ANY.RUN
INTERACTIVE MALWARE ANALYSIS

General Info

File name:	3a787a7b850b92a99d20f52747f1e13428039a149b7dd6295f6ca11995d88e0a.zip
Full analysis:	https://app.any.run/tasks/f38b139d-a33a-4e6c-b1eb-7ea1023eaf05
Verdict:	Malicious activity
Analysis date:	June 17, 2026 at 10:27:34
OS:	Windows 10 Professional (build: 19044, 64 bit)
Tags:	auto generic
Indicators:	
MIME:	application/zip
File info:	Zip archive data, at least v5.1 to extract, compression method=AES Encrypted
MD5:	B3BC758A103FDF072AF617068249DA0D
SHA1:	76A3CEC6D8FE425DA95FF4024F7FFB5F646B51C1
SHA256:	2410608D238851AB44FA66430DFF3AD6A46400C0F72059C9322E315E162BF1DE
SSDEEP:	49152:GKztcCNtqdRTEAaps7LnUJc7jwjAz73PlNobT4jWF15dzO6E6CCCBT8EV2ZyoYQp:GKuMtel2G8jwsHHobT95U6E6CCCtz2Zz

Software environment set and analysis options

Launch configuration

Task duration:	60 seconds	Heavy Evasion option:	off	Network geolocation:	off
Additional time used:	none	MITM proxy:	off	Privacy:	Public submission
Fakenet option:	off	Route via Tor:	off	Autoconfirmation of UAC:	on
Network:	on				

Software preset

- Internet Explorer 11.3636.19041.0
- Adobe Acrobat (64-bit) (23.001.20093)
- Adobe Flash Player 32 NPAPI (32.0.0.465)
- Adobe Flash Player 32 PPAPI (32.0.0.465)

Hotfixes

- Client LanguagePack Package
- DotNetRollup
- DotNetRollup 481
- FodMetadata Package

- CCleaner (6.20)
- Google Chrome (133.0.6943.127)
- Google Update Helper (1.3.36.51)
- Java 8 Update 271 (64-bit) (8.0.2710.9)
- Java Auto Updater (2.8.271.9)
- Java(TM) SE Development Kit 25.0.2 (64-bit) (25.0.2.0)
- Microsoft Edge (133.0.3065.92)
- Microsoft Office Professional 2019 - de-de (16.0.16026.20146)
- Microsoft Office Professional 2019 - en-us (16.0.16026.20146)
- Microsoft Office Professional 2019 - es-es (16.0.16026.20146)
- Microsoft Office Professional 2019 - it-it (16.0.16026.20146)
- Microsoft Office Professional 2019 - ja-jp (16.0.16026.20146)
- Microsoft Office Professional 2019 - ko-kr (16.0.16026.20146)
- Microsoft Office Professional 2019 - pt-br (16.0.16026.20146)
- Microsoft Office Professional 2019 - tr-tr (16.0.16026.20146)
- Microsoft Office Professionnel 2019 - fr-fr (16.0.16026.20146)
- Microsoft Office профессиональный 2019 - ru-ru (16.0.16026.20146)
- Microsoft OneNote - en-us (16.0.16026.20146)
- Microsoft Update Health Tools (3.74.0.0)
- Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.30501 (12.0.30501.0)
- Microsoft Visual C++ 2013 x64 Additional Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2013 x64 Minimum Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2015-2022 Redistributable (x64) - 14.36.32532 (14.36.32532.0)
- Microsoft Visual C++ 2015-2022 Redistributable (x86) - 14.36.32532 (14.36.32532.0)
- Microsoft Visual C++ 2022 X64 Additional Runtime - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X64 Minimum Runtime - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X86 Additional Runtime - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X86 Minimum Runtime - 14.36.32532 (14.36.32532)
- Mozilla Firefox (x64 en-US) (136.0)
- Mozilla Maintenance Service (136.0)
- Notepad++ (64-bit x64) (7.9.1)
- Office 16 Click-to-Run Extensibility Component (16.0.15726.20202)
- Office 16 Click-to-Run Licensing Component (16.0.16026.20146)
- Office 16 Click-to-Run Localization Component (16.0.15726.20202)
- Office 16 Click-to-Run Localization Component (16.0.15928.20198)
- Foundation Package
- Hello Face Package
- InternetExplorer Optional Package
- KB5003791
- KB5011048
- KB5015684
- KB5033052
- LanguageFeatures Basic en us Package
- LanguageFeatures Handwriting en us Package
- LanguageFeatures OCR en us Package
- LanguageFeatures Speech en us Package
- LanguageFeatures TextToSpeech en us Package
- MSPaint FoD Package
- MediaPlayer Package
- Microsoft OneCore ApplicationModel Sync Desktop FOD Package
- Microsoft OneCore DirectX Database FOD Package
- NetFx3 OnDemand Package
- Notepad FoD Package
- OpenSSH Client Package
- PowerShell ISE FOD Package
- Printing PMCPPC FoD Package
- Printing WFS FoD Package
- ProfessionalEdition
- QuickAssist Package
- RollupFix
- ServicingStack
- ServicingStack 3989
- StepsRecorder Package
- TabletPCMath Package
- UserExperience Desktop Package
- WordPad FoD Package

- PowerShell 7-x64 (7.3.5.0)
- Update for Windows 10 for x64-based Systems (KB4023057) (2.59.0.0)
- Update for Windows 10 for x64-based Systems (KB4023057) (2.63.0.0)
- Update for Windows 10 for x64-based Systems (KB4480730) (2.55.0.0)
- Update for Windows 10 for x64-based Systems (KB5001716) (8.93.0.0)
- VLC media player (3.0.11)
- WinRAR 5.91 (64-bit) (5.91.0)
- Windows PC Health Check (3.6.2204.08001)

Behavior activities

MALICIOUS

GENERIC has been found (auto)
- WinRAR.exe (PID: 3376)

SUSPICIOUS

Office application creates ActiveX control cache
- WINWORD.EXE (PID: 1328)

INFO

Reads Microsoft Office registry keys
- WinRAR.exe (PID: 3376)

Reads security settings of Internet Explorer
- WinRAR.exe (PID: 3376)

Malware configuration

No Malware configuration.

Static information

TRiD

.zip | ZIP compressed archive (100)

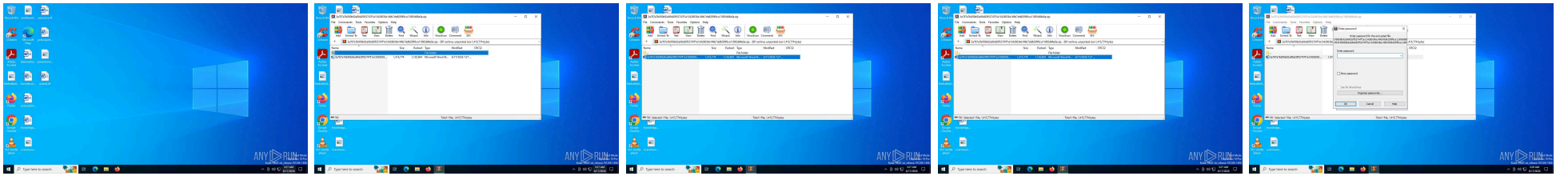
EXIF

ZIP

ZipRequiredVersion:	51
ZipBitFlag:	0x0003
ZipCompression:	Unknown (99)
ZipModifyDate:	2026:06:17 07:27:04

ZipCRC:	0xfe4d1eb8
ZipCompressedSize:	1130864
ZipUncompressedSize:	1415774
ZipFileName:	3a787a7b850b92a99d20f52747f1e13428039a149b7dd6295 f6ca11995d88e0a.docm

Video and screenshots



Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
154	3	1	0

Behavior graph

Specs description

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

Process information

PID	CMD	Path	Indicators	Parent process
1328	"C:\Program Files\Microsoft Office\Root\Office16\WINWORD.EXE" /n "C:\Users\admin\AppData\Local\Temp\Rar$DIb3376.41634\3a787a7b850b92a99d20f52747f1e13428039a149b7dd6295f6ca11995d88e0a.docm" /o ""	C:\Program Files\Microsoft Office\root\Office16\WINWORD.EXE		WinRAR.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Microsoft Word
Version:	16.0.16026.20146		

3376	"C:\Program Files\WinRAR\WinRAR.exe" C:\Users\admin\AppData\Local\Temp\3a787a7b850b92a99d20f52747f1e13428039a149b7dd6295f6ca11995d88e0a.zip	C:\Program Files\WinRAR\WinRAR.exe	☣	explorer.exe

Information

User:	admin	**Company:**	Alexander Roshal
Integrity Level:	MEDIUM	**Description:**	WinRAR archiver
Version:	5.91.0		

7468	"C:\Program Files\Microsoft Office\root\VFS\ProgramFilesCommonX64\Microsoft Shared\OFFICE16\ai.exe" "D0AF2ABD-B46E-4291-B129-5361F1034051" "82E1FD7A-A6BC-4067-8584-25A7DF36252C" "1328"	C:\Program Files\Microsoft Office\root\VFS\ProgramFilesCommonX64\Microsoft Shared\OFFICE16\ai.exe	–	WINWORD.EXE

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Artificial Intelligence (AI) Host for the Microsoft® Windows® Operating System and Platform x64.
Version:	0.12.2.0		

Registry activity

Total events	Read events	Write events	Delete events
15 943	15 673	248	22

Modification events

(PID) Process:	(3376) WinRAR.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\WinRAR\ArcHistory
Operation:	write	**Name:**	3
Value:	C:\Users\admin\Desktop\chromium_ext.zip		

(PID) Process:	(3376) WinRAR.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\WinRAR\ArcHistory

Operation: write **Name:** 2
Value: C:\Users\admin\Desktop\omni_23_10_2024_.zip

(PID) Process: (3376) WinRAR.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\WinRAR\ArcHistory
Operation: write **Name:** 1
Value: C:\Users\admin\Downloads\chromium_build 1.zip

(PID) Process: (3376) WinRAR.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\WinRAR\ArcHistory
Operation: write **Name:** 0
Value: C:\Users\admin\AppData\Local\Temp\3a787a7b850b92a99d20f52747f1e13428039a149b7dd6295f6ca11995d88e0a.zip

(PID) Process: (3376) WinRAR.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\WinRAR\FileList\FileColumnWidths
Operation: write **Name:** name
Value: 120

(PID) Process: (3376) WinRAR.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\WinRAR\FileList\FileColumnWidths
Operation: write **Name:** size
Value: 80

(PID) Process: (3376) WinRAR.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\WinRAR\FileList\FileColumnWidths
Operation: write **Name:** type
Value: 120

(PID) Process: (3376) WinRAR.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\WinRAR\FileList\FileColumnWidths
Operation: write **Name:** mtime
Value: 100

(PID) Process: (3376) WinRAR.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3d\52C64B7E
Operation: write **Name:** @C:\Program Files\Microsoft Office\Root\VFS\ProgramFilesCommonX64\Microsoft Shared\Office16\oregres.dll,-124
Value: Microsoft Word Macro-Enabled Document

(PID) Process: (3376) WinRAR.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\WinRAR\Interface
Operation: write **Name:** ShowPassword
Value: 0

(PID) Process: (3376) WinRAR.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\MuiCache\3d\52C64B7E
Operation: write **Name:** @C:\Program Files\Microsoft Office\root\VFS\ProgramFilesCommonX64\Microsoft Shared\Office16\oregres.dll,-205
Value: Word

(PID) Process:	(3376) WinRAR.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.docm\OpenWithProgids
Operation:	write	**Name:**	Word.DocumentMacroEnabled.12
Value:			

(PID) Process:	(3376) WinRAR.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached
Operation:	write	**Name:**	{5985FC23-2588-4D9A-B38B-7E7AFFAB3155} {886D8EEB-8CF2-4446-8D02-CDBA1DBDCF99} 0xFFFF
Value:	01000000000000001C7974D62AFEDC01		

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\CrashPersistence\WINWORD\1328
Operation:	write	**Name:**	0
Value:	0B0E10ABC962D8A64DD34FB3AE4AC07704CB1B2300469FC784B8ADC5BFEE016A04102400449A7D64B29D01008500A907556E6B6E6F776EC906022222CA0DC2190000C91003783634C51 1B00AD2120B770069006E0077006F00720064002E00650078006500C51620C517808004C91808323231322D44656300		

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages
Operation:	write	**Name:**	en-US
Value:	2		

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages
Operation:	write	**Name:**	de-de
Value:	2		

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages
Operation:	write	**Name:**	fr-fr
Value:	2		

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages
Operation:	write	**Name:**	es-es
Value:	2		

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages
Operation:	write	**Name:**	it-it
Value:	2		

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages
Operation:	write	**Name:**	ja-jp
Value:	2		

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages
Operation:	write	**Name:**	ko-kr

Value: 2

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages
Operation: write **Name:** pt-br
Value: 2

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages
Operation: write **Name:** ru-ru
Value: 2

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages
Operation: write **Name:** tr-tr
Value: 2

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Word\Resiliency\StartupItems
Operation: write **Name:** jz#
Value: 6A7A2300300500000100000000000000544A08D72AFEDC0100000000

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\ClientTelemetry\Sampling
Operation: write **Name:** 0
Value: 017012000000001000B24E9A3E020000000000000006000000000000000

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages
Operation: write **Name:** en-US
Value: 1

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages
Operation: write **Name:** de-de
Value: 1

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages
Operation: write **Name:** es-es
Value: 1

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages
Operation: write **Name:** fr-fr
Value: 1

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages

Operation: write **Name:** it-it
Value: 1

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages
Operation: write **Name:** ja-jp
Value: 1

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages
Operation: write **Name:** ko-kr
Value: 1

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages
Operation: write **Name:** pt-br
Value: 1

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages
Operation: write **Name:** ru-ru
Value: 1

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages
Operation: write **Name:** tr-tr
Value: 1

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common
Operation: write **Name:** SessionId
Value: FA83A737DC63864A95C7768AE8484A4F

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\GracefulExit\WINWORD\2200
Operation: delete value **Name:** 0
Value: ฃ鴛毅□娴ι□꿝◆褞◆□닜□椿c$驄摽鶲▨逮湫瞥쥮Ê₹◌ᢐ¢ᔓ衾▨笞袬예뎃좧□캖ǫ□砌佢ㄴ ᪠ᓚ看椀济明藛嫻搀ᑫ攀砀攀笞ı৲◌ᢣ串종甭㈱㈱膊捥

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\GracefulExit\WINWORD\2200
Operation: delete key **Name:** (default)
Value:

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\CrashPersistence\WINWORD\1328
Operation: write **Name:** 0

Value: 0B0E10ABC962D8A64DD34FB3AE4AC07704CB1B2300469FC784B8ADC5BFEE016A04102400449A7D64B29D01008500A907556E6B6E6F776EC906022222CA0DC2190000C50E8908C91003783634C511B00AD2120B770069006E0077006F00720064002E00650078006500C51620C517808004C91808323231322D44656300

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Word\Resiliency\StartupItems
Operation: write **Name:** 2{#
Value: 327B2300300500000400000000000000A45B3AD72AFEDC018C0000000100000084000000 3E0043003A005C00550073006500720073005C00610064006D0069006E005C0041007000700440061007400610 05C0052006F0061006D0069006E0067005C004D00690063007200 6F0073006F00660074005C00540065006D0070006C00610074006500730 05C004E006F0072006D00610 06C002E0064006F0074006D00000000000000

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Word\Resiliency\StartupItems
Operation: delete value **Name:** 2{#
Value: 笄#□

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\CrashPersistence\WINWORD\1328
Operation: write **Name:** 0
Value: 0B0E10ABC962D8A64DD34FB3AE4AC07704CB1B2300469FC784B8ADC5BFEE016A04102400449A7D64B29D01008500A907556E6B6E6F776EC906022222CA0DA201C2190000C50E8908C91003783634C511B00AD2120B770069006E0077006F00720064002E00650078006500C51620C517808004C91808323231322D44656300

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Word\Resiliency\StartupItems
Operation: write **Name:** ?|#
Value: 3F7C2300300500000200000000000000C7D04FD72AFEDC01A000000001000000740000002000000063003A005C00700072006F006700720061006D00200066006900 6C00650073005C006D006900630072006F0073006F006600740020006F006600660069006300650 05C0072006F006F0074005C006F006600660069006300650 0310036005C00670065006E006B006F002E0064006C006C000000670065006E006B006F002E0063006F006E006E00650063007400310032000000

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Internet\WebServiceCache\AllUsers\officeclient.microsoft.com\config16--lcid=1033&syslcid=1033&uilcid=1033&build=16.0.16026&crev=3\0
Operation: write **Name:** FilePath
Value: officeclient.microsoft.com\A0DA7B77-86BD-4172-863F-597C3193FD11

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Internet\WebServiceCache\AllUsers\officeclient.microsoft.com\config16--lcid=1033&syslcid=1033&uilcid=1033&build=16.0.16026&crev=3\0
Operation: write **Name:** StartDate
Value: 30E556D72AFEDC01

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Internet\WebServiceCache\AllUsers\officeclient.microsoft.com\config16--lcid=1033&syslcid=1033&uilcid=1033&build=16.0.16026&crev=3\0
Operation: write **Name:** EndDate
Value: 30A5C001F4FEDC01

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Word\AddinsData\Genko.Connect12
Operation: write **Name:** LoadCount

Value: 5

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Word\AddInLoadTimes
Operation: write **Name:** Genko.Connect12
Value: 040000007D0000002F0000003F0000001000000000000000

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Word\Resiliency\StartupItems
Operation: delete value **Name:** ?|#
Value: 簿#□

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\CrashPersistence\WINWORD\1328
Operation: write **Name:** 0
Value: 0B0E10ABC962D8A64DD34FB3AE4AC07704CB1B2300469FC784B8ADC5BFEE016A04102400449A7D64B29D01008500A907556E6B6E6F776EC906022222CA0DA200C2190000C50E8908C91003783634C511B00AD2120B770069006E0077006F00720064002E00650078006500C51620C517808004C91808323231322D44656300

