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASMANCS\ Value: None		2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASMANCS\EnableFileTracing Value: 0		2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASMANCS\EnableConsoleTracing Value: 0		2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASMANCS\FileTracing\Mask\Value: fff0000		2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASMANCS\ConsoleTracingMask Value: ffff0000		2344
Write Registry Key Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASMANCS\MaxFileSize Value: 100000 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\WINWORD_RASMANCS\FileDirectory Value: \%windir\%\tracing		2344
Call Service API	API Name: OpenServiceA Args: (26d2520, rasman, 4) Return: 26d24a8		2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable Value: 0		2344

Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Internet Settings\ProxyOverride Value: None	2344
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Internet Settings\AutoConfigURL Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Internet Settings\Connections\SavedLegacySettings Value: None	2344
Call Service API	API Name: OpenServiceA Args: (26d26d8, RASMAN, 4) Return: 26d2660	2344
Call Network API	API Name: socket Args: (23, 1, 6) Return: 5e0	2344
Call Network API	API Name: socket Args: (23, 1, 6) Return: 5e0	2344
Call Network API	API Name: socket Args: (2, 2, 0) Return: 608	2344
Call Network API	API Name: socket Args: (23, 2, 0) Return: 608	2344
Call Network API	API Name: socket Args: (23, 1, 6) Return: 5f4	2344
Vrite Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Internet Settings\Connections\DefaultConnectionSettings Value: None	2344
Call Network API	API Name: socket Args: (2, 1, 6) Return: 620	2344
Call Network API	API Name: bind Args: (620, 0.0.0.49166, 16) Return: 0	2344
Detection	Threat Characteristic: Listens on port 0.0.0.0:49166	
Call Network API	API Name: connect Args: (620, 198.46.132.185:80, 16) Return: ffffffff	2344
call Network API	API Name: send Args: (620, OPTIONS / HTTP/1.1\r\nUser-Agent: Microsoft Office Protocol Discovery\r\nHost: 198. 46.132.185\r\nContent-Length: 0\r\nConnection: Keep-Alive\r\n\r\n\r\n, 203, 0) Return: 203	2344
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 198.46.132.185:80 Content: OPTIONS / HTTP/1.1\r\nUser-Agent: Microsoft Office Protocol Discovery\r\nHost: 198.46.132.185\r\nContent-Con	
Call Network API	API Name: recv Args: (620, , 1024, 0) Return: ?	2344
Call Network API	API Name: recv Args: (620, , 1, 2) Return: ?	2344
dd Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Intermet\Server Cache\ Value: None	2344
/rite Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Intermet\Server Cache\Count Value: 1	2344
dd Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\http://198.46.132.185/	2344
Vrite Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\http://198.46.132.185/	2344
Vrite Registry Key	-AType Value: 0 Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\http://198.46.132.185/	2344
/rite Registry Key	-A/Protocol Value: 0 Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Intermet\Server Cache\http://198.46.132.185/	2344
	-/\Version Value: 0	2344
Vrite Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\http://198.46.132.185/\AFlags Value: 0	
Vrite Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Internet\Server Cache\http://198.46.132.185//Expiration Value: None	2344
dd Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\ Value: None	2344
/rite Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft\SmartScreen.dll\LogSession\Name \Value: stdout	2344
Vrite Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\Active Value: 1	2344
Vrite Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft.SmartScreen.dll\ControlFlags Value: 1	2344
dd Registry Key	$Key: HKEY_LOCAL_MACHINE \\ SOFTWARE \\ Microsoft \\ Windows NT \\ Current \\ Version \\ NT \\ Current \\ NT \\ Version \\ NT \\ NT \\ Version \\ NT \\ N$	2344
Vrite Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWAREIMicrosoft\Windows NT\CurrentVersion\Tracing\Microsoft\SmartScreen.dll\Regular\Guid Value: 7e4b70ee-8296-4 f0f-a3ba-f58ef7bb4e96	2344
Vrite Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current\Version\Tracing\Microsoft\SmartScreen.dll\Regular\BitNames Value: Error Unusu	2344
2 H 2 : 4Bl	al Noise Entry Exit Probability Cracking CrackingError Debug	2044
Call Service API	API Name: OpenServiceW Args: (26d1b70, Webclient, 5) Return: 26d1b98	2344
all Internet Helper API	API Name: WNetAddConnection3W Args: (b017c, Remote<\\198.46.132.185\DavWWWRoot\ Local<\\198.46.132. 185\DavWWWRoot\), , c) Return: 35	2344
Vrite Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Shell Extensions\Cached\\BDEADF00-C265-11D0-BCED-00A0C90AB50F\} {0002 14E6-0000-0000-C000-000000000046} 0xFFFF Value: None	2344
all Internet Helper API	API Name: InternetGetConnectedStateExW Args: (2011ec, 0, 0, 0) Return: 1	2344
Call Network API	API Name: socket Args: (2, 2, 17) Return: 654	2344
Call Network API	API Name: bind Args: (654, 127.0.0.1:62203, 16) Return: 0	2344
Detection	Threat Characteristic: Listens on port 127.0.0.1:62203	
Call Internet Helper API	API Name: InternetOpenW Args: (Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET	2344
Call Custom ADI	CLR 3.0.30729; Media Center PC 6.0; InfoPath.2; .NET4.0C; .NET4.0E), 0, , , 10000000) Return: cc0004	2011
all System API	API Name: DnsQueryExW Args: (198.46.132.185, 1, 50000000) Return: 0	2344
Call Internet Helper API	API Name: InternetConnectW Args: (cc0004, 198.46.132.185, 80, , , 3, 0, 40813440) Return: cc0008	2344
all Internet Helper API	API Name: httpOpenRequestW Args: (cc0008, GET, / wbk, , , 2100704, 4261904, 4 0813440) Return: cc000c	2344
Detection	Threat Characteristic: Connects to remote URL or IP address http://198.46.132.185/wbk	
Call Network API	API Name: recv Args: (620, , 1, 2) Return: ?	2344
all Network API	API Name: recv Args: (620, , 1, 2) Return: ?	2344
all Network API	API Name: socket Args: (2, 1, 6) Return: 620	2344
all Network API	API Name: bind Args: (620, 0.0.0.49168, 16) Return: 0	2344
etection	Threat Characteristic: Listens on port 0.0.0.0:49168	
	API Name: connect Args: (620, 198.46.132.185:80, 16) Return: ffffffff	2344
all Network API	API Name: recv Args: (654, , 32, 0) Return: ?	2344
		_
Call Network API Call Network API Call Network API	API Name: send Args: (654, !, 1, 0) Return: 1	2344

