



General Info

File name:	sample.doc
Full analysis:	https://app.any.run/tasks/ea9a0ed6-ca7b-4a76-a3c9-db7efbd6bb33
Verdict:	Malicious activity
Analysis date:	October 20, 2025 at 20:57:41
OS:	Windows 10 Professional (build: 19044, 64 bit)
Tags:	generated-doc cve-2022-30190 exploit
Indicators:	
MIME:	application/vnd.openxmlformats-officedocument.wordprocessingml.document
File info:	Microsoft Word 2007+
MD5:	52945AF1DEF85B171870B31FA4782E52
SHA1:	06727FFDA60359236A8029E0B3E8A0FD11C23313
SHA256:	4A24048F81AFBE9FB62E7A6A49ADB01FAF41F266B5F9FEECDCEB567AEC096784
SSDEEP:	192:AEHm7fIUU09264wptGheab8h7Z/c+8poF1d3jvvtl59rGxjPQDasYBcG7h+:AqWflz092hwLGAabkcfa7pr1lzyxjPQ9

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)
- CCleaner (6.20)
- FileZilla 3.65.0 (3.65.0)
- 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)
- 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)
- PowerShell 7-x64 (7.3.5.0)
- Update for Windows 10 for x64-based Systems (KB4023057) (2.59.0.0)

Hotfixes

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

- 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	SUSPICIOUS	INFO
CVE-2022-30190 detected <ul style="list-style-type: none">• WINWORD.EXE (PID: 7740)	No suspicious indicators.	An automatically generated document <ul style="list-style-type: none">• WINWORD.EXE (PID: 7740)

Malware configuration

No Malware configuration.

Static information

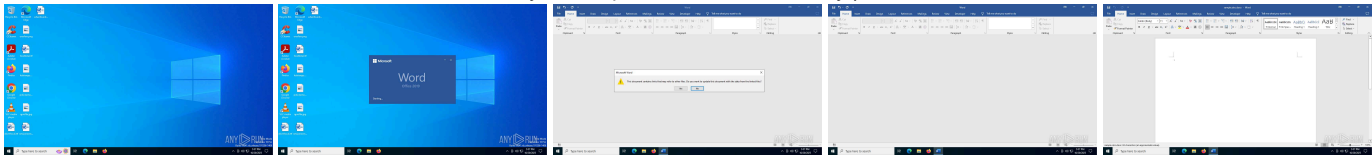
TRiD

- .docx | Word Microsoft Office Open XML Format document (52.2)
- .zip | Open Packaging Conventions container (38.8)
- .zip | ZIP compressed archive (8.8)

EXIF

ZIP	
ZipRequiredVersion:	20
ZipBitFlag:	-
ZipCompression:	Deflated
ZipModifyDate:	2022:05:26 23:08:14
ZipCRC:	0x6cd2a4df
ZipCompressedSize:	340
ZipUncompressedSize:	1312
ZipFileName:	[Content_Types].xml
XML	
Template:	Normal
TotalEditTime:	-
Pages:	1
Words:	-
Characters:	-
Application:	Microsoft Office Word
DocSecurity:	None
Lines:	-
Paragraphs:	-
ScaleCrop:	No
Company:	-
LinksUpToDate:	No
CharactersWithSpaces:	-
SharedDoc:	No
HyperlinksChanged:	No
AppVersion:	16
Keywords:	-
LastModifiedBy:	KIS2
RevisionNumber:	3
CreateDate:	2022:05:25 13:14:00Z
ModifyDate:	2022:05:25 13:14:00Z
XMP	
Title:	-
Subject:	-
Creator:	KIS2
Description:	-

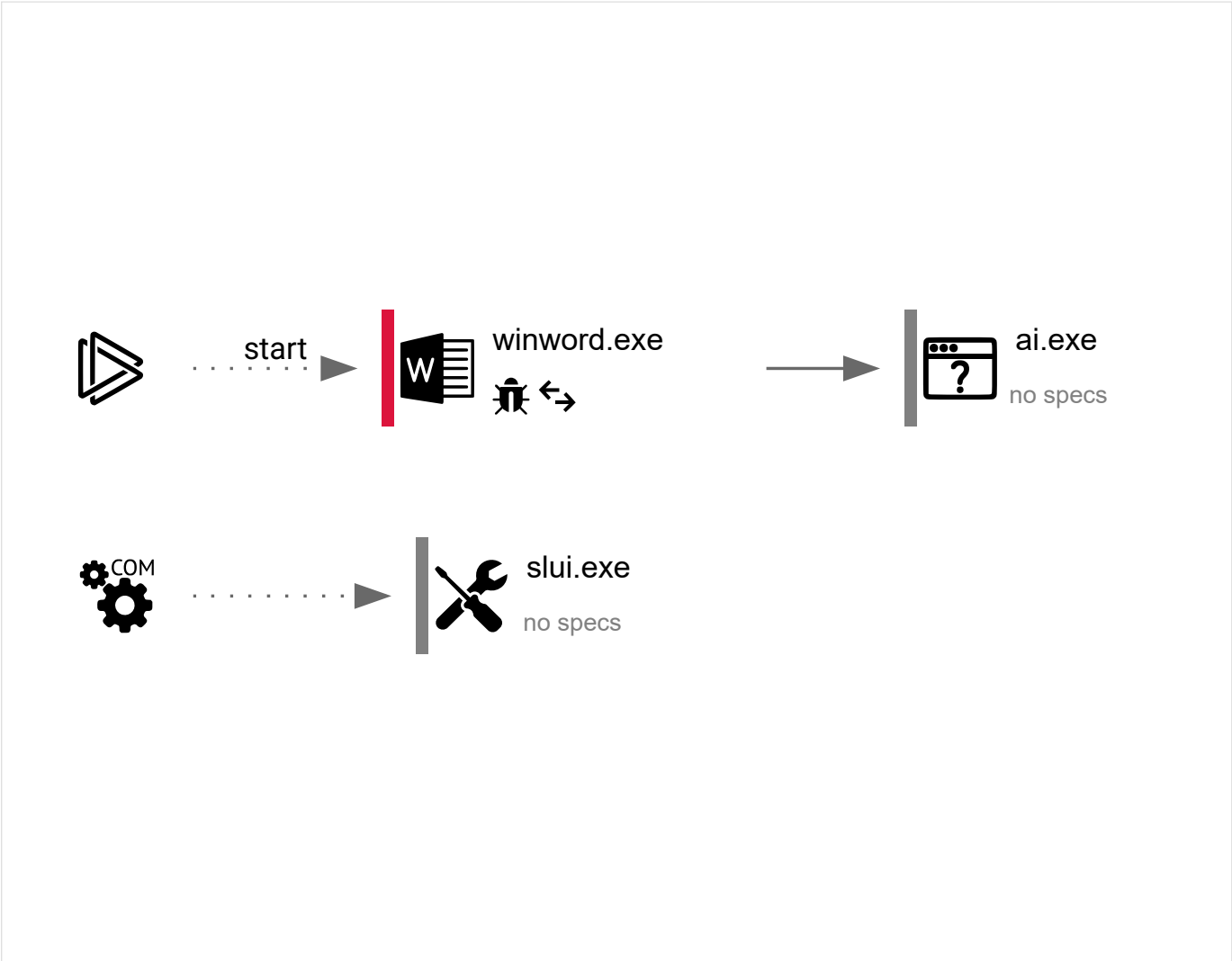
Video and screenshots



Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
147	3	1	0

Behavior graph



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

Process information

PID	CMD	Path	Indicators	Parent process
796	C:\WINDOWS\System32\slui.exe -Embedding	C:\Windows\System32\slui.exe	—	svchost.exe
Information				
User: admin		Company: Microsoft Corporation		
Integrity Level: MEDIUM		Description: Windows Activation Client		
Version: 10.0.19041.1 (WinBuild.160101.0800)				

1584

"C:\Program Files\Microsoft Office\root\VFS\ProgramFilesCommonX64\Microsoft Shared\OFFICE16\ai.exe" "F00A4B91-357D-4531-B3BA-0F5F19170409" "4C20B05C-7ACD-47A6-B421-E389BB6966F5" "7740"

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

7740

"C:\Program Files\Microsoft Office\Root\Office16\WINWORD.EXE" /n C:\Users\admin\AppData\Local\Temp\sample.doc.docx /o ""

C:\Program Files\Microsoft Office\root\Office16\WINWORD.EXE



explorer.exe

Information

User:

admin

Company:

Microsoft Corporation

Integrity Level:

MEDIUM

Description:

Microsoft Word

Version:

16.0.16026.20146

Registry activity

Total events	Read events	Write events	Delete events
15 279	14 936	322	21

Modification events

(PID) Process:	(7740) WINWORD.EXE	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Word\Resiliency\StartupItems
Operation:	write	Name:	?z-
Value:	3F7A2D003C1E00000100000000000000CC092908EB41DC0100000000		

(PID) Process:	(7740) WINWORD.EXE	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common
Operation:	write	Name:	SessionId
Value:	66F69639AA2AEA409BC52962E5E9A540		

(PID) Process:	(7740) WINWORD.EXE	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	Name:	ProxyBypass
Value:	1		

(PID) Process:	(7740) WINWORD.EXE	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	Name:	IntranetName
Value:	1		

(PID) Process:	(7740) WINWORD.EXE	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	Name:	UNCAsIntranet
Value:	1		

(PID) Process:	(7740) WINWORD.EXE	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	Name:	AutoDetect
Value:	0		

(PID) Process:	(7740) 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\821E54C0-B244-4330-91FD-30145CBE6EE6		

(PID) Process:	(7740) 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:	A09A7708EB41DC01		

(PID) Process:	(7740) 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:	A05AE135B442DC01		

(PID) Process:	(7740) WINWORD.EXE	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Word\AddinsData\Genko.Connect12
Operation:	write	Name:	LoadCount
Value:	5		

(PID) Process:	(7740) WINWORD.EXE	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\ClientTelemetry\Sampling
Operation:	write	Name:	0
Value:	017012000000001000B24E9A3E020000000000000600000000000000		

(PID) Process:	(7740) WINWORD.EXE	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\CrashPersistence\WINWORD\7740
Operation:	write	Name:	0

Value: 0B0E107E7A9C59EAA7124AAA0378B8202E4D5723004681C687D9B0BD90EE016A04102400449A7D64829D01008500A907556E6B6E6F776EC906022222CA0DC2190000C91003783634C511BC3CD2120B770069006E0077006F00720064002E00650078006500C51620C517808004C91808323231322D44656300			
(PID) Process:	(7740) WINWORD.EXE	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages
Operation:	write	Name:	en-US
Value:	2		
(PID) Process:	(7740) WINWORD.EXE	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages
Operation:	write	Name:	de-de
Value:	2		
(PID) Process:	(7740) WINWORD.EXE	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages
Operation:	write	Name:	fr-fr
Value:	2		
(PID) Process:	(7740) WINWORD.EXE	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages
Operation:	write	Name:	es-es
Value:	2		
(PID) Process:	(7740) WINWORD.EXE	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages
Operation:	write	Name:	it-it
Value:	2		
(PID) Process:	(7740) WINWORD.EXE	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages
Operation:	write	Name:	ja-jp
Value:	2		
(PID) Process:	(7740) WINWORD.EXE	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages
Operation:	write	Name:	ko-kr
Value:	2		
(PID) Process:	(7740) WINWORD.EXE	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages
Operation:	write	Name:	pt-br
Value:	2		
(PID) Process:	(7740) WINWORD.EXE	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages
Operation:	write	Name:	ru-ru
Value:	2		
(PID) Process:	(7740) WINWORD.EXE	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages
Operation:	write	Name:	tr-tr
Value:	2		
(PID) Process:	(7740) WINWORD.EXE	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages
Operation:	write	Name:	en-US
Value:	1		
(PID) Process:	(7740) WINWORD.EXE	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages
Operation:	write	Name:	de-de
Value:	1		
(PID) Process:	(7740) WINWORD.EXE	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages
Operation:	write	Name:	es-es
Value:	1		
(PID) Process:	(7740) WINWORD.EXE	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages
Operation:	write	Name:	fr-fr
Value:	1		
(PID) Process:	(7740) WINWORD.EXE	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages
Operation:	write	Name:	it-it
Value:	1		
(PID) Process:	(7740) WINWORD.EXE	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages
Operation:	write	Name:	ja-jp
Value:	1		
(PID) Process:	(7740) WINWORD.EXE	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages
Operation:	write	Name:	ko-kr
Value:	1		
(PID) Process:	(7740) WINWORD.EXE	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages
Operation:	write	Name:	pt-br
Value:	1		
(PID) Process:	(7740) WINWORD.EXE	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages
Operation:	write	Name:	ru-ru
Value:	1		
(PID) Process:	(7740) WINWORD.EXE	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LanguageResources\EnabledEditingLanguages