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\CrashPersistence\WINWORD\1328
Operation: write **Name:** 0
Value: 0B0E10ABC962D8A64DD34FB3AE4AC07704CB1B2300469FC784B8ADC5BFEE016A04102400449A7D64B29D01008500A907556E6B6E6F776EC906022222CA0D2201A200C2190000C50E8908C91003783634C511B00AD2120B770069006E0077006F00720064002E00650078006500C51620C517808004C91808323231322D44656300

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Word\Resiliency\StartupItems
Operation: write **Name:** {|#
Value: 7B7C23003005000006000000010000000FD6C6CD72AFEDC01040100000200000F400000004000000630003A005C007500730065007200730005C00610064006D0069006E005C006100700070064006100740061005C006C006F00630061006C005C00740065006D0070005C007200610072002400640069006200330033003700360002E00340031003600330034005C003300610037003800370061003700620038003500300062003900320061003900390064003200300066003500320037003400370066003100650031003300340032003800300033003900610031003400390062003700640064003600320039003500660036006300610031003100390039003500640038003800650030006100 2E0064006F0063006D00000000000000

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Roaming
Operation: write **Name:** RoamingConfigurableSettings
Value: DC000000000000000803A09004106010001000100000000000000000000000000000000000000000000000201C0000201C000080510100805101008051010080510100805101008051010080F4030080F4030080F403002C010000840300008051010000000000840300008051010000A0000001E0000001E000000000000000000000000805101000100000001000000000000000000000000000000000000000000008D2700008D2700008D2700010000000A000000805101000000300000000300000003000000000000840300008051010010E000000840300008051010005000000050000000050000000

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Roaming
Operation: write **Name:** RoamingConfigurableSettings
Value: DC000000000000000803A0900EA0706000300110007001C000700120100000000000000000000000000201C0000201C000080510100805101008051010080510100805101008051010080F4030080F4030080F403002C010000840300008051010000000000840300008051010000A0000001E0000001E000000000000000000000000805101000100000001000000000000000000000000000000000000000000008D2700008D2700008D2700010000000A000000805101000000300000000300000003000000000000840300008051010010E000000840300008051010005000000050000000050000000

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs
Operation: write **Name:** CountryCode

Value: std::wstring|GB

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word
Operation: write **Name:** Expires
Value: int64_t|0

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word
Operation: delete value **Name:** ConfigIds

Value: P-D-29635-1-1,P-D-27087-1-9,P-D-29719-1-1,P-D-29718-1-1,P-D-29593-1-1,P-X-46178-1-3,P-X-45046-7-9,P-E-38713-2-4,P-E-38485-C1-6,P-E-38231-C1-4,P-R-45365-2-4,P-R-41741-18-10,P-R-38306-C17-3,P-R-35717-4-26,P-R-34019-4-3,P-D-37560-2-4,extes787:4008,exnop721cf:3280,P-E-29662-2-3,P-R-46411-1-3,P-R-46410-1-3,P-R-46111-1-4,P-R-45967-1-2,P-R-45966-1-2,P-R-45965-1-2,P-R-45964-1-5,P-R-45117-4-3,P-R-44092-2-3,P-R-44090-2-3,P-R-42512-1-2,P-R-42555-2-2,P-R-42557-2-3,P-R-42418-2-3,P-R-42417-2-2,P-R-40543-18-13,P-R-40169-8-9,P-R-39747-2-3,P-R-39746-2-3,P-R-39588-2-4,P-R-39582-2-5,P-R-39574-1-3,P-R-39568-1-3,P-R-39554-1-3,P-R-39522-1-4,P-R-39521-1-3,P-R-39467-2-4,P-R-39120-18-25,P-R-38704-4-6,P-R-37389-18-16,P-R-32143-5-17,P-R-36664-4-3,P-R-36385-18-10,P-R-35973-2-3,P-R-35946-6-3,P-R-35846-8-3,P-R-35476-2-3,P-R-35407-4-3,P-R-35234-14-6,P-R-35150-2-3,P-R-35129-2-3,P-R-35101-14-3,P-R-35056-4-3,P-R-35049-4-5,P-R-34904-2-3,P-R-34889-8-3,P-R-34044-2-3,P-R-33911-4-4,P-R-33824-1-4,P-R-33786-18-5,P-R-33718-6-4,P-R-33678-2-4,P-R-33459-1-4,P-R-33197-4-7,P-R-33176-4-17,P-R-33137-1-3,P-R-33136-2-6,P-R-32252-C39-56,P-R-32240-1-7,P-R-31921-C19-59,P-R-30649-1-5,P-R-30509-18-10,P-R-30293-4-7,P-R-29310-2-5,P-R-29301-4-10,P-R-29230-2-8,P-R-29224-5-11,P-R-29207-3-7,P-R-29208-2-4,P-R-29304-2-5,P-R-29279-2-8,P-R-29204-2-5,P-R-29056-2-4,P-R-29054-2-5,P-R-29025-9-26,P-R-28999-3-9,P-R-29000-4-7,P-R-28992-8-9,P-R-28988-8-11,P-R-28984-8-11,P-R-28644-1-4,P-R-25886-3-5,P-R-24037-1-6,P-R-23445-3-6,P-R-23410-1-5,P-R-23370-2-6,P-R-23485-1-6,P-R-23434-3-6,P-R-23403-3-6,P-R-20642-2-8,P-R-20640-1-7,P-R-19608-2-12,P-R-19841-2-8,P-R-18513-1-30,P-R-19024-9-58,P-D-34699-4-3,P-D-34697-2-3,P-D-34683-6-3,P-D-34675-1-3,P-D-34673-1-3,P-D-34654-1-3,P-D-34638-1-3,P-D-34609-1-3,P-D-34607-3-3,P-D-34587-3-3,P-D-34281-1-3,P-D-34278-4-3,P-D-34266-1-3,P-D-34263-1-3,P-D-34262-1-3,P-D-34260-1-3,P-D-34258-2-3,P-D-34250-1-3,P-D-34247-5-3,P-D-34225-1-3,P-D-32487-1-3,P-D-32471-3-3,P-D-32465-1-3,P-D-32459-2-3,P-D-32458-5-3,P-D-32403-1-3,P-D-30203-1-2,P-D-30202-1-3,P-D-30201-1-2,P-D-27615-1-3,P-D-27593-1-4,P-R-44990-1-4,P-R-43597-1-3,P-R-42114-18-8,P-R-42643-18-9,P-R-39888-1-3,P-R-39119-18-31,P-R-38346-2-3,P-R-37340-12-25,P-R-35848-14-14,P-R-33661-C17-6,P-R-33115-18-21,P-R-32298-18-11,P-R-25893-1-6,P-R-25867-1-5,P-R-25316-1-6,P-R-23348-1-7,P-X-45362-1-3,P-X-42197-2-3,P-E-44774-C1-6,P-E-29661-C1-3,P-R-46701-1-3,P-R-46309-1-4,P-R-46205-1-3,P-R-45832-1-4,P-R-45584-16-7,P-R-45452-2-3,P-R-45269-1-5,P-R-44738-16-3,P-R-44068-C15-4,P-R-44058-1-3,P-R-43957-C15-3,P-R-43718-16-4,P-R-42866-16-6,P-R-42865-16-8,P-R-42702-16-10,P-R-42794-2-2,P-R-42732-16-10,P-R-42547-16-12,P-R-42356-16-8,P-R-38028-C17-32,P-R-41047-16-19,P-R-41391-1-3,P-R-41370-18-10,P-R-40791-C15-7,P-R-37391-20-19,P-R-38531-16-16,P-R-39129-2-6,P-R-29934-6-17,P-R-36893-16-15,P-R-37769-16-19,P-R-38732-16-10,P-R-37487-16-14,P-R-37773-18-33,P-R-36381-16-14,P-R-36130-54-7,P-R-36102-8-3,P-R-35880-16-20,P-R-35006-4-3,P-R-34998-6-3,P-R-34958-2-3,P-R-34091-12-13,P-R-33918-1-5,P-R-33895-1-4,P-R-33883-2-4,P-R-33875-4-4,P-R-33738-2-11,P-R-32032-3-4,P-R-32026-12-7,P-R-31600-5-4,P-R-30442-20-52,P-R-27730-2-10,P-R-26653-1-4,P-R-26642-1-4,P-D-34604-1-3,P-D-32551-1-3,P-D-32550-1-3,P-D-32472-6-3,wotes819:3296,wotes907cf:1474,P-R-33555-1-4,P-R-46377-10-5,P-R-38462-1-11,P-R-30262-9-40,P-R-36932-2-11,P-R-46186-1-4,P-R-44014-1-6,P-R-43910-1-3,P-R-43909-1-3,P-R-43644-C5-10,P-R-42448-1-3,P-R-39912-1-2,P-R-39488-C3-7,P-R-39283-4-8,P-R-36539-10-4,P-R-24084-1-12,P-R-46100-20-5,P-R-45558-2-6,P-R-45546-1-5,P-R-37550-20-7,P-R-32186-C27-24,P-R-34049-2-3,P-D-41781-1-2,P-D-41780-1-2,P-D-40447-1-3,P-D-37672-1-2,P-D-36846-1-3,P-D-36843-1-4,P-R-39146-14-11,P-R-39147-14-9,P-R-28546-6-9,P-R-28165-6-25,P-R-24390-5-8,P-R-20518-9-39,P-R-19046-2-18,P-R-18975-1-29,P-R-18279-2-64,P-D-34200-4-4,P-R-39113-22-29,P-R-35209-8-3,P-D-34664-3-3,P-R-45538-1-4,P-R-45368-1-4,P-R-44875-6-5,P-R-43085-18-8,P-R-42578-1-3,P-R-42482-1-3,P-R-41670-18-10,P-R-40990-12-12,P-R-39594-18-13,P-R-39333-C17-20,P-R-39336-18-21,P-R-35387-18-13,P-R-37272-18-10,P-R-37469-8-9,P-R-36616-14-9,P-R-35972-2-3,P-R-35968-2-3,P-R-35572-2-3,P-R-33215-18-17,P-R-32653-18-18,P-R-31352-12-17,P-R-28751-2-19,P-R-20580-8-34,P-D-34495-2-9,P-D-34269-2-3,P-E-28677-2-3,P-R-44907-5-7,P-R-41912-1-2,P-R-41699-C15-18,P-R-38702-1-3,P-E-42700-C1-4,P-R-46706-2-2,P-R-46558-2-3,P-R-45837-1-4,P-R-40106-C17-13,P-R-45197-2-6,P-R-37650-1-5,P-R-43723-2-5,P-R-39825-22-28,P-R-42920-1-8,P-R-42797-2-4,P-R-42457-18-4,P-R-32234-25-67,P-R-41994-9-19,P-R-41742-C17-22,P-R-41640-7-20,P-R-41538-2-2,P-R-40648-2-7,P-R-39029-5-17,P-R-38835-18-39,P-R-36315-10-28,P-R-38026-1-5,P-R-37492-18-8,P-R-37467-18-42,P-R-36646-6-7,P-R-36624-10-5,P-R-36575-4-5,P-R-36478-2-3,P-R-36310-4-3,P-R-35945-10-3,P-R-35436-22-13,P-R-35417-16-7,P-R-35340-16-10,P-R-35143-4-3,P-R-35043-10-5,P-R-35008-18-4,P-R-34955-16-9,P-R-34817-8-7,P-R-34748-18-27,P-R-34331-4-8,P-R-34079-12-12,P-R-33996-18-20,P-R-33994-10-5,P-R-33597-12-8,P-R-33553-4-4,P-R-32261-1-4,P-R-32239-1-5,P-R-32236-1-8,P-R-31384-1-4,P-R-29809-1-6,P-R-28464-12-11,P-R-28276-1-4,P-R-27861-1-4,P-R-26968-3-8,P-R-46232-2-2,P-R-46170-2-2,P-R-41916-C17-14,P-R-40405-1-5,P-R-39876-18-22,P-R-38085-12-9,P-R-37017-18-23,P-R-37374-9-22,P-R-36450-18-17,P-R-35907-6-3,P-R-35850-10-4,P-R-35849-4-5,P-R-35389-18-34,P-R-33530-14-9,P-R-32169-3-4,P-R-30530-8-16,P-R-30067-18-7,P-R-18744-6-21,P-D-34659-8-3,P-D-34259-2-3,P-D-34257-9-3,P-D-34239-1-3,P-R-46080-2-3,P-R-38953-1-9,P-R-36551-18-14,P-R-31346-2-6,P-R-43355-C17-5,P-R-42383-18-8,P-R-40152-18-5,P-R-39981-18-7,P-R-39509-10-13,P-R-39328-18-8,P-R-39121-18-9,P-R-38296-18-11,P-R-38167-18-12,P-R-37675-8-25,P-R-37667-12-16,P-R-35869-18-9,P-R-35665-12-3,P-R-35337-16-5,P-R-35203-4-3,P-R-33916-1-4,P-R-33741-4-4,P-R-33739-1-4,P-R-33580-C7-7,P-R-33575-1-5,P-R-33560-4-4,P-R-32042-2-13,P-R-31966-3-10,P-R-31960-7-4,P-R-31949-4-4,P-R-31948-8-7,P-R-31946-3-4,P-R-20347-4-21,P-R-46404-2-2,P-R-40475-18-13,P-R-37668-C25-43,P-R-35891-18-3,P-R-32433-18-16,P-R-32004-2-4,P-R-38410-18-22,P-R-37609-18-12,P-R-20504-8-18,P-R-43232-1-15,P-R-42696-18-10,P-R-35680-8-4,P-R-32106-7-27,P-R-30085-1-8,P-R-30011-15-17,P-R-29138-38-73,P-R-29315-36-59,P-R-28033-14-54,P-R-25157-8-12,P-R-19898-1-20,P-R-19814-1-53,P-R-19262-2-12,P-R-35109-4-3,P-R-23378-2-6,P-R-45595-2-4,P-R-41433-18-25,P-R-40253-6-18,P-R-40254-6-17,P-R-35412-4-3,P-R-32107-22-21,P-R-32704-1-4,P-R-26006-3-5,P-R-34130-6-3,P-R-44921-2-2,P-R-40407-18-5,P-R-37603-3-6,P-R-36477-6-3,P-R-35887-18-9,P-R-35489-16-7,P-R-35454-16-5,P-R-35073-4-3,P-R-33746-2-6,P-R-40464-18-5,P-R-39227-18-8,P-R-37589-1-3,P-R-42510-1-3,P-R-41441-10-18,P-R-39073-1-5,P-R-38719-10-29,P-R-35442-2-6,P-R-28753-1-9,P-R-27070-1-4,P-R-26515-4-14,P-R-45019-1-4,P-R-32703-10-10,P-R-33970-10-7,P-R-33969-10-7,P-R-45554-1-3,P-R-44835-1-3,P-R-33737-1-4,P-R-35623-2-3,P-R-26442-1-7,P-R-23681-2-7,P-D-32502-2-3,P-D-32501-2-3,P-D-32415-2-3,P-R-46845-1-3,P-R-46844-1-3,P-R-46841-1-3,P-R-46580-3-5,P-R-46484-1-3,P-R-46233-1-3,P-R-46122-1-3,P-R-46121-3-5,P-R-46068-2-4,P-R-46067-2-4,P-R-46066-2-4,P-R-46065-2-4,P-R-46064-2-4,P-R-46062-2-4,P-R-46060-2-4,P-R-46059-2-4,P-R-46058-2-4,P-R-46056-2-4,P-R-46055-2-4,P-R-46054-2-4,P-R-46041-2-4,P-R-45865-2-6,P-R-45858-1-3,P-R-45241-1-3,P-R-44950-1-3,P-R-43966-1-3,P-R-43502-5-7,P-R-43238-3-5,P-R-43188-2-4,P-R-43094-8-10,P-R-42949-1-3,P-R-42635-1-3,P-R-42122-1-3,P-R-38248-7-11,P-R-41430-1-3,P-R-41033-2-4,P-R-40892-1-3,P-R-39375-2-6,P-R-40751-3-5,P-R-40273-3-5,P-R-39238-1-3,P-R-39045-1-3,P-R-38878-1-3,P-R-38682-2-4,P-R-37588-1-3,P-R-35713-2-4,P-R-35675-1-3,P-R-35606-3-5,P-R-35373-1-3,P-R-34355-4-6,P-R-23737-6-9,P-R-26211-3-9,P-R-26266-3-8,P-R-23733-14-19,P-R-26834-2-7,P-R-24662-12-18,P-R-27205-3-10,P-R-27299-2-7,P-R-27479-5-10,P-R-26056-5-13,P-R-27006-6-11,P-R-23722-17-22,P-R-32191-3-5,P-R-30338-1-5,P-R-30178-9-11,P-R-30053-2-4,P-R-27458-1-5,P-R-26722-6-8,P-R-25822-7-10,P-R-25653-1-4,P-R-25269-6-9,P-R-25083-5-8,P-R-24690-10-14,P-R-24689-1-4,P-R-24666-1-4,P-R-24663-3-8,P-R-24659-6-9,P-R-24658-3-6,P-R-23762-5-7,P-R-23747-6-8,P-R-23746-13-16,P-R-23744-6-8,P-R-23743-8-10,P-R-23741-7-9,P-R-23740-7-9,P-R-23739-6-8,P-R-23738-9-11,P-R-23736-11-13,P-R-23734-7-9,P-R-23732-7-9,P-R-23731-7-9,P-R-23730-15-18,P-R-23729-7-9,P-R-23728-7-9,P-R-23725-6-8,P-R-23723-6-8,P-R-23718-6-8,P-R-23717-7-9,P-R-23715-7-9,P-R-23714-8-10,P-R-23713-7-9,P-D-32589-1-3,P-

D-32588-1-3,P-D-32534-1-3,P-D-32524-1-3,P-D-32518-1-3,P-D-32512-1-3,P-D-32509-1-3,P-D-32504-1-3,P-D-32486-1-3,P-D-32485-1-3,P-D-32484-1-3,P-D-32405-1-3,P-R-29928-1-13,P-R-26544-7-57,P-R-40220-1-4,P-R-35099-2-3,P-E-29576-C1-7,P-E-29325-2-4,P-R-40586-18-25,P-R-40732-18-13,P-R-39143-18-20,P-D-40316-9-3,P-R-35513-4-3,P-R-33892-1-4,P-R-33696-1-4,P-R-33569-1-6,P-R-31987-1-4,P-R-33504-1-4,P-R-42379-2-2,P-R-42378-2-2