cleristic: Connects to remote URL or IP address 1894.6.132.185.80 17		2344 2344 2344 2344 2344 2344 2344 2344
		2344 2344
MSOffice 12]vinAccept-Encoding: gzip, deflate/nhHost: 198.46.132.185vinConnection: Keep-Alivelvini/n cov Args: (620, 1024, 0) Return: ? and Args: (654, 1, 1, 0) Return: 1 cov Args: (654, 1, 1, 0) Return: ? cov Args: (654, 1, 2) Return: ? cov Args: (620, 1024, 0) Return: ? cov Args: (620, 1024, 0) Return: ? cov Args: (620, 1, 2) Return: ? cov Args: (620,		2344 2344
cov Args: (620, 1024, 0) Return: ? end Args: (654, 1, 1, 0) Return: 1 eov Args: (654, 1, 1, 0) Return: ? eov Args: (620, 1024, 0) Return: ? eov Args: (620, 1, 12) Re		2344 2344
and Args: (654, 1, 1, 0) Return: 1 cov Args: (654, 32, 0) Return: ? cov Args: (620, 1024, 0) Return: ? cov Args: (620, 1, 12) Return: ? co		2344 2344
cov Args: (654, 32, 0) Return: ? cov Args: (620, 1024, 0) Return: ? cov Args: (620, 1, 12) Return: ? cov		2344 2344
tex Args: (620, , 1024, 0) Return: ? Exer Args: (620, , 1, 2) Return: ? Exer Args: (610, , 1, 2) Ret		2344 2344
cov Args: (620, 1, 1, 2) Return: ? CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 1 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 2 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 2 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 3 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 3 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 5 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 6 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 6 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 8 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 8 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 9 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 9 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 10 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 11 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 11 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 13 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 13 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 15 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 15 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 16 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 16 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 16 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 18 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 19 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 19 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 19 Value:		2344 2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Max Display Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 1 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 2 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 3 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 4 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 5 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 6 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 6 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 8 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 9 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 10 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 11 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 12 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 13 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 14 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 14 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 17 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 16 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 16 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 18 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 18 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 18 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 19 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 19 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 19 Value: None		2344 2344 2344 2344 2344 2344 2344 2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 1 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 3 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 3 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 4 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 5 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 6 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 7 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 8 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 9 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 9 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 10 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 11 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 16 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 17 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 18 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 18 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 19 Value\ None		2344 2344 2344 2344 2344 2344 2344 2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 2 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 3 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 4 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 5 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 6 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 7 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 8 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 9 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 9 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 10 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 11 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 11 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 12 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 13 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 14 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 15 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 16 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 17 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 17 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 18 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 19 Value: None		2344 2344 2344 2344 2344 2344 2344 2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 3 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 4 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 6 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 6 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 6 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 7 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 9 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 9 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 10 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 11 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 12 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 13 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 14 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 15 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 16 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 16 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 17 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 18 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 19 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 19 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 19 Value\ None		2344 2344 2344 2344 2344 2344 2344 2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 3 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 4 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 6 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 6 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 6 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 7 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 9 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 9 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 10 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 11 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 12 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 13 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 14 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 15 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 16 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 16 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 17 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 18 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 19 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 19 Value\ None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 19 Value\ None		2344 2344 2344 2344 2344 2344 2344 2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 4 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 5 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 6 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 7 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 8 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 9 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 10 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 11 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 12 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 12 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 13 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 14 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 15 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 15 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 16 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 17 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 16 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 18 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 18 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 19 Value: None		2344 2344 2344 2344 2344 2344 2344 2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 5 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 6 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 7 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 8 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 9 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 10 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 11 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 12 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 12 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 13 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 14 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 15 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 16 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 17 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 18 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 18 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 18 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 19 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 19 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 20 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 20 Value: None		2344 2344 2344 2344 2344 2344 2344 2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 6 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 8 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 9 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 9 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 10 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 11 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 11 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 12 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 13 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 14 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 15 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 16 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 17 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 18 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 18 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 18 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 19 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 19 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 20 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 20 Value: None		2344 2344 2344 2344 2344 2344 2344 2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 7 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 8 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 9 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 10 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 11 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 12 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 13 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 13 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 14 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 15 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 16 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 17 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 18 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 18 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 19 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 19 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 19 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 20 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 20 Value: None		2344 2344 2344 2344 2344 2344 2344 2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 8 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 9 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 10 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 11 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 12 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 13 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 14 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 15 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 16 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 16 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 17 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 18 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 19 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 19 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 19 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 20 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 20 Value: None		2344 2344 2344 2344 2344 2344 2344 2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 9 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 10 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 11 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 12 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 13 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 14 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 15 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 16 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 16 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 17 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 18 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 19 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 19 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 20 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 20 Value: None		2344 2344 2344 2344 2344 2344 2344 2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 10 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 11 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 12 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 13 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 14 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 15 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 15 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 16 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 17 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 18 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 19 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 19 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 20 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 20 Value: None		2344 2344 2344 2344 2344 2344 2344 2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 11 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 12 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 13 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 14 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 15 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 16 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 17 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 18 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 19 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 19 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 19 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 20 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 21 Value: None		2344 2344 2344 2344 2344 2344 2344 2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 12 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 13 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 14 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 15 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 16 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 17 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 17 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 18 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 19 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 20 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 20 Value: None		2344 2344 2344 2344 2344 2344 2344 2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 13 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 14 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 15 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 16 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 17 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 18 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 19 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 20 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 20 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 20 Value: None		2344 2344 2344 2344 2344 2344 2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 14 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 15 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 16 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 17 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 18 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 19 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 19 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 20 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 20 Value: None		2344 2344 2344 2344 2344 2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 15 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 16 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 17 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 18 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 19 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 20 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 20 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 21 Value: None		2344 2344 2344 2344 2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 16 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 17 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 18 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 19 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 20 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 20 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 21 Value: None		2344 2344 2344 2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 17 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 18 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 19 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 20 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 21 Value: None		2344 2344 2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 17 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 18 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 19 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 20 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 21 Value: None		2344 2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 18 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 19 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 20 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 21 Value: None		2344 2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 19 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 20 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 21 Value: None		2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 20 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 21 Value: None		
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 21 Value: None		
		2344
CURRENT_USER\Software\microsoft\Onice\12.0\word\File mro\nem 22 Value: None		
		2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 23 Value: None		2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 24 Value: None		2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 25 Value: None		2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 26 Value: None		2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 27 Value: None		2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 28 Value: None		2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 29 Value: None		2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 30 Value: None		2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 31 Value: None		2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 32 Value: None		2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 33 Value: None		2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 34 Value: None		2344
		2344
		2344
		2344
		2344
		2344
		2344
		2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 42 Value: None		2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 43 Value: None		2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 44 Value: None		2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 45 Value: None		2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 46 Value: None		2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 47 Value: None		2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 48 Value: None		2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 49 Value: None		2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 50 Value: None		2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Max Display Value: None		2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 1 Value: None		2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 2 Value: None		2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 3 Value: None		2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 4 Value: None		2344
		2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 5 Value: None		2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 5 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 6 Value: None		2344
		2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 6 Value: None		2344
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 6 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 7 Value: None		
CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 6 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 7 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 8 Value: None		2344
	CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 43 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 45 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 46 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 46 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 47 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 47 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 49 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 49 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 50 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 50 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 12 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 3 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 3 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 3 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 4 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\tem 5 Value: None	CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRUItlem 36 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRUItlem 37 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRUItlem 38 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRUItlem 39 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRUItlem 40 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRUItlem 40 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRUItlem 41 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRUItlem 42 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRUItlem 42 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRUItlem 43 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRUItlem 44 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRUItlem 45 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRUItlem 46 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRUItlem 47 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRUItlem 47 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRUItlem 49 Value: None CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRUItlem 10 Value

Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 12 Value: None	2344
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 13 Value: None	2344
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 14 Value: None	2344
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\\tem 15 Value: None	2344
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\\tem 16 Value: None	2344
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 17 Value: None	2344
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 18 Value: None	2344
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 19 Value: None	2344
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 20 Value: None	2344
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 21 Value: None	2344
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 22 Value: None	2344
		2344
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 23 Value: None	
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 24 Value: None	2344
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 25 Value: None	2344
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 26 Value: None	2344
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 27 Value: None	2344
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 28 Value: None	2344
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 29 Value: None	2344
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 30 Value: None	2344
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 31 Value: None	2344
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 32 Value: None	2344
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 33 Value: None	2344
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 34 Value: None	2344
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 35 Value: None	2344
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 36 Value: None	2344
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 37 Value: None	2344
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 38 Value: None	2344
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 39 Value: None	2344
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 40 Value: None	2344
		2344
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 41 Value: None	
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 42 Value: None	2344
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 43 Value: None	2344
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 44 Value: None	2344
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 45 Value: None	2344
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\\tem 46 Value: None	2344
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 47 Value: None	2344
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\Item 48 Value: None	2344
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 49 Value: None	2344
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\File MRU\ltem 50 Value: None	2344
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Office\Recent\Quote 2405987021.docx.LNK) Return: 0	2344
Call Internet Helper API	API Name: NetShareEnum Args: (, 503, 71df0250, -1, 1fd974, 1fd970, 0) Return: 0	2344
Detection	Threat Characteristic: Executes commands or uses API to obtain system information Process ID: 2344	
	Info: Enums share folder from API result	
Call Filesystem API	API Name: DeleteFileW Args: (%APPDATA%IMicrosoft\Office\Recent\WTYOSLM.LNK) Return: 0	2344
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\}% Value: None	2344
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Schemas\MS Word_restart.xml) Return: 0	2344
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\6s% Value: None	2344
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\StartupItems\ Value: None	2344
Delete Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Resiliency\ Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Arial Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Courier New Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Symbol Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Wingdings Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Mincho Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Batang Value: None	2344
		2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\SimSun Value: None	
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\PMingLiU Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Gothic Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Dotum Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\SimHei Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MingLiU Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Gulim Value: None	2344
	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Century Value: None	2344
Write Registry Key		2344
Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Angsana New Value: None	
	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Angsana New Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Cordia New Value: None	2344
Write Registry Key		2344
Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Cordia New Value: None	
Write Registry Key Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Cordia New Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Mangal Value: None	2344
Write Registry Key Write Registry Key Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Cordia New Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Mangal Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Latha Value: None	2344 2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Cordia New Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Latha Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Latha Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Sylfaen Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Vrinda Value: None	2344 2344 2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Cordia New Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Mangal Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Latha Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Sylfaen Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Vrinda Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Vrinda Value: None	2344 2344 2344 2344 2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Cordia New Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Latha Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Latha Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Sylfaen Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Vrinda Value: None	2344 2344 2344 2344

	K HIKEV CHEDENT HEEDIG A HIKE WAS IT THE IT IN IN	0044
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Tunga Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Estrangelo Edessa Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Cambria Math Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Arial Unicode MS Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Tahoma Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Marlett Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@Batang Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\BatangChe Value: None	
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@BatangChe Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Gungsuh Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@Gungsuh Value: None	2344
Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Gungsuh\Che Value: None	2344
	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@GungsuhChe Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\DaunPenh Value: None	2344
Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\DokChampa Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Euphemia Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Vani Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@Gulim Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\GulimChe Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@GulimChe Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@Dotum Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\DotumChe Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@DotumChe Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Impact Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\lskoola Pota Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Kalinga Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Kartika Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Khmer UI Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Lao UI Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Lucida Console Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Malgun Gothic Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@Malgun Gothic Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Meiryo Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@Meiryo Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Meiryo UI Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@Meiryo UI Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Microsoft Himalaya Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Microsoft JhengHei Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@Microsoft JhengHei Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Microsoft YaHei Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@Microsoft YaHei Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@MingLiU Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@PMingLiU Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MingLiU_HKSCS Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@MingLiU_HKSCS Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MingLiU-ExtB Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@MingLiU-ExtB Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\PMingLiU-ExtB Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@PMingLiU-ExtB Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MingLiU_HKSCS-ExtB Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@MingLiU_HKSCS-ExtB Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Mongolian Baiti Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@MS Gothic Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS PGothic Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@MS PGothic Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS UI Gothic Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@MS UI Gothic Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@MS Mincho Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS PMincho Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@MS PMincho Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MV Boli Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Microsoft New Tai Lue Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Nyala Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Microsoft PhagsPa Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Plantagenet Cherokee Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Segoe Script Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Segoe UI Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Segoe UI Semibold Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Segoe UI Light Value: None	2344
	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Segoe UI Symbol Value: None	2344
Write Registry Key		
Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@SimSun Value: None	2344

Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@NSimSun Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\SimSun-ExtB Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@SimSun-ExtB Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Microsoft Tai Le Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Shonar Bangla Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Microsoft Yi Baiti Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Microsoft Sans Serif Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Aparajita Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Ebrima Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Gisha Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Kokila Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Leelawadee Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Microsoft Uighur Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MoolBoran Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Utsaah Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Vijaya Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Andalus Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Arabic Typesetting Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Simplified Arabic Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Simplified Arabic Fixed Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Sakkal Majalla Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Traditional Arabic Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Aharoni Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\David Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\FrankRuehl Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Levenim MT Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Miriam\Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Miriam Fixed Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Narkisim Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Rod Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\FangSong Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@FangSong Value: None	2344
		2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@SimHei Value: None	
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\KaiTi Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@KaiTi Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER:Software\Microsoft\Shared Tools\Panose\AngsanaUPC Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Browallia New Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\BrowalliaUPC Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\CordiaUPC Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\DilleniaUPC Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\EucrosiaUPC Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\FreesiaUPC Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\IrisUPC Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\JasmineUPC Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\KodchiangUPC Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\LilyUPC Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\DFKai-SB Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@DFKai-SB Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Lucida Sans Unicode Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Arial Black Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Candara Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Comic Sans MS Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Consolas Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Constantia Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Corbel Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Franklin Gothic Medium Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Gabriola Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Georgia Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Palatino Linotype Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Segoe Print Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Trebuchet MS Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Verdana Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Webdings Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Agency FB Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Arial Rounded MT Bold Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Blackadder ITC Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Bodoni MT Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Bodoni MT Black Value: None	2344
write registry rey	•	
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Bodoni MT Condensed Value: None	2344
Write Registry Key	Key: HKEY_CURRENI_USER\Software\Microsoft\Shared lools\Panose\Book Antiqua Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Book Antiqua Value: None	2344

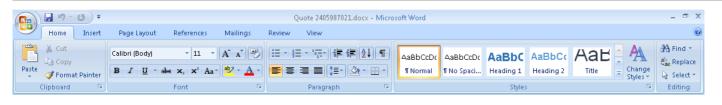
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Calisto MT Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Castellar Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Century Gothic Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Century Schoolbook Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Copperplate Gothic Bold Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Copperplate Gothic Light Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Curlz MT Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Edwardian Script ITC Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Elephant Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Engravers MT Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Eras Bold ITC Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Eras Demi ITC Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Eras Light ITC Value: None	2344
Write Registry Key	$Key: HKEY_CURRENT_USER (Software) Microsoft (Shared Tools) Panose (Eras Medium ITC Value: None Medium ITC Value) Panose (Medium ITC Value) Panose $	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Felix Titling Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Forte Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Franklin Gothic Book Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Franklin Gothic Demi Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Franklin Gothic Demi Cond Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Franklin Gothic Heavy Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Franklin Gothic Medium Cond Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\French Script MT Value: None	2344
Write Registry Key	Key: HKEY CURRENT USER\Software\Microsoft\Shared Tools\Panose\Gigi Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Gill Sans MT Ext Condensed Bold Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Gill Sans MT Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Gill Sans MT Condensed Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Gill Sans Ultra Bold Value: None	2344
Write Registry Key		
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Gill Sans Ultra Bold Condensed Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Gloucester MT Extra Condensed Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Goudy Old Style Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Goudy Stout Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Haettenschweiler Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Imprint MT Shadow Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Lucida Sans Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Lucida Sans Typewriter Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Maiandra GD Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Monotype Corsiva Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\OCR A Extended Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Palace Script MT Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Papyrus Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Perpetua Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Perpetua Titling MT Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Pristina Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Rage Italic Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Rockwell Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Rockwell Condensed Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Rockwell Extra Bold Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Script MT Bold Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Tw Cen MT Value: None	
		2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Tw Cen MT Condensed Value: None	
Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Tw Cen MT Condensed Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Wingdings 2 Value: None	2344
		2344 2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Wingdings 2 Value: None	2344 2344 2344
Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Wingdings 2 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Wingdings 3 Value: None	2344 2344 2344 2344
Write Registry Key Write Registry Key Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Wingdings 2 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Wingdings 3 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Reference Sans Serif Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Reference Specialty Value: None	2344 2344 2344 2344 2344 2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Wingdings 2 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Wingdings 3 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Reference Sans Serif Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Reference Specialty Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Reference Specialty Value: None	2344 2344 2344 2344 2344 2344 2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Wingdings 2 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Wingdings 3 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Reference Sans Serif Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Reference Specialty Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Reference Specialty Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Outlook Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Outlook Value: None	2344 2344 2344 2344 2344 2344 2344 2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Wingdings 2 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Wingdings 3 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Reference Sans Serif Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Reference Specialty Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS County Condensed Extra Bold Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Outlook Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Outlook Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Outlook Value: None	2344 2344 2344 2344 2344 2344 2344 2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Wingdings 2 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Wingdings 3 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Reference Sans Serif Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Reference Specialty Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Outlook Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Outlook Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS overline Symbol 7 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS overline Symbol 7 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS overline Symbol 7 Value: None	2344 2344 2344 2344 2344 2344 2344 2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Wingdings 2 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Wingdings 3 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Reference Sans Serif Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Reference Specialty Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Cerence Specialty Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Outlook Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Bookshelf Symbol 7 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Feestyle Script Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Feestyle Script Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Juice ITC Value: None	2344 2344 2344 2344 2344 2344 2344 2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Wingdings 2 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Wingdings 3 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Reference Sans Serif Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Reference Specialty Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Ceference Specialty Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Outlook Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Outlook Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\HS Outlook Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Freestyle Script Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Undersoft\Undersoft\Shared Tools\Panose\Undersoft\Undersoft\Undersoft\Shared Tools\Panose\Undersoft\Undersoft\Undersoft\Shared Tools\Panose\Undersoft\Under	2344 2344 2344 2344 2344 2344 2344 2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Wingdings 2 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Wingdings 3 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Ms Reference Sans Serif Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Ms Reference Specialty Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Ms Cen MT Condensed Extra Bold Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Ms Outlook Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Book\shelf Symbol 7 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Panose\Unice ITC Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Unice ITC Value: None	2344 2344 2344 2344 2344 2344 2344 2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Wingdings 2 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Wingdings 3 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Reference Sans Serif Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Reference Specialty Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Ceference Specialty Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Outlook Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Outlook Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\HS Outlook Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Freestyle Script Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Undersoft\Undersoft\Shared Tools\Panose\Undersoft\Undersoft\Undersoft\Shared Tools\Panose\Undersoft\Undersoft\Undersoft\Shared Tools\Panose\Undersoft\Under	2344 2344 2344 2344 2344 2344 2344 2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Wingdings 2 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Wingdings 3 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Ms Reference Sans Serif Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Ms Reference Specialty Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Ms Cen MT Condensed Extra Bold Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Ms Outlook Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Book\shelf Symbol 7 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Panose\Unice ITC Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Unice ITC Value: None	2344 2344 2344 2344 2344 2344 2344 2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Wingdings 2 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Wingdings 3 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Mis Reference Sans Serif Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Mis Reference Specialty Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Mis Outlook Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Mis Outlook Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Mis Soript Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Mis Soript Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Mis To Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Mis To Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Mis ITC Value: None	2344 2344 2344 2344 2344 2344 2344 2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Wingdings 2 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Wingdings 3 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Ms Reference Sans Serif Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Ms Reference Specialty Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Ms Reference Specialty Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Ms Outlook Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Bookshelf Symbol 7 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Panos	2344 2344 2344 2344 2344 2344 2344 2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Wingdings 2 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Wingdings 3 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Mis Reference Sans Serif Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Mis Reference Specialty Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Mis Reference Specialty Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Mis Outlook Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Box\shaft Symbol 7 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Panose\Panose\Microsoft\Shared Tools\Panose\Microsoft\Shared Tools\Pano	2344 2344 2344 2344 2344 2344 2344 2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Wingdings 2 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Wingdings 3 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Ms Reference Sans Serif Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Ms Reference Specialty Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Ms Outlook Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Ms Outlook Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Hspanose\H	2344 2344 2344 2344 2344 2344 2344 2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Wingdings 2 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Wingdings 3 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Ms Reference Sans Serif Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Ms Reference Specialty Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Ms Outlook Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Ms Outlook Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Hsos\Panose\Panose\Hsos\Panose\Pa	2344 2344 2344 2344 2344 2344 2344 2344 2344 2344 2344 2344 2344 2344 2344 2344 2344 2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Wingdings 2 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Wingdings 3 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Mis Reference Sans Serif Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Mis Reference Specialty Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Mis Outlook Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Mis Outlook Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Bookshelf Symbol 7 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Foots\Panose\Foots\Panose\P	2344 2344 2344 2344 2344 2344 2344 2344 2344 2344 2344 2344 2344 2344 2344 2344 2344 2344 2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Wingdings 2 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Wingdings 3 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Wingdings 3 Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Reference Sans Serif Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Reference Specialty Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Outlook Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MS Outlook Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Hseta Serift Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Hrestyle Serift Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Hristen ITC Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Lucida Handwriting Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Mistral Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Mistral Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Mistral Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Arial Narrow Value: None	2344 2344