<https://any.run/report/4a24048f81afbe9fb62e7a6a49adbd1faf41f266b5f9feecdceb567aec096784/ea9a0ed6-ca7b-4a76-a3c9-db7efbd6bb33> 7/87

[illegible]

<https://any.run/report/4a24048f81afbe9fb62e7a6a49adbd1faf41f266b5f9feecdceb567aec096784/ea9a0ed6-ca7b-4a76-a3c9-db7efbd6bb33> 10/87

<https://any.run/report/4a24048f81afbe9fb62e7a6a49adbd1faf41f266b5f9feecdceb567aec096784/ea9a0ed6-ca7b-4a76-a3c9-db7efbd6bb33>

<https://any.run/report/4a24048f81afbe9fb62e7a6a49adbd1faf41f266b5f9feecdceb567aec096784/ea9a0ed6-ca7b-4a76-a3c9-db7efbd6bb33> 12/87

[illegible]

[illegible][illegible]

[illegible]

(PID) Process:	(7740) WINWORD.EXE	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation:	write	Name:	1.11

[illegible]

[illegible][illegible]

(PID) Process:	(7740) WINWORD.EXE	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation:	write	Name:	1.14
Value:	737472696E77C7B205C22537562A4E616D657370616365735C22203A207B205C225363656E7172696F5C22203A207B205C224576656E74735C22203A207B205C2255706461746555461736B557064617465546574656374696F6E6325C22203A207B205C224576656E74466C61675C22203A2032207D2C205C22496E7374616C6C5461736B466F6E74735C22203A207B205C224576656E		

<https://any.run/report/4a24048f81afbe9fb62e7a6a49adbd1faf41f266b5f9feecdceb567aec096784/ea9a0ed6-ca7b-4a76-a3c9-db7efbd6bb33>

[illegible]

<https://any.run/report/4a24048f81afbe9fb62e7a6a49adbd1faf41f266b5f9feecdceb567aec096784/ea9a0ed6-ca7b-4a76-a3c9-db7efbd6bb33> 24/87

(PID) Process:	(7740) WINWORD.EXE	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation:	write	Name:	ChunkCount
Value:	uint64_t[20]		

[illegible]

[illegible]

```
(PID) Process: (7740) WINWORD.EXE      Key: HKKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write                        Name: ChunkCount
Value: uint64_t121

(PID) Process: (7740) WINWORD.EXE      Key: HKKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write                        Name: 1.22
Value: 645C22203A207B205C224576656E74466C61675C22203A2031207D2C205C225061737465496D616765496E76616C696446696C655C22203A207B205C224576656E74466C61675C22203A2
031207D2C205C2246696C654F70656E486F7374546F74AD616E7952657175657374756C22203A207B205C224576656E74466C61675C22203A2031207D2C205C225472616E736974696F6E4
E0F6E4D6574726F3A616E46F74436F766572745C2203A207B205C224576656E74466C61675C22203A2031207D2C205C22556E7375707674726F74656446656174757265734770656E496E
4465736B7465736C22203A207B205C224576656E74466C61675C22203A2031207D2C205C22556E6B6E6F776E35343630338375C22203A207B205C224576656E74466C61675C22203A2031
207D2C205C22424245787465726616C57F72B626F6E6B4C696E6B7344697361626C65645C2203A207B205C224576656E74466C61675C22203A2031207D2C205C22424576657375707
6F7274656446656E74757265736C22203A207B205C224576656E74466C61675C22203A2031207D2C205C2257726F6E67576F726B626F6E6B50617373776F72645C22203A207B205C224576
656E74466C61675C22203A2031207D2C205C2246696C654F70656E486F73745637276696365556E617661696C61626C655C2203A207B205C224576656E74466C61675C22203A2031207D
2C205C22556E6B6E6F776E353437336363535C22203A207B205C224576656E74466C61675C22203A2031207D2C205C22446973636F74696E756F757353656C656374696E6E426C6F36B
696E675C22203A207B205C224576656E74466C61675C22203A2031207D2C205C22456373466F7441363650707452657175657374735C22203A207B205C224576656E74466C61675C22203A2
031207D2C205C224563734F7547664D656D6F72795C22203A207B205C224576656E74466C61675C22203A2031207D2C205C22556E6B6E6F776E35343831737535C22203A207B205C22
4576656E74466C61675C22203A2031207D2C205C22461696436F674656E7453697A655A65726F46696C654F70656E4572726F725C22203A207B205C224576656E74466C61675C22203A2031
2031207D2C205C22456373436F6D6756E69636174696F6E4C6F774C65766564C5472726F725C22203A207B205C224576656E74466C61675C22203A2031207D2C205C2245347261736844
7572696E67426F6745C22203A207B205C224576656E74466C61675C22203A2031207D2C205C224F7065726174696F6E517565755646756C656E6B6E6F726F726F725C22203A207B205C224576656E74466C6167
5C22203A2031207D2C205C22556E6B6E6F776E353437313435315C22203A207B205C224576656E74466C61675C22203A2031207D2C205C225656226E6B6E6F776E35343838731385C22203A20
7B205C224576656E74466C61675C22203A2031207D2C205C22496E7344656C43656C673509766F745461626C655C22203A207B205C224576656E74466C61675C22203A2031207D2C205
C22496E7344656C43656C673526F7773466F7272686F6C65436F6756D6E5C2203A207B205C2247656E74466C61675C22203A2031207D2C205C225368656744F70734636F6E669726
D44656C6574655C22203A207B205C224576656E74466C61675C22203A2031207D2C205C22556E6B6E6F776E353437353531345C22203A207B205C224576656E74466C61675C22203A2031
207D2C205C224696C654F70656E41636356737344656E69564475655446753657372697475936577474696E67735C22203A207B205C224576656E74466C61675C22203A2031207D2C20
5C224167367469766174654C6F63616C58746F726167655C22203A207B205C224576656E74466C61675C22203A2031207D2C205C2242425787465726E16C57F726B626F6E6B4C696E6B73
53686F774572726F725C22203A207B205C2247656E74466C61675C22203A2031207D2C205C2256E6B6E6F776E3534373130395C22203A207B205C224576656E74466C61675C22203A2031
2031207D2C205C224F6C6170536368656D614661696C5C22203A207B205C224576656E74466C61675C22203A2031207D2C205C225069766F745461626C65436F6E746578744D656E754F76
65726174696E6E4661696C7572655C22203A207B205C224576656E74466C61675C22203A2031207D2C205C22536865657450726F74656374696F6E4572726F725C22203A207B205C224576
656E74466C61675C22203A2031207D2C205C22461696C65446F46E17669676174655C22203A207B205C224576656E74466C61675C22203A2031207D2C205C223A316E76617312565E64
6572696E674661696C7572655C22203A207B205C224576656E74466C61675C22203A2031207D2C205C224661696C656454F652656726573685C22203A207B205C224576656E74466C6167
5C22203A2031207D2C205C22536C696365446F776E6C6F1644661696C65645C22203A207B205C224576656E74466C61675C22203A2031207D2C205C22496E7616C69644661636865654656
6965773656737369F6E5C22203A207B205C224576656E74466C61675C22203A2031207D2C205C2257365724F75744F64656D6F7279447572696E675365737369F6E6E6F726F726F725C22203A207B20
5C224576656E74466C61675C2
```


[illegible]

(PID) Process: (7740) 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:	(7740) WINWORD.EXE	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation:	write	Name:	ChunkCount

<https://any.run/report/4a24048f81afbe9fb62e7a6a49adb1faf41f266b5f9feecdceb567aec096784/ea9a0ed6-ca7b-4a76-a3c9-db7efbd6bb33> 32/87

(PID) Process: (7740) WINWORD.EXE	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write	Name: ChunkCount
Value: uint64_t[28]	

<https://any.run/report/4a24048f81afbe9fb62e7a6a49adbd1faf41f266b5f9feecdceb567aec096784/ea9a0ed6-ca7b-4a76-a3c9-db7efbd6bbb33> 33/87

[illegible]

[illegible][illegible]

[illegible]

[illegible]

<https://any.run/report/4a24048f81afbe9fb62e7a6a49adbd1faf41f266b5f9feecdceb567aec096784/ea9a0ed6-ca7b-4a76-a3c9-db7efbd6bb33>

[illegible]

[illegible][illegible]

[illegible][illegible]

<https://any.run/report/4a24048f81afbe9fb62e7a6a49adbd1faf41f266b5f9feecdceb567aec096784/ea9a0ed6-ca7b-4a76-a3c9-db7efbd6bb33> 44/87

[illegible]

<https://any.run/report/4a24048f81afbe9fb62e7a6a49adbd1faf41f266b5f9feecdceb567aec096784/ea9a0ed6-ca7b-4a76-a3c9-db7efbd6bb33> 46/87

[illegible]

7446656465721746554496465674697475222203A207B205C224576565E74466C61675C22203A203107D2C205C224676565E6978456E7469746C656D656E7446657463685C22203A207B205C224576656E74466C61675C22203A203107D2C205C224672656E697853966E656E74543576236726970474696F6E41637469766174696F6E5C22203A207B205C224576656E74466C61675C22203A203107D2C205C224672656E697853966E656E745375627363726970474696F6E41637469766174696F6E466C6F75C22203A207B205C224576656E74466C61675C22203A203107D2C205C22466972737452756E4787056726956563655C22203A207B205C224576656E74466C61675C22203A203107D2C205C22456D1696C4164642765373557361765496E5369676E496E526571756573745C22203A207B205C224576656E74466C61675C22203A203107D2C205C22557361765496E5369676E496E526571756573745C22203A207B205C224576656E697849674637416C6C057676696E655C22203A207B205C224576656E74466C61675C22203A203107D2C205C2245D5434175746850726F6D70454656656D657472795C22203A207B205C224576656E74466C61675C22203A203107D2C205C224F4944557361765496E5369676E496E526571756573745C22203A207B205C224576656E74466C61675C22203A203107D2C205C22476574436F6666967546F6B865E466F74964656746974795C22203A207B205C224576656E74466C61675C22203A203107D2C205C224F4944557361765496E5369676E496E526571756573745C22203A207B205C224576656E74466C61675C22203A203107D2C205C224144546F6B865E4173796E63506572665C22203A207B205C224576656E74466C61675C22203A203107D2C205C224164644163636F756E744661696C7572655C22203A207B205C224576656E74466C61675C22203A203107D2C205C225375624E16D65737061363573C22203A207B205C224F49363547726F750735C22203A207B205C224576656E74735C22203A207B205C225375636367373667565245534526571756573745C22203A207B205C224576656E74466C61675C22203A203107D2C205C22455345265717565737473575636357373526174655C22203A207B205C224576656E74735C22203A207B205C22763525C22203A207B205C224576656E74466C61675C22203A203107D2C205C225254535447726F72737697468457276F74736F6E74656E745C22203A207B205C224576656E74735C22203A207B205C22276325C22203A207B205C224576656E74466C61675C22203A203107D2C205C224163636F756E74735C22203A207B205C224576656E74735C22203A203107D2C205C224175746850726F6D70454656656D657472795C22203A207B205C224576656E74466C61675C22203A203107D2C205C224F4944557361765496E5369676E496E526571756573745C22203A207B205C224576656E74466C61675C22203A203107D2C205C224672656E697853966E656E74543576236726970474696F6E41637469766174696F6E5C22203A207B205C224576656E74466C61675C22203A203107D2C205C224672656E697853966E656E745375627363726970474696F6E41637469766174696F6E466C6F75C22203A207B205C224576656E74466C61675C22203A203107D2C205C22466972737452756E4787056726956563655C22203A207B205C224576656E74466C61675C22203A203107D2C205C22456D1696C4164642765373557361765496E5369676E496E526571756573745C22203A207B205C224576656E74466C61675C22203A203107D2C205C22557361765496E5369676E496E526571756573745C22203A207B205C224576656E697849674637416C6C057676696E655C22203A207B205C224576656E74466C61675C22203A203107D2C205C2245D5434175746850726F6D70454656656D657472795C22203A207B205C224576656E74466C61675C22203A203107D2C205C224F4944557361765496E5369676E496E526571756573745C22203A207B205C224576656E74466C61675C22203A203107D2C205C224144546F6B865E4173796E63506572665C22203A207B205C224576656E74466C61675C22203A203107D2C205C224164644163636F756E744661696C7572655C22203A207B205C224576656E74466C61675C22203A203107D2C205C225375624E16D65737061363573C22203A207B205C224F49363547726F750735C22203A207B205C224576656E74735C22203A207B205C225375636367373667565245534526571756573745C22203A207B205C224576656E74466C61675C22203A203107D2C205C22455345265717565737473575636357373526174655C22203A207B205C224576656E74735C22203A207B205C22763525C22203A207B205C224576656E74466C61675C22203A203107D2C205C225254535447726F72737697468457276F74736F6E74656E745C22203A207B205C224576656E74735C22203A207B205C22276325C22203A207B205C224576656E74466C61675C22203A203107D2C205C224163636F756E74735C22203A207B205C224576656E74735C22203A203107D2C205C224175746850726F6D70454656656D657472795C22203A207B205C224576656E74466C61675C22203A203107D2C205C224F4944557361765496E5369676E496E526571756573745C22203A207B205C224576656E74466C61675C22203A203107D2C205C224672656E697853966E656E74543576236726970474696F6E41637469766174696F6E5C22203A2