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word
Operation:	delete value	**Name:**	ETag
Value:			

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\AddinClassifier
Operation:	write	**Name:**	9a3e8255d7eb9a1a1f397175007c13fc
Value:	v2:1;0;1781681287		

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Roaming
Operation:	write	**Name:**	RoamingLastSyncTimeWord
Value:	EA07060003001100070001C000700A902		

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Roaming
Operation:	write	**Name:**	RoamingLastWriteTimeWord
Value:	EA07060003001100070001C000700A902		

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation:	write	**Name:**	ChunkCount
Value:	uint64_t|0		

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation:	write	**Name:**	ChunkCount
Value:	uint64_t|1		

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation:	write	**Name:**	ChunkCount
Value:	uint64_t|2		

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation:	write	**Name:**	ChunkCount
Value:	uint64_t|3		

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation:	write	**Name:**	ChunkCount
Value:	uint64_t|4		

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation:	write	**Name:**	ChunkCount
Value:	uint64_t|5		

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation:	write	**Name:**	ChunkCount
Value:	uint64_t|6		

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation:	write	**Name:**	ChunkCount
Value:	uint64_t|7		

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation:	write	**Name:**	ChunkCount
Value:	uint64_t|8		

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation:	write	**Name:**	ChunkCount
Value:	uint64_t|9		

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation:	write	**Name:**	ChunkCount
Value:	uint64_t|10		

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation:	write	**Name:**	ChunkCount
Value:	uint64_t|11		

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation:	write	**Name:**	ChunkCount
Value:	uint64_t|12		

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation:	write	**Name:**	ChunkCount
Value:	uint64_t|13		

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation:	write	**Name:**	ChunkCount

Value: uint64_t|14

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write **Name:** ChunkCount
Value: uint64_t|15

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write **Name:** ChunkCount
Value: uint64_t|16

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write **Name:** ChunkCount
Value: uint64_t|17

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write **Name:** ChunkCount
Value: uint64_t|18

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write **Name:** ChunkCount
Value: uint64_t|19

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write **Name:** ChunkCount
Value: uint64_t|20

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write **Name:** ChunkCount
Value: uint64_t|21

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write **Name:** ChunkCount
Value: uint64_t|22

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write **Name:** ChunkCount
Value: uint64_t|23

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData

Operation: write **Name:** ChunkCount
Value: uint64_t|24

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write **Name:** ChunkCount
Value: uint64_t|25

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write **Name:** ChunkCount
Value: uint64_t|26

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write **Name:** ChunkCount
Value: uint64_t|27

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write **Name:** ChunkCount
Value: uint64_t|28

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write **Name:** ChunkCount
Value: uint64_t|29

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write **Name:** ChunkCount
Value: uint64_t|30

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write **Name:** ChunkCount
Value: uint64_t|31

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write **Name:** ChunkCount
Value: uint64_t|32

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write **Name:** ChunkCount
Value: uint64_t|33

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation:	write	**Name:**	ChunkCount
Value:	uint64_t|34		

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation:	write	**Name:**	ChunkCount
Value:	uint64_t|35		

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation:	write	**Name:**	ChunkCount
Value:	uint64_t|36		

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation:	write	**Name:**	ChunkCount
Value:	uint64_t|37		

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation:	write	**Name:**	ChunkCount
Value:	uint64_t|38		

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation:	write	**Name:**	ChunkCount
Value:	uint64_t|39		

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation:	write	**Name:**	ChunkCount
Value:	uint64_t|40		

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation:	write	**Name:**	ChunkCount
Value:	uint64_t|41		

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation:	write	**Name:**	ChunkCount
Value:	uint64_t|42		

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation:	write	**Name:**	ChunkCount

Value: uint64_t|43

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write **Name:** ChunkCount
Value: uint64_t|44

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write **Name:** ChunkCount
Value: uint64_t|45

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write **Name:** ChunkCount
Value: uint64_t|46

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write **Name:** ChunkCount
Value: uint64_t|47

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write **Name:** ChunkCount
Value: uint64_t|48

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write **Name:** ChunkCount
Value: uint64_t|49

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write **Name:** ChunkCount
Value: uint64_t|50

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write **Name:** ChunkCount
Value: uint64_t|51

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write **Name:** ChunkCount
Value: uint64_t|52

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData

Operation: write **Name:** ChunkCount
Value: uint64_t|53

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write **Name:** ChunkCount
Value: uint64_t|54

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write **Name:** ChunkCount
Value: uint64_t|55

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write **Name:** ChunkCount
Value: uint64_t|56

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write **Name:** ChunkCount
Value: uint64_t|57

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write **Name:** ChunkCount
Value: uint64_t|58

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write **Name:** ChunkCount
Value: uint64_t|59

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write **Name:** ChunkCount
Value: uint64_t|60

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write **Name:** ChunkCount
Value: uint64_t|61

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write **Name:** ChunkCount
Value: uint64_t|62

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write **Name:** ChunkCount
Value: uint64_t|63

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write **Name:** ChunkCount
Value: uint64_t|64

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write **Name:** ChunkCount
Value: uint64_t|65

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write **Name:** ChunkCount
Value: uint64_t|66

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write **Name:** 1.67
Value:
6963726F736F66742E4F66666963652E54656C656D657472792E557365526567696F6E4177617265436F6E66696755726C73222C20225622203A2022626F6F6C7C3122207D205D2C2022464
347726F75704D61705F313422203A205B207B20224622203A20224D6963726F736F66742E4F66666963652E5543492E456E61626C65496E446F63756D656E74506172616D4C6F63616C5365
61726368222C20225622203A2022626F6F6C7C3122207D2C207B20224622203A20224D6963726F736F66742E4F66666963652E5543492E456E61626C65496E446F63756D656E74536561726
368222C20225622203A2022626F6F6C7C3122207D2C207B20224622203A20224D6963726F736F66742E4F66666963652E5543492E456E61626C65496E446F63756D656E7453656172636846
696E6450616E65222C20225622203A2022626F6F6C7C3122207D2C207B20224622203A20224D6963726F736F66742E4F66666963652E5543492E456E61626C65496E446F63756D656E74536
561726368526570 6C616365222C20225622203A2022626F6F6C7C3122207D2C207B20224622203A20224D6963726F736F66742E4F66666963652E5543492E456E61626C65496E446F63756D
656E74537469636B7946696C74657273222C20225622203A2022626F6F6C7C3122207D2C207B20224622203A20224D6963726F736F66742E4F66666963652E5543492E456E61626C654C6F6
3616C536561726368222C20225622203A2022626F6F6C7C3122207D2C207B20224622203A20224D6963726F736F66742E4F66666963652E5543492E456E61626C6553796E634C6F63616C53
6561726368222C20225622203A2022626F6F6C7C3122207D2C207B20224622203A20224D6963726F736F66742E4F66666963652E5543492E536861726564536572706C6574466561747572
547617465313522 2C20225622203A2022626F6F6C7C3122207D2C207B20224622203A20224D6963726F736F66742E4F66666963652E5543492E536861726564536572706C65744665617475
726547617465333022 2C20225622203A2022626F6F6C7C3122207D2C207B20224622203A20224D6963726F736F66742E4F66666963652E5543492E536861726564536572706C65744665617
475726547617465333122 2C20225622203A2022626F6F6C7C3122207D2C207B20224622203A20224D6963726F736F66742E4F66666963652E5543492E536861726564536572706C65744665
617475726547617465343022 2C20225622203A2022626F6F6C7C3122207D2C207B20224622203A20224D6963726F736F66742E4F66666963652E5543492E536861726564536572706C65744
665617475726547617465362222C20225622203A2022626F6F6C7C3122207D2C207B20224622203A20224D6963726F736F66742E4F66666963652E5543492E536861726564536572706C6574
466561747572654761746538222C20225622203A2022626F6F6C7C3122207D2C207B20224622203A20224D6963726F736F66742E4F66666963652E5543492E536861726564536572706C657
446656174757265476174653922 2C20225622203A2022626F6F6C7C3122207D2C207B20224622203A20224D6963726F736F66742E4F66666963652E5543492E54656C6C4D652E416E737765
72526573756C7451756572794C656E677468546872657 3686F6C64222C20225622203A2022696E7436345F747C3622207D2C207B20224622203A20224D6963726F736F66742E4F666669636
52E5543492E54656C6C4D652E48656C705465726D53756767657374696F6E73456E61626C6564222C20225622203A2022626F6F6C7C3122207D2C207B20224622203A20224D6963726F736
F66742E4F66666963652E5543492E54656C6C4D652E497347657448656C70526573756C74456E61626C6564222C20225622203A2022626F6F6C7C3122207D2C207B20224622203A20224D6
963726F736F66742E4F66666963652E5543492E54656C6C4D652E497348656C70416374696F6E526573756C7473456E61626C6564222C20225622203A2022626F6F6C7C3122207D2C207B20
224622203A20224D6963726F736F66742E4F66666963652E5543492E54656C6C4D652E497352656D6F76696E67446566696E6974696F6E456E61626C6564222C20225622203A2022626F6F6
C7C3122207D2C207B20224622203A20224D6963726F736F66742E4F66666963652E5543492E54656C6C4D652E4D756C74694C616E67756167654D6F64656C4E616D65222C20225622203A2
0227374643A3A77737472696E677C4D756C74694C616E67756167655F54656C6C4D6557696E33324368696C644D4C434D6F64656C576F726422207D2C207B20224622203A20224D6963726
F736F66742E4F66666963652E5543492E54656C6C4D652E4E756D6265724F664E6F746573537567676573746 96F6E73546F53686F77222C20225622203A2022696E7436345F747C3222207D
2C207B20224622203A20224D6963726F736F66742E4F66666963652E5543492E54656C6C4D652E4F6E6C696E65436F6D6D616E64526573756C7473456E61626C6564222C20225622203A20
22626F6F6C7C3122207D2C207B20224622203A20224D6963726F736F66742E4F66666963652E5543492E54656C6C4D652E4F70656E4F6E656E6F74654E6F746573496E576562222C2022562
2203A2022626F6F6C7C3122207D2C207B20224622203A20224D6963726F736F66742E4F66666963652E5543492E54656C6C4D652E54656C6C4D654E6F746573537567676573746 96F6E497
3456E61626C6564222C20225622203A2022626F6F6C7C3122207D205D2C2022464347726F75704D61705F313522203A205B207B20224622203A20224D6963726F736F66742E4F666669636
52E576F72642E4175676C6F6F702E436F70696C6F74436F6D706F73652E456E61626C6552617748746D6C45786368616E6765222C20225622203A2022626F6F6C7C3122207D2C207B202246
22203A20224D6963726F736F66742E4F66666963652E576F72642E43686F6F736546617374657257686564676579464765744361416E63686F72436F6D6D656E74436F7265222C2022

5622203A2022626F6F6C7C3122207D2C207B20224622203A20224D6963726F736F66742E4F66666963652E576F72642E436C65616E436F726554656C656D4D696E44697274446974222C2
0225622203A2022696E7436345F747C3622207D2C207B20224622203A20224D6963726F736F66742E4F66666963652E576F72642E436C65616E436F726554656C656D4D696E506167657322
2C20225622203A2022696E7436345F747C3622207D2C207B20224622203A20224D6963726F736F66742E4F66666963652E576F72642E43757272656E74417574686F725465616368696E674
3616C6C6F7574222C20225622203A2022626F6F6C7C3122207D2C207B20224622203A20224D6963726F736F66742E4F66666963652E576F72642E4661737465724647657443614164E63686F
72436F6D6D656E74436F7265222C20225622203A2022626F6F6C7C3122207D2C207B20224622203A20224D6963726F736F66742E4F66666963652E576F72642E4C61796F7574416E6444697
3706C61792E3637697A7746697865734E6F76656D6265723230323222C20225622203A2022626F6F6C7C3022207D2C207B20224622203A20224D6963726F736F66742E4F66666963652E57
6F72642E4C61796F7574416E64446973706C61792E46436F766572476F6E65446563656D6265723230323222C20225622203A2022626F6F6C7C3022207D2C207B20224622203A20224D696
3726F736F66742E4F66666963652E576F72642E4C61796F7574416E64446973706C61792E49706764446F6343704E6577496E5265706167546F43704E6F76656D6265723230322C2022562
2203A2022626F6F6C7C3022207D2C207B20224622203A20224D6963726F736F66742E4F66666963652E576F72642E4C61796F7574416E64446973706C61792E4E6577506167696E6174696F
6E496E7465726661636573496E46496E6974506A4E6F76656D6265723230323222C20225622203A2022626F6F6C7C3022207D2C207B20224622203A20224D6963726F736F66742E4F66666
963652E576F72642E4C61796F7574416E64446973706C61792E5065726D6974436C65616E436F72654E6F76656D6265723230323243686163E676573222C20225622203A2022626F6F6C7C31
22207D2C207B20224622203A20224D6963726F736F66742E4F66666963652E576F72642E4E756C6C436865636B506361646765744361416E63686F72436F6D6D656E74436F7265222C20225
622203A2022626F6F6C7C3022207D2C207B20224622203A20224D6963726F736F66742E4F66666963652E576F72642E547261636B4368616E6765436F6E7465787475616
686F72222C20225622203A2022626F6F6C7C3122207D2C207B20224622203A20224D6963726F736F66742E4F66666963652E576F72642E547261636B4368616E6765436F6E7465787475616
C4361726473222C20225622203A2022626F6F6C7C3122207D2C207B20224622203A20224D6963726F736F66742E4F66666963652E576F72642E557365436F6D6D656E7441504973466F7241
747264536861646548 6F7456617273222C20225622203A2022626F6F6C7C3022207D2C207B20224622203A20224D6963726F736F66742E4F66666963652E576F72642E557365436F6D6D656
E7441706973466F725374727563744C5352554E616E644F5346222C20225622203A2022626F6F6C7C3022207D2C207B20224622203A20224D6963726F736F66742E4F66666963652E576F72
642E566572696679466173746572464765744361416E63686F72436F6D6D656E74436F7265222C20225622203A2022626F6F6C7C3022207D2C207B20224622203A20224D6963726F736F667
42E4F66666963652E576F72642E666130303030303033392E4175676C6F6F702E436F70696C6F74436F6D706F73652E456E61626C6552617748746D6C45786368616E6765222C20225622
203A2022626F6F6C7C3122207D205D207D207D

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write **Name:** ChunkCount
Value: uint64_t|67

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write **Name:** VersionId
Value: uint16_t|1

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word
Operation: write **Name:** ETag
Value: std::wstring|"Qm6mWo++ovGVZ+csiPrU12NHz+PRsSEVNNE7g+aQNnQ="

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word
Operation: write **Name:** Expires
Value: int64_t|1781695687

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word
Operation: write **Name:** DeferredConfigs
Value: std::wstring|ofsh6c2b1tla1a31,ofcrui4yvdulbf31,ofhpex3jznepoo31,ofpioygfqmufst31,ofjhlwlmoc1pz531

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\CrashPersistence\WINWORD\1328
Operation: write **Name:** 0
Value: 0B0E10ABC962D8A64DD34FB3AE4AC07704CB1B2300469FC784B8ADC5BFEE016A04102400449A7D64B29D01008500A907556E6B6E6F776EC9062E22516D366D576F2B2B6F7647565A2B63
736950725531324E487A2B5052735345564E4E4537672B61514E6E513D22CA0D2201A200C2190000C50E8908C91003783634C511B00AD2120B770069006E0077006F00720064002E006500
78006500C51620C517808004C91808323231322D44656300

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\IOAV
Operation: write **Name:** LastBootTime
Value: 0000000000000000

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\19FA16
Operation: write **Name:** 19FA16
Value: 04000000300500007900000043003A005C00550073006500720073005C00610064006D0069006E005C0041007000700044006100740061005C004C006F00630061006C005C00540065006D0
070005C005200610072002400440049006200330033003700360002E0034003100360033003400 5C003300610037003800370061003700620038003500300062003900320061003900390064 0
032003000660035003200370034003700660031006500310033003400320038003000330039006100310034003900620037006400640036003200390035006600360063006100310031003100390
039003500640038003800650030006100 2E0064006F0063006D0045000000330061003700380037006100370062003800350030006200390032006100390039006400320030006600350032 0
037003400370066003100650031003300340032003800300033003900610031003400390062003700640064003600320039003500660036006300610031003100390039003500640038003800380
06500300061002E0064006F0063006D0000000000010000000000000074E8384CFEDC0116FA190016FA1900000000001F05000000000000000000000000000000000000000000000000
0FFFFFFF000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000FFFFFFFF00000000000
00000

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\VBA\Forms3\Controls
Operation: write **Name:** EnableActiveXControlArchitetureIndependent
Value: 0

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\VBA\Forms3\Controls
Operation: write **Name:** EnableActiveXControlMSWebBrowserArchiteturePersistenceIssue
Value: 0

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\CrashPersistence\WINWORD\1328
Operation: write **Name:** 0
Value: 0B0E10ABC962D8A64DD34FB3AE4AC07704CB1B2300469FC784B8ADC5BFEE016A04102400449A7D64B29D01008500A907556E6B6E6F776EC9062E22516D366D576F2B2B6F7647565A2B63
736950725531324E487A2B5052735345564E4E4537672B61514E6E513D22CA0D2201A200C20701C2190000C50E8908C91003783634C511B00AD2120B770069006E0077006F00720064002E
00650078006500C51620C517808004C91808323231322D44656300

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Word\Resiliency
Operation: write **Name:** PotentialDataLossInfo2

Value: 1800280001000000ABC962D8A64DD34FB3AE4AC07704CB1B31396FDE8F8AF744AE8E62D24CE61E4490E2BE1406020000737B74DE2AFEDC010200000000000000

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Word\Resiliency\StartupItems
Operation: delete value **Name:** jz#
Value: 稱#□