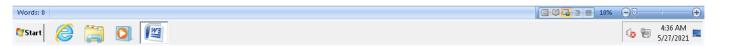
W. 5	IV. HIVEV CHIPPETE HAPPING A. HIV. WOL. IT. LID. ID. HIVED I. LIVE III.	2011
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Bernard MT Condensed Value: None	2344
Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Bodoni MT Poster Compressed Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Britannic Bold Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Broadway Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Brush Script MT Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Californian FB Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Centaur Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Chiller Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Colonna MT Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Cooper Black Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Footlight MT Light Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Harlow Solid Italic Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Harrington Value: None	2344
Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\High Tower Text Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Jokerman Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Kunstler Script Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Lucida Bright Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Lucida Calligraphy Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Lucida Fax Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Magneto Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Matura MT Script Capitals Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Modern No. 20 Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Niagara Engraved Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Niagara Solid Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Old English Text MT Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Onyx Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Parchment Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Playbill Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Poor Richard Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Ravie Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Informal Roman Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Showcard Gothic Value: None	2344
Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Snap ITC Value: None Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Stencil Value: None	2344
Write Registry Key	Key: HKEY CURRENT USER\Software\Microsoft\Shared Tools\Panose\Viner Hand ITC Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Vivaldi Value: None	2344
Write Registry Key	Key: HKEY CURRENT USER\Software\Microsoft\Shared Tools\Panose\Vladimir Script Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\Wide Latin Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\@Arial Unicode MS Value: None	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose\MT Extra Value: None	2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00002109F100A0C00000000000F01F EC\Usage\SpellingAndGrammarFiles_3082 Value: 52bb0004	2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00002109F100A0C00000000000F01F	2344
Write Registry Key	EC/Usage/SpellingAndGrammarFiles_3082 Value: 52bb0005 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100A0C0000000000F01F	2344
Write Registry Key	EC!Usage\SpellingAndGrammarFiles_3082 Value: 52bb0006 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\lnstaller\UserData\S-1-5-18\Products\00002109F1009040000000000F01FE	2344
	C\Usage\SpellingAndGrammarFiles_1033 Value: 52bb0005	
Call Network API	API Name: recv Args: (620, , 1, 2) Return: ? You HVEY LOCAL MACHINE COETIMA PENNices of Ministration Installated Level Color (24 & 18) Description (2000) 1000 1000 1000 1000 1000 1000 1000	2344
Write Registry Key	Key: HKEY_LOCAL_MACHINEISOFTWAREIMicrosoftWindows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F1009040000000000F01FE C\Usage\SpellingAndGrammarFiles_1033 Value: 52bb0006	2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00002109F1009040000000000F01FE C\Usage\SpellingAnd\Grammar\Files_1033\Value: 52bb0007	2344
Write Registry Key	Key: HKEY_LOCAL_MACHINEISOFTWAREIMicrosoftIWindows\Current\Version\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF1005403838 9C\Usage\SpelllingAndGrammarFiles_1033 \Value: 52bb0011	2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF1005403838 9C\Usage\SpellingAndGrammarFiles_1033 \Value: 52bb0012	2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00002109F100C0400000000000F01F EC\Usage\SpellingAndGrammarFiles_1036 Value: 52bb0005	2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00002109F100C040000000000F01F EC\Usage\SpellingAndGrammarFiles_1036 \Value: 52bb0006	2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF1005403838 9C\Usage\Spelling\AndGrammar\Files_1033\Value: 52bb0013	2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF1005403838 9C\Usage\SpellingAndGrammarFiles_1033 Value: 52bb0014	2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF1005403838 9C\Usage\SpellingAndGrammarFiles_1033 Value: 52bb0015	2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\9040110900063D11C8EF1005403838 9C\Usage\SpellingAndGrammarFiles_1033 Value: 52bb0016	2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\lnstaller\UserData\S-1-5-18\Products\9040110900063D11C8EF1005403838 9C\Usage\SpellingAndGrammarFiles_1033 \Value: 52bb0017	2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\lnstaller\UserData\S-1-5-18\Products\9040110900063D11C8EF1005403838 9C\Usage\SpellingAndGrammarFiles_1033 \Value: 52bb0018	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\QMSessionCount Value: 2	2344
Write Registry Key	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Common\Licensing\0638C49DB88B4CD1B191051E8F325736 Value: None	2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\CLSID\{42042206-2D85-11D3-8CFF-005004838597}\Version\12\(Default) Value: %ProgramFiles%\Microsoft Office\	2344

Delete Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Edit\command\ Value: None	2344
Delete Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Edit\ Value: None	2344
Add Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Edit\ Value: None	2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Edit\(Default\) Value: &Edit	2344
Add Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Edit\command\ Value: None	2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Edit\command\(Default\) Value: "%ProgramFiles%\Microsoft Office\Office12\msohtmed.exe" %1	2344
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\command\ Value: None	2344
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\deexec\Application\ Value: None	2344
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\deexec\Topic\ Value: None	2344
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\deexec\ Value: None	2344
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ Value: None	2344
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\ Value: None	2344
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Intermet Explorer\Default HTML Editor\ Value: None	2344
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\ Value: None	2344
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\ Value: None	2344
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ Value: None	2344
		2344
Delete Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\Description Value: None	
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\(Default)\ Value: &Edit	2344
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\command\ Value: None	2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\command\(Default\) Value: "%ProgramFiles%\Microsoft Office\OFFICE11\WINWORD.EXE" /n /dde	2344
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\deexec\ Value: None	2344
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\tedit\ddeexec\Application\ Value: None	2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\tedit\ddeexec\Application\(Default) Value: WinWord	2344
Add Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\deexec\Topic\ Value: None	2344
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Default HTML Editor\shell\edit\ddeexec\Topic\(Default\) Value: System	2344
Delete Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Print\command\ Value: None	2344
Delete Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Print\ Value: None	2344
Add Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Print\ Value: None	2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Print\(Default\) Value: &Print	2344
Add Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Print\command\ Value: None	2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shell\Print\command\(Default\) Value: "%ProgramFiles%\Microsoft Office\Office\Office\12\msohtmed.exe" /p %1	2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\Defaultl\con\(Default\) Value: "%1"	2344
		2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\htmlfile\shellex\lconHandler\(Default)\ Value: \(\frac{42042206-2085-11D3-8CFF-005004838597\}\)	
Write Registry Key	Key: HKEY_CLASSES_ROOT\CLSID\(42042206-2D85-11D3-8CFF-005004838597\)InprocServer32\((Default)\) Value: %ProgramFiles%\(Microsoft\) Office\(Office\) 12\(\mathrea\) msohevi.dll	2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\CLSID\(42042206-2D85-11D3-8CFF-005004838597)\InprocServer32\ThreadingModel Value: Apartment	2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Word\shell\edit\(Default\) Value: &Open	2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Word\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\OFFICE11\W INWORD.EXE" /n /dde	2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\Open\WithList\Microsoft Office Word\shell\edit\deexec\Application\(Default)\ Value: Win\Word	2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Word\shell\edit\deexec\Topic\(Default) Value: System	2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\WinWord.exe\shell\edit\(Default\) Value: &Open	2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\WinWord.exe\shell\edit\command\(Default\) Value: "%ProgramFiles%\Microsoft Office\OFFICE11\\WINWOR D.EXE" in Idde	2344
Write Registry Key	Key: HKEY CLASSES ROOTi.htm\OpenWithList\WinWord.exe\shell\edit\ddeexec\Application\(Default\) Value: WinWord	2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\WinWord.exe\shell\edit\ddeexec\Topic\(Default\) Value: System	2344
Write Registry Key Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\Open\WithList\Microsoft Office Excel\shell\edit\(Default\) Value: &Open Key: HKEY_CLASSES_ROOT\.htm\Open\WithList\Microsoft Office Excel\shell\edit\(Command\(Default\)) Value: "%ProgramFiles%\Microsoft Office\Office\12\EXC	2344
	EL.EXE" /e	
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Excel\shell\edit\deexec\application\(Default) Value: Excel	2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Exce\shell\edit\deexec\topic\(Default\) Value: system	2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Excel.exe\shell\edit\(Default\) Value: &Open	2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Excel.exe\shell\edit\command\(Default)\Value: "%ProgramFiles%\Microsoft\Office\Office\Office\Office\12\EXCEL.EXE" /e	2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Excel.exe\shell\edit\ddeexec\application\(Default)\Value: Excel	2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\Open\WithList\Excel.exe\shell\edit\ddeexec\topic\(Default\) Value: system	2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\Open\WithList\Microsoft Office Publisher\shell\edit\(Default\) Value: &Open	2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\Microsoft Office Publisher\shell\edit\command\(Default) Value: "%ProgramFiles%\Microsoft Office\Office\Office12\\ MSPUB.EXE" %1	2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\MSPub.exe\shell\edit\(Default\) Value: &Open	2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\.htm\OpenWithList\MSPub.exe\shell\edit\command\(Default\) Value: "%ProgramFiles%\Microsoft Office\Office\Office\Office\12\MSPUB.EXE"	2344
Delete Registry Key	%1 Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Edit\command\ Value: None	2344
Delete Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Edit\ Value: None	2344
Add Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Edit\ Value: None	2344
Write Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Edit\(Default\) Value: &Edit	2344
Add Registry Key	Key: HKEY_CLASSES_ROOT\mhtmlfile\shell\Edit\command\ Value: None	2344
Call Network API	API Name: recv Args: (620, , 1, 2) Return: ?	2344
Call Filesystem API		2344
	API Name: DeleteFileW Args: (%WorkingDir%)-\$ote 2405987021.docx) Return: 1 API Name: DeleteFileW Args: (%LOCAL APPDATA%\\Microsoft\Windows\Temporary Internet Files\Content Word\-WPS/2006D4FC-2228.4BDA.B059.CCB0	
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{2996D4FC-2228-4BDA-B059-CCB0} 31414187\temp) Return: 1	2344
	API Name: DeleteFileW Args: (%APPDATA%\Microsoft\Templates\~\$Normal.dotm) Return: 1	2344
Call Filesystem API		
Call Filesystem API Delete File	Path: %APPDATA%\Microsoft\Templates\~\$Normal.dotm Type: VSDT_COM_DOS	2344