[illegible]

[illegible]

[illegible]

(PID) Process: (7740) WINWORD.EXE	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write	Name: ChunkCount
Value: uint64_t[50]	

Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData

Name: 1.51

(PID) Process: (7740) WINWORD.EXE	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write	Name: ChunkCount
Value: uint64_t[51]	

Operation:	write	Name:	1.52
------------	-------	-------	------

[illegible]

[illegible][illegible]

[illegible]

[illegible]

(PID) Process:

(7740) WINWORD.EXE

Operation:

write

Value:

uint64_t[56]

(PID) Process:

(7740) WINWORD.EXE

Operation:

write

Key:

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Experiment\Configs\Ecs\word\ConfigContextData

Name:

1.57

Value:

675C2220A2031207D2C205C22436F726556697375616C6C795265616479536C6F775C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22576F7069546F68656E526566726573684661696C6564466F72629664656E5C2220A207B205C224576656E74466C61675C2220A2031207D2C205C224C6F6164476566572696356697275735C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22456D70747950617374655C2220A207B205C224576656E74466C61675C2220A2031207D2C205C224869768366976874496E74657266616C4572726F725C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22466F6164416371756972654C6F6368566737065636966696564661696C7572655C2220A3207B205C224576656E74466C61675C2220A2031207D2C205C224C6F61644765665726963466F74417077267F7026917465646616967572655C2220A207B205C224576656E74466C61675C2220A2031207D2C205C2235672436C696368656452657472794F70655E496E4465736B746F705C2220A207B205C224576656E74466C61675C2220A2031207D2C205C2576F7069546F68656E52656726573684661696C6564566E1754686F72697A65645C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22576F72645265706C69636174696F6E486F73744E6574776F726B436F6E6663744661696C7572655C2220A207B205C224576656E74466C61675C2220A2031207D2C205C224C6F6164496E76616C69645840AC447572696E6F74E6F726D616C697A6174696F6E5C2220A207B205C224576656E74466C61675C2220A2031207D2C205C224C6F6164486F73744E6574776F726B436F6E6E563744661696C7572655C2220A207B205C224576656E74466C61675C2220A2031207D2C205C224C6F616446C6F636B5626571756573744661696C65C2220A207B205C224576656E74466C61675C2220A2031207D2C205C224696C65506963686572426F6F744661696C65645C2220A207B205C224576656E74466C61675C2220A2031207D2C205C224C6F6164486F73744E6574776F726B5265717565737446616E63656C65645C2220A207B205C224576656E74466C61675C2220A2031207D2C205C2254696D656F75745C2220A207B205C224576656E74466C61675C2220A2031207D2C205C2243616E6E6F74526706C69636174654772617068556E65787065374656496E76616C69644DF64656C5C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22576F72645265706C69636174696F6E486F73744E6574776F726B5265717565737443616E63656C65645C2220A207B205C224576656E74466C61675C2220A2031207D2C205C224617650616E6557064617465416374696F6E4661696C7572655C2220A207B205C224576656E74466C61675C2220A2031207D2C205C224368616E657654757473696454368172466F736974696F6E5C2207B205C224576656E74466C61675C2220A2031207D2C205C22566B6E6F776E313043535C2220A207B205C224576656E74466C61675C2220A2031207D2C205C224666696365426F6F7374737476176C1705724E6F744C6F616465645C2220A207B205C224576656E74466C61675C2220A2031207D2C205C2246E1766967617465564F41637469766974794661696C65645C2220A207B205C22456656E74466C61675C2220A2031207D2C205C2256726F6D57F70694661696C7572655C2220A207B205C224576656E74466C61675C2220A2031207D2C205C224C6F6164477657443656C6F734D697373696E6746696C6549645C2220A207B205C224576656E74466C61675C2220A2031207D2C205C224C6F6164486F73744E6574776F726B5365637572654368616E6E656C4661696C7572655C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22566B6E6F776E31303531696C2220A207B205C224576656E74466C61675C2220A2031207D2C205C225669735616C6C795265616479536C6F726726F6D55736572436C6963685C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22436F6D6B656E74472656174696F6E4661696C65645C2220A207B205C224576656E74466C61675C2220A2031207D2C205C224E65737465645461626C65466F756E645C2220A207B205C224576656E74466C61675C2220A2031207D2C205C2247261706869636496E76616C69645C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22466F76616C696443686172466F736974696F6E5C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22446776E6C6F616447667696E616C55726C4661696C65645C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22496E76616C69645465787452616E67655C2220A207B205C224576656E74466C61675C2220A2031207D2C205C224576656E74466C61675C2220A2031207D2C205C22446F776E6C6F61645069637475726546726F6D486F73744661696C65645C2220A207B205C224576656E74466C61675C2220A2031207D2C205C2253686172654496F16C6F748616E46C65672486F7374526706F72746564661696C7572655C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22466176654368616E6E656C45C2220A207B205C224576656E74466C61675C2220A2031207D2C205C2256726F6D57F70694661696C7572655C2220A207B205C224576656E74466C61675C2220A2031207D2C205C224C6F6164477657443656C6F734D697373696E6746696C6549645C2220A207B205C224576656E74466C61675C2220A2031207D2C205C224C6F6164486F73744E6574776F726B5365637572654368616E6E656C4661696C7572655C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22566B6E6F776E31303531696C2220A207B205C224576656E74466C61675C2220A2031207D2C205C225669735616C6C795265616479536C6F726726F6D55736572436C6963685C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22436F6D6B656E74472656174696F6E4661696C65645C2220A207B205C224576656E74466C61675C2220A2031207D2C205C224E65737465645461626C65466F756E645C2220A207B205C224576656E74466C61675C2220A2031207D2C205C2247261706869636496E76616C69645C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22466F76616C696443686172466F736974696F6E5C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22446776E6C6F616447667696E616C55726C4661696C65645C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22496E76616C69645465787452616E67655C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22446F776E6C6F61645069637475726546726F6D486F73744661696C65645C2220A207B205C224576656E74466C61675C2220A2031207D2C205C2253686172654496F16C6F748616E46C65672486F7374526706F72746564661696C7572655C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22466176654368616E6E656C45C2220A207B205C224576656E74466C61675C2220A2031207D2C205C2256726F6D57F70694661696C7572655C2220A207B205C224576656E74466C61675C2220A2031207D2C205C224C6F6164477657443656C6F734D697373696E6746696C6549645C2220A207B205C224576656E74466C61675C2220A2031207D2C205C224C6F6164486F73744E6574776F726B5365637572654368616E6E656C4661696C7572655C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22566B6E6F776E31303531696C2220A207B205C224576656E74466C61675C2220A2031207D2C205C225669735616C6C795265616479536C6F726726F6D55736572436C6963685C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22436F6D6B656E74472656174696F6E4661696C65645C2220A207B205C224576656E74466C61675C2220A2031207D2C205C224E65737465645461626C65466F756E645C2220A207B205C224576656E74466C61675C2220A2031207D2C205C2247261706869636496E76616C69645C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22466F76616C696443686172466F736974696F6E5C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22446776E6C6F616447667696E616C55726C4661696C65645C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22496E76616C69645465787452616E67655C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22446F776E6C6F61645069637475726546726F6D486F73744661696C65645C2220A207B205C224576656E74466C61675C2220A2031207D2C205C2253686172654496F16C6F748616E46C65672486F7374526706F72746564661696C7572655C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22466176654368616E6E656C45C2220A207B205C224576656E74466C61675C2220A2031207D2C205C2256726F6D57F70694661696C7572655C2220A207B205C224576656E74466C61675C2220A2031207D2C205C224C6F6164477657443656C6F734D697373696E6746696C6549645C2220A207B205C224576656E74466C61675C2220A2031207D2C205C224C6F6164486F73744E6574776F726B5365637572654368616E6E656C4661696C7572655C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22566B6E6F776E31303531696C2220A207B205C224576656E74466C61675C2220A2031207D2C205C225669735616C6C795265616479536C6F726726F6D55736572436C6963685C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22436F6D6B656E74472656174696F6E4661696C65645C2220A207B205C224576656E74466C61675C2220A2031207D2C205C224E65737465645461626C65466F756E645C2220A207B205C224576656E74466C61675C2220A2031207D2C205C2247261706869636496E76616C69645C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22466F76616C696443686172466F736974696F6E5C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22446776E6C6F616447667696E616C55726C4661696C65645C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22496E76616C69645465787452616E67655C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22446F776E6C6F61645069637475726546726F6D486F73744661696C65645C2220A207B205C224576656E74466C61675C2220A2031207D2C205C2253686172654496F16C6F748616E46C65672486F7374526706F72746564661696C7572655C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22466176654368616E6E656C45C2220A207B205C224576656E74466C61675C2220A2031207D2C205C2256726F6D57F70694661696C7572655C2220A207B205C224576656E74466C61675C2220A2031207D2C205C224C6F6164477657443656C6F734D697373696E6746696C6549645C2220A207B205C224576656E74466C61675C2220A2031207D2C205C224C6F6164486F73744E6574776F726B5365637572654368616E6E656C4661696C7572655C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22566B6E6F776E31303531696C2220A207B205C224576656E74466C61675C2220A2031207D2C205C225669735616C6C795265616479536C6F726726F6D55736572436C6963685C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22436F6D6B656E74472656174696F6E4661696C65645C2220A207B205C224576656E74466C61675C2220A2031207D2C205C224E65737465645461626C65466F756E645C2220A207B205C224576656E74466C61675C2220A2031207D2C205C2247261706869636496E76616C69645C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22466F76616C696443686172466F736974696F6E5C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22446776E6C6F616447667696E616C55726C4661696C65645C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22496E76616C69645465787452616E67655C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22446F776E6C6F61645069637475726546726F6D486F73744661696C65645C2220A207B205C224576656E74466C61675C2220A2031207D2C205C2253686172654496F16C6F748616E46C65672486F7374526706F72746564661696C7572655C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22466176654368616E6E656C45C2220A207B205C224576656E74466C61675C2220A2031207D2C205C2256726F6D57F70694661696C7572655C2220A207B205C224576656E74466C61675C2220A2031207D2C205C224C6F6164477657443656C6F734D697373696E6746696C6549645C2220A207B205C224576656E74466C61675C2220A2031207D2C205C224C6F6164486F73744E6574776F726B5365637572654368616E6E656C4661696C7572655C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22566B6E6F776E31303531696C2220A207B205C224576656E74466C61675C2220A2031207D2C205C225669735616C6C795265616479536C6F726726F6D55736572436C6963685C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22436F6D6B656E74472656174696F6E4661696C65645C2220A207B205C224576656E74466C61675C2220A2031207D2C205C224E65737465645461626C65466F756E645C2220A207B205C224576656E74466C61675C2220A2031207D2C205C2247261706869636496E76616C69645C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22466F76616C696443686172466F736974696F6E5C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22446776E6C6F616447667696E616C55726C4661696C65645C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22496E76616C69645465787452616E67655C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22446F776E6C6F61645069637475726546726F6D486F73744661696C65645C2220A207B205C224576656E74466C61675C2220A2031207D2C205C2253686172654496F16C6F748616E46C65672486F7374526706F72746564661696C7572655C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22466176654368616E6E656C45C2220A207B205C224576656E74466C61675C2220A2031207D2C205C2256726F6D57F70694661696C7572655C2220A207B205C224576656E74466C61675C2220A2031207D2C205C224C6F6164477657443656C6F734D697373696E6746696C6549645C2220A207B205C224576656E74466C61675C2220A2031207D2C205C224C6F6164486F73744E6574776F726B5365637572654368616E6E656C4661696C7572655C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22566B6E6F776E31303531696C2220A207B205C224576656E74466C61675C2220A2031207D2C205C225669735616C6C795265616479536C6F726726F6D55736572436C6963685C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22436F6D6B656E74472656174696F6E4661696C65645C2220A207B205C224576656E74466C61675C2220A2031207D2C205C224E65737465645461626C65466F756E645C2220A207B205C224576656E74466C61675C2220A2031207D2C205C2247261706869636496E76616C69645C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22466F76616C696443686172466F736974696F6E5C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22446776E6C6F616447667696E616C55726C4661696C65645C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22496E76616C69645465787452616E67655C2220A207B205C224576656E74466C61675C2220A2031207D2C205C22446F776E6C6F61645069637475726546726F6D486F73744661696C65645C2220A207B205C224576656E