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\CrashPersistence\WINWORD\1328
Operation: write **Name:** 0
Value: 0B0E10ABC962D8A64DD34FB3AE4AC07704CB1B2300469FC784B8ADC5BFEE016A04102400449A7D64B29D01008500A907556E6B6E6F776EC9062E22516D366D576F2B2B6F7647565A2B63736950725531324E487A2B5052735345564E4E4537672B61514E6E513D22CA0D2201A201C20701C2190000C50E8908C91003783634C511B00AD2120B770069006E0077006F00720064002E00650078006500C51620C517808004C91808323231322D44656300

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Word\Resiliency\StartupItems
Operation: write **Name:** j+$
Value: 6A2B2400300500000200000000000000077DC95DE2AFEDC01B2000000010000007400000032000000063003A005C00700072006F006700720061006D002000660069006C00650073005C006D006900630072006F0073006F006600740020006F006600660069006900630065005C0072006F006F0074005C006F006600660069006300650031003600 5C00670065006E006B006F002E0064006C006C0000006D006900630072006F0073006F006600740020007700 7006F0072006400200 0D0C6E0ACC0C9200094CD00AC200030AEA5B20000

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Word\Resiliency\StartupItems
Operation: delete value **Name:** j+$
Value: ▯$▯

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\CrashPersistence\WINWORD\1328
Operation: write **Name:** 0
Value: 0B0E10ABC962D8A64DD34FB3AE4AC07704CB1B2300469FC784B8ADC5BFEE016A04102400449A7D64B29D01008500A907556E6B6E6F776EC9062E22516D366D576F2B2B6F7647565A2B63736950725531324E487A2B5052735345564E4E4537672B61514E6E513D22CA0D22014201A200C20701C2190000C50E8908C91003783634C511B00AD2120B770069006E0077006F00720064002E00650078006500C51620C517808004C91808323231322D44656300

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{BB00E856-A12F-4AB7-B2C8-4E80CAEA5B07}
Operation: delete key **Name:** (default)
Value:

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor\{DAF0B914-9C1C-450A-81B2-FEA7244F6FFA}
Operation: delete key **Name:** (default)
Value:

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ETWMonitor
Operation: delete key **Name:** (default)
Value:

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe\ULSMonitor
Operation:	delete key	**Name:**	(default)
Value:			

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ClientTelemetry\RulesMetadata\winword.exe
Operation:	delete key	**Name:**	(default)
Value:			

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\IOAV
Operation:	write	**Name:**	LastBootTime
Value:	EC45326A00000000		

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Word\Resiliency\StartupItems
Operation:	delete value	**Name:**	{|#
Value:	类#□		

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Word\Resiliency\StartupItems
Operation:	delete key	**Name:**	(default)
Value:			

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\CrashPersistence\WINWORD\1328
Operation:	write	**Name:**	0
Value:	0B0E10ABC962D8A64DD34FB3AE4AC07704CB1B2300469FC784B8ADC5BFEE016A04102400449A7D64B29D01008500A907556E6B6E6F776EC9062E22516D366D576F2B2B6F7647565A2B63736950725531324E487A2B5052735345564E4E4537672B61514E6E513D22CA0D020122014201A200C20701C2190000C50E8908C91003783634C511B00AD2120B770069006E0077006F00720064002E00650078006500C51620C517808004C91808323231322D44656300		

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Fonts
Operation:	write	**Name:**	CloudFontsVersion
Value:	4		

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\TargetedMessagingService\MessageMetadata\0_MsgId:BizBar
Operation:	delete key	**Name:**	(default)
Value:			

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\TargetedMessagingService\MessageMetadata\0_MsgId:BizBar
Operation:	write	**Name:**	AppIdOnAction
Value:			

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\TargetedMessagingService\MessageMetadata\0_MsgId:BizBar

Operation: write **Name:** CallDelta
Value: 86400

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\TargetedMessagingService\MessageMetadata\0_MsgId:BizBar
Operation: write **Name:** MaxWait
Value: 2000

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\TargetedMessagingService\MessageMetadata\0_MsgId:BizBar
Operation: write **Name:** MessageId
Value: 0

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\TargetedMessagingService\MessageMetadata\0_MsgId:BizBar
Operation: write **Name:** Provider
Value: 1

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\TargetedMessagingService\MessageMetadata\0_MsgId:BizBar
Operation: write **Name:** SetUserAction
Value: 0

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\TargetedMessagingService\MessageMetadata\0_MsgId:BizBar
Operation: write **Name:** ShouldShowBadging
Value: 1

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\TargetedMessagingService\MessageMetadata\0_MsgId:BizBar
Operation: write **Name:** TimeToNextcall
Value: 2026-06-18T07:28:20Z

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Licensing
Operation: delete value **Name:** EligibleForExtendedGrace
Value:

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Internet\WebServiceCache
Operation: write **Name:** LastClean
Value: A0441BDF2AFEDC01

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Word\Security\FileBlock
Operation: write **Name:** FileTypeBlockList
Value:

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Word\Security\FileBlock
Operation:	write	**Name:**	OoxmlConverterBlockList
Value:			

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\FileIO
Operation:	write	**Name:**	FileActivityStoreVersion
Value:	3		

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\TargetedMessagingService\MessageData\0:en-US:BizBar
Operation:	write	**Name:**	TransactionId
Value:	00000000-0000-0000-0000-000000000000		

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
Operation:	write	**Name:**	CachePrefix
Value:			

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
Operation:	write	**Name:**	CachePrefix
Value:	Cookie:		

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
Operation:	write	**Name:**	CachePrefix
Value:	Visited:		

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\WordDocBibs\1033
Operation:	write	**Name:**	TM02851216
Value:	[A:TM02851216][F:apasixtheditionofficeonline][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp02851216.cab][G:][L:3][O:0]		

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033
Operation:	write	**Name:**	TM03328884
Value:	[A:TM03328884][F:architecture][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp03328884.cab][G:][L:3][O:1]		

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\Themes\1033
Operation:	write	**Name:**	TM03090430
Value:	[A:TM03090430][F:Banded][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp0309043001.cab][G:][L:3][O:2]		

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\Themes\1033
Operation:	write	**Name:**	TM03457444

Value: [A:TM03457444][F:Basis][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp0345744402.cab][G:][L:3][O:3]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\Themes\1033
Operation: write **Name:** TM04033917
Value: [A:TM04033917][F:Berlin][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp0403391701.cab][G:][L:3][O:4]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033
Operation: write **Name:** TM03328893
Value: [A:TM03328893][F:BracketList][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp03328893.cab][G:][L:3][O:5]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033
Operation: write **Name:** TM03328905
Value: [A:TM03328905][F:Chevron Accent][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp03328905.cab][G:][L:3][O:6]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\WordDocBibs\1033
Operation: write **Name:** TM02851217
Value: [A:TM02851217][F:chicago][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp02851217.cab][G:][L:3][O:7]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033
Operation: write **Name:** TM03328908
Value: [A:TM03328908][F:Circle Process][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp03328908.cab][G:][L:3][O:8]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\Themes\1033
Operation: write **Name:** TM04033919
Value: [A:TM04033919][F:Circuit][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp0403391901.cab][G:][L:3][O:9]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033
Operation: write **Name:** TM03328916
Value: [A:TM03328916][F:Converging Text][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp03328916.cab][G:][L:3][O:10]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\Themes\1033
Operation: write **Name:** TM04033921
Value: [A:TM04033921][F:Damask][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp0403392101.cab][G:][L:3][O:11]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\Themes\1033
Operation: write **Name:** TM03457464
Value: [A:TM03457464][F:Dividend][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp0345746401.cab][G:][L:3][O:12]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033

Operation: write **Name:** TM03328986

Value: [A:TM03328986][F:Theme Picture Grid][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp03328986.cab][G:][L:3][O:46]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\Themes\1033

Operation: delete value **Name:** TM10001105

Value: [A:TM10001105][F:Crop][M:1/30/2007 00:00:00 AM][U:https://omextemplates.content.office.net/support/templates/en-us/tp10001105.cab][G:][L:0]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\Themes\1033

Operation: delete value **Name:** TM10001106

Value: [A:TM10001106][F:Badge][M:1/30/2007 00:00:00 AM][U:https://omextemplates.content.office.net/support/templates/en-us/tp10001106.cab][G:][L:0]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\Themes\1033

Operation: write **Name:** TM04033925

Value: [A:TM04033925][F:Droplet][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp0403392501.cab][G:][L:3][O:13]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\WordDocParts\1033

Operation: write **Name:** TM03998158

Value: [A:TM03998158][F:Element][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp03998158.cab][G:][L:3][O:14]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\WordDocParts\1033

Operation: write **Name:** TM01840907

Value: [A:TM01840907][F:Equations][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp01840907.cab][G:][L:3][O:15]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\Themes\1033

Operation: write **Name:** TM03457475

Value: [A:TM03457475][F:Frame][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp0345747501.cab][G:][L:3][O:16]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\Themes\1033

Operation: write **Name:** TM10001114

Value: [A:TM10001114][F:Gallery][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp1000111403.cab][G:][L:3][O:17]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\WordDocBibs\1033

Operation: write **Name:** TM02851218

Value: [A:TM02851218][F:gb][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp02851218.cab][G:][L:3][O:18]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\WordDocBibs\1033

Operation: write **Name:** TM02851219

Value: [A:TM02851219][F:gostname][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp02851219.cab][G:][L:3][O:19]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\WordDocBibs\1033
Operation: write **Name:** TM02851220
Value: [A:TM02851220][F:gosttitle][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp02851220.cab][G:][L:3][O:20]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\WordDocBibs\1033
Operation: write **Name:** TM02851221
Value: [A:TM02851221][F:harvardanglia2008officeonline][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp02851221.cab][G:][L:3][O:21]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033
Operation: write **Name:** TM03328919
Value: [A:TM03328919][F:Hexagon Radial][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp03328919.cab][G:][L:3][O:22]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\WordDocBibs\1033
Operation: write **Name:** TM02851222
Value: [A:TM02851222][F:ieee2006officeonline][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp02851222.cab][G:][L:3][O:23]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\WordDocParts\1033
Operation: write **Name:** TM03998159
Value: [A:TM03998159][F:Insight][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp03998159.cab][G:][L:3][O:24]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033
Operation: write **Name:** TM03328925
Value: [A:TM03328925][F:Interconnected Block Process][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp03328925.cab][G:][L:3][O:25]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\WordDocBibs\1033
Operation: write **Name:** TM02851223
Value: [A:TM02851223][F:iso690][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp02851223.cab][G:][L:3][O:26]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\WordDocBibs\1033
Operation: write **Name:** TM02851224
Value: [A:TM02851224][F:iso690nmerical][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp02851224.cab][G:][L:3][O:27]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\Themes\1033
Operation: write **Name:** TM04033927
Value: [A:TM04033927][F:Main Event][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp0403392701.cab][G:][L:3][O:28]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\Themes\1033
Operation: write **Name:** TM03457485

Value: [A:TM03457485][F:Mesh][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp0345748501.cab][G:][L:3][O:29]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\Themes\1033
Operation: write **Name:** TM03457491
Value: [A:TM03457491][F:Metropolitan][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp0345749101.cab][G:][L:3][O:30]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\WordDocBibs\1033
Operation: write **Name:** TM02851225
Value: [A:TM02851225][F:mlaseventheditionofficeonline][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp02851225.cab][G:][L:3][O:31]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\Themes\1033
Operation: write **Name:** TM03457496
Value: [A:TM03457496][F:Parallax][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp0345749601.cab][G:][L:3][O:32]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\Themes\1033
Operation: write **Name:** TM10001115
Value: [A:TM10001115][F:Parcel][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp1000111502.cab][G:][L:3][O:33]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033
Operation: write **Name:** TM03328932
Value: [A:TM03328932][F:Picture Frame][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp03328932.cab][G:][L:3][O:34]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033
Operation: write **Name:** TM03328935
Value: [A:TM03328935][F:Picture Organization Chart][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp03328935.cab][G:][L:3][O:35]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033
Operation: write **Name:** TM03328940
Value: [A:TM03328940][F:Radial Picture List][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp03328940.cab][G:][L:3][O:36]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033
Operation: write **Name:** TM03328998
Value: [A:TM03328998][F:Rings][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp03328998.cab][G:][L:3][O:37]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\Themes\1033
Operation: write **Name:** TM03457510
Value: [A:TM03457510][F:Savon][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp0345751001.cab][G:][L:3][O:38]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\WordDocBibs\1033

Operation: write **Name:** TM02851227

Value: [A:TM02851227][F:sist02][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp02851227.cab][G:][L:3][O:39]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\Themes\1033

Operation: write **Name:** TM04033929

Value: [A:TM04033929][F:Slate][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp0403392901.cab][G:][L:3][O:40]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033

Operation: write **Name:** TM03328972

Value: [A:TM03328972][F:Tab List][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp03328972.cab][G:][L:3][O:41]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033

Operation: write **Name:** TM03328951

Value: [A:TM03328951][F:Tabbed Arc][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp03328951.cab][G:][L:3][O:42]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\WordDocParts\1033

Operation: write **Name:** TM02835233

Value: [A:TM02835233][F:Text Sidebar (Annual Report Red and Black design)][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp02835233.cab][G:][L:3][O:43]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033

Operation: write **Name:** TM03328975

Value: [A:TM03328975][F:Theme Picture Accent][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp03328975.cab][G:][L:3][O:44]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033

Operation: write **Name:** TM03328983

Value: [A:TM03328983][F:Theme Picture Alternating Accent][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp03328983.cab][G:][L:3][O:45]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\WordDocBibs\1033

Operation: write **Name:** TM02851226

Value: [A:TM02851226][F:turabian][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp02851226.cab][G:][L:3][O:47]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\Themes\1033

Operation: write **Name:** TM04033937

Value: [A:TM04033937][F:Vapor Trail][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp0403393701.cab][G:][L:3][O:48]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033

Operation: write **Name:** TM03328990

Value: [A:TM03328990][F:Varying Width List][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp03328990.cab][G:][L:3][O:49]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\Themes\1033
Operation: write **Name:** TM03457515
Value: [A:TM03457515][F:View][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp0345751501.cab][G:][L:3][O:50]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\Themes\1033
Operation: write **Name:** TM03090434
Value: [A:TM03090434][F:Wood Type][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp0309043402.cab][G:][L:3][O:51]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\Themes\1033
Operation: delete value **Name:** TM03457503
Value: [A:TM03457503][F:Quotable][M:1/30/2007 00:00:00 AM][U:https://omextemplates.content.office.net/support/templates/en-us/tp03457503.cab][G:][L:0]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\Themes\1033
Operation: delete value **Name:** TM10001103
Value: [A:TM10001103][F:Headlines][M:1/30/2007 00:00:00 AM][U:https://omextemplates.content.office.net/support/templates/en-us/tp10001103.cab][G:][L:0]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\Themes\1033
Operation: delete value **Name:** TM10001104
Value: [A:TM10001104][F:Feathered][M:1/30/2007 00:00:00 AM][U:https://omextemplates.content.office.net/support/templates/en-us/tp10001104.cab][G:][L:0]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033
Operation: write **Name:** TM03328908
Value: [A:TM03328908][F:Circle Process][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp03328908.cab][G:][L:0][O:8]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\WordDocBibs\1033
Operation: write **Name:** TM02851221
Value: [A:TM02851221][F:harvardanglia2008officeonline][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp02851221.cab][G:][L:0][O:21]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\WordDocBibs\1033
Operation: write **Name:** TM02851227
Value: [A:TM02851227][F:sist02][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp02851227.cab][G:][L:0][O:39]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033
Operation: write **Name:** TM03328975
Value: [A:TM03328975][F:Theme Picture Accent][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp03328975.cab][G:][L:0][O:44]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\WordDocParts\1033

Operation: write **Name:** TM03998158

Value: [A:TM03998158][F:Element][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp03998158.cab][G:][L:0][O:14]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033

Operation: write **Name:** TM03328905

Value: [A:TM03328905][F:Chevron Accent][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp03328905.cab][G:][L:0][O:6]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\WordDocParts\1033

Operation: write **Name:** TM01840907

Value: [A:TM01840907][F:Equations][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp01840907.cab][G:][L:0][O:15]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\WordDocBibs\1033

Operation: write **Name:** TM02851222

Value: [A:TM02851222][F:ieee2006officeonline][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp02851222.cab][G:][L:0][O:23]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033

Operation: write **Name:** TM03328983

Value: [A:TM03328983][F:Theme Picture Alternating Accent][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp03328983.cab][G:][L:0][O:45]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033

Operation: write **Name:** TM03328884

Value: [A:TM03328884][F:architecture][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp03328884.cab][G:][L:0][O:1]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\WordDocBibs\1033

Operation: write **Name:** TM02851224

Value: [A:TM02851224][F:iso690nmerical][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp02851224.cab][G:][L:0][O:27]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\WordDocParts\1033

Operation: write **Name:** TM02835233

Value: [A:TM02835233][F:Text Sidebar (Annual Report Red and Black design)][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp02835233.cab][G:][L:0][O:43]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033

Operation: write **Name:** TM03328951

Value: [A:TM03328951][F:Tabbed Arc][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp03328951.cab][G:][L:0][O:42]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\WordDocBibs\1033

Operation: write **Name:** TM02851226

Value: [A:TM02851226][F:turabian][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp02851226.cab][G:][L:0][O:47]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033
Operation: write **Name:** TM03328919
Value: [A:TM03328919][F:Hexagon Radial][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp03328919.cab][G:][L:0][O:22]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033
Operation: write **Name:** TM03328925
Value: [A:TM03328925][F:Interconnected Block Process][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp03328925.cab][G:][L:0][O:25]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\WordDocBibs\1033
Operation: write **Name:** TM02851223
Value: [A:TM02851223][F:iso690][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp02851223.cab][G:][L:0][O:26]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033
Operation: write **Name:** TM03328986
Value: [A:TM03328986][F:Theme Picture Grid][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp03328986.cab][G:][L:0][O:46]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\WordDocBibs\1033
Operation: write **Name:** TM02851220
Value: [A:TM02851220][F:gosttitle][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp02851220.cab][G:][L:0][O:20]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033
Operation: write **Name:** TM03328916
Value: [A:TM03328916][F:Converging Text][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp03328916.cab][G:][L:0][O:10]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033
Operation: write **Name:** TM03328940
Value: [A:TM03328940][F:Radial Picture List][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp03328940.cab][G:][L:0][O:36]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033
Operation: write **Name:** TM03328932
Value: [A:TM03328932][F:Picture Frame][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp03328932.cab][G:][L:0][O:34]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033
Operation: write **Name:** TM03328990
Value: [A:TM03328990][F:Varying Width List][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp03328990.cab][G:][L:0][O:49]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033