▼ Screenshot





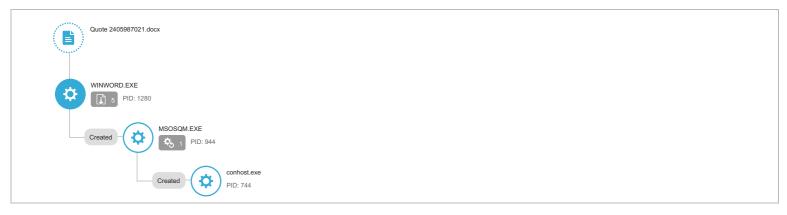


▼ Object 1 - Quote 2405987021.docx (Office Word 2007 document)

File name	Quote 2405987021.docx
File type	Office Word 2007 document
SHA-1	F1A0ABB5F96C21F8A799E4F65C4216BD968C29B7
SHA-256	5274C7FEA16B84E327D5AF683B6EF0C3E1FE1649B6CEA88399E029ED5DEEEE 6F
MD5	992ACD038FD49F200BD5510C029E74B1
Size	10356 byte(s)

Risk Level	High risk
Detection	TROJ_FRS.VSNW19E21
Exploited vulnerabilities	-
Threat Characteristics	File drop, download, sharing, or replication (5) Malformed, defective, or with known malware traits (1) Process, service, or memory object change (1)
	Suspicious network or messaging activity (15)

Process Graph



Process Graph Legend

MITRE ATT&CK™ Framework Tactics and Techniques 🕜

Tactics	Techniques	Notable Threat Characteristics
Defense Evasion	File Deletion	Characteristics: 1, 2, 3, 4, 5
Command and Control	Commonly Used Port	Characteristics: 1, 2 Characteristics: 1, 2
	Standard Application Layer Protocol	Characteristics: 1, 2 Characteristics: 1, 2

© ATT&CK™ is a trademark of The MITRE Corporation.

▼ Notable Threat Characteristics

▼ File drop, download, sharing, or replication (5)

Characteristic	Significance	Details
Deletes file to compromise the system or to remove traces of the infection	•••	Process ID: 1280 File: %TEMP%JETF46A.tmp Type: VSDT_EMPTY
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 1280 File: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.laccdb Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 1280 File: %TEMP%\{79E67E4E-6583-4317-BA5A-34825494C066} Type: VSDT_COM_DOS
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 1280 File: %TEMP%JETF295.tmp Type: VSDT_EMPTY
Deletes file to compromise the system or to remove traces of the infection	•	Process ID: 1280 File: %TEMP%\{3C8A72AF-9DD6-4AC7-8EE8-D2062BD73573} Type: VSDT_COM_DOS

▼ Malformed, defective, or with known malware traits (1)

Characteristic	Significance	Details
Detected as known malware		Source: ATSE Detection Name: TROJ_FRS.VSNW19E21 Engine Version: 12.500.1008 Malware Pattern Version: 16.743.92

▼ Process, service, or memory object change (1)

Characteristic	Significance	Details
Creates process	•	Process ID: 944 Image Path: %CommonProgramFiles(x86)%Microsoft Shared\Office15\msosqm.exe

▼ Suspicious network or messaging activity (15)

Characteristic	Significance	Details
Attempts to connect to suspicious host		198.46.132.185
Attempts to connect to malicious URL		URL: http://198.46.132.185/ Threat Name: LOW-REPUTATION-URL_BLOCKED-LIST.SCORE.WRS
Attempts to connect to suspicious URL		http://198.46.132.185/dashboard/
Attempts to connect to suspicious URL		http://198.46.132.185/
Attempts to connect to malicious URL		URL: http://198.46.132.185/wbk Threat Name: EXPLOIT_MSOFFICE.WRS
Connects to remote URL or IP address	•==	Connection: 198.46.132.185:80 Content: GET /wbk HTTP/1.1\r\nAccept: "\"\r\nUser-Agent: Mozilla/4.0 [compatible] e; MSIE 7.0; Windows NT 6.2; WOW64; Trident/8.0; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; ms-office; MS Office 15]\r\nAccept-Encoding: gzip, deflate\r\nHost: 198.46.132.185\r\nConnection: Keep-Alive\r\n\r\n
Connects to remote URL or IP address	•••	Connection: 198.46.132.185:80 Content: OPTIONS /dashboard/ HTTP/1.1\n\nConnection: Keep-Alive\n\nUser-Agent: Microsoft Office Word 2013\n\nX-MSGETWEBURL: (\n\nX-IDCRL_ACC EPTED: (\n\n) hlost: 198.46.132.185\n\n\n\n'n\n'n
Connects to remote URL or IP address	•••	Connection: 198.46.132.185:80 Content: OPTIONS / HTTP/1.1\r\nConnection: Keep-Aliveir\nUser-Agent: Microsoft Office Word 2013\r\nX-MSGETWEBURL: \text{tr\nX-IDCRL_ACCEPTED: \text{tr\n}} nHost: 198.46.132.185\r\n\r\n'n
Connects to remote URL or IP address	•••	Connection: 198.46.132.185:80 Content: HEAD /
Connects to remote URL or IP address	•••	Connection: 198.46.132.185:80 Content: OPTIONS / HTTP/1.1\r\inConnection: Keep-Alive\r\nUser-Agent: Microsoft Office Word 2013\r\inX-MSGE TWEBURL: \t\r\inX-IDCRL_ACCEPTED: \t\r\inHost: 198.46.132.185\r\in\r\in
Connects to remote URL or IP address		http://198.46.132.185/wbk
Listens on port		0.0.0.049425
Listens on port		0.0.0.0:49424
Listens on port		0.0.0.049423
Queries DNS server		198 46 132 185

▼ Network Destinations

IP Address	Port	Location	Risk Level	Threat	Accessed By
198.46.132.185	80	-	-	-	Quote 2405987021.docx

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
198.46.132.185	-	53	-	-	-	Quote 2405987021.docx
www.microsoft.com	2.22.42.141	53	-	No risk	-	Quote 2405987021.docx

URL	Site Category	Risk Level	Threat	Accessed By
http://198.46.132.185/	Disease Vector	High	LOW-REPUTATION-URL_BLOCKED-LIST.SCO RE.WRS	Quote 2405987021.docx
http://198.46.132.185/dashboard/	Untested	-	-	Quote 2405987021.docx
http://198.46.132.185/	Untested	-	-	Quote 2405987021.docx
http://198.46.132.185/ wb	Malware Accomplice	High	EXPLOIT_MSOFFICE.WRS	Quote 2405987021.docx

▼ Dropped or Downloaded Files

File	Risk Level	Threat	Threat Characteristics	Source URL	Size (bytes)	SHA-1
CentralTable.laccdb	No risk	-	-	-	64	3BC77FC29337CCDB5090B97287E0E40190 D23B47
~WRS{F270CA65-BCCD-49D7-8 207-B10AF65C41D2}.tmp	No risk	-	-	-	1024	A62F70A7B17863E69759A6720E75FC80E12 B46E6
~\$ote 2405987021.docx	No risk	-	-	-	162	9A605092E5C5DEA15E50423F57C658951D D41F5C
~\$Normal.dotm	No risk	-	-	-	162	9A605092E5C5DEA15E50423F57C658951D D41F5C
FSF-{0E1EEE64-E8C6-4E2A-975 9-63CF07FD8988},FSF	No risk	-	-	-	114	5AE926758881C0151BE31075D8BB2EDD99 5039FD
CentralTable.ini	No risk	-	-	-	36	BDF230E1F33AFBA5C9D5A039986C6505E8 B09665
msosqmcached.dat	No risk	-	-	-	788	56CBB77569780AC8E929E5882EF8CE5F62 A22CA4
~WRS{6F1EE5B2-D71A-4F3D-B6 01-F5B7764D2686}.tmp	No risk	-	-	-	1024	DBB111419C704F116EFA8E72471DD83E86 E49677
{79E67E4E-6583-4317-BA5A-348 25494C066}	No risk	-	-	-	131072	3E4AD7FE1A1E7278FD173628FF3EB36E84 8CAC65
CVR7172.tmp.cvr	No risk	-	-	-	0	DA39A3EE5E6B4B0D3255BFEF95601890AF D80709

▼ Suspicious Objects

Туре	Object	Risk Level
URL	http://198.46.132.185:80/dashboard/	Medium
File (SHA1)	F1A0ABB5F96C21F8A799E4F65C4216BD968C29B7	High
URL	http://198.46.132.185:80/	Medium
URL	http://198.46.132.185:80/	High
URL	http://198.46.132.185:80/wbk	High