[illegible]

Malware analysis sample.doc Malicious activity | ANY.RUN - Malware Sandbox Online

```
Process: (7740) WINWORD.EXE
on: write
uint64_t]58
Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Name: ChunkCount
```

(PID) Process:	(7740) WINWORD.EXE	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation:	write	Name:	ChunkCount

[illegible]

Process: (7740) WINWORD.EXE	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData
Operation: write	Name: ChunkCount
Offset: uint64_t[61]	

[illegible]

<https://anv.run/report/4a24048f81afbe9fb62e7a6a49adb1f4f41f266b5f9feecdceb567aec096784/ea9a0ed6-ca7b-4a76-a3c9-db7efbd6bb33>

[illegible]

[illegible]

[illegible]

Malware analysis sample.doc Malicious activity | ANY.RUN - Malware Sandbox Online

```
Process: (7740) WINWORD.EXE
Operation: write
Path: \\.\C:\ProgramData\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word\ConfigContextData\
Offset: 0
Size: 4
Type: uint64_t[66]
```

Value: 203A207B2022464347726F75704D61705F3122203A205B207B20224622203A20224D6963726F736F66742E4F666666963652E41697253706163652E426C6F636B6564477261

Value: uint64_t|67

<https://any.run/report/4a24048f81afbe9fb62e7a6a49adbd1faf41f266b5f9feecdceb567aec096784/ea9a0ed6-ca7b-4a76-a3c9-db7efbd6bb33> 68/87