Operation: write **Name:** TM03328972

Value: [A:TM03328972][F:Tab List][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp03328972.cab][G:][L:0][O:41]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\WordDocBibs\1033

Operation: write **Name:** TM02851219

Value: [A:TM02851219][F:gostname][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp02851219.cab][G:][L:0][O:19]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\WordDocBibs\1033

Operation: write **Name:** TM02851225

Value: [A:TM02851225][F:mlaseventheditionofficeonline][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp02851225.cab][G:][L:0][O:31]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033

Operation: write **Name:** TM03328998

Value: [A:TM03328998][F:Rings][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp03328998.cab][G:][L:0][O:37]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033

Operation: write **Name:** TM03328935

Value: [A:TM03328935][F:Picture Organization Chart][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp03328935.cab][G:][L:0][O:35]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033

Operation: write **Name:** TM03328893

Value: [A:TM03328893][F:BracketList][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp03328893.cab][G:][L:0][O:5]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033

Operation: write **Name:** NextUpdate

Value: F07CBA837A00DD01

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033

Operation: write **Name:** LastUpdate

Value: D58201EC2AFEDC01

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\WordDocBibs\1033

Operation: write **Name:** TM02851217

Value: [A:TM02851217][F:chicago][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp02851217.cab][G:][L:0][O:7]

(PID) Process: (1328) WINWORD.EXE **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\WordDocBibs\1033

Operation: write **Name:** TM02851218

Value: [A:TM02851218][F:gb][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp02851218.cab][G:][L:0][O:18]

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\WordDocBibs\1033
Operation:	write	**Name:**	TM02851216
Value:	[A:TM02851216][F:apasixtheditionofficeonline][M:1/30/2007 00:00:00 AM][U:https://binaries.templates.cdn.office.net/support/templates/en-us/tp02851216.cab][G:][L:0][O:0]		

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\WordDocBibs\1033
Operation:	write	**Name:**	NextUpdate
Value:	F07CBA837A00DD01		

(PID) Process:	(1328) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\WordDocBibs\1033
Operation:	write	**Name:**	LastUpdate
Value:	D58201EC2AFEDC01		

Files activity

Executable files	Suspicious files	Text files	Unknown types
32	118	18	0

Dropped files

PID	Process	Filename	Type
1328	WINWORD.EXE	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\E2C6CBAF0AF08CF203BA74BF0D0AB6D5_EAF5D55D93603A879FA973006301F24F **MD5:** 7BF746674690DF9A15E17B985ADC6022 **SHA256:** EFDAD6535DAEFEB8882F55E8C8483BD457559479FAAB19D68F9F53C5AEDC829C	binary
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Office\16.0\AddInClassifierCache\OfficeSharedEntities.bin **MD5:** CC90D669144261B198DEAD45AA266572 **SHA256:** 89C701EEFF939A44F28921FD85365ECD87041935DCD0FE0BAF04957DA12C9899	text
3376	WinRAR.exe	C:\Users\admin\AppData\Local\Temp\Rar$DIb3376.41634\3a787a7b850b92a99d20f52747f1e13428039a149b7dd6295f6ca11995d88e0a.docm **MD5:** BDF9FC731ACC96EE6FE16538ABD9E4A0 **SHA256:** 5B98EE9CEB25C802CE40EA108D7E6FE66DFAE7F9C3B15CDE4762EB0237BD7616	binary
1328	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\~$Normal.dotm **MD5:** 780B86127A13C75EB8C716BAB756D00B **SHA256:** AA9082CE88826EB53A39ECD8A1356E94BC0E021D6FCB0CD9EB31E6BF044A790D	binary
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\A0DA7B77-86BD-4172-863F-597C3193FD11	xml

		MD5: 82138A26CD6A8D837EB0262E1BA65E19 **SHA256:** 0848ED09A081C702731F8B28AA155CD84591B82FEF5B35BF1BDDA9DAA7C1A6AB	
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\Rar$DIb3376.41634\~$787a7b850b92a99d20f52747f1e13428039a149b7dd6295f6ca11995d88e0a.doc m **MD5:** 98ABABBD4D60B7DFFEB4D64CF4BF452A **SHA256:** 59F70810C7AFC86B78A0FAD8A5279B8A53232C214F69F1A0887C71A4F83E3B9B	binary
1328	WINWORD.EXE	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\B76BE66D46C355931939D8CF818D03FD_879AFEB08DCB01270758 2D902977FF92 **MD5:** 7FC4484899FDAA08E8C1E29889979ABF **SHA256:** 0613A14BF642815F86E401D71D229C103CF78DF2EB48D93F2CD8F8D83533BE09	binary
1328	WINWORD.EXE	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\E2C6CBAF0AF08CF203BA74BF0D0AB6D5_EAF5D55D93603A879FA9 73006301F24F **MD5:** 7BF82CF24E7EF15F7D9C960CD97AD1EC **SHA256:** 4F9EF653839C490B315416AB2053E74B830DE6417B68DA919D119E7054A78E27	binary
1328	WINWORD.EXE	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\B76BE66D46C355931939D8CF818D03FD_879AFEB08DCB0127075 82D902977FF92 **MD5:** 632159B3258A41349F6B87D847F268DA **SHA256:** 13060595C7C1E1DD232CA4BD2B357103EB79D4DEEB751123E0B405E3D49C9CC4	binary
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\TokenBroker\Cache\56a61aeb75d8f5be186c26607f4bb213abe7c5ec.tbres **MD5:** 3A512EC57B4AC530FE932DF52A80432C **SHA256:** C651345083B01FA9FB27295DDC5BAB9CA9366992FBA9B62DAF01B5308E675ECB	binary
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\msoF841.tmp **MD5:** BEB742DAC5080AA0B6DF56689A5A397F **SHA256:** 409DBD42A3491FC8FF646685A7C90C9E0C926321EB75775E96EBCC12414926F1	binary
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\FontCache\4\Catalog\ListAll.Json **MD5:** 7C5578BC58BDE6DC855D5C929CF54232 **SHA256:** A48ACBE81F33E5918B096A6B89687E505DA0E79196F74DC48B6E068708378A3F	text
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\TokenBroker\Cache\5475cb191e478c39370a215b2da98a37e9dc813d.tbres **MD5:** 78FF928948E90A24291F696429F442D1 **SHA256:** 6C532B662EA07F64E374567F4C86AA2102F7848C01F62BE159337B4AD6EF5611	binary
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\6B2A9397.wmf **MD5:** 090147207D855777D9A1CF6616FAB88D **SHA256:** D673D078EC15C9E34706881EBD1C1AE89FA96516B47604C7686626CC55316A74	binary
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\D1B6A8AC.dat **MD5:** 2BB608EE90D91B9DC9A8104637FFB733 **SHA256:** 45CC795F7939D1C5F753EE207EF009DA52D2DAD09A52A9CD3C9E14ED7A701EAB	binary
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\Word8.0\MSForms.exd **MD5:** EB7391E920D6452E4222BA7EAC6FA511 **SHA256:** F930554181F74D38465E388292ED3963BDE98DE8DDF477DD0AC7A0605E368D8C	binary
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\FontCache\4\PreviewFont\flat_officeFontsPreview_4_42.ttf **MD5:** 8BDF396FED21EED0F788CB9A23775A1E **SHA256:** BD6575CBCF808C13421BF03886E008624B85B6CE23651949BCFBD10EBD8452BE	binary
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Office\16.0\AddInClassifierCache\OfficeSharedEntitiesUpdated.bin	text

		MD5: ED53F903620E0985E7400BCDCC930959 **SHA256:** 872D998F1E357DFEB60E0968C19DC94D26EADD2A741BE44E5A7CCF0D9DB666CA	
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\TokenBroker\Cache\089d66ba04a8cec4bdc5267f42f39cf84278bb67.tbres **MD5:** DC387FC2998C8FFB48E6CB8A2C73D5A5 **SHA256:** 3298DEB6C2B24D512D78603CEC8B6F5DD8F04A15CF0F0F811D534AED6A6F7481	binary
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Office\16.0\Personalization\Governance\Anonymous\floodgatecampaigns.json.tmp **MD5:** B4E4AED13FF56E2BE6247B863AA7C9F8 **SHA256:** 5927002BA510D4915E3A59BDE6A85E4F87D8535B3D5882B2E9DCD3A6394F76B7	text
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Office\16.0\Personalization\Governance\Anonymous\floodgatecampaigns.json **MD5:** B4E4AED13FF56E2BE6247B863AA7C9F8 **SHA256:** 5927002BA510D4915E3A59BDE6A85E4F87D8535B3D5882B2E9DCD3A6394F76B7	text
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Office\16.0\UsageMetricsStore\FileActivityStoreV3\Word\ASkwMDAwMDAwMC0wMDAwLTAwMDAtMDAwMC0wMDAwMDAwMDAwMDBfTnVsbAA.S **MD5:** D8AE2367BB14A3805EF14888F7863470 **SHA256:** 715135D60D9B86ADAB67147F6185C5277B47947BFA109F58C952D2197690278D	binary
1328	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\ZSYLDFZ7MBS1O6W3GUIV.temp **MD5:** E4A1661C2C886EBB688DEC494532431C **SHA256:** B76875C50EF704DBBF7F02C982445971D1BBD61AEBE2E4B28DDC58A1D66317D5	binary
1328	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\fb3b0dbfee58fac8.customDestinations-ms **MD5:** E4A1661C2C886EBB688DEC494532431C **SHA256:** B76875C50EF704DBBF7F02C982445971D1BBD61AEBE2E4B28DDC58A1D66317D5	binary
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab4EAF.tmp **MD5:** 1D6F8E73A0662A48D332090A4C8C898F **SHA256:** 8077C92C66D15D7E03FBFF3A48BD9576B80F698A36A44316EABA81EE8043B673	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\fb3b0dbfee58fac8.customDestinations-ms~RF1a2423.TMP **MD5:** 4FCB2A3EE025E4A10D21E1B154873FE2 **SHA256:** 90BF6BAA6F968A285F88620FBF91E1F5AA3E66E2BAD50FD16F37913280AD8228	binary
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab4EB4.tmp **MD5:** 69EDB3BF81C99FE8A94BBA03408C5AE1 **SHA256:** CEBE759BC4509700E3D23C6A5DF8D889132A60EBC92260A74947EAA1089E2789	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab4EB5.tmp **MD5:** 205AF51604EF96EF1E8E60212541F742 **SHA256:** DF3FFF163924D08517B41455F2D06788BA4E49C68337D15ECF329BE48CF7DA2D	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab4ED6.tmp **MD5:** F10DF902980F1D5BEEA96B2C668408A7 **SHA256:** E0100320A4F63E07C77138A89EA24A1CBD69784A89FE3BF83E35576114B4CE02	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab4ED8.tmp **MD5:** 6D787B1E223DB6B91B69238062CCA872 **SHA256:** DA2F261C3C82E229A097A9302C8580F014BB6442825DB47C008DA097CFCE0EE4	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab4EB0.tmp **MD5:** 51804E255C573176039F4D5B55C12AB2 **SHA256:** 3C6F66790C543D4E9D8E0E6F476B1ACADF0A5FCDD561B8484D8DDDADFDF8134B	compressed

1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab4EC5.tmp **MD5:** ABBF10CEE9480E41D81277E9538F98CB	**SHA256:** 557E0714D5536070131E7E7CDD18F0EF23FE6FB12381040812D022EC0FEE7957	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab4F0C.tmp **MD5:** E3C64173B2F4AA7AB72E1396A9514BD8	**SHA256:** 16C08547239E5B969041AB201EB55A3E30EAD400433E926257331CB945DFF094	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab4F0D.tmp **MD5:** 4EFA48EC307EAF2F9B346A073C67FCFB	**SHA256:** 3EE9AE1F8DAB4C498BD561D8FCC66D83E58F11B7BB4B2776DF99F4CDA4B850C2	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab4F0E.tmp **MD5:** 89A9818E6658D73A73B642522FF8701F	**SHA256:** F747DD8B79FC69217FA3E36FAE0AB417C1A0759C28C2C4F8B7450C70171228E6	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab4F1E.tmp **MD5:** F913DD84915753042D856CEC4E5DABA5	**SHA256:** AA03AFB681A76C86C1BD8902EE2BBA31A644841CE6BCB913C8B5032713265578	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab4EDA.tmp **MD5:** 91AADBEC4171CFA8292B618492F5EF34	**SHA256:** 7E1A90CDB2BA7F03ABCB4687F0931858BF57E13552E0E4E54EC69A27325011EA	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab4F3F.tmp **MD5:** 66C5199CF4FB18BD4F9F3F2CCB074007	**SHA256:** 4A7DC4ED098E580C8D623C51B57C0BC1D601C45F40B60F39BBA5F063377C3C1F	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab4EDB.tmp **MD5:** DA3380458170E60CBEA72602FDD0D955	**SHA256:** 6F8FFB225F3B8C7ADE31A17A02F941FC534E4F7B5EE678B21CD9060282034701	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab4EDC.tmp **MD5:** C455C4BC4BEC9E0DA67C4D1E53E46D5A	**SHA256:** 40E9AF9284FF07FDB75C33A11A794F5333712BAA4A6CF82FA529FBAF5AD0FED0	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab4EB1.tmp **MD5:** 53EE9DA49D0B84357038ECF376838D2E	**SHA256:** 9E46B8BA0BAD6E534AF33015C86396C33C5088D3AE5389217A5E90BA68252374	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab4EB2.tmp **MD5:** D3C9036E4E1159E832B1B4D2E9D42BF0	**SHA256:** 434576EB1A16C2D14D666A33EDDE76717C896D79F45DF56742AFD90ACB9F21CE	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab4EB3.tmp **MD5:** 92A819D434A8AAEA2C65F0CC2F33BB3A	**SHA256:** 5D13F9907AC381D19F0A7552FD6D9FC07C9BD42C0F9CE017FFF75587E1890375	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab4F8F.tmp **MD5:** 21A4B7B71631C2CCDA5FBBA63751F0D2	**SHA256:** AE0C5A2C8377DBA613C576B1FF73F01AE8EF4A3A4A10B078B5752FB712B3776C	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab4F90.tmp		compressed

		MD5: 0EBC45AA0E67CC435D0745438371F948	**SHA256:** 3744BFA286CFCFF46E51E6A68823A23F55416CD6619156B5929FED1F7778F1C7
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab4FA0.tmp **MD5:** 7C645EC505982FE529D0E5035B378FFC	compressed **SHA256:** 298FD9DADF0ACEBB2AA058A09EEBFAE15E5D1C5A8982DEE6669C63FB6119A13D
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab4FC1.tmp **MD5:** E532038762503FFA1371DF03FA2E222D	compressed **SHA256:** 5C70DD1551EB8B9B13EFAFEEAF70F08B307E110CAEE75AD9908A6A42BBCCB07E
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab4FC2.tmp **MD5:** B9A6FF715719EE9DE16421AB983CA745	compressed **SHA256:** E3BE3F1E341C0FA5E9CB79E2739CF0565C6EA6C189EA3E53ACF04320459A7070
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab507F.tmp **MD5:** D30AD26DBB6DECA4FDD294F48EDAD55D	compressed **SHA256:** 6B1633DD765A11E7ED26F8F9A4DD45023B3E4ADB903C934DF3917D07A3856BFF
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab511E.tmp **MD5:** 486CBCB223B873132FFAF4B8AD0AD044	compressed **SHA256:** B217393FD2F95A11E2C594E736067870212E3C5242A212D6F9539450E8684616
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab50B0.tmp **MD5:** 8B29FAB506FD65C21C9CD6FE6BBBC146	compressed **SHA256:** 773AC516C9B9B28058128EC9BE099F817F3F90211AC70DC68077599929683D6F
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab516E.tmp **MD5:** 21437897C9B88AC2CB2BB2FEF922D191	compressed **SHA256:** 372572DCBAD590F64F5D18727757CBDF9366DDE90955C79A0FCC9F536DAB0384
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab517F.tmp **MD5:** 84D8F3848E7424CBE3801F9570E05018	compressed **SHA256:** B4BC3CD34BD328AAF68289CC0ED4D5CF8167F1EE1D7BE20232ED4747FF96A80A
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab516F.tmp **MD5:** 93FA9F779520AB2D22AC4EA864B7BB34	compressed **SHA256:** 6A3801C1D4CF0C19A990282D93AC16007F6CACB645F0E0684EF2EDAC02647833
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab51C0.tmp **MD5:** EF9CB8BDFBC08F03BEF519AD66BA642F	compressed **SHA256:** 93A2F873ACF5BEAD4BC0D1CC17B5E89A928D63619F70A1918B29E5230ABEAD8E
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab51C1.tmp **MD5:** 7BF88B3CA20EB71ED453A3361908E010	compressed **SHA256:** E555A610A61DB4F45A29A7FB196A9726C25772594252AD534453E69F05345283
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab4F40.tmp **MD5:** C47E3430AF813DF8B02E1CB4829DD94B	compressed **SHA256:** F2DB1E60533F0D108D5FB1004904C1F2E8557D4493F3B251A1B3055F8F1507A3
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab5080.tmp **MD5:** EE0129C7CC1AC92BBC3D6CB0F653FCAE	compressed **SHA256:** 345AA5CA2496F975B7E33C182D5E57377F8B740F23E9A55F4B2B446723947B72