▼ Analysis

▼ Analysis			
Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Attempts to connect to suspicious host	Talcittib	110
Detection	198.46.132.185		
Detection	Threat Characteristic: Attempts to connect to malicious URL		
	URL: http://198.46.132.185//		
	Threat Name: LOW-REPUTATION-URL_BLOCKED-LIST.SCORE.WRS		
Detection	Threat Characteristic: Attempts to connect to suspicious URL http://198.46.132.185/dashboard/		
Detection			
Detection	Threat Characteristic: Attempts to connect to suspicious URL http://198.46.132.185/		
Detection	Threat Characteristic: Attempts to connect to malicious URL		
	URL: http://198.46.132.185/wbk		
	Threat Name: EXPLOIT_MSOFFICE.WRS		
Detection	Threat Characteristic: Detected as known malware Source: ATSE		
	Detection Name: TROJ_FRS.VSNW19E21		
	Engine Version: 12.500.1008		
	Malware Pattern Version: 16.743.92		
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\ Value: None		1280
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\ Value: None		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems\ax(\Value: None		1280
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000		1280
	C\Usage\WORDFiles Value: 52bb012d		
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: Off		1280
Write Registry Key			
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LanguageResources\EnabledLanguages\1033 Value: On		1280
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000		1280
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\Themes\1033\NextUpdate Value: None		1280
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\WordDocParts\1033\NextUpdate Value: None		1280
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\SmartArt\1033\NextUpdate Value: None		1280
Delete Negistry Ney	Rey. FIRET_CONNENT_OCENGOT FWARE INITIOSON CONTINUED CON		1200
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\LCCache\WordDocBibs\1033\NextUpdate Value: None		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTT Value: None		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems(Value: None		1280
Add File	Path: %APPDATA%Microsoft\Templates\~\$Normal.dotm Type: VSDT_COM_DOS		1280
Write File	Path: %APPDATA%Microsoft\Templates\~\$Normal.dotm Type: VSDT_COM_DOS		1280
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\StartupItems(Value: None		1280
Call Network API	API Name: DnsQuery_W Args: (www.microsoft.com, 1c, 6000, 0, b9bf510, 0) Return: 0		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\RoamingConfigurableSettings Value: None		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Roaming\LRoami		1280
Write Registry Key	Key: HKEY CURRENT USERISOFTWAREIMicrosoft\Office\15.0\Common\Roaming\Roaming\LastWriteTime Value: None		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Resiliency\Startup\tems\=~(Value: None		1280
Call System API	API Name: PathFileExistsW Args: (%windir%\Sys\WOW64\propsys.dll) Return: 1		1280
			1280
Call System API	API Name: PathFileExistsW Args: (%windir%\SysWOW64\propsys.dll) Return: 1		
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000		1280
Call System API	API Name: DeviceloControl Args: (954, 2d1400, 111efa4, 12, 111eefc, 40, ,) Return: 1		1280
Add File	Path: %TEMP%(\(3C8A72AF-9DD6-4AC7-8EE8-D2062BD73573\) Type: VSDT_COM_DOS		1280
Write File	Path: %TEMP%(\(3C8A72AF-9DD6-4AC7-8EE8-D2062BD73573\) Type: VSDT_COM_DOS		1280
Add File	Path: %LOCALAPPDATA%/Microsoft/Office\15.0/OfficeFileCache\FSD-CNRY.FSD Type: VSDT COM DOS		1280
Write File	Path: %LOCALAPPDATA%iMicrosoftOffice\15.0\OfficeFileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS Path: %LOCALAPPDATA%iMicrosoftOffice\15.0\OfficeFileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS		1280
	**		
Call Filesystem API	API Name: CopyFileExW Args: (%TEMP%\(3C8A72AF-9DD6-4AC7-8EE8-D2062BD73573\), %LOCALAPPDATA%\(Microsoft\)OfficeFileCache\(\mathbb{F}\)S D-CNRY.FSD, 6bc1298e, 0, 0, 9) Return: 1		1280
Delete File	Path: %TEMP%\{3C8A72AF-9DD6-4AC7-8EE8-D2062BD73573} Type: VSDT_COM_DOS		1280
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection		
	Process ID: 1280		
	File: %TEMP%(3C8A72AF-9DD6-4AC7-8EE8-D2062BD73573)		
Call File and term AC'	Type: VSDT_COM_DOS		4000
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\{3C8A72AF-9DD6-4AC7-8EE8-D2062BD73573}) Return: 1		1280
Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\{3C8A72AF-9DD6-4AC7-8EE8-D2062BD73573}) Return: 0		1280
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS		1280
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS		1280
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\FSD-CNRY.FSD Type: VSDT_COM_DOS		1280
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.ini Type: VSDT_COM_DOS		1280
14/1 F1	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.ini Type: VSDT_COM_DOS		1280
Write File			
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\LocalSyncClientDiskLocation Value: None		1280

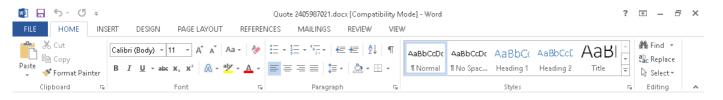
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000		1280		
Write Registry Key	CiUsage\AceFiles Value: 52bb0001 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109E6009040000000000000000000000000000000		1280		
Write Registry Key	C\Usage\AceFilesIntl_1033 Value: 52bb0001 Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109E600904000000000000F01FE		1280		
=	C\Usage\AceFilesIntl_1033 Value: 52bb0002		1280		
Add File	Path: %LOCALAPPDATA%Microsoft\Office\15.0\Office\FileCache\CentralTable.accdb Type: VSDT_MDB				
Write File Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\Office\FileCache\CentralTable.acodb Type: VSDT_MDB Path: %LOCALAPPDATA%\Microsoft\Office\15.0\Office\FileCache\CentralTable.lacodb Type: VSDT_EMPTY		1280		
Write Registry Key	Key: HKEY LOCAL MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109E600904000000000000F01FE		1280		
mic region, rey	C\Usage\AceFilesIntt_1033 Value: 52bb0003		1200		
Write File	Path: %LOCALAPPDATA%IMicrosoft\Office\15.0\OfficeFileCache\CentralTable.accdb Type: VSDT_MDB		1280		
Write File	Path: %LOCALAPPDATA%IMicrosoft\Office\15.0\OfficeFileCache\CentralTable.laccdb Type: VSDT_COM_DOS		1280		
Delete File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.laccdb Type: VSDT_COM_DOS		1280		
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1280 File: %LOCALAPPDATA%IMicrosoft\Office\15.0\OfficeFileCache\CentralTable.laccdb Type: VSDT_COM_DOS				
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.laccdb) Return: 1		1280		
Delete File	Path: %TEMP%IJETF295.tmp Type: VSDT_EMPTY		1280		
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1280 File: %TEMP%\JETF295.tmp Type: VSDT_EMPTY				
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.laccdb Type: VSDT_COM_DOS		1280		
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000		1280		
Add File	Path: %TEMP%\{79E67E4E-6583-4317-BA5A-34825494C066} Type: VSDT_COM_DOS		1280		
Write File	Path: %TEMP%\{79E67E4E-6583-4317-BA5A-34825494C066} Type: VSDT_COM_DOS		1280		
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD Type: VSDT_COM_DOS		1280		
Write File	Path: %LOCALAPPDATA%IMicrosoft(Office\15.0\Office\FileCache\LocalCacheFileEditManager\FSD-CNRY.FSD Type: VSDT_COM_DOS		1280		
Call Filesystem API	API Name: CopyFileEXW Args: (%TEMP%(79E67E4E-6583-4317-BA5A-34825494C066), %LOCALAPPDATA%(Microsoft)Office116.0\OfficeFileCache\Local CacheFileEditMoaper\FSD-CNRY.FSD, 6bb1298e, 0, 0, 9) 4817#-8148-8148-8148-8148-8148-8148-8148-814		1280		
Call Filesystem API Call Filesystem API	API Name: DeleteFileW Args: (%TEMP%\{79E67E4E-6583-4317-BA5A-34825494C066\}) Return: 1 API Name: DeleteFileW Args: (%TEMP%\{79E67E4E-6583-4317-BA5A-34825494C066\}) Return: 0		1280		
Delete File	Path: %TEMP%\{79E67E4E-6583-4317-BA5A-34825494C006\} Type: VSDT_COM_DOS		1280		
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1280 File: %TEMP%\{79E67E4E-6583-4317-BA5A-34825494C066} Type: VSDT_COM_DOS				
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD Type: VSDT_COM_DOS		1280		
Write File	Path: %LOCALAPPDATA%IMicrosoft(Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD Type: VSDT_COM_DOS		1280		
Write File Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0		1280		
Write File	e: VSDT_COM_DOS Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF Typ e: VSDT_COM_DOS		1280		
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-(C859F6E6-7E3F-4010-A8D6-20827AEC5B1E),FSD Type: VSDT_COM_DOS		1280		
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{CB59F6E6-7E3F-4010-A8D6-20827AEC5B1E},FSD Type: \SDT_COM_DOS		1280		
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988},FSF Type: \SDT_COM_DOS		1280		
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{CB59F6E6-7E3F-4010-A8D6-20827AEC5B1E},FSD Type: \NSDT_COM_DOS		1280		
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{CB59F6E6-7E3F-4010-A8D6-20827AEC5B1E}.FSD Type: VSDT_COM_DOS		1280		
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{CB59F6E6-7E3F-4010-A8D6-20827AEC5B1E},FSD Type: VSDT_COM_DOS		1280		
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\ Value: None		1280		
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\Version Value: 1		1280		
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%Microsoft/Windows)\NetCache) Return: 1		1280		
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00000011911000000000000000000000000000		1280		
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current\Version\Internet Settings\ProxyEnable Value: 0		1280		
Delete Registry Key Call Network API	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current\Version\Internet Settings\ProxyServer Value: None API Name: socket Args: (23, 1, 6) Return: b74		1280		
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current\Version\Internet Settings\ProxyOverride Value: None		1280		
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current\Version\Intermet Settings\AutoConfigURL Value: None		1280		
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current\Version\Internet Settings\AutoDetect Value: None		1280		
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings Value: None		1280		
Call Service API	API Name: OpenServiceW Args: (c583358, WinHttpAutoProxySvc, 94) Return: c5837e0		1280		
Call System API	API Name: WinHttpCloseHandle Args: (c5f2260) Return: 1		1280		
Call Service API	API Name: OpenServiceW Args: (c4f4498, NetSetupSvc, 4) Return: c4f4538		1280		
Call System API	API Name: WinHttpCloseHandle Args: (c5eabb0) Return: 1		1280		
Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%MicrosoftWindows) Return: 1		1280		
Call System API Call System API	API Name: PathFileExistsW Args: (%LOCALAPPDATA%MicrosoftWindows) Return: 1 API Name: PathFileExistsW Args: (%LOCALAPPDATA%IMicrosoftWindows)History) Return: 1		1280		
	API Name: socket Args: (23, 1, 6) Return: c08		1280		
Call Network API					