Value:	uint64_t[135]		
(PID) Process:	(7740) 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:	(7740) WINWORD.EXE	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word
Operation:	write	Name:	ETag
Value:	std::wstring hzaMeMP3JGTH686nDL7WJb3e6APavU7M1SPOEzEAnk="		
(PID) Process:	(7740) WINWORD.EXE	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word
Operation:	write	Name:	Expires
Value:	int64_t[1]760997469		
(PID) Process:	(7740) WINWORD.EXE	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word
Operation:	write	Name:	DeferredConfigs
Value:	std::wstring ofsh6c2b1ta1a3i,ofcrui4yvdulbf31,ofhpex3jznepoo31,ofpioyfqgmufst31,ofjhwlmcoc1pz531		
(PID) Process:	(7740) WINWORD.EXE	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\ExperimentConfigs\Ecs\word
Operation:	write	Name:	ConfigIds
Value:	std::wstring P-R-1098158-1-5,P-R-76757-1-2,P-R-26146-5-17,P-D-29635-1-1,P-D-27087-1-9,P-R-79688-1-3,P-X-1056196-2-3,P-R-1075539-4-6,P-R-1040574-4-8,P-R-1021491-4-4,P-R-1020730-2-10,P-R-1019591-4-4,P-R-1004561-4-4,dhied660:448381,P-X-98518-6-9,P-X-1061470-2-3,P-X-1021965-1-7,P-X-1021968-2-3,P-X-73639-1-5,P-R-1078275-4-7,P-R-1076518-4-6,P-R-1069515-4-6,P-R-1025444-4-5,P-R-33774-18-250,blockedgraphicsadapter5:475899,fee651667:361658,72h8b859:284400,80ebc365:276205,aidgi533:380177,P-R-58640-1-3,P-X-74718-1-9,P-R-1074048-6-7,P-R-35099-2-4,auenta724:577753,P-R-1081431-8-6,P-R-1053478-8-5,P-R-34843-4-6,P-X-71274-1-7,P-R-33822-14-66,P-R-45483-16-53,P-R-50717-18-60,P-R-87587-4-4,P-R-75069-1-3,P-R-75001-1-3,P-R-68152-18-21,P-R-52316-18-37,P-R-49162-18-13,P-R-49161-18-13,P-R-40253-6-19,P-R-40254-6-18,P-R-35401-6-7,P-R-32107-22-22,clpro105:466762,P-X-109189-1-5,P-X-1003556-1-5,P-X-109176-1-9,P-R-52315-18-26,P-R-24980-8-48,P-R-18279-2-65,cu673:325969,cuisf464:446654,cuisf838:330718,P-X-1036908-1-3,P-R-113915-8-7,P-R-52982-18-34,P-R-51145-2-7,g5b4b507:286055,P-X-1012533-1-5,P-R-1069405-4-8,P-R-1050194-32-21,P-R-41046-22-83,diasy932:273280,P-X-1077198-2-5,P-X-1048408-2-5,P-X-1004791-1-3,P-X-85359-1-13,P-X-95573-1-9,P-X-89012-1-11,P-R-1061651-8-6,P-R-1042420-4-3,P-R-1036164-4-7,P-R-113508-8-6,P-R-95616-8-5,P-R-79616-1-3,P-R-77621-1-3,P-R-77204-1-3,P-R-76107-1-3,P-R-74334-1-3,P-R-74439-1-3,P-R-73642-1-3,P-R-68938-1-6,P-R-62875-2-4,P-R-60579-2-2,P-R-60333-1-3,P-R-58107-2-2,P-R-55743-1-3,P-R-51958-1-5,P-R-38085-12-9,P-R-35389-18-38,usepreprotc:373788,usev2endpointtreatment:333993,d0985:451145,nativewin32rld:186744,docslppwin32:404568,docshomepagesearchenableaggregatedmresearchsource:175739,P-R-1034169-10-7,P-R-1078576-2-3,P-X-1059111-1-3,P-X-80742-1-11,P-X-93787-3-11,P-X-1056177-2-3,P-X-79961-1-7,P-X-1033356-2-3,P-X-99044-1-3,P-X-96141-1-3,P-E-286777-2-3,P-R-55122-8-6,P-R-100255-10-9,P-R-45314-10-16,79321789:355490,3jgh9488:375227,expow344:375555,expivotnondestructiveautogroup:387179,j92h3770:336114,exavo833:249893,smartrealc-treatment:431112,modernbrowserosauthdialog:208943,exisr448:208934,P-X-1240823-1-3,P-E-38231-C1-4,P-R-1245662-15-4,P-R-108342-14-17,P-R-95225-14-17,P-R-94661-14-13,P-R-94560-14-12,P-R-94189-14-13,P-R-93882-14-26,P-R-61147-C17-2,P-R-54728-16-23,P-R-54698-16-16,P-R-54658-18-19,P-R-40049-7-29,P-R-38306-C17-3,P-R-34019-4-3,win32devicecanary:541483,win32devicecanary:541483,P-X-1047057-1-9,P-X-1046414-1-7,P-X-1058568-1-5,P-X-113191-1-15,P-X-1045426-2-7,P-X-1027551-2-7,P-X-1066678-3-7,P-X-1056983-2-3,P-X-1054122-2-7,P-X-1053321-1-9,P-X-1007274-3-17,P-X-1007275-13-45,P-X-85896-1-19,P-X-1038156-1-19,P-X-1037148-2-3,P-X-1035871-1-3,P-X-1028554-1-3,P-X-1014431-1-7,P-X-1005445-1-5,P-X-1011435-1-3,P-X-116115-1-9,P-X-107595-1-5,P-X-116990-1-5,P-X-86282-1-7,P-X-61102-3-11,P-X-51262-1-11,P-X-52591-1-11,P-X-88241-1-5,P-X-96956-1-9,P-X-98655-1-9,P-X-98655-1-5,P-X-84464-1-5,P-X-84633-1-3,P-X-54358-1-7,P-X-69301-1-5,P-X-53975-3-9,P-X-69189-1-7,P-X-56274-1-9,P-X-63134-1-7,P-X-58678-1-5,P-X-55832-1-6,P-X-56147-1-5,P-X-56154-1-5,P-X-54212-1-5,P-R-1554130-4-5,P-R-1554127-4-5,P-R-1554122-4-6,P-R-1074839-8-5,P-R-1074407-8-5,P-R-1074030-8-4,P-R-1072326-8-6,P-R-1062852-8-9,P-R-1053269-8-5,P-R-95082-8-5,P-R-93970-8-4,P-R-69065-1-3,P-R-59193-1-3,P-R-45609-14-6,P-R-45177-18-24,P-R-45197-2-6,P-R-40980-18-16,P-R-39029-5-18,P-R-35165-2-7,P-R-29809-1-7,P-R-26968-3-9,P-R-18425-8-62,P-R-18426-5-30,P-R-18424-4-34,P-D-1109907-4-12,h1a5h132:345901,742ab422:449631,djhec859t:366718,fiisc844:419232,fhopture:444595,715gh573:380346,g45hb810:353963,f03fc15t:344239,vectorclockenabled:334934,defaulttoodborfornr wfile:348225,hneditors:518234,5min10mcin10mingraceprocessor:517789,fiilis466:736702,happy085953:1:398313,c6egf484:334219,movclockdatadephemeralstoreforocs:295185,happy072122-1:356273,betterbreadcrumbs:490836,fasarchival:330783,fises921:241699,fiall198:498887,fibac967:608571,fioocs200:449498,fisw161:317604,fites217:161468,firf346:34525,fimoc589:28979,f icac124:207757,fipar839:191062,graphapiforenabledrollout:394156,onedriveconvergenceenlightenedrollout:159038,fioni293:118081,fiski225:498874,fiena947:30635,fishe957:64062,fista40 7:61027,fiena903:65944,fidav265:55035,ficac841:49664,fiena415:38780,fiena490:34181,remotemovedevice:42500,fiena276:41004,fiena381:49997,P-X-1020353-1-7,P-R-1236530-8-3,P-R-1078571-18-8,P-R-1046340-18-15,P-R-1033579-18-11,P-R-1034118-18-20,P-R-1026354-18-21,P-R-1018359-2-2,P-R-61707-28-22,P-R-53545-4-5,P-R-49736-6-22,P-R-30085-1-9,P-R-25157-8-14,P-R-24363-6-13,P-R-19814-1-62,P-R-19012-1-57,flena214:526824,flena214:526824,P-X-1024448-1-3,05b5382:403331,P-X-1056456-2-11,P-X-1018564-3-9,P-X-6102597-1-7,P-X-1051512-1-3,P-X-1009329-1-7,P-X-1006279-1-7,P-X-1011442-1-11,P-X-1019632-1-3,P-X-1015554-1-5,P-X-1010314-1-5,P-X-108364-1-3,P-X-77742-1-5,P-X-81056-1-25,P-X-86395-1-5,P-X-84321-1-5,P-X-73637-1-9,P-X-50220-1-3,P-X-49730-1-3,P-R-1043885-6-6,P-R-1014452-8-8,P-R-64841-22-15,P-R-63100-24-15,P-R-52038-28-18,P-R-36683-18-40,P-R-40990-12-15,P-R-35972-5-5,P-R-35572-2-3,P-R-32744-14-15,P-R-32741-32-16,P-R-28751-2-20,iu457512:449178,brakingskip:388631,gralt193:411215,82bj3355:373906,gralt222:345547,grhid528:460996,grgfx906:423905,gr234:434316,grsk1455:578553,gr312:613341,gr370:583087,grdel 347:127628,greana316:619261,grsv960:452690,gruse444:124091,grall464:134386,gruse488:570358,grico406:19777,P-X-1650712-1-3,P-X-105899-1-5,P-R-1650813-8-14,17ge1117:862153,24a93365:147747,P-R-50429-18-8,P-R-36539-10-5,P-R-24084-1-16,P-X-1559553-1-3,P-X-1049225-1-3,P-X-1033360-1-5,P-X-1033355-1-3,P-X-1011173-1-5,P-R-1576884-13-16,P-R-1445924-8-6,P-R-1101081-8-5,P-R-1077610-8-5,P-R-1026542-8-4,P-R-1021725-18-50,P-R-53421-28-14,P-R-40475-28-28,P-R-35985-14-23,P-R-32004-2-5,7a9ac840:826029,9795c320:359820,2dbb5579:286225,i83da489:388038,id592:288714,P-X-88035-1-5,Jalan231:140781,P-X-1276509-1-5,P-X-1051111-2-5,P-X-1019629-3-16,P-X-85741-1-17,P-X-1006736-3-21,P-X-113501-2-8,P-X-103786-1-3,P-X-70078-23-44,P-R-1280425-13-17,P-R-70703-1-5,P-R-61248-18-7,P-R-51995-18-28,P-R-42896-74-141,P-R-40212-42-73,oid76970:598689,hibc1399:344495,documenttaskuwinmacwpv:532457,happy060721-1:232704,multievelliststopart:317758,lemic505:207137,leisu74:610784,imagesupportstage2:322074,P-X-1044514-2-7,P-X-1061723-2-5,P-X-1076252-1-6,P-X-1049649-2-5,P-X-1047715-2-7,P-X-104195-4-19,P-X-1026131-2-5,P-X-1027913-1-11,P-X-1017745-8-14,P-X-807671-137,P-X-108643-2-7,P-X-1009048-1-9,P-X-95605-2-3,P-R-1700476-1-2,P-R-1058675-8-4,P-R-1036576-4-4,P-R-98110-4-5,P-R-79963-1-2,P-R-60816-10-19,P-R-51764-1-4,P-R-42392-2-4,P-R-39073-1-5,pipchybrnd:336265,2z9fj618:362490,9jg4c893:357444,4gh9e205:483778,6151j613:447619,gd8h8755:317990,jj050827:245162,a0e72269:322094,7g636832:989531,e9bh651:5:244499,76e4g 975:324979,ijs30:571995,g0hd0221:450355,P-R-1123376-10-14,P-R-1009855-12-14,P-R-98856-18-48,P-R-1061239-8-6,P-R-43489-30-15,P-R-1021426-2-3,P-X-1229360-3-15,P-X-92644-1-9,P-X-77136-1-27,P-X-1027156-1-7,P-X-1012950-4-7,P-X-1074536-1-3,P-X-1066546-1-13,P-X-89878-1-5,P-X-1050665-3-7,P-X-1030245-1-5,P-X-1039347-2-11,P-X-1039576-2-3,P-X-1019581-1-3,P-X-1013016-1-3,P-X-1006174-1-5,P-X-118320-1-4,P-X-83824-1-3,P-X-51759-1-13,P-R-1565428-1-3,P-R-1249370-4-5,P-R-1094115-4-4,P-R-1089192-6-5,P-R-1017066-4-5,P-R-117941-4-4,P-R-59534-1-3,P-R-54557-1-3,P-R-37603-3-6,ch371179:600396,enablemanifestxmslsignatureverification:274990,experimentationsdxpreload:77729,125h7935:351847,oesetupdell yverfalfback3:445075,9b8da955:449924,belowopendivider:542557,oeuil820:326124,oeenablesidentifitymanager:449919,4c6hd279:463721,d3gie564:283853,99f1d616:283854,oeomic639:3977 53,oeall419:414571,oeall843:375887,oeena555:420386,oeeco133:361172,oeomac358:20502,P-R-71360-18-19,P-X-76555-1-3,onmap366:81740,P-D-1476540-1-3,P-D-1248350-1-3,P-D-1236472-3-4,P-D-1220644-7-5,P-D-1036061-3-3,P-D-1157717-1-3,P-D-1149436-1-3,P-D-113129-6-7,P-D-1110956-4-3,P-D-1084565-3-3,P-D-1075543-1-3,P-D-1073014-5-3,P-D-1037541-7-6,P-D-1033391-2-4,P-D-1031537-1-3,P-D-1031536-1-3,P-D-1031534-4-3,P-D-1031532-1-3,P-D-1031529-1-3,P-D-1031527-1-3,P-D-1031525-1-3,P-D-1031521-2-3,P-D-1031520-2-3,P-D-1031512-1-3,P-D-1031510-1-3,P-D-1031509-1-3,P-D-1031508-1-3,P-D-1031493-1-3,P-D-1031486-1-3,P-D-1031484-1-3,P-D-1031482-1-3,P-D-1031479-1-3,P-D-1031460-1-3,P-D-1031050-4-3,P-D-1031022-1-3,P-D-1031018-1-3,P-D-1031012-1-3,P-D-1030964-1-3,P-D-1030963-1-3,P-D-1030956-1-3,P-D-1030928-1-3,P-D-1030927-1-3,P-D-1030926-1-3,P-D-1030923-3,P-D-1030920-2-3,P-D-1030908-2-3,P-D-1030907-2-3,P-D-1030904-2-3,P-D-1030902-2-3,P-D-1030900-2-3,P-D-1030898-2-3,P-D-1030896-2-3,P-D-1030893-2-3,P-D-1030891-2-3,P-D-1030889-2-3,P-D-1030887-2-3,P-D-1030885-2-3,P-D-1030883-2-3,P-D-1030881-2-3,P-D-1030879-2-3,P-D-1030877-2-3,P-D-1030876-2-3,P-D-1030875-2-3,P-D-1030873-2-3,P-D-1030872-2-3,P-D-1030871-2-3,P-D-1030870-2-3,P-D-1030869-2-3,P-D-1030868-2-3,P-D-1030867-2-3,P-D-1030866-2-3,P-D-1030865-2-3,P-D-1030864-2-3,P-D-1030862-2-3,P-D-1030860-2-3,P-D-1030858-2-3,P-D-1030856-2-3,P-D-1030854-2-3,P-D-1030852-2-3,P-D-1030850-2-3,P-D-1030848-2-3,P-D-1030847-2-3,P-D-1030846-2-3,P-D-1030844-2-3,P-D-1030841-2-3,P-D-1030840-2-3,P-D-1030838-2-3,P-D-1030836-2-3,P-D-1030834-2-3,P-D-1030832-2-3,P-D-1030830-2-3,P-D-1030828-2-3,P-D-1030826-2-3,P-D-1030824-2-3,P-D-1030822-2-3,P-D-1030819-2-3,P-D-1030816-2-3,P-D-1030812-2-3,P-D-1030811-2-3,P-D-1030810-2-3,P-D-1030808-2-3,P-D-1030806-2-3,P-D-1030803-2-3,P-D-1030801-2-3,P-D-1030800-2-3,P-D-1030799-2-3,P-D-1030798-2-3,P-D-1030797-2-3,P-D-1030796-2-3,P-D-1030795-2-3,P-D-1030794-2-3,P-D-1030793-2-3,P-D-1030792-2-3,P-D-1030791-2-3,P-D-1030789-2-3,P-D-1030787-2-3,P-D-1030786-2-3,P-D-1030785-2-3,P-D-1030783-2-3,P-D-1030781-2-3,P-D-1030779-2-3,P-D-1030777-2-3,P-D-1030775-2-3,P-D-1030773-2-3,P-D-1030771-2-3,P-D-1030769-2-3,P-D-1030767-2-3,P-D-1030765-2-3,P-D-1030763-2-3,P-D-1030761-2-3,P-D-1030760-2-3,P-D-1030759-2-3,P-D-1030758-2-3,P-D-1030757-2-3,P-D-1030756-2-3,P-D-1030755-2-3,P-D-1030753-2-3,P-D-1030751-2-3,P-D-1030749-2-3,P-D-1030747-2-3,P-D-1030745-2-3,P-D-1030743-2-3,P-D-1030740-3-3,P-D-1030738-2-3,P-D-1030737-2-3,P-D-1030736-2-3,P-D-1030734-2-3,P-D-1030732-2-3,P-D-1030730-2-3,P-D-1030728-2-3,P-D-1030726-2-3,P-D-1030724-2-3,P-D-1030722-2-3,P-D-1030719-2-3,P-D-1030717-2-3,P-D-1030715-2-3,P-D-1030713-2-3,P-D-1030712-2-3,P-D-1030711-2-3,P-D-1030710-2-3,P-D-1030709-2-3,P-D-1030708-2-3,P-D-1030707-2-3,P-D-1030706-2-3,P-D-1030705-2-3,P-D-1030704-2-3,P-D-1030703-2-3,P-D-1030702-2-3,P-D-1030701-2-3,P-D-1030699-2-3,P-D-1030697-2-3,P-D-1030696-2-3,P-D-1030695-2-3,P-D-1030693-2-3,P-D-1030691-2-3,P-D-1030690-2-3,P-D-1030689-2-3,P-D-1030687-2-3,P-D-1030685-2-3,P-D-1030683-2-3,P-D-1030681-2-3,P-D-1030679-2-3,P-D-1030677-2-3,P-D-1030675-2-3,P-D-1030673-2-3,P-D-1030671-2-3,P-D-1030669-2-3,P-D-1030668-2-3,P-D-1030666-2-3,P-D-1030665-2-3,P-D-1030664-2-3,P-D-1030663-2-3,P-D-1030661-2-3,P-D-1030659-2-3,P-D-1030656-1-3,P-D-1030649-1-3,P-D-1030642-12-8,P-D-1030637-7-3,P-D-1030636-7-3,P-D-1030635-7-3,P-D-1030634-1-5,P-D-1030633-1-3,P-D-1030628-4-4,P-D-1030591-1-3,P-D-1030561-1-3,P-D-1030547-2-4,P-D-1030545-1-3,P-D-1030542-1-3,P-D-1030541-3-5,P-D-1030219-3-5,P-D-1030218-3-5,P-D-1029521-5-4,P-D-1029517-1-3,P-D-1029515-1-3,P-D-1029514-1-3,P-D-1029513-1-3,P-D-1029512-1-3,P-D-1029511-1-3,P-D-1029509-1-3,P-D-1029508-1-3,P-D-1029506-1-3,P-D-1029505-1-3,P-D-1029444-1-3,P-D-1029430-1-3,P-D-1029428-1-3,P-D-1029426-1-3,P-D-1029416-1-3,P-D-1029414-1-3,P-D-1029371-1-3,P-D-1029338-1-3,P-D-1029293-2-3,P-D-1029289-16-4,P-D-1029276-1-3,P-D-1029275-1-3,P-D-1029272-1-3,P-D-1029270-1-3,P-D-1029267-6-4,P-D-1029250-1-3,P-D-1029243-1-3,P-D-1029238-1-3,P-D-1029237-1-3,P-D-1029234-1-3,P-D-1029205-1-3,P-D-1029203-1-3,P-D-1029148-3-4,P-D-1029137-1-3,P-D-1029097-2-3,P-D-1029096-2-3,P-D-1029093-2-3,P-D-1029091-2-3,P-D-1029090-2-3,P-D-1029086-1-3,P-D-1029083-12-3,P-D-1029082-12-3,P-D-1029080-8-5,P-D-1029078-1-3,P-D-1029077-1-3,P-D-1029075-7-4,P-D-1029065-1-3,P-D-1029063-12-3,P-D-1028977-1-3,P-D-1028974-1-3,P-D-1028956-3-4,P-D-1028914-1-3,P-D-1028874-1-3,P-D-1021730-2-4,P-D-1021729-2-4,P-D-1021020-2-4,P-D-1021019-2-4,P-D-1021017-2-4,P-D-1021016-2-4,P-D-1021015-5-7,P-D-1021014-2-4,P-D-1021013-2-4,P-D-1021012-2-4,P-D-1021011-2-4,P-D-1021010-2-4,P-D-1021008-2-4,P-X-1043160-1-13,d94c5e56:490490,P-X-1052910-1-3,P-X-1020529-1-3,P-R-1016539-8-5,P-R-82473-1-4,P-R-56618-1-3,191g5705:433160,peimp694:246849,P-X-1006499-1-13,P-R-108437-1-3,P-R-99549-1-5,P-X-82377-1-3,P-R-35513-4-4,P-R-33696-1-5,P-R-33569-1-9,P-R-31987-1-6,peen353:407649,peena788:193430,tulipsv2:177885,enablealwaysonrefresh:224888,P-R-39912-1-2,P-R-50380-18-18,P-X-115166-1-3,pu469:434493,P-X-1070041-2-3,P-X-1027341-2-5,P-X-1048046-1-3,P-X-1050569-1-5,P-X-1041355-1-5,P-X-1045059-1-3,P-X-1044286-1-5,P-X-100569-6-19,P-X-1038081-2-5,P-X-1018117-1-5,P-X-1009576-3-15,P-X-1021187-1-3,P-X-1015526-1-5,P-X-117740-1-3,P-R-1531055-8-2,P-R-1088777-8-5,P-R-1081668-8-4,P-R-1075135-8-5,P-R-1074372-4-5,P-R-1074077-4-5,P-R-1064159-8-4,P-R-1040579-26-17,P-R-1038629-8-5,P-R-63338-18-11,P-R-58251-18-12,P-R-33373-1-4,jf8h7165:687897,jcgcd970:365642,8r9fb771:396982,8b0at1245:454831,99f5d601:736891,66eh1308:345918,3fh1b283:383666,h156g585:368013,e0916802:490791,justificationotherwithsecuri tywarning:451234,scepd200:420343,36823626:526439,sefg838:346869,graphicsfilterextxalcloudrun:496048,P-X-78543-1-5,P-X-71939-13-22,P-X-1017616-1-7,P-X-1014227-1-3,P-X-116286-1-3,P-X-116085-1-3,P-X-116078-1-5,P-X-116065-1-3,P-X-74234-1-11,P-E-29662-2-3,P-R-61358-C17-22,P-R-1049526-2-8,P-R-1049535-2-8,P-R-29303-2-20,P-R-29031-2-20,P-R-36316-6-20,P-R-30290-6-23,P-R-28982-3-18,P-R-63947-18-2,P-R-63357-18-19,P-R-61361-18-26,P-R-61360-18-21,P-R-48634-2-15,P-R-47422-18-11,P-R-45579-18-8,P-R-42512-1-3,P-R-40520-2-13,P-R-38704-4-6,P-R-38212-2-11,P-R-35946-6-4,P-R-35846-6-4,P-R-35407-4-3,P-R-33434-2-1,P-R-30292-4-4,P-R-28644-1-1,P-R-24037-1-7,P-R-23445-3-7,P-R-23370-2-9,P-R-23434-3-4,P-R		