1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab51AF.tmp **MD5:** 9A07035EF802BF89F6ED254D0DB02AB0 **SHA256:** 6CB03CEBAB2C28BF5318B13EEEE49FBED8DCEDAF771DE78126D1BFE9BD81C674	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab5020.tmp **MD5:** 97F5B7B7E9E1281999468A5C42CB12E7 **SHA256:** 1CF5C2D0F6188FFFF117932C424CC55D1459E0852564C09D7779263ABD116118	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\7396C420A8E1BC1DA97F1AF0D10BAD21 **MD5:** E07178901A4EAAC2816BB238EC3A80DB **SHA256:** EEBD04C1272661E1091084108083CE44F7C961013791892D866B2F92EE3DEDA8	binary
1328	WINWORD.EXE	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\37C951188967C8EB88D99893D9D191FE **MD5:** 00E85A7D2A0849E4AD5387A6B2D68DAA **SHA256:** F2D95F6785DFB370F4B1E8D531E7511DDE8D9A776404BDC4B8BA1696DBD27854	binary
1328	WINWORD.EXE	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\696F3DE637E6DE85B458996D49D759AD **MD5:** 6872FAE8288DB34207D9E7EE350157F4 **SHA256:** 50795B027E2BC566D3B7ACB89913F8EFD23B70615C9DB9BF5B23323AD3132A7D	binary
1328	WINWORD.EXE	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\696F3DE637E6DE85B458996D49D759AD **MD5:** DF8B309582F5B3995ADCC62762A0FCCB **SHA256:** 05AFEB19FDAC1A2EC6A12CBC7A09E60427C71D6B958AE7AA7F050953D4645B98	binary
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab525F.tmp **MD5:** E1101CCA6E3FEDB28B57AF4C41B50D37 **SHA256:** 69B2675E47917A9469F771D0C634BD62B2DFA0F5D4AF3FD7AFE9196BF889C19E	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\F90F18257CBB4D84216AC1E1F3BB2C76 **MD5:** 539B6E823053D9B42495445DD22AD0F2 **SHA256:** 378B2BF272859F079B30609386B5A1010FFD05D4F2BB9EEFCBE9704424E538F2	binary
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD52C1.tmp\Element design set.dotx **MD5:** 0744EF6AB596DE190C01621DD03FBBBE **SHA256:** 73181A364116625D1B67CD790EA0FD0AE314497EA9321365A9DB36E170C5440C	binary
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD52AF.tmp\chevronaccent.glox **MD5:** 7BC0A35807CD69C37A949BBD51880FF5 **SHA256:** BD3A013F50EBF162AAC4CED11928101554C511BD40C2488CF9F5842A375B50CA	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab4ED9.tmp **MD5:** 62863124CDCDA135ECC0E722782CB888 **SHA256:** 23CCFB7206A8F77A13080998EC6EF95B59B3C3E12B72B2D2AD4E53B0B26BB8C3	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab4ED7.tmp **MD5:** E033CCBC7BA787A2F824CE0952E57D44 **SHA256:** D250EB1F93B43EFB7654B831B4183C9CAEC2D12D4EFEE8607FEE70B9FAB20730	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab524E.tmp **MD5:** E29CE2663A56A1444EAA3732FFB82940 **SHA256:** 3732EB6166945DB2BF792DA04199B5C4A0FB3C96621ECBFDEAF2EA1699BA88EE	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\F90F18257CBB4D84216AC1E1F3BB2C76	binary

		MD5: E95AF9B03513D729D28FD890CFF4EBE9 **SHA256:** B19F80A5970542F71E1728CDEEE5D4534598329BA22FABF5BBD2280EBD6BA629	
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD52C1.tmp\Content.inf **MD5:** 0F98498818DC28E82597356E2650773C **SHA256:** 4587CA0B2A60728FF0A5B8E87D35BF6C6FDF396747E13436EC856612AC1C6288	text
1328	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\Word Document Building Blocks\1033\TM03998158[[fn=Element]].dotx **MD5:** 77979D3955149C7F06D2F9C9A284E279 **SHA256:** A0F15EDF4943FF9A862E29BA8C598C98DDD88FC10C4895FF6EB778D7C2DFD9FF	binary
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD52AF.tmp\Content.inf **MD5:** 4DD225E2A305B50AF39084CE568B8110 **SHA256:** 6F00DD73F169C73D425CB9895DAC12387E21C6E4C9C7DDCFB03AC32552E577F4	text
1328	WINWORD.EXE	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\C0018BB1B5834735BFA60CD063B31956 **MD5:** DDE97D900210CA79F7FEEDD95322FF3E **SHA256:** EAD40ACA9887C241AFB566A25A21A8BB5283CAC4C3D89D90B3C74D2E21471AEA	binary
1328	WINWORD.EXE	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\C0018BB1B5834735BFA60CD063B31956 **MD5:** CF9B25FB6EA2655F0DC927D4B5050C11 **SHA256:** 1DF9B268EE5C1A2446148C9542E7FDF79EC9304E7561FB0736472C895578BAB7	binary
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD52C0.tmp\Content.inf **MD5:** 93149E194021B37162FD86684ED22401 **SHA256:** 50BE99A154A6F632D49B04FCEE6BCA4D6B3B4B7C1377A31CE9FB45C462D697B2	text
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD52C0.tmp\Equations.dotx **MD5:** 2AB22AC99ACFA8A82742E774323C0DBD **SHA256:** BC9D45D0419A08840093B0BF4DCF96264C02DFE5BD295CD9B53722E1DA02929D	binary
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD52C2.tmp\ThemePictureAlternatingAccent.glox **MD5:** 8FDC5D57F2C6D4624F6ECFC56D3B8C06 **SHA256:** 2AFD4F0138B01758678036D0FAE8DC4A76402CB3256ABDCA7E40C23F5A2BA00D	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD52AE.tmp\ieee2006officeonline.xsl **MD5:** 0C9731C90DD24ED5CA6AE283741078D0 **SHA256:** ABCE25D1EB3E70742EC278F35E4157EDB1D457A7F9D002AC658AAA6EA4E4DCDF	xml
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD52C2.tmp\Content.inf **MD5:** 3D52060B74D7D448DC733FFE5B92CB52 **SHA256:** BB980559C6FC38B703D1E9C41720D5CE8D00D2FF86D4F25136DB02B1E54B1518	text
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD52D2.tmp\CircleProcess.glox **MD5:** 950F3AB11CB67CC651082FEBE523AF63 **SHA256:** 9C5E4D8966A0B30A22D92DB1DA2F0DBF06AC2EA75E7BB8501777095EA0196974	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD52D2.tmp\Content.inf **MD5:** D04EC08EFE18D1611BDB9A5EC0CC00B1 **SHA256:** FA60500F951AFAF8FFDB6D1828456D60004AE1558E8E1364ADC6ECB59F5450C9	text
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD52D3.tmp\HexagonRadial.glox **MD5:** 20621E61A4C5B0FFEEC98FFB2B3BCD31 **SHA256:** 223EA2602C3E95840232CACC30F63AA5B050FA360543C904F04575253034E6D7	compressed

1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD52D3.tmp\Content.inf **MD5:** E8B30D1070779CC14FBE93C8F5CF65BE **SHA256:** 2E90434BE1F6DCEA9257D42C331CD9A8D06B848859FD4742A15612B2CA6EFACB	text
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD52D5.tmp\architecture.glox **MD5:** 8109B3C170E6C2C114164B8947F88AA1 **SHA256:** F320B4BB4E57825AA4A40E5A61C1C0189D808B3EACE072B35C77F38745A4C416	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD52D4.tmp\InterconnectedBlockProcess.glox **MD5:** 08D3A25DD65E5E0D36ADC602AE68C77D **SHA256:** 58B45B9DBA959F40294DA2A54270F145644E810290F71260B90F0A3A9FCDEBC1	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD52D4.tmp\Content.inf **MD5:** 1309D172F10DD53911779C89A06BBF65 **SHA256:** C190F9E7D00E053596C3477455D1639C337C0BE01012C0D4F12DFCB432F5EC56	text
1328	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\SmartArt Graphics\1033\TM03328905[[fn=Chevron Accent]].glox **MD5:** 7BC0A35807CD69C37A949BBD51880FF5 **SHA256:** BD3A013F50EBF162AAC4CED11928101554C511BD40C2488CF9F5842A375B50CA	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\Word Document Building Blocks\1033\TM01840907[[fn=Equations]].dotx **MD5:** CEE6069BD7A22315BB5B328A3AD3B498 **SHA256:** 2DE8631B2A69AE54C962AF917BB57A9AE06949E606DA5088F256B866DF8CDABA	binary
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD52E6.tmp\iso690.xsl **MD5:** FF0E07EFF1333CDF9FC2523D323DD654 **SHA256:** 3F925E0CC1542F09DE1F99060899EAFB0042BB9682507C907173C392115A44B5	xml
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD52E7.tmp\iso690nmerical.xsl **MD5:** 3BF8591E1D808BCCAD8EE2B822CC156B **SHA256:** 7194396E5C833E6C8710A2E5D114E8E24338C64EC9818D51A929D57A5E4A76C8	xml
1328	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\SmartArt Graphics\1033\TM03328983[[fn=Theme Picture Alternating Accent]].glox **MD5:** 2F8998AA9CF348F1D6DE16EAB2D92070 **SHA256:** 8A216D16DEC44E02B9AB9BBADF8A11F97210D8B73277B22562A502550658E580	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD52E8.tmp\TabbedArc.glox **MD5:** A72DDBBCF3F9DB72F727CB72BFDA03F5 **SHA256:** DF19B8462BC83C9F585B05B9BA9143AA5366886C06643C908B6B6EF59E5D8383	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD52E7.tmp\Content.inf **MD5:** 9C00979164E78E3B890E56BE2DF00666 **SHA256:** 21CCB63A82F1E6ACD6BAB6875ABBB37001721675455C746B17529EE793382C7B	text
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD52D5.tmp\Content.inf **MD5:** D79B5DE6D93AC06005761D88783B3EE6 **SHA256:** 96125D6804544B8D4E6AE8638EFD4BD1F96A1BFB9EEF57337FFF40BA9FF4CDD1	text
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD52E6.tmp\Content.inf **MD5:** 9B8D7EFE8A69E41CDC2439C38FE59FAF **SHA256:** 70042F1285C3CD91DDE8D4A424A5948AE8F1551495D8AF4612D59709BEF69DF2	text
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD52EC.tmp\Content.inf	text

		MD5: 4EC6724CBBA516CF202A6BD17226D02C **SHA256:** 18E408155A2C2A24D91CD45E065927FFDA726356AAB115D290A3C1D0B7100402	
1328	WINWORD.EXE	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\37C951188967C8EB88D99893D9D191FE **MD5:** 2E27BAAF47A335DF008DC83F0F1A7270 **SHA256:** CFAA887CBF7755F3CB7B088A4FB18A68C3CEDEC58C889C8BBC3653BC4E217B93	binary
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD52EA.tmp\Content.inf **MD5:** 2F7A8FE4E5046175500AFFA228F99576 **SHA256:** 1495B4EC56B371148EA195D790562E5621FDBF163CDD8A5F3C119F8CA3BD2363	text
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD52E8.tmp\Content.inf **MD5:** 16711B951E1130126E240A6E4CC2E382 **SHA256:** 855342FE16234F72DA0C2765455B69CF412948CFBE70DE5F6D75A20ACDE29AE9	text
1328	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\SmartArt Graphics\1033\TM03328919[[fn=Hexagon Radial]].glox **MD5:** 20621E61A4C5B0FFEEC98FFB2B3BCD31 **SHA256:** 223EA2602C3E95840232CACC30F63AA5B050FA360543C904F04575253034E6D7	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\A583E2A51BFBDC1E492A57B7C8325850 **MD5:** FDB0DD089AC4E725267C389B58B05603 **SHA256:** 6068704DAFA6065CD5B2272B9306B9BC832CA656F07FE3CCDAFEFF61DF6442EE	binary
1328	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\SmartArt Graphics\1033\TM03328884[[fn=architecture]].glox **MD5:** 8109B3C170E6C2C114164B8947F88AA1 **SHA256:** F320B4BB4E57825AA4A40E5A61C1C0189D808B3EACE072B35C77F38745A4C416	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\SmartArt Graphics\1033\TM03328951[[fn=Tabbed Arc]].glox **MD5:** E35903E8B62F3605F5F796D4B94FA946 **SHA256:** 1BE16FE0F1EFB26B6DA07FBEEB5F887DF27433F353DFE7D2CFC3E052E4FCB0BD	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD52EB.tmp\Content.inf **MD5:** 6C489D45F3B56845E68BE07EA804C698 **SHA256:** 3FE447260CDCDEE287B8D01CF5F9F53738BFD6AAEC9FB9787F2826F8DEF1CA45	text
1328	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\SmartArt Graphics\1033\TM03328925[[fn=Interconnected Block Process]].glox **MD5:** 08D3A25DD65E5E0D36ADC602AE68C77D **SHA256:** 58B45B9DBA959F40294DA2A54270F145644E810290F71260B90F0A3A9FCDEBC1	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD52EB.tmp\ThemePictureAccent.glox **MD5:** 42A840DC06727E42D42C352703EC72AA **SHA256:** 02CCE7D526F844F70093AC41731D1A1E9B040905DCBA63BA8BFFC0DBD4D3A7A7	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD52EC.tmp\harvardanglia2008officeonline.xsl **MD5:** 33A829B4893044E1851725F4DAF20271 **SHA256:** C40451CADF8944A9625DD690624EA1BA19CECB825A67081E8144AD5526116924	xml
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD52EA.tmp\Text Sidebar (Annual Report Red and Black design).docx **MD5:** C306CF49E1BF811C7D461247E9E12B81 **SHA256:** 2122778EECCBE47490196865B79D8593554BA5F59C5BE1B8660EFB3C0C218A17	binary
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD52E9.tmp\turabian.xsl	xml

		MD5: F079EC5E2CCB9CD4529673BCDFB90486	**SHA256:** 3B651258F4D0EE1BFFC7FB189250DED1B920475D1682370D6685769E3A9346DB
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD52E9.tmp\Content.inf	text
		MD5: C15EB3F4306EBF75D1E7C3C9382DEECC	**SHA256:** 23C262DF3AEACB125E88C8FFB7DBF56FD23F66E0D476AFD842A68DDE69658C7F
1328	WINWORD.EXE	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\7396C420A8E1BC1DA97F1AF0D10BAD21	binary
		MD5: 68AB8A7B4A60598CC4FF97A8D102ABCB	**SHA256:** 4A8FFAF63C06C395EF17E68170CB2AE6D9F51DA41D942D85741255365E02B16C
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab5327.tmp	compressed
		MD5: 26BEAB9CCEAFE4FBF0B7C0362681A9D2	**SHA256:** 217EC1B6E00A24583B166026DEC480D447FB564CF3BCA81984684648C272F767
1328	WINWORD.EXE	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\A583E2A51BFBDC1E492A57B7C8325850	binary
		MD5: 5941D61E5EA46F136CBD494AA319FF38	**SHA256:** C8F983967D814637D6AB65B09367043B7C4A211EA5F433852C965B4C466EC92B
1328	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\SmartArt Graphics\1033\TM03328908[[fn=Circle Process]].glox	compressed
		MD5: BE6F200A72712F4715D1FE7F76F5158A	**SHA256:** 2A83980A6665DC80C0C829454FE75A977A76F74D0A3E5A0DBC223B9146951005
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD52AE.tmp\Content.inf	text
		MD5: F25AC64EC63FA98D9E37782E2E49D6E6	**SHA256:** 834046A829D1EA836131B470884905856DBF2C3C136C98ADEEFA0F206F38F8AB
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD5324.tmp\RadialPictureList.glox	compressed
		MD5: CDC1493350011DB9892100E94D5592FE	**SHA256:** F637A67799B492FEFFB65632FED7815226396B4102A7ED790E0D9BB4936E1548
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD5323.tmp\sist02.xsl	xml
		MD5: F883B260A8D67082EA895C14BF56DD56	**SHA256:** EF4835DB41A485B56C2EF0FF7094BC2350460573A686182BC45FD6613480E353
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD531D.tmp\Content.inf	text
		MD5: 6F8FE7B05855C203F6DEC5C31885DD08	**SHA256:** B7F58DF058C938CCF39054B31472DC76E18A3764B78B414088A261E440870175
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab536B.tmp	compressed
		MD5: BF95E967E7D1CEC8EFE426BC0127D3DE	**SHA256:** 4C3B008E0EB10A722D8FEDB325BFB97EDAA609B1E901295F224DD4CB4DF5FC26
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD531D.tmp\ThemePictureGrid.glox	compressed
		MD5: 031C246FFE0E2B623BBBD231E414E0D2	**SHA256:** 2D76C8D1D59EDB40D1FBBC6406A06577400582D1659A544269500479B6753CF7
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD531C.tmp\ConvergingText.glox	compressed
		MD5: C9F9364C659E2F0C626AC0D0BB519062	**SHA256:** 6FC428CA0DCFC27D351736EF16C94D1AB08DDA50CB047A054F37EC028DD08AA2
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD5323.tmp\Content.inf	text
		MD5: 149948E41627BE5DC454558E12AF2DA4	**SHA256:** 1B981DC422A042CDDEBE2543C57ED3D468288C20D280FF9A9E2BB4CC8F4776ED