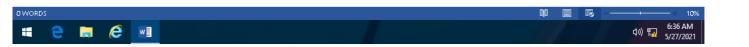
Call Network API	API Name: socket Args: (2, 1, 6) Return: c5c	1280
Call Network API	API Name: bind Args: (c5c, 0.0.0.0:49423, 128) Return: 0	1280
Detection	Threat Characteristic: Listens on port	
Call System API	0.0.0.0'49423 API Name: ConnectEx Args: (c5c, 198.46.132.185:80, 16, 0, 0, 0, c5073b0) Return: 0	1280
Call Network API	API Name: send Args: (c5c, OPTIONS / Microsoft Office Word	1280
oui notifoliti i	2013ir\nX-MSGETWEBURL: t\r\nX-IDCRL_ACCEPTED: t\r\nHost: 198.46.132.185ir\n\r\n, 1, 214) Return: 0	1200
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 198.46.132.185:80 Content: OPTIONS /	
Call System API	API Name: WinHttpCloseHandle Args: (c5f2260) Return: 1	1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\Count Value: 1	1280
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185// Value: None	1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185//Type Value: 0	1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185//Protocol Value: 0	1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185//Version Value: 0	1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185/	1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185/	1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185//CobaltMinor\Version Value: 0	1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185/	1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185//WebUrl Value: None	1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185//Expiration Value: None	1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185//EnableBHO Value: 0	1280
Call System API	API Name: WinHttpCloseHandle Args: (14fd918) Return: 1	1280
Call Network API	API Name: send Args: (c5c, HEAD /	1280
Detection	Threat Characteristic: Connects to remote URL or IP address	
	Connection: 198.46.132.185:80 Content: HEAD I	
Call Service API	API Name: OpenServiceW Args: (c4f4ad8, Webclient, 5) Return: c4f4b50	1280
Call Network API	API Name: socket Args: (2, 1, 6) Return: c54	1280
Call Network API	API Name: bind Args: (c54, 0.0.0.0:49424, 128) Return: 0	1280
Detection	Threat Characteristic: Listens on port 0.0.0.049424	
Call System API	API Name: ConnectEx Args: (c54, 198.46.132.185:80, 16, 0, 0, 0, c507b90) Return: 0	1280
Call Network API	API Name: send Args: (c54, OPTIONS / HTTP/1.1\n\nConnection: Keep-Alive\nUser-Agent: Microsoft Office Word 2013\n\nX-MSGETWEBURL: t\n\nX-IDCR	1280
	L_ACCEPTED: (\r/\nHost: 198.46.132.185\r/\n\r/\n, 1, 147) Return: 0	
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 198.46.132.185:80 Content: OPTIONS / HTTP/1.1lv\nConnection: Keep-Alive\r\nUser-Agent: Microsoft Office Word 2013\r\nX-MSGETWEBURL: t\r\nX-IDCRL_ACCEPTED: t\r\n Host: 198.46.132.185\r\n\n\r\n	
Call Network API	API Name: send Args: (c54, OPTIONS /dashboard/ HTTP/1.1\r\nConnection: Keep-Alive\r\nUser-Agent: Microsoft Office Word 2013\r\nX-MSGETWEBURL: t\r\nX-IDCRL_ACCEPTED: t\r\nHost: 198.46.132.185\r\n\r\n, 1, 157) Return: 0	1280
Detection	Threat Characteristic: Connects to remote URL or IP address Connection: 198.46.132.185:80 Content: OPTIONS /dashboard/ HTTP/1.1\nConnection: Keep-Alive\nUser-Agent: Microsoft Office Word 2013\nNX-MSGETWEBURL: t\nX-IDCRL_ACCE PTED: t\nHost: 198.46.132.185\n\n\n'n	
Call System API	API Name: WinHttpCloseHandle Args: (c5e3360) Return: 1	1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\Count Value: 2	1280
Add Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185/\ Value: None	1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185\/Type Value: 0	1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185\/Protocol Value: 0	1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185\Version Value: 0	1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185\/Flags Value: 0	1280
Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185\\CobaltMajor\Version Value: 0 Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185\\CobaltMinor\Version Value: 0	1280
······································	Key: HKEY_CURRENT_USER\SOFTWARE\microsoft\Office\15.0\Common\Internet\Server Cache\nttp://196.46.132.185\\MsDavExt Value: 0 Key: HKEY_CURRENT_USER\SOFTWARE\microsoft\Office\15.0\Common\Internet\Server Cache\nttp://198.46.132.185\\MsDavExt Value: 0	1280
Write Registry Kev	,	1280
	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185/\WebUrl Value: None	
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185\\WebUrl Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185\\Expiration Value: None	1280
Write Registry Key Write Registry Key		1280 1280
Write Registry Key Write Registry Key Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185\/Expiration Value: None	
Write Registry Key Write Registry Key Write Registry Key Write Registry Key Call Internet Helper API Call System API	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185\Expiration Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185\EnableBHO Value: 0 API Name: InternetOpenW Args: (Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/8.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NE	1280
Write Registry Key Write Registry Key Write Registry Key Call Internet Helper API Call System API	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185\Expiration Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185\EnableBHO Value: 0 API Name: InternetOpenW Args: (Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/8.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NE T CLR 3.0.30729; .NET CLR 3.5.30729), 0, , , 10000000) Return: cc0004	1280 1280
Write Registry Key Write Registry Key Write Registry Key Call Internet Helper API	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185\Expiration Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185\EnableBHO Value: 0 API Name: InternetOpenW Args: (Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/8.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NE T CLR 3.0.30729; .NET CLR 3.5.30729), 0, , , 10000000) Return: cc0004 API Name: DnsQueryEx Args: (198.46.132.185, 1, 50020000) Return: 0 Threat Characteristic: Queries DNS server	1280 1280
Write Registry Key Write Registry Key Write Registry Key Call Internet Helper API Call System API Detection	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185\Expiration Value: None Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Internet\Server Cache\http://198.46.132.185\EnableBHO Value: 0 API Name: InternetOpenW Args: (Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/8.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NE T CLR 3.0.30729; .NET CLR 3.5.30729; .O., . 10000000) Return: cc0004 API Name: DnsQueryEx Args: (198.46.132.185, 1, 50020000) Return: 0 Threat Characteristic: Queries DNS server 198.46.132.185	1280 1280 1280