1697113-15-3,P-R-1694200-1-3,P-R-1692659-3-5,P-R-1692658-2-4,P-R-1692655-2-4,P-R-38248-23-31,P-R-1616290-1-3,P-R-1585887-4-6,P-R-1551153-1-3,P-R-1236953-12-16,P-R-1547617-1-3,P-R-1526875-34-4,P-R-1526874-34-4,P-R-1526873-34-4,P-R-1526872-34-4,P-R-1526870-34-4,P-R-1526868-34-4,P-R-1526867-34-4,P-R-1526866-57-5,P-R-1526862-15-3,P-R-1479674-3-5,P-R-1415183-51-5,P-R-1415182-51-5,P-R-1415181-32-4,P-R-1415180-51-5,P-R-1415179-51-5,P-R-1280186-1-3,P-R-1267084-2-6,P-R-1261918-2-4,P-R-1245804-67-6,P-R-1245296-4-6,P-R-1183639-81-7,P-R-1183631-81-7,P-R-1183628-62-6,P-R-1157570-2-4,P-R-1140998-117-9,P-R-1140997-117-9,P-R-1140996-94-8,P-R-1140995-94-8,P-R-1140994-94-8,P-R-1140993-94-8,P-R-1140992-94-8,P-R-1140991-94-8,P-R-1140990-117-9,P-R-1140989-117-9,P-R-1132821-2-4,P-R-1119013-1-3,P-R-1106768-105-9,P-R-1106767-105-9,P-R-1106766-105-9,P-R-1106765-105-9,P-R-1106764-105-9,P-R-1106763-128-10,P-R-1106762-105-9,P-R-1103277-1-3,P-R-1098796-1-3,P-R-1094445-1-3,P-R-1058643-5-9,P-R-1080412-1-3,P-R-1080101-115-10,P-R-1080099-115-10,P-R-1080097-115-10,P-R-1080096-115-10,P-R-1080095-115-10,P-R-1080094-138-11,P-R-1080093-115-10,P-R-1080092-115-10,P-R-1080091-96-9,P-R-1080090-115-10,P-R-1080089-96-9,P-R-1080088-132-11,P-R-1073291-4-6,P-R-1071761-1-3,P-R-1069769-2-4,P-R-1069203-1-3,P-R-1068115-1-3,P-R-1024076-4-8,P-R-1024074-4-8,P-R-1059329-123-11,P-R-1059328-163-13,P-R-1059326-123-11,P-R-1059325-123-11,P-R-1059324-123-11,P-R-1059323-163-13,P-R-1059322-163-13,P-R-1059321-87-9,P-R-1059320-104-10,P-R-1059319-123-11,P-R-1059318-104-10,P-R-1059317-123-11,P-R-1059316-123-11,P-R-1059315-123-11,P-R-1059314-123-11,P-R-1059312-123-11,P-R-1059311-123-11,P-R-1059310-123-11,P-R-1059309-123-11,P-R-1059308-123-11,P-R-1059307-123-11,P-R-1059306-123-11,P-R-1059305-123-11,P-R-1059304-123-11,P-R-1059303-140-12,P-R-1059302-123-11,P-R-1059301-140-12,P-R-1059300-123-11,P-R-1059299-140-12,P-R-1059298-123-11,P-R-1059297-140-12,P-R-1059296-146-12,P-R-1059295-123-11,P-R-1059294-123-11,P-R-1059293-123-11,P-R-1059292-71-8,P-R-1059291-140-12,P-R-1059290-104-10,P-R-1059289-123-11,P-R-1059288-123-11,P-R-1059287-123-11,P-R-1059286-123-11,P-R-1059285-123-11,P-R-1059284-123-11,P-R-1059283-123-11,P-R-1059282-123-11,P-R-1059281-123-11,P-R-1059280-123-11,P-R-1059279-123-11,P-R-1059278-123-11,P-R-1059277-123-11,P-R-1059276-123-11,P-R-1059275-123-11,P-R-1059274-123-11,P-R-1059273-123-11,P-R-1059272-123-11,P-R-1059271-123-11,P-R-1059270-146-12,P-R-1059269-123-11,P-R-1059268-123-11,P-R-1059267-104-10,P-R-1059266-123-11,P-R-1059265-123-11,P-R-1059264-123-11,P-R-1059263-123-11,P-R-1059262-123-11,P-R-1059261-123-11,P-R-1059260-123-11,P-R-1059259-123-11,P-R-1059258-123-11,P-R-1059257-146-12,P-R-1059256-123-11,P-R-1059255-123-11,P-R-1059254-146-12,P-R-1059253-146-12,P-R-1059252-146-12,P-R-1059251-146-12,P-R-1059250-146-12,P-R-1059249-123-11,P-R-1059248-146-12,P-R-1059247-146-12,P-R-1059246-146-12,P-R-1059245-146-12,P-R-1059244-163-13,P-R-1059243-146-12,P-R-1059242-146-12,P-R-1059241-146-12,P-R-1059146-162-14,P-R-1059053-154-13,P-R-1058988-162-14,P-R-1058987-154-13,P-R-1058986-154-13,P-R-1058985-170-15,P-R-1058984-170-15,P-R-1058983-178-16,P-R-1058982-179-15,P-R-1058981-154-13,P-R-1058980-154-13,P-R-1058979-170-15,P-R-1058978-170-15,P-R-1058977-186-17,P-R-1058976-179-15,P-R-1058975-179-15,P-R-1058974-179-15,P-R-1058973-179-15,P-R-1058972-179-15,P-R-1058971-179-15,P-R-1058969-179-15,P-R-1058968-179-15,P-R-1058967-155-15,P-R-1058966-136-14,P-R-1058965-131-12,P-R-1058964-154-13,P-R-1058963-154-13,P-R-1058962-154-13,P-R-1058961-154-13,P-R-1058960-154-13,P-R-1058959-154-13,P-R-1058958-162-14,P-R-1058957-131-12,P-R-1058956-148-13,P-R-1058955-148-13,P-R-1058954-171-14,P-R-1058953-148-13,P-R-1058952-148-13,P-R-1058951-148-13,P-R-1058950-148-13,P-R-1058949-148-13,P-R-1058948-148-13,P-R-1058947-148-13,P-R-1058946-148-13,P-R-1058945-148-13,P-R-1058944-162-14,P-R-1058943-162-14,P-R-1058942-178-16,P-R-1058941-162-14,P-R-1058940-162-14,P-R-1058939-139-13,P-R-1058938-162-14,P-R-1058937-162-14,P-R-1058936-162-14,P-R-1058935-162-14,P-R-1049175-1-3,P-R-1045118-2-4,P-R-1044408-1-3,P-R-1037887-1-3,P-R-1037879-1-3,P-R-1036293-1-3,P-R-1036292-1-3,P-R-1036289-2-4,P-R-1036288-1-3,P-R-1036068-2-4,P-R-1036039-2-4,P-R-1035933-2-4,P-R-1035149-2-4,P-R-1033624-2-4,P-R-1028550-2-4,P-R-1028168-1-3,P-R-1027535-3-5,P-R-1024680-4-6,P-R-1024071-2-4,P-R-1010393-1-3,P-R-1006896-1-3,P-R-1006894-1-3,P-R-1006562-2-4,P-R-1000061-2-4,P-R-115946-3-5,P-R-111682-1-3,P-R-105731-36-38,P-R-104435-13-15,P-R-100294-1-3,P-R-99633-1-3,P-R-98929-2-4,P-R-98926-1-3,P-R-98250-1-3,P-R-94556-2-4,P-R-93077-1-3,P-R-90895-3-5,P-R-88309-2-4,P-R-86118-1-3,P-R-83408-2-4,P-R-80517-7-9,P-R-78852-3-5,P-R-78325-5-9,P-R-78112-4-6,P-R-76918-2-4,P-R-76721-1-3,P-R-76253-1-3,P-R-75440-2-4,P-R-75436-1-3,P-R-75434-1-3,P-R-75433-1-3,P-R-74528-4-6,P-R-72449-7-10,P-R-68069-2-4,P-R-66975-1-3,P-R-65671-3-3,P-R-60602-3-5,P-R-58471-2-4,P-R-58093-1-3,P-R-53309-1-3,P-R-52633-1-3,P-R-52171-2-4,P-R-51921-8-10,P-R-51258-8-10,P-R-50752-2-4,P-R-50681-4-6,P-R-50599-4-6,P-R-50596-4-8,P-R-50585-18-20,P-R-50553-1-3,P-R-49597-3-5,P-R-49458-2-4,P-R-48530-7-9,P-R-47948-1-4,P-R-46580-3-5,P-R-46484-10-12,P-R-46122-1-3,P-R-45858-2-4,P-R-44950-1-3,P-R-43966-2-4,P-R-43502-19-21,P-R-43238-3-5,P-R-43188-6-8,P-R-41430-1-3,P-R-40751-8-10,P-R-40273-4-6,P-R-39238-5-7,P-R-38878-2-4,P-R-38682-3-5,P-R-37588-2-4,P-R-34355-8-10,P-R-26266-4-9,P-R-26834-3-8,P-R-24662-16-22,P-R-24749-6-11,P-R-26056-7-15,P-R-27006-7-12,P-R-32191-9-11,P-R-30338-3-7,P-R-30178-79-81,P-R-30053-8-10,P-R-27458-1-5,P-R-25083-6-9,P-R-24690-46-50,P-R-24689-2-5,P-R-24666-2-5,P-R-24663-6-11,P-R-24659-7-10,P-R-23762-5-8,P-R-23744-7-9,P-R-23739-7-9,P-R-23736-1-7,P-R-23734-7-9,P-R-23730-21-24,P-R-23723-10-12,P-R-32589-1-3,P-D-32588-1-3,P-D-32584-1-3,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-32485-1-4,P-D-32484-1-4,P-D-32405-1-3,P-X-1025485-1-5,P-X-1014972-2-6,P-R-1037459-2-5,P-X-1036987-2-3,P-X-1036173-2-3,P-X-1033573-1-5,P-X-1031592-1-3,P-X-1030035-2-3,P-X-1028341-3-16,P-X-1017029-2-5,P-X-1025213-1-3,P-X-117829-3-13,P-X-1020568-1-3,P-X-1020380-1-5,P-X-1015283-2-7,P-X-1004373-1-5,P-X-93407-1-5,P-X-1012979-2-5,P-X-1003177-2-5,P-X-87484-7-17,P-X-111730-1-5,P-X-108481-1-5,P-X-109250-1-5,P-X-77890-1-5,P-X-79635-17-7,P-X-79335-5-27,P-X-73171-1-7,P-X-73179-1-7,P-X-71999-3-11,P-X-71819-1-3,P-R-1087141-4-7,P-R-1075199-6-4,P-R-1013930-4-5,P-R-60571-18-30,P-R-53085-18-13,P-R-5318-18-8,P-R-47046-26-24,P-R-4761-16-13,P-R-46900-18-8,P-R-45817-20-16,P-R-40152-18-16,P-R-33916-1-5,P-R-33580-8-10,P-R-32042-2-4,P-R-31966-21-25,Ad0eb633:270221,ucisd288_document_level_clickstreamcf:262264,5gg7780_t:283535,jf4ce893:308973,fj2eg623:288508,hfjg8229:286491,7b3gc341:308975,app_specific_find_header_trea tment:306197,2bjg1468:270141,zeromtrfind_treatment:282094,eieci960:275589,kpccursor:309088,ucsha247:295892,ucena469:247386,search_engagement_activestate_wxjpot_treatment:262 199,uc405:235311,ucsha05:233051,uctel918cf:251037,notes_treatment_winx2:248467,nb_cil:fjffj789:197216,ucru519:179022,uctel258_compressionenabled:221518,linelinetparticles_trea tmtment:205044,uctel147:90496,uctel354:153520,uc163:259214,268b6348:181975,enablenotesearch:149734,ucsha660:76558,uctel674:80889,P-X-1064973-1-7,P-X-1051763-2-7,P-X-1028571-2-5,P-X-113161-1-7,P-X-10106731-3,P-X-1010572-1-3,P-X-1000465-1-3,P-X-1174001-1-3,P-X-117320-1-3,P-X-82496-1-5,P-X-82497-1-5,P-X-110267-1-5,P-X-105697-1-9,P-X-97445-3-15,P-X-97120-1-5,P-X-94972-1-3,P-X-71712-1-5,P-X-73120-1-5,P-X-67656-1-3,P-R-1672191-13-1,P-R-1111984-4-5,P-R-1084354-8-7,P-R-1079254-8-7,P-R-1035921-4-4,P-R-59820-18-105,P-R-61426-18-9,P-R-59426-1-3,P-R-53773-18-60,P-R-46913-18-8,P-R-42780-14-19,P-R-25867-1-6,95agg357:872427,mecontrol_weaktpr_integration_enabled:717769,ad7j455:452298,sharemenu:279987,uxena409:287488,ux446:470683,uxflu234:452003,uxmadiumconluminance:353455,ux 289:326257,uxacc516:282118,uxacc113:282117,ux786:201454,fluentbackstagegerfresh:246421,micaiflight:377514,mppeopleenarme:213720,uxena101:288818,checkoutdeviceonpaint:122110,uxsho645:190378,uxacc787:56194,P-R-19262-2-12,P-R-1676280-1-5,P-X-1472664-1-3,P-X-1249997-1-3,P-X-1120063-2-3,P-X-1105324-2-3,P-X-1100631-9-P,X-76599-1-11,P-X-1004806-1-9,P-X-1053291-1-7-21,P-X-1072230-1-3,P-X-1072228-1-3,P-X-1055141-2-5,P-X-1065669-2-5,P-X-1040649-2-5,P-X-1029963-3-11,P-X-1058686-1-7,P,X-1061308-1-5,P,X-1061330-1-3,P-X-1060688-1-3,P-X-105493-1-3,P-X-1059061-2-3,P-X-96531-1-5,P-X-1058121-2-3,P,X-1054948-1-5,P,X-1056751-2-3,P-X-1055139-2-3,P,X-1055077-2-3,P,X-1054320-1-3,P,X-1050588-2-7,P,X-1030280-2-5,P-X-1048836-1-3,P-X-1047756-1-3,P-X-1047638-1-3,P-X-1047022-2-3,P-X-1046381-1-3,P-X-1046135-2-3,P-X-1045242-1-3,P-X-91049-1-5,P-X-1000193-1-5,P-X-1043902-1-3,P-X-1043777-2-3,P-X-1043745-1-3,P-X-1043008-2-3,P-X-1042275-2-3,P-X-1041359-2-5,P-X-1041011-2-5,P-X-1039841-2-3,P-X-1039436-1-3,P-X-1039080-2-3,P-X-1038739-1-3,P-X-1037732-2-3,P-X-1037320-2-5,P-X-1037196-1-3,P-X-1036666-2-3,P-X-1036540-2-3,P-X-1035646-2-3,P-X-1033768-2-3,P-X-1033332-2-3,P-X-1012500-5-18,P-X-1028284-2-5,P-X-1028163-1-3,P-X-1027861-1-3,P-X-1016387-1-7,P-X-1027081-2-5,P-X-1024767-2-3,P-X-1021665-2-5,P-X-1019425-1-3,P-X-107619-1-5,P-X-1076192-1-3,P-X-1014738-1-3,P-X-1014738-1-3,P-X-1012871-5,P-X-1002507-1-5,P-X-1008672-1-3,P-X-1006450-1-5,P-X-1006980-1-3,P-X-117611-1-7,P-X-1005490-1-3,P-X-84316-3-21,P-X-1004616-1-3,P-X-1004615-1-3,P-X-1003782-1-3,P-X-1003661-1-3,P-X-1003289-1-3,P-X-1000467-1-3,P-X-117699-1-3,P-X-1151671-3-3,P-X-98899-1-5,P-X-106677-1-3,P-X-94157-1-5,P-X-95233-1-5,P-X-93936-1-3,P-X-92829-1-3,P-X-92807-1-5,P-X-91539-1-3,P-X-87859-1-9,P-X-89713-1-5,P-X-85497-1-5,P-X-84868-1-3,P-X-84702-1-3,P-X-78548-1-3,P-X-75242-1-5,P-X-77184-1-3,P-X-64207-1-5,P-X-72616-1-5,P-X-67509-1-3,P-X-55651-1-5,P-X-42197-2-3,P-E-29661-C1-3,P-R-1676487-13-11,P-R-1609-13-3,P-R-64317-13-3,P-R-77139-13-3,P-R-1658-13-7,P-R-3809-13-7,P-R-64691-13-5,P-R-79051-8-5,P-R-64884-10-3,P-R-74643-13-5,P-R-1432-14-3,P-R-1472674-13-15,P-R-1250129-13-15,P-R-1002297-17-7,P-R-1168532-8-6,P-R-1426-11-5,P-R-1145332-11-4,P-R-1137583-8-3,P-R-1131097-8-4,P-R-1120132-21-5,P-R-1120092-14-14,P-R-64891-17-9,P-R-1117043-13-5,P-R-1485-13-3,P-R-1435-33-13,P-R-110630-8-8,P-R-1107966-12-7,P-R-1104862-8-7,P-R-1099774-8-7,P-R-1097462-8-7,P-R-1092653-8-8,P-R-1091684-12-11,P-R-1091662-8-7,P-R-1090691-12-5,P-R-1090444-12-7,P-R-1085940-8-7,P-R-1079731-8-6,P-R-1079015-4-7,P-R-1078838-4-8,P-R-1076119-8-7,P-R-1075089-8-7,P-R-1069447-8-4,P-R-1069576-8-8,P-R-1069194-8-7,P-R-1066662-8-7,P-R-1063829-8-8,P-R-1063405-8-7,P-R-1062318-8-7,P-R-1061753-8-8,P-R-1056474-8-5,P-R-1051178-8-6,P-R-1048230-8-9,P-R-1048024-6-8,P-R-1045408-8-4,P-R-1040610-8-4,P-R-1037882-8-7,P-R-1036942-8-6,P-R-1033843-8-9,P-R-1028630-8-7,P-R-1026155-8-7,P-R-1025949-8-7,P-R-1023536-8-7,P-R-1019160-8-7,P-R-1019089-8-7,P-R-1014565-8-8,P-R-1014448-8-7,P-R-1011591-8-7,P-R-1007288-8-7,P-R-1006767-8-8,P-R-1005172-6-1,P-R-1004550-6-10,P-R-1003948-6-16,P-R-117977-8-7,P-R-11711-8-8,P-R-116689-8-7,P-R-116688-8-8,P-R-11866-8-7,P-R-1001799-8-7,P-R-97061-8-8,P-R-95007-14-2,P-R-77374-1-8,P-R-69354-58-9,P-R-62603-16-18,P-R-62119-16-13,P-R-53700-16-20,P-R-49863-1-3,P-R-39401-14-34,P-R-35873-20-20,P-R-35006-4-4,P-R-33895-1-6,52fda4593:889107,33292609:766378,5a760260:592175,926011786:4771124,831a721:5559971,wo301:399349,woena434:393693,wotak480:391835,c7i6b307:453555,2641f178:428088,243j357 9:509713,aa5d848:410322,e033a910:401975,7f0d6510:320013,bfi48489-treatment-fasternonnulvalidation:442047,a9778247:383208,noidleumintreatment:667531,a98h4781:480364,fi56719:392009,3939g266:378271,chjfa985:393205,woccon656:327830,ad098930:391813,25f 5887:340325,a9100279:359262,h8i11312:409967,ebc4a09:396036,719hi403:447653,bd453194:354139,ahbh304:281701,19811241:338656,aeg4315:405764,6cib452:331249,h3b05298:338 352,bjfhf541:448419,i7h9f447:408653,19f47567:376881,wocle775:201551,neuralvoiceservicerequestthrottlengained:627050,b9d60115:386576,7jd4b177:727980,fixbadbookmark:391869,ibb 30443:299014,g1h6b692:334682,d83j4718:288830,linkmore:328280,enablehemerbiboptimization:332023,58iaj243:324618,bcgch266:317516,549g4857:440226,e0ebb330:354263,g6j20384:717 238,43f3b843:291239,nullicheckpitbsrf:279008,g82j8877:294674,enablethemefontupdateattreatment:448332,f1jb4973:317865,noodt3:502990,w738treatment:262465,wdsxdredtrollinrill- t:337512,womtywilid:448368,c7141783:281696,allowattomerge:276604,85be1596:453558,d7jbc702:268591,ig6ee887:389710,wodel235:379566,wofus947:453532,wofix664:254645,wodoc677: 419903,wo906:356686,wothrA694:355913,woset1109:225366,wofen618:226085,wowin895:357453,wolay755:227357,woc687:197273,wouse189:463420,readaloudneuralvoiceenablednew:530779, woche668:418304,fenaleconcontextmenutrypoint:380012,womod470:417509,woena769:454353,wocuh620:228508,woski306:246381,woimp331:224819,wo380754:346025,wouse867:180078, woena363:424345,wolay505:144348,woena695:196449,wolay111:295900,wocon578:303181,wocov453:144956,wos29853:176812,wojun311:152976,wotes317:377504,wouse438:124242,wal y340:124223,wododf13:devices:122236,woin543:198756,woyalw809:124232,wobre556:196059,wocoi936:80031,wofii163:71802,worem277:72193,woena288:242955,checkallanguages:36323, wotes907cf:1474,woyalw809:124232,woski306:246381,woset1109:225366,wos31:224819,wo301:399349,wocuh620:228508,fenaleconcontextmenutrypoint:380012,woena695:196449,woc687: 197273,wolay111:295900,readaloudneuralvoiceenablednew:530779,woena769:454353,wofus947:453532,bfi48489-treatment-fasternonnulvalidation:442047,woena363:424345,woche668:418304,womod470:417509,P-R-1641587-1-6,P-R-1583865-1-6,P-R-1563945-1-8,P-R-1098412-1-5,P-R-1091267-1-59,P-R-81720-1-2,P-R-58406-1-5,P-D-50697-2-4,P-D-29719-1-1,P-D-29718-1-1,P-D-29593-1-6