1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD531C.tmp\Content.inf **MD5:** 923D406B2170497AD4832F0AD3403168 **SHA256:** EBF9CF474B25DDFE0F6032BA910D5250CBA2F5EDF9CF7E4B3107EDB5C13B50BF	text
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD5325.tmp\gosttitle.xsl **MD5:** F425D8C274A8571B625EE66A8CE60287 **SHA256:** DD7B7878427276AF5DBF8355ECE0D1FE5D693DF55AF3F79347F9D20AE50DB938	xml
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD5324.tmp\Content.inf **MD5:** 52BD0762F3DC77334807DDFC60D5F304 **SHA256:** 30C20CC835E912A6DD89FD1BF5F7D92B233B2EC24594F1C1FE0CADB03A8C3FAB	text
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD532C.tmp\VaryingWidthList.glox **MD5:** 67766FF48AF205B771B53AA2FA82B4F4 **SHA256:** 160D05B4CB42E1200B859A2DE00770A5C9EBC736B70034AFC832A475372A1667	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\SmartArt Graphics\1033\TM03328986[[fn=Theme Picture Grid]].glox **MD5:** F364235BB9B5F8010CFF885424DB91A9 **SHA256:** A29819AE3DE2E61E81609066A7DDE34DC747A1FEC01DD43058F2982AED5C9BC5	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\SmartArt Graphics\1033\TM03328975[[fn=Theme Picture Accent]].glox **MD5:** 42A840DC06727E42D42C352703EC72AA **SHA256:** 02CCE7D526F844F70093AC41731D1A1E9B040905DCBA63BA8BFFC0DBD4D3A7A7	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD531F.tmp\TabList.glox **MD5:** BE6F200A72712F4715D1FE7F76F5158A **SHA256:** 2A83980A6665DC80C0C829454FE75A977A76F74D0A3E5A0DBC223B9146951005	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD531E.tmp\pictureorgchart.glox **MD5:** 586CEBC1FAC6962F9E36388E5549FFE9 **SHA256:** 1595C0C027B12FE4C2B506B907C795D14813BBF64A2F3F6F5D71912D7E57BC40	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD5325.tmp\Content.inf **MD5:** A0D51783BFEE86F3AC46A810404B6796 **SHA256:** 47B43E7DBDF8B25565D874E4E071547666B08D7DF4D736EA8521591D0DED640F	text
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD5320.tmp\Content.inf **MD5:** 1A314B08BB9194A41E3794EF54017811 **SHA256:** 9025DD691FCAD181D5FD5952C7AA3728CD8A2CAF20DEA14930876419BED9B379	text
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD5329.tmp\rings.glox **MD5:** 6C24ED9C7C868DB0D55492BB126EAFF8 **SHA256:** 48AF17267AD75C142EFA7AB7525CA48FAB579592339FB93E92C4C4DA577D4C9F	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD532C.tmp\Content.inf **MD5:** 63E8B0621B5DEFE1EF17F02EFBFC2436 **SHA256:** 9243D99795DCDAD26FA857CB2740E58E3ED581E3FAEF0CB3781CBCD25FB4EE06	text
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD532B.tmp\Content.inf **MD5:** 69757AF3677EA8D80A2FBE44DEE7B9E4 **SHA256:** 0F14CA656CDD95CAB385F9B722580DDE2F46F8622E17A63F4534072D86DF97C3	text
1328	WINWORD.EXE	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\4C7F163ED126D5C3CB9457F68EC64E9E	binary

		MD5: AA19435EDE4656C3E74B668CC6877589 **SHA256:** E922EF4A390E4ADD161F106F4212CA97EEADC39D191D2C96A92ED81B8DBF512B	
1328	WINWORD.EXE	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\4C7F163ED126D5C3CB9457F68EC64E9E **MD5:** E8D6A85051DE11FFDA0620B26A6B5AC2 **SHA256:** A7B55AB168DAE196FD74C137326EAE7AAC8DB251BFBE404AB51B2C9E7B0A6556	binary
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD531E.tmp\Content.inf **MD5:** C1B36A0547FB75445957A619201143AC **SHA256:** 4DFF7D1CEF6DD85CC73E1554D705FA6586A1FBD10E4A73EEE44EAABA2D2FFED9	text
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD5328.tmp\Content.inf **MD5:** 877A8A960B2140E3A0A2752550959DB9 **SHA256:** FE07084A41CF7DB58B06D2C0D11BCACB603D6574261D1E7EBADCFF85F39AFB47	text
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD5321.tmp\APASixthEditionOfficeOnline.xsl **MD5:** 5632C4A81D2193986ACD29EADF1A2177 **SHA256:** 06DE709513D7976690B3DD8F5FDF1E59CF456A2DFBA952B97EACC72FE47B238B	xml
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD5322.tmp\gostname.xsl **MD5:** 9888A214D362470A6189DEFF775BE139 **SHA256:** C64ED5C2A323C00E84272AD3A701CAEBE1DCCEB67231978DE978042F09635FA7	xml
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD5329.tmp\Content.inf **MD5:** 2240CF2315F2EB448CEA6E9CE21B5AC5 **SHA256:** 0F7D0BD5A8CED523CFF4F99D7854C0EE007F5793FA9E1BA1CD933B0894BFBD0D	text
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD5320.tmp\BracketList.glox **MD5:** 5D9BAD7ADB88CEE98C5203883261ACA1 **SHA256:** 8CE600404BB3DB92A51B471D4AB8B166B566C6977C9BB63370718736376E0E2F	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD532B.tmp\PictureFrame.glox **MD5:** D32E93F7782B21785424AE2BEA62B387 **SHA256:** 2DC7E71759D84EF8BB23F11981E2C2044626FEA659383E4B9922FE5891F5F478	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD531F.tmp\Content.inf **MD5:** A6B2731ECC78E7CED9ED5408AB4F2931 **SHA256:** 6A2F9E46087B1F0ED0E847AF05C4D4CC9F246989794993E8F3E15B633EFDD744	text
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD5326.tmp\mlaseventheditionofficeonline.xsl **MD5:** 377B3E355414466F3E3861BCE1844976 **SHA256:** 4AC5B26C5E66E122DE80243EF621CA3E1142F643DD2AD61B75FF41CFEE3DFFAF	xml
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD532A.tmp\chicago.xsl **MD5:** 9AC6DE7B629A4A802A41F93DB2C49747 **SHA256:** 52984BC716569120D57C8E6A360376E9934F00CF31447F5892514DDCCF546293	xml
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD532A.tmp\Content.inf **MD5:** 4A9A2E8DB82C90608C96008A5B6160EF **SHA256:** 4FA948EEB075DFCB8DCA773A3F994560C69D275690953625731C4743CD5729F7	text
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD5322.tmp\Content.inf **MD5:** 8D9B02CC69FA40564E6C781A9CC9E626 **SHA256:** 1D4483830710EF4A2CC173C3514A9F4B0ACA6C44DB22729B7BE074D18C625BAE	text

1328	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\SmartArt Graphics\1033\TM03328932[[fn=Picture Frame]].glox **MD5:** D32E93F7782B21785424AE2BEA62B387 **SHA256:** 2DC7E71759D84EF8BB23F11981E2C2044626FEA659383E4B9922FE5891F5F478	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab53DA.tmp **MD5:** 1C12315C862A745A647DAD546EB4267E **SHA256:** 4E2E93EBAC4AD3F8690B020040D1AE3F8E7905AB7286FC25671E07AA0282CAC0	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\SmartArt Graphics\1033\TM03328940[[fn=Radial Picture List]].glox **MD5:** CDC1493350011DB9892100E94D5592FE **SHA256:** F637A67799B492FEFFB65632FED7815226396B4102A7ED790E0D9BB4936E1548	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\SmartArt Graphics\1033\TM03328916[[fn=Converging Text]].glox **MD5:** 8FDC5D57F2C6D4624F6ECFC56D3B8C06 **SHA256:** 2AFD4F0138B01758678036D0FAE8DC4A76402CB3256ABDCA7E40C23F5A2BA00D	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD5328.tmp\gb.xsl **MD5:** 51D32EE5BC7AB811041F799652D26E04 **SHA256:** 6230814BF5B2D554397580613E20681752240AB87FD354ECECF188C1EABE0E97	xml
1328	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\SmartArt Graphics\1033\TM03328990[[fn=Varying Width List]].glox **MD5:** 67766FF48AF205B771B53AA2FA82B4F4 **SHA256:** 160D05B4CB42E1200B859A2DE00770A5C9EBC736B70034AFC832A475372A1667	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD5326.tmp\Content.inf **MD5:** 333BA58FCE326DEA1E4A9DE67475AA95 **SHA256:** 66142D15C7325B98B199AB6EE6F35B7409DE64EBD5C0AB50412D18CBE6894097	text
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD5321.tmp\Content.inf **MD5:** C3216C3FC73A4B3FFFE7ED67153AB7B5 **SHA256:** 7CF1D6A4F0BE5E6184F59BFB1304509F38E480B59A3B091DBDC43B052D2137CB	text
1328	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\SmartArt Graphics\1033\TM03328998[[fn=Rings]].glox **MD5:** 6C24ED9C7C868DB0D55492BB126EAFF8 **SHA256:** 48AF17267AD75C142EFA7AB7525CA48FAB579592339FB93E92C4C4DA577D4C9F	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab53DC.tmp **MD5:** 828F96031F40BF8EBCB5E52AAEEB7E4C **SHA256:** 640AD075B555D4A2143F909EAFD91F54076F5DDE42A2B11CD897BC564B5D7FF7	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\SmartArt Graphics\1033\TM03328972[[fn=Tab List]].glox **MD5:** 8FDC5D57F2C6D4624F6ECFC56D3B8C06 **SHA256:** 2AFD4F0138B01758678036D0FAE8DC4A76402CB3256ABDCA7E40C23F5A2BA00D	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab53DB.tmp **MD5:** D4EAC009E9E7B64B8B001AE82B8102FA **SHA256:** 8B0631DA4DC79E036251379A0A68C3BA977F14BCC797BA0EB9692F8BB90DDB4D	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\SmartArt Graphics\1033\TM03328935[[fn=Picture Organization Chart]].glox **MD5:** 586CEBC1FAC6962F9E36388E5549FFE9 **SHA256:** 1595C0C027B12FE4C2B506B907C795D14813BBF64A2F3F6F5D71912D7E57BC40	compressed

1328	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\SmartArt Graphics\1033\TM03328893[[fn=BracketList]].glox **MD5:** 5D9BAD7ADB88CEE98C5203883261ACA1 **SHA256:** 8CE600404BB3DB92A51B471D4AB8B166B566C6977C9BB63370718736376E0E2F	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab53DD.tmp **MD5:** 748A53C6BDD5CE97BD54A76C7A334286 **SHA256:** 9AF92B1671772E8E781B58217DAB481F0AFBCF646DE36BC1BFFC7D411D14E351	compressed
1328	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab545B.tmp **MD5:** 65828DC7BE8BA1CE61AD7142252ACC54 **SHA256:** 849E2E915AA61E2F831E54F337A745A5946467D539CCBD0214B4742F4E7E94FF	compressed

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
75	83	32	1

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
1772	svchost.exe	GET	304	48.209.138.189:443	https://settings-win.data.microsoft.com/settings/v3.0/WSD/UpdateHealthTools?os=Windows&osVer=10.0.19041.1.amd64fre.vb_release.191206-&sku=48&deviceClass=Windows.Desktop&locale=en-US&deviceId=s:BAD99146-31D3-4EC6-A1A4-BE76F32BA5D4&sampleId=s:95271487&appVer=10.0.19041.3626&FlightRing=Retail&TelemetryLevel=1&HidOverGattReg=C%3A%5CWINDOWS%5CSystem32%5CDriverStore%5CFileRepository%5Chidbthle.inf_amd64_9610b4821fdf82a5%5CMicrosoft.Bluetooth.Profiles.HidOverGatt.dll&AppVer=&ProcessorIdentifier=AMD64%20Family%2023%20Model%201%20Stepping%202&OEMModel=DELL&UpdateOfferedDays=4294967295&ProcessorManufacturer=AuthenticAMD&InstallDate=1661339444&OEMModelBaseBoard=&BranchReadinessLevel=CB&OEMSubModel=J5CR&IsCloudDomainJoined=0&DeferFeatureUpdatePeriodInDays=30&IsDeviceRetailDemo=0&FlightingBranchName=&OSUILocale=en-US&DeviceFamily=Windows.Desktop&WuClientVer=10.0.19041.3996&UninstallActive=1&IsFlightingEnabled=0&OSSkuId=48&ProcessorClockSpeed=3094&TotalPhysicalRAM=6144&SecureBootCapable=0&App=SedimentPack&ProcessorCores=6&CurrentBranch=vb_release&InstallLanguage=en-US&DeferQualityUpdatePeriodInDays=0&OEMName_Uncleaned=DELL&TPMVersion=0&PrimaryDiskTotalCapacity=262144	US	—	—	whitelisted

					&InstallationType=Client&AttrDataVer=186&ProcessorModel=AMD%20Ryzen%205%203500%206-Core%20Processor&IsEdgeWithChromiumInstalled=1&OSVersion=10.0.19045.4046&IsMDMEnrolled=0&ActivationChannel=Retail&FirmwareVersion=A.40&TrendInstalledKey=1&OSArchitecture=AMD64&DefaultUserRegion=244&UpdateManagementGroup=2				
5276	MoUsoCoreWorker.exe	GET	200	23.216.77.42:80	http://crl.microsoft.com/pki/crl/products/MicRooCerAut2011_2011_03_22.crl	NL	binary	825 b	whitelisted
5276	MoUsoCoreWorker.exe	GET	200	23.52.181.212:80	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl	US	binary	814 b	whitelisted
—	—	GET	200	23.11.40.157:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTrjrydRyt%2BApF3GSPypfHBxR5XtQQUs9tIpPmhxdiuNkHMEWNpYim8S8YCEAjTxtAB8my1oj8MfWpz%2F7Y%3D	NL	binary	313 b	whitelisted
—	—	GET	200	204.79.197.203:80	http://oneocsp.microsoft.com/ocsp/MFQwUjBQME4wTDAJBgUrDgMCGgUABBQ3L3%2F%2Fa6ADK8NraY2GXzVaYrHG4AQUb6t%2B2v%2BXQ3LsO2d33oJhNYhHQoUCEzMAAAAGb6JMMcOVb6sAAAAAAAY%3D	US	binary	958 b	whitelisted
9108	svchost.exe	POST	200	20.190.159.2:443	https://login.live.com/RST2.srf	US	xml	1.24 Kb	whitelisted
9108	svchost.exe	POST	400	20.190.159.2:443	https://login.live.com/ppsecure/deviceaddcredential.srf	US	text	203 b	whitelisted
8608	SIHClient.exe	GET	304	74.178.76.128:443	https://slscr.update.microsoft.com/SLS/%7B522D76A4-93E1-47F8-B8CE-07C937AD1A1E%7D/x64/10.0.19045.4046/0?CH=686&L=en-US&P=&PT=0x30&WUA=10.0.19041.3996&MK=DELL&MD=DELL	US	—	—	whitelisted
8608	SIHClient.exe	GET	200	74.178.240.51:443	https://fe3cr.delivery.mp.microsoft.com/clientwebservice/ping	US	—	—	whitelisted
8608	SIHClient.exe	GET	200	74.178.76.128:443	https://slscr.update.microsoft.com/sls/ping	US	—	—	whitelisted
8608	SIHClient.exe	GET	304	74.178.76.128:443	https://slscr.update.microsoft.com/SLS/%7BE7A50285-D08D-499D-9FF8-180FDC2332BC%7D/x64/10.0.19045.4046/0?CH=686&L=en-US&P=&PT=0x30&WUA=10.0.19041.3996&MK=DELL&MD=DELL	US	—	—	whitelisted
9108	svchost.exe	POST	400	20.190.159.2:443	https://login.live.com/ppsecure/deviceaddcredential.srf	US	text	203 b	whitelisted
9108	svchost.exe	POST	400	20.190.159.2:443	https://login.live.com/ppsecure/deviceaddcredential.srf	US	text	203 b	whitelisted
9108	svchost.exe	GET	200	23.11.40.157:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEWVxDlQQUTiJUIBiV5uNu5g%2F6%2BrkS7QYXjzkCEAz1vQYrVgL0erhQLCPM8GY%3D	NL	binary	471 b	whitelisted

9108	svchost.exe	POST	400	20.190.159.2:443	https://login.live.com/ppsecure/deviceaddcredential.srf	US	text	203 b	whitelisted
4288	svchost.exe	POST	403	88.221.169.205:443	https://go.microsoft.com/fwlink/?LinkID=2257403&clcid=0x409	US	html	386 b	whitelisted
4288	svchost.exe	POST	403	88.221.169.205:443	https://go.microsoft.com/fwlink/?LinkID=2257403&clcid=0x409	US	html	386 b	whitelisted
4288	svchost.exe	POST	403	88.221.169.205:443	https://go.microsoft.com/fwlink/?LinkID=2257403&clcid=0x409	US	html	386 b	whitelisted
4288	svchost.exe	POST	403	88.221.169.205:443	https://go.microsoft.com/fwlink/?LinkID=2257403&clcid=0x409	US	html	386 b	whitelisted
4288	svchost.exe	POST	403	88.221.169.205:443	https://go.microsoft.com/fwlink/?LinkID=2257403&clcid=0x409	US	html	386 b	whitelisted
4288	svchost.exe	POST	403	88.221.169.205:443	https://go.microsoft.com/fwlink/?LinkID=2257403&clcid=0x409	US	html	386 b	whitelisted
4288	svchost.exe	POST	403	88.221.169.205:443	https://go.microsoft.com/fwlink/?LinkID=2257403&clcid=0x409	US	html	386 b	whitelisted
1328	WINWORD.EXE	GET	200	52.110.17.39:443	https://officeclient.microsoft.com/config16/?lcid=1033&syslcid=1033&uilcid=1033&build=16.0.16026&crev=3	US	xml	190 Kb	whitelisted
1328	WINWORD.EXE	GET	200	23.11.40.157:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEWVxDlQQUTiJUIBiV5uNu5g%2F6%2BrkS7QYXjzkCEAsMayxGaRewR3PGR9SvwMg%3D	NL	binary	471 b	whitelisted
1328	WINWORD.EXE	POST	200	52.110.17.73:443	https://roaming.svc.cloud.microsoft/rs/RoamingSoapService.svc	US	text	654 b	whitelisted
8608	SIHClient.exe	GET	200	88.221.169.152:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Product%20Root%20Certificate%20Authority%202018.crl	US	binary	420 b	whitelisted
1328	WINWORD.EXE	GET	200	52.123.243.222:443	https://ecs.office.com/config/v2/Office/word/16.0.16026.20146/Production/CC?&Clientid=%7bD61AB268-C26A-439D-BB15-2A0DEDFCA6A3%7d&Application=word&Platform=win32&Version=16.0.16026.20146&MsoVersion=16.0.16026.20002&SDX=fa000000002.2.0.1907.31003&SDX=fa000000005.1.0.1909.30011&SDX=fa000000006.1.0.1909.13002&SDX=fa000000008.1.0.1908.16006&SDX=fa000000009.1.0.1908.6002&SDX=fa000000016.1.0.1810.13001&SDX=fa000000029.1.0.1906.25001&SDX=fa000000033.1.0.1908.24001&SDX=wa104381125.1.0.1810.9001&ProcessName=winword.exe&Audience=Production&Build=ship&Architecture=x64&Language=en-US&SubscriptionLicense=false&PerpetualLicense=2019&LicenseCategory=6&LicenseSKU=Professional2019Retail&OsVersion=10.0&OsBuild=19045&Channel=CC&InstallType=C2R&	US	text	346 Kb	whitelisted