Separation Parl American (1997 1997	
March Marc	1280
Mile	1280
Description	1280
Coltypera Mines Commit App Int 1886 DE 1888 1.00	1280
Milland	
An Name and page 10, CMT 10 10 10 10 10 10 10 1	1280
Procession of Section 1989 (1989) 1989 (198	ccept: */*\r\nUser-Agent: Mozill 1280
Control CERT Control CERT Control CERT Control CERT Control CERT Control CERT CONTROL CONT	
Cell Spotts APP APP	
Cell Systems APT	1280
Call System AFF	1280
No. No.	1280
Note Registry Key	1280
Mile Regulary Key	ady Value: 0 1280
Miles Registry Key	est Value: 2021-05-27T11:35: 1280
172	ady Value: 1 1280
T2	le Value: 2021-05-27T11:35:2 1280
Call Filesystem AP AP Name: DelateFileV Args. (\$LOCALAPPDATA),MicrosoftSchemasMS Word_restart xm1) Raturn: 0	te Value: 2021-05-27T11:38:2 1280
Debets Ragistry Key	1280
Delete Registry Key	1280
Delete Registry Key	1280
Write Registry Key	1280
EOUtage(SpellingAndGrammaFiles, 3082 Value: 52b00268 1280 1	
ECULaga(SpellingAndGrammarFiles_1030 Values 52bb002e)F100A0C0000000000F01F 1280
Cubage(SpellingAndGrammarFiles_1033 Value: 52bb005f)F100C040000000000F01F 1280
ECIUsage SpellingAndGrammarFiles_3082 Value: 52bb0021	3F10090400000000000F01FE 1280
ECIJsage\SpellingAndGrammarFiles_3082 Value: 52bb0030	3F100A0C0000000000F01F 1280
ECUsage\SpellingAndGrammarFiles_1036 Value: 52bb0027	3F100A0C0000000000F01F 1280
ECUsage SpellingAndGrammarFiles_1038 Value: 52bb0030	3F100C04000000000F01F 1280
C\Usage\SpellingAndGrammarFiles_1033 Value: 52bb0060 Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Universion\Installer\UserData\S-1.5-18\Products\00005109F100904000000000F01FE C\Usage\SpellingAndGrammarFiles_1033 Value: 52bb0061 Write Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Universion\Installer\UserData\S-1.5-18\Products\00005109F100904000000000F01FE Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Universion\Installer\UserData\S-1.5-18\Products\00005109F100904000000000F01FE C\Usage\SpellingAndGrammarFiles_1033 Value: 52bb0062 Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Universion\Installer\UserData\S-1.5-18\Products\00005109F100904000000000F01FE C\Usage\SpellingAndGrammarFiles_1033 Value: 52bb0063 Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Universion\Installer\UserData\S-1.5-18\Products\00005109F100904000000000F01FE C\Usage\SpellingAndGrammarFiles_1033 Value: 52bb0063 Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Universion\Installer\UserData\S-1.5-18\Products\00005109F1009040000000000F01FE C\Usage\SpellingAndGrammarFiles_1033 Value: 52bb0064 Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Universion\Installer\UserData\S-1.5-18\Products\00005109F100904000000000F01FE 1280 C\Usage\SpellingAndGrammarFiles_1033 Value: 52bb0064 Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Universion\Installer\UserData\S-1.5-18\Products\00005109F100904000000000F01FE 1280 C\Usage\SpellingAndGrammarFiles_1033 Value: 52bb0065 Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Universion\Installer\UserData\S-1.5-18\Products\00005109F100904000000000F01FE 1280 C\Usage\SpellingAndGrammarFiles_1033 Value: 52bb0065 API Name: DeleteFileW Args: (%WorkingDir%\-\$ote 2405987021.docx) Return: 1	3F100C04000000000F01F 1280
CUsage\SpellingAndGrammarFiles_1033 Value: 52bb0061 Write Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Licensing\09D07EFC505F4D9CBFD5ACE3217F6654 Value: None 1280 Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109F1009040000000000F01FE C\Usage\SpellingAndGrammarFiles_1033 Value: 52bb0062 Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109F1009040000000000F01FE C\Usage\SpellingAndGrammarFiles_1033 Value: 52bb0063 Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109F1009040000000000F01FE C\Usage\SpellingAndGrammarFiles_1033 Value: 52bb0064 Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109F1009040000000000F01FE 1280 Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109F10090400000000000F01FE 1280 Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109F1009040000000000F01FE 1280 C\Usage\SpellingAnd\GrammarFiles_1033 Value: 52bb0065 Write Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Undows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109F1009040000000000F01FE API Name: DeleteFileW Args: (%WorkingDir\%\-\$ote 2405987021.docx) Return: 1	F1009040000000000001FE 1280
Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F1009040000000000F01FE CUsage\SpellingAndGrammarFiles_1033 Value: 52bb0062 Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100904000000000F01FE CUsage\SpellingAndGrammarFiles_1033 Value: 52bb0063 Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F1009040000000000F01FE CUsage\SpellingAndGrammarFiles_1033 Value: 52bb0064 Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F1009040000000000F01FE 1280 Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F1009040000000000F01FE 1280 CUsage\SpellingAndGrammarFiles_1033 Value: 52bb0065 Write Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\000fce\15.0\Common\Toolbars\Settings\Microsoft\Word Value: None 1280 Call Filesystem API API Name: DeleteFileW Args: (%WorkingDir\%\-\$ote 2405987021.docx) Return: 1	3F10090400000000000F01FE 1280
CUsage\SpellingAndGrammarFiles_1033 Value: 52bb0062 Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109F100904000000000F01FE CUsage\SpellingAndGrammarFiles_1033 Value: 52bb0063 Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109F1009040000000000F01FE CUsage\SpellingAndGrammarFiles_1033 Value: 52bb0064 Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109F1009040000000000F01FE CUsage\SpellingAndGrammarFiles_1033 Value: 52bb0065 Write Registry Key Key: HKEY_CORRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Toolbars\Settings\Microsoft\Word Value: None 1280 Call Filesystem API API Name: DeleteFileW Args: (%WorkingDir%\-\\$ote 2405987021.docx) Return: 1	54 Value: None 1280
CUsage\SpellingAndGrammarFiles_1033 Value: 52bb0063 Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109F1009040000000000F01FE CUsage\SpellingAndGrammarFiles_1033 Value: 52bb0064 Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\00005109F1009040000000000F01FE 1280 Cusage\SpellingAndGrammarFiles_1033 Value: 52bb0065 Write Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Toolbars\Settings\Microsoft\Word Value: None 1280 Call Filesystem API API Name: DeleteFile\Wargs: (\%Working\Dir\%\-\\$ote 2405987021.docx) Return: 1	3F1009040000000000F01FE 1280
CÜJSage\SpellingAndGrammarFiles_1033 Value: 52bb0064 Write Registry Key Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00005109F100904000000000F01FE CÜJSage\SpellingAndGrammarFiles_1033 Value: 52bb0065 Write Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Toolbars\Settings\Microsoft Word Value: None 1280 Call Filesystem API API Name: DeleteFileW Args: (%WorkingDir%\-\$ote 2405987021.docx) Return: 1	3F1009040000000000F01FE 1280
CÜJSage\SpellingAndGrammarFiles_1033 Value: 52bb0065 Write Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Toolbars\Settings\Microsoft Word Value: None 1280 Call Filesystem API API Name: DeleteFileW Args: (%WorkingDir%\-\$ote 2405987021.docx) Return: 1 1280	3F1009040000000000F01FE 1280
Call Filesystem API API Name: DeleteFileW Args: (%WorkingDir%\-\$ote 2405987021.docx) Return: 1 1280	3F1009040000000000F01FE 1280
	1280
Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Windows\NetCache\Content\Word\~WRS(F270CA65-BCCD-49D7-8207-R10AF65C41D2)\tm 1280	1280
p) Return: 1	JD7-8207-B10AF65C41D2).lm 1280
Write Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Data\Settings Value: None 1280	1280
Write Registry Key Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\Options\VisiFlm Value: 0 1280	
Call Filesystem API API Name: DeleteFileW Args: (%APPDATA%Microsoft/Templates\~SNormal.dotm) Return: 1 1280	
Call Filesystem API API Name: DeleteFileW Args: (%LOCALAPPDATA%Microsoft;Windows\NetCache\Content.Word\~WRS(6F1EE5B2-D71A-4F3D-B601-F587764D2686).tm p) Return: 1	·
Delete File Path: %APPDATA%Microsoft\Templates\-\\$Normal.dotm Type: VSDT_COM_DOS 1280	
Call System API API Name: WinHttpCloseHandle Args: (c57a208) Return: 1 1280 Call System API API Name: WinHttpCloseHandle Args: (c4f0778) Return: 1 1280	
Call System API API Name: WinHttpCloseHandle Args: (c4f9778) Return: 1 1280	
Call Thread API API Name: NtResumeThread Args: (Process:944,) Return: ? 1280 Call System API API Name: evtchann.SendEvent Args: (e), pid[944], ppid[1280) Return: 1 1280	
Call Process API API Name: CreateProcessW Args: (%CommonProgramFiles(x86)%Microsoft Shared(Office15/msosqm.exe, Process:944:msosqm.exe) Return: 1 1280	
Detection Threat Characteristic: Creates process Process ID: 944	1200
Image Path: %CommonProgramFiles(x86)%Microsoft Shared\Office15\msosqm.exe	
Call Mutex API API Name: CreateMutex A Args: (0, 0, LocalMsoSqmExeMutex) Return: 238 1280 944	1280 944

Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000		1280
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000		1280
Add File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\msosqmcached.dat Type: VSDT_COM_DOS	1280	944
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\msosqmcached.dat Type: VSDT_COM_DOS	1280	944
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\QMSessionCount Value: 2	1280	944
Write Registry Key	Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\000051191100000000000000000000000000000		1280
Call Filesystem API	API Name: DeleteFileW Args: (%LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.laccdb) Return: 1		1280
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.accdb Type: VSDT_MDB		1280
Write File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.laccdb Type: VSDT_COM_DOS		1280
Delete File	Path: %LOCALAPPDATA%\Microsoft\Office\15.0\OfficeFileCache\CentralTable.laccdb Type: VSDT_COM_DOS		1280
Delete File	Path: %TEMP%IJETF46A.tmp Type: VSDT_EMPTY		1280
Detection	Threat Characteristic: Deletes file to compromise the system or to remove traces of the infection Process ID: 1280 File: %TEMP%JETF46A.tmp Type: VSDT_EMPTY		
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTF Value: 7b6		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTA Value: 7b6		1280
Delete Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Word\MTTT Value: None		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Common\Feedback\AppUsageData_1 Value: None		1280
Write Registry Key	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\UID Value: None		1280
Write Registry Key	Key: HKEY CURRENT USER\SOFTWARE\Microsoft\Office\Common\UserName Value: Administrator		1280

▼ Screenshot





CentOS w Docker Environment-specific risk level High risk The object exhibited highly suspicious characteristics that are commonly associated with malware. Detections TROJ_FRS.VSNW19E21 Exploited vulnerabilities -

File name	Quote 2405987021.docx
File type	Office Word 2007 document
SHA-1	F1A0ABB5F96C21F8A799E4F65C4216BD968C29B7
SHA-256	5274C7FEA16B84E327D5AF683B6EF0C3E1FE1649B6CEA88399E029ED5DEEEE 6F
MD5	992ACD038FD49F200BD5510C029E74B1
Size	10356 byte(s)

Risk Level	High risk
Detection	TROJ_FRS.VSNW19E21
Exploited vulnerabilities	-
Threat Characteristics	Malformed, defective, or with known malware traits (1)

▼ Notable Threat Characteristics

▼ Malformed, defective, or with known malware traits (1)

Characteristic	Significance	Details
Detected as known malware		Source: ATSE Detection Name: TROJ_FRS.VSNW19E21 Engine Version: 12.500.1008 Malware Pattern Version: 16.743.92

▼ Suspicious Objects

Туре	Object	Risk Level
File (SHA1)	F1A0ABB5F96C21F8A799E4F65C4216BD968C29B7	High

▼ Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Detected as known malware Source: ATSE Detection Name: TROJ_FRS_VSNW19E21 Engine Version: 12.500.1008 Malware Pattern Version: 16.743.92		

Process Graph Legend