(PID) Process:	(7740) WINWORD.EXE	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\CrashPersistence\WINWORD\7740
Operation:	write	Name:	0
Value:	0B0E107E7A9C59EAA7124AAA0378B8202E4D5723004681C687D9B0BD90EE016A04102400449A7D64829D01008500A907556E6B6E6F776EC906E22687A614D654D50334A4754483638366E7744AC37574A623365364150617655374D3153504F455A65414E6B3D22CA0D2201A200C2190000C50E8908C91003783634C511BC3CD2120B770069006E0077006F00720064002E00650078006500C51620C517808004C91808323231322D44656300		
(PID) Process:	(7740) WINWORD.EXE	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\AddinClassifier
Operation:	write	Name:	9a3e8255d7eb9a1a1f397175007c13fc
Value:	v2:1;0;1760983068		
(PID) Process:	(7740) WINWORD.EXE	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Roaming
Operation:	write	Name:	RoamingConfigurableSettings
Value:	DC00000000000000803A09004106010001000100000000000000000000000000000000201C000201C0000805101008051010080510100805101008051010080F4030080F403002C01000084030000805101000000000084030000805101000A0000001E0000001E0000000000000000000000805101000100000001000		

<https://any.run/report/4a24048f81afbe9fb62e7a6a49adbd1faf41f266b5f9feecdceb567aec096784/ea9a0ed6-ca7b-4a76-a3c9-db7efbd6bb33> 71/87