					SessionId=%7bD862C9AB-4DA6-4FD3-B3AE-4AC07704CB1B%7d&LabMachine=false				
8608	SIHClient.exe	GET	200	88.221.169.152:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Secure%20Server%20CA%202.1.crl	US	binary	407 b	whitelisted
1328	WINWORD.EXE	GET	200	23.216.77.174:443	https://omex.cdn.office.net/addinclassifier/officesharedentities	NL	text	314 Kb	whitelisted
9108	svchost.exe	POST	400	20.190.159.2:443	https://login.live.com/ppsecure/deviceaddcredential.srf	US	text	203 b	whitelisted
9108	svchost.exe	POST	400	20.190.159.2:443	https://login.live.com/ppsecure/deviceaddcredential.srf	US	text	203 b	whitelisted
1328	WINWORD.EXE	GET	200	52.111.236.4:443	https://messaging.engagement.office.com/campaignmetadataaggregator?app=0&platform=10&OFC_CHANNEL=CC&OFC_AUDIENCE=Production&OFC_FLIGHTS=ofsh6c2b1tla1a31%3Bofcrui4yvdulbf31%3Bofhpex3jznepoo31%3Bofpioygfqmufst31%3Bofjhlwlmoc1pz531&ver=16.0.16026.20002&hwid=04111-083-043729AED3&OSVersion=10.0.19045&country=US&locale=en-US&OFC_LICENSECATEGORY=6&OFC_LICENSESKU=Professional2019Retail&ContentType=CampaignContent	US	text	59 b	whitelisted
1328	WINWORD.EXE	POST	200	4.251.34.91:443	https://editor.svc.cloud.microsoft/NlEditor/CloudSuggest/V1	US	text	155 b	whitelisted
1328	WINWORD.EXE	GET	—	23.55.161.163:443	https://binaries.templates.cdn.office.net/support/templates/en-us/tp0309043001.cab	NL	—	—	whitelisted
9108	svchost.exe	POST	400	20.190.159.2:443	https://login.live.com/ppsecure/deviceaddcredential.srf	US	text	203 b	whitelisted
1328	WINWORD.EXE	GET	200	52.111.231.13:443	https://messaging.lifecycle.office.com/getcustommessage16?app=0&ui=en-US&src=BizBar&messagetype=BizBar&hwid=04111-083-043729&ver=16.0.16026&lc=en-US&platform=10%3A0%3A19045%3A2%3A0%3A0%3A256%3A1%3A&productid=%7B1717C1E0-47D3-4899-A6D3-1022DB7415E0%7D%3A00411-10830-43729-AA720%3AOffice%2019%2C%20Office19Professional2019R_Retail%20edition&clientsessionid=%7BD862C9AB-4DA6-4FD3-B3AE-4AC07704CB1B%7D&datapropertybag=%7B%22Audience%22%3A%22Production%22%2C%22AudienceGroup%22%3A%22Production%22%2C%22AudienceChannel%22%3A%22CC%22%2C%22Flight%22%3A%22ofsh6c2b1tla1a31%2Cofcrui4yvdulbf31%2Cofhpex3jznepoo31%2Cofpioygfqmufst31%2Cofjhlwlmoc1pz531%22%7D	US	text	542 b	whitelisted
9108	svchost.exe	POST	400	20.190.159.2:443	https://login.live.com/ppsecure/deviceaddcredential.srf	US	text	203 b	whitelisted
1328	WINWORD.EXE	POST	—	13.69.116.107:443	https://self.events.data.microsoft.com/OneCollector/1.0/	US	—	—	whitelisted

3280	svchost.exe	GET	200	88.221.169.152:80	http://www.microsoft.com/pkiops/crl/Microsoft%20Time-Stamp%20PCA%202010(1).crl	US	binary	814 b	whitelisted
1328	WINWORD.EXE	GET	200	104.102.63.189:443	https://fs.microsoft.com/fs/4.42/flatFontAssets.pkg	US	compressed	529 Kb	whitelisted
1328	WINWORD.EXE	POST	200	13.69.116.107:443	https://self.events.data.microsoft.com/OneCollector/1.0/	US	text	9 b	whitelisted
3280	svchost.exe	GET	200	88.221.169.152:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Signing%20CA%202.3.crl	US	binary	401 b	whitelisted
3280	svchost.exe	GET	200	88.221.169.152:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Signing%20CA%202.2.crl	US	binary	402 b	whitelisted
3280	svchost.exe	GET	200	2.16.241.19:80	http://crl.microsoft.com/pki/crl/products/MicRooCerAut_2010-06-23.crl	NL	binary	824 b	whitelisted
1328	WINWORD.EXE	GET	200	184.86.103.7:443	https://metadata.templates.cdn.office.net/client/templates/gallery?lcid=1033&syslcid=1033&uilcid=1033&app=0&ver=16&tl=2&build=16.0.16026&gtype=0%2C1%2C2%2C5%2C	NL	xml	10.5 Kb	whitelisted
1328	WINWORD.EXE	GET	—	23.55.161.163:443	https://binaries.templates.cdn.office.net/support/templates/en-us/tp0309043402.cab	NL	—	—	whitelisted
1328	WINWORD.EXE	GET	—	23.55.161.163:443	https://binaries.templates.cdn.office.net/support/templates/en-us/tp03328893.cab	NL	—	—	whitelisted
1328	WINWORD.EXE	GET	—	23.55.161.163:443	https://binaries.templates.cdn.office.net/support/templates/en-us/tp03328908.cab	NL	—	—	whitelisted
1328	WINWORD.EXE	GET	—	23.55.161.163:443	https://binaries.templates.cdn.office.net/support/templates/en-us/tp03328916.cab	NL	—	—	whitelisted
1328	WINWORD.EXE	GET	—	23.55.161.163:443	https://binaries.templates.cdn.office.net/support/templates/en-us/tp03328905.cab	NL	—	—	whitelisted
1328	WINWORD.EXE	GET	—	23.55.161.163:443	https://binaries.templates.cdn.office.net/support/templates/en-us/tp0345747501.cab	NL	—	—	whitelisted
1328	WINWORD.EXE	GET	—	23.55.161.163:443	https://binaries.templates.cdn.office.net/support/templates/en-us/tp0345748501.cab	NL	—	—	whitelisted
1328	WINWORD.EXE	GET	—	23.55.161.163:443	https://binaries.templates.cdn.office.net/support/templates/en-us/tp0345749601.cab	NL	—	—	whitelisted
1328	WINWORD.EXE	GET	—	23.55.161.163:443	https://binaries.templates.cdn.office.net/support/templates/en-us/tp0345749101.cab	NL	—	—	whitelisted
1328	WINWORD.EXE	GET	—	23.55.161.163:443	https://binaries.templates.cdn.office.net/support/templates/en-us/tp03328919.cab	NL	—	—	whitelisted

1328	WINWORD.EXE	GET	—	23.55.161.163:443	https://binaries.templates.cdn.office.net/support/templates/en-us/tp03328925.cab	NL	—	—	whitelisted
—	—	GET	—	2.16.241.19:80	http://crl.microsoft.com/pki/crl/products/microsoftrootcert.crl	NL	—	—	whitelisted
1328	WINWORD.EXE	GET	200	23.55.161.163:443	https://binaries.templates.cdn.office.net/support/templates/en-us/tp02851217.cab	NL	compressed	32.8 Kb	whitelisted
1328	WINWORD.EXE	GET	200	23.55.161.163:443	https://binaries.templates.cdn.office.net/support/templates/en-us/tp02851224.cab	NL	compressed	30.2 Kb	whitelisted
1328	WINWORD.EXE	GET	200	23.55.161.163:443	https://binaries.templates.cdn.office.net/support/templates/en-us/tp02851223.cab	NL	compressed	32.0 Kb	whitelisted
1328	WINWORD.EXE	GET	200	23.55.161.163:443	https://binaries.templates.cdn.office.net/support/templates/en-us/tp02851226.cab	NL	compressed	34.6 Kb	whitelisted
1328	WINWORD.EXE	GET	200	23.55.161.163:443	https://binaries.templates.cdn.office.net/support/templates/en-us/tp02851221.cab	NL	compressed	30.8 Kb	whitelisted
1328	WINWORD.EXE	GET	200	23.55.161.163:443	https://binaries.templates.cdn.office.net/support/templates/en-us/tp02851218.cab	NL	compressed	31.0 Kb	whitelisted
1328	WINWORD.EXE	GET	200	23.55.161.163:443	https://binaries.templates.cdn.office.net/support/templates/en-us/tp02851219.cab	NL	compressed	30.8 Kb	whitelisted
1328	WINWORD.EXE	GET	200	23.55.161.163:443	https://binaries.templates.cdn.office.net/support/templates/en-us/tp02851225.cab	NL	compressed	30.2 Kb	whitelisted
1328	WINWORD.EXE	GET	200	23.55.161.163:443	https://binaries.templates.cdn.office.net/support/templates/en-us/tp02851216.cab	NL	compressed	34.0 Kb	whitelisted
3280	svchost.exe	GET	200	88.221.169.152:80	http://www.microsoft.com/pkiops/crl/Microsoft%20Update%20Signing%20CA%202.2.crl	US	binary	813 b	whitelisted
3280	svchost.exe	GET	200	88.221.169.152:80	http://www.microsoft.com/pkiops/crl/Microsoft%20Update%20Signing%20CA%202.3.crl	US	binary	813 b	whitelisted
1328	WINWORD.EXE	GET	200	23.55.161.163:443	https://binaries.templates.cdn.office.net/support/templates/en-us/tp02851227.cab	NL	compressed	30.7 Kb	whitelisted
1328	WINWORD.EXE	GET	200	23.55.161.163:443	https://binaries.templates.cdn.office.net/support/templates/en-us/tp02851220.cab	NL	compressed	30.7 Kb	whitelisted
1328	WINWORD.EXE	GET	200	23.55.161.163:443	https://binaries.templates.cdn.office.net/support/templates/en-us/tp02851222.cab	NL	compressed	28.2 Kb	whitelisted
1328	WINWORD.EXE	GET	200	204.79.197.203:80	http://oneocsp.microsoft.com/ocsp/MFQwUjBQME4wTDAJBgUrDgMCGgUABBR0TBEVYklX7A9yLoLD9hqmCWDxFgQU3	US	binary	2.23 Kb	whitelisted

1328	WINWORD.EXE	GET	200	23.55.161.163:443	pGGSLehMVkx8UtfB6nciHnaqHYCEzMAAAAOQpOPJdxRqZs [illegible] templates.cdn.office.net/support/templates/en-us/tp02835233.cab	NL	compressed	45.3 Kb	whitelisted
1328	WINWORD.EXE	GET	200	23.55.161.163:443	https://binaries.templates.cdn.office.net/support/templates/en-us/tp01840907.cab	NL	compressed	42.6 Kb	whitelisted
1328	WINWORD.EXE	GET	200	23.55.161.163:443	https://binaries.templates.cdn.office.net/support/templates/en-us/tp03328884.cab	NL	compressed	21.4 Kb	whitelisted

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
4	System	192.168.100.255:137	—	Not routed	—	whitelisted
—	—	48.209.138.168:443	—	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
5276	MoUsoCoreWorker.exe	23.216.77.42:80	crl.microsoft.com	AKAMAI-ASN1	NL	whitelisted
5276	MoUsoCoreWorker.exe	23.52.181.212:80	www.microsoft.com	AKAMAI-AS	US	whitelisted
—	—	128.24.231.64:443	activation-v2.sls.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
1772	svchost.exe	48.209.138.168:443	—	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
5532	SearchApp.exe	92.123.104.66:443	www.bing.com	AKAMAI-ASN1	NL	whitelisted
—	—	23.11.40.157:80	ocsp.digicert.com	AKAMAI-AMS	NL	whitelisted
—	—	204.79.197.203:80	oneocsp.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
4	System	192.168.100.255:138	—	Not routed	—	whitelisted
9108	svchost.exe	20.190.159.2:443	login.live.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
9108	svchost.exe	23.11.40.157:80	ocsp.digicert.com	AKAMAI-AMS	NL	whitelisted
3428	svchost.exe	172.211.123.249:443	client.wns.windows.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
1772	svchost.exe	48.209.138.189:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
4288	svchost.exe	88.221.169.205:443	go.microsoft.com	AKAMAI-AS	US	whitelisted

1328	WINWORD.EXE	52.110.17.39:443	officeclient.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
1328	WINWORD.EXE	52.110.17.73:443	roaming.svc.cloud.microsoft	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
1328	WINWORD.EXE	52.123.243.222:443	ecs.office.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
1328	WINWORD.EXE	23.216.77.174:443	omex.cdn.office.net	AKAMAI-ASN1	NL	whitelisted
8608	SIHClient.exe	74.178.76.128:443	slscr.update.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
1328	WINWORD.EXE	23.11.40.157:80	ocsp.digicert.com	AKAMAI-AMS	NL	whitelisted
1328	WINWORD.EXE	204.79.197.203:80	oneocsp.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
8608	SIHClient.exe	88.221.169.152:80	www.microsoft.com	AKAMAI-AS	US	whitelisted
8608	SIHClient.exe	74.178.240.51:443	fe3cr.delivery.mp.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
1328	WINWORD.EXE	104.102.63.189:443	fs.microsoft.com	AKAMAI-AS	US	whitelisted
1328	WINWORD.EXE	52.111.236.4:443	messaging.engagement.office.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
1328	WINWORD.EXE	52.111.231.13:443	messaging.lifecycle.office.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
1328	WINWORD.EXE	4.251.34.91:443	editor.svc.cloud.microsoft	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
1328	WINWORD.EXE	13.69.116.107:443	self.events.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
3280	svchost.exe	88.221.169.152:80	www.microsoft.com	AKAMAI-AS	US	whitelisted
3280	svchost.exe	2.16.241.19:80	crl.microsoft.com	AKAMAI-ASN1	NL	whitelisted
1328	WINWORD.EXE	184.86.103.7:443	metadata.templates.cdn.office.net	AKAMAI-ASN1	NL	whitelisted
1328	WINWORD.EXE	23.55.161.163:443	binaries.templates.cdn.office.net	AKAMAI-ASN1	NL	whitelisted
1328	WINWORD.EXE	2.16.241.19:80	crl.microsoft.com	AKAMAI-ASN1	NL	whitelisted

DNS requests

Domain	IP	Reputation

self.events.data.microsoft.com	40.74.98.194 13.69.116.107	whitelisted
crl.microsoft.com	23.216.77.42 23.216.77.6 23.216.77.28 23.216.77.20 2.16.241.19 2.16.241.12	whitelisted
www.microsoft.com	23.52.181.212 88.221.169.152	whitelisted
activation-v2.sls.microsoft.com	128.24.231.64	whitelisted
www.bing.com	92.123.104.66 92.123.104.62 92.123.104.63 92.123.104.7 92.123.104.64 92.123.104.59 92.123.104.6 92.123.104.57 92.123.104.58	whitelisted
google.com	142.251.110.102 142.251.110.100 142.251.110.138 142.251.110.113 142.251.110.101 142.251.110.139	whitelisted
ocsp.digicert.com	23.11.40.157	whitelisted
oneocsp.microsoft.com	204.79.197.203	whitelisted
login.live.com	20.190.159.2 20.190.159.0 40.126.31.3 40.126.31.73 40.126.31.131 40.126.31.2 40.126.31.0	whitelisted

	20.190.159.64	
client.wns.windows.com	172.211.123.249	whitelisted
settings-win.data.microsoft.com	48.209.138.189	whitelisted
go.microsoft.com	88.221.169.205	whitelisted
officeclient.microsoft.com	52.110.17.39 52.110.17.64 52.110.17.63 52.110.17.68	whitelisted
roaming.svc.cloud.microsoft	52.110.17.73 52.110.17.49 52.110.17.67 52.110.17.39	whitelisted
ecs.office.com	52.123.243.222 52.123.243.78 52.123.243.205 52.123.243.87 52.123.243.213 52.123.224.69 52.123.243.73 52.123.243.206	whitelisted
omex.cdn.office.net	23.216.77.174 23.216.77.148 23.216.77.137 23.216.77.145	whitelisted
slscr.update.microsoft.com	74.178.76.128	whitelisted
fe3cr.delivery.mp.microsoft.com	74.178.240.51	whitelisted
fs.microsoft.com	104.102.63.189	whitelisted
messaging.engagement.office.com	52.111.236.4	whitelisted
messaging.lifecycle.office.com	52.111.231.13	whitelisted
editor.svc.cloud.microsoft	4.251.34.91	whitelisted

metadata.templates.cdn.office.net	184.86.103.7 184.86.103.22	whitelisted
binaries.templates.cdn.office.net	23.55.161.163 23.55.161.161	whitelisted

Threats

PID	Process	Class	Message
1772	svchost.exe	Unknown Traffic	ET USER_AGENTS Microsoft Dr Watson User-Agent (MSDW)

Debug output strings

Process	Message
WINWORD.EXE	WebView2: Failed to find an installed WebView2 runtime or non-stable Microsoft Edge installation.
WINWORD.EXE	WebView2: Failed to find an installed WebView2 runtime or non-stable Microsoft Edge installation.
WINWORD.EXE	WebView2: Failed to find an installed WebView2 runtime or non-stable Microsoft Edge installation.