(PID) Process: Operation: Value:	(7740) WINWORD.EXE write 86400	Key: Name:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\TargetedMessagingService\MessageMetadata\0_MsgId:BizBar CallDelta
(PID) Process: Operation: Value:	(7740) WINWORD.EXE write 2000	Key: Name:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\TargetedMessagingService\MessageMetadata\0_MsgId:BizBar MaxWait
(PID) Process: Operation: Value:	(7740) WINWORD.EXE write 0	Key: Name:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\TargetedMessagingService\MessageMetadata\0_MsgId:BizBar MsgsgId
(PID) Process: Operation: Value:	(7740) WINWORD.EXE write 1	Key: Name:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\TargetedMessagingService\MessageMetadata\0_MsgId:BizBar Provider
(PID) Process: Operation: Value:	(7740) WINWORD.EXE write 0	Key: Name:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\TargetedMessagingService\MessageMetadata\0_MsgId:BizBar SetUserAction
(PID) Process: Operation: Value:	(7740) WINWORD.EXE write 1	Key: Name:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\TargetedMessagingService\MessageMetadata\0_MsgId:BizBar ShouldShowBadging
(PID) Process: Operation: Value:	(7740) WINWORD.EXE write 2025-10-21T17:57:53Z	Key: Name:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\TargetedMessagingService\MessageMetadata\0_MsgId:BizBar TimeToNextcall
(PID) Process: Operation: Value:	(7740) WINWORD.EXE write 0	Key: Name:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\VBA\Forms3\Controls EnableActiveXControlArchitetureIndependent
(PID) Process: Operation: Value:	(7740) WINWORD.EXE write 0	Key: Name:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\VBA\Forms3\Controls EnableActiveXControlMSWebBrowserArchiteturePersistencelssue
(PID) Process: Operation: Value:	(7740) WINWORD.EXE write A0E8580EEB41DC01	Key: Name:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Internet\WebServiceCache LastClean
(PID) Process: Operation: Value:	(7740) WINWORD.EXE write	Key: Name:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Word\Security\FileBlock FileTypeBlockList
(PID) Process: Operation: Value:	(7740) WINWORD.EXE write	Key: Name:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Word\Security\FileBlock OoxmlConverterBlockList
(PID) Process: Operation: Value:	(7740) WINWORD.EXE delete value 篋-L	Key: Name:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Word\Resiliency\StartupItems -
(PID) Process: Operation: Value:	(7740) WINWORD.EXE delete key	Key: Name:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Word\Resiliency\StartupItems (default)
(PID) Process: Operation: Value:	(7740) WINWORD.EXE write 4	Key: Name:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\Fonts CloudFontsVersion
(PID) Process: Operation: Value:	(7740) WINWORD.EXE write	Key: Name:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\IdentityCRL\Immersive\production\Token\{2B379600-B42B-4FE9-A59C-A312FB934935} DeviceTicket
Value: 0100000001000000D08C9DDF0115D1118C7A00C04FC297EB01000000F293F768B82C8446AA21C22E5D7DDB8A000000002000000000106600000001000020000000693DC6278ABAF1A3E5D250B6AB3B8B510A901EB24F15D59DB9D12677D337778F000000000E8000000002000020000000AB30AD30E517F2C24BC918FC6901FD6A08BFFEE06C11B0BDB0C54F71733055A0E5006000E6409749189B186E32D7779C9B0E34C51C09644020388B01A8C1644211A1F1F044FAAD071C3A2C6888FA1E6F7992C2E99005059DE6B6FDA6D7CDCA66C6D3381DE22AC8965306D4B69A3F84E53B659E4BDC545EB2C04D9E6C223B812083D5389D6A9843C4B4700666F314240FE99005CEA3C3339DA1B0523B6E6C901E34939ED758480B7C757B75831926DFEFD786A59C7469F3AA17E0FE7C89927337D8D121E91ED23B981836DB24504839E02FDB42FA80518BEAC739EF9254F395AF83B089855EF52F8281DD5E3C598C276E31B5F8F4420EBF487AAE3D2A678CA50D5248FD7045339FA0EDD2EF9978AC414BAA7CFBE4FE85FE7DE6274A6D3DBCC53074CA5C727EB24999FDECFDAEA3F5D6AB016801FE830EC09443ADA7BAF5EB04F636E53304AD5C15E7F9470D1F8241078F25ED973DB06C56F12039E06DBC3CE2E2559B385A9E42B551BF4B8C50A9FEAD344499562629A33C8D053722ECC37558FABADA2703EEB007A41D542422622D20F7FCDE079974769F1F8A7513FE0A3FC141714480D73C94017A367A7B67D32885365729D9362B7B6B375E613A6052E67BB06E6E45357AD2C01C420FF2CD6615BD90A668F794E189EB0160D46D290572EBE0EAF1916E07E00E5F234A74DEE43E67A1E074266F9D6E634B7F016BFED497CA8416B22200C066281F891ADB018CBA98574E98A68CB87D3C42EE248EC87715BF6D8405535C593C78E1049CB80EFDAA35BC0182D4AC87B802F68EAC8E7A8D109932DEF17061782E2888B6582FE761DD05B822999266E683490E1805574D4011B757C9423F24F12785C432D115BC8250E142C35B22ED4FA3F076ABD4ADBA462FB423E764DA43ED80201EBA8B1EAEAAE14189B53699563E5982089FA20151267D2135A3411915043E8A80CF704621512AF4FBE31F3B7E3507AA5D58F2FE2D46C291FD4ED2C89EDB66C37BA5DB2A090D52EDF3CC1DF4543446F86C81AE724ADD53673C78F734265F94CD6BC6D39D6660C9230D0A0B334A71A2F64ED62613D685705AD70620A0F25E8481D5E547B48B8E15478B41D6440B9965E5E6B442150FEDB3CCC3BD803F95CAD9FE8F49B7887F8E856414511CC3F55A8E9D0A1C3DC8967825CDDC3F77F2DE19EC49ECA976BB7E8DC79439737D742A36C19BD1AE3D32D6639580C46FAA0B9BE7CE094B8C22BC4A2A251C940C849E11C52F1E16CFA64868423644FD84676B6DF69B0710E66FA4763BFE80E18F22A409FDF68F9B90592FA5B0F6449DCFA6D272E41969D16737C14F83A59018CF2B7F11DFCBA51C96BCC690474D3AD82BD6D485AA5A3E98007A21E1E3E0AA4D3543B34E8B07804A11C3947D4E649D6705A67CF7B7648521221EC11F18B6F479B372A944E8CE7CFC451C2ED8CC264296723DD2D9C977A54920B633C3255F92560607DA920762575215036FF56BFA51012B59806ACF0B34DB87786BD353623AF71B1AFA71E0C0267AB7A20B66689E1DA0B420C9EA1933FDB595F5B8463EB63231D4379F7515AA1EF2B39ECD25B1219590B0A674DD09113C3669852196F0E4AAAB431BEB7EF1E464276A829D7E4A6982C3DCB9739C9C88EDFC3DB90B1520CF15D08EB09672426BE2F0824324EC7C141E0C14DF8B903107BC001CBC513A8745431D3AFFE44F0D08525CF582D267294C8AFFF7D4827ED24756DB6E6FE6845C4FA80039DA2DB9C925A85DED012BEC2C7BEF9DDE516674A3D780CE6829C9E3AE222174B414B27106D0E877860DB643EB083D92F51ABFC1BBCC6843E1ED5D481B9113CB1285D50304D8B0CC43553FF57CC979650D29F37632156985C119098AACA4006CDA9BC53F607532974F9F5C46B59A8AA84E5A01DEE8EE639D9DCD5FA7312F90847CBFD0881DB816ACAFEF8989CE4B1D15F350B2FDA5C67B63AF15EBB79BA0366FCB503124B27F3D98776B717B249895EC75BCBBD56B33D191ED88047A1C8057CD618D1636B220D991A7DF73FC638EB0121C1703F9362C54E3DB8A1498F701E089F6D6233E4AE66D5B0A22EDC37EBB21F584C09FE5FDAE69D88678D9AEC7D490D6CC6209A42364F884B550C12A59AC8800C243E8FE8EC5D7FAB35E33EDAD99263C042B5263ECC7A0BA371DD9D0096540F1E8D16A1A13815106C9281B9FD9DFA2F72429E1E89502E9210E800649F52BD225E7C71297ADA62E37AB83549642B820F896989870D24E1C967AF8C9CA035FC79F05E7DC097DB3E45DD17422497B1B957D213FEFB4D49AE7F67F451CBDF8E3B9CE60D92561F68875B52B3D524B9E9FF56707DDA19A340000000BC7A62486CD2BF03E37CAEB7070AEA6557B4A92D8FAB8F71997DA60AECAB68192D9215826DA13D693FEBDAF1103E2FBD35AC1D139C7EE848CB62573426A4A3879			

(PID) Process: (7740) WINWORD.EXE	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\IdentityCRL\Immersive\production\Token\{2B379600-B42B-4FE9-A59C-A312FB934935}
Operation: write	Name: DeviceId
Value: 00188014E9AA38DD	
(PID) Process: (7740) WINWORD.EXE	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\IdentityCRL\Immersive\production\Token\{2B379600-B42B-4FE9-A59C-A312FB934935}
Operation: write	Name: ApplicationFlags
Value: 1	
(PID) Process: (7740) WINWORD.EXE	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\Common\ClientTelemetry\Volatile
Operation: write	Name: MsaDevice
Value: t=GwD2AbuEBAAUT8E2pcttyweiwH80omnEMQMzYo0OZgAAEGVQCCXpxqdnNXtZtZgT6mTAASWTwDi0oDXXcRQotblyBzGVAvx1+CVzjR2Br8eQOKc9rOyVBOC5IbZ/KlRrQhKAXw+FSReKrBSIj2SL EASKdpt0VKRljguvQl/xVxvhAHqPGpruqq0OXkHB+vA6QDCD/agHy5fJ7b4XqAm/77zt8qn1S4AysZlA0pQ8WuG//do1dr1ZNFGrCk2GUsEMK2WErVi7hGcGYKDgU0UyyZVNp5l04HJLrkU1GcKrz5bV yY6qEq4aPCfK9raQXTdSvSkc619vQNERlqkSkvFu5l2tPjwPzA+1cEbLOm//uUs7DU3RfOU2lPnClen8Gf+ey8viBiHs1WrMSuTorhJTU9QkCNezyRPheXmRsbr+Bp3Nc4s5MHRHwF/hLL0dg5d+3acwYj g0PbYuyt5z7s/hhMN30rwqxmgpPbyKfvXnGyl74j5po6As+76wHoEOGk3U6LtPre26nkUipUElUYIZSbh/UCIFOVRD033PoZiwKt1zlVbGlfCNkNIYCo2LptY//rP5F6GXfs0ib8Aj+C/Rm6FvTKQFrMg4jfVl HPMgdnwIOxgzNK0HMBcBt/qoPDNvKXT8ucg2kduClyY+ylt0ZzTnAsX3AQ==&p=	
(PID) Process: (7740) WINWORD.EXE	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
Operation: write	Name: CachePrefix
Value:	
(PID) Process: (7740) WINWORD.EXE	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
Operation: write	Name: CachePrefix
Value: Cookie:	
(PID) Process: (7740) WINWORD.EXE	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
Operation: write	Name: CachePrefix
Value: Visited:	
(PID) Process: (7740) 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: (7740) 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: (7740) 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: (7740) 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: (7740) 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: (7740) 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: (7740) 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: (7740) 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: (7740) 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: (7740) 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: (7740) 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: (7740) 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: (7740) 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: (7740) 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:	(7740) 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:	(7740) 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:	(7740) 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:	(7740) 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:	(7740) 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:	(7740) 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:	(7740) 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:	(7740) 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:	(7740) 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:	(7740) 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:	(7740) 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:	(7740) 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:	(7740) 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:	(7740) 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:	(7740) 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:	(7740) 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:	(7740) 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:	(7740) 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:	(7740) 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:	(7740) 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:	(7740) 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:	(7740) 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:	(7740) 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:	(7740) 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:	(7740) 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:	(7740) 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:	(7740) 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:	(7740) 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:	(7740) 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:	(7740) 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:	(7740) 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:	(7740) 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:	(7740) 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:	(7740) 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:	(7740) 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:	(7740) WINWORD.EXE	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\WordDocBibs\1033
Operation:	write	Name:	TM02851218
Value:	[A:TM02851218][F:gjb][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:	(7740) 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:	(7740) 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:	(7740) 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: (7740) WINWORD.EXE Operation: write 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]	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033 Name: TM03328919
(PID) Process: (7740) WINWORD.EXE Operation: write 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]	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\WordDocBibs\1033 Name: TM02851222
(PID) Process: (7740) WINWORD.EXE Operation: write 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]	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\WordDocParts\1033 Name: TM03998159
(PID) Process: (7740) WINWORD.EXE Operation: write 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]	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033 Name: TM03328986
(PID) Process: (7740) WINWORD.EXE Operation: write 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]	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\WordDocBibs\1033 Name: TM02851219
(PID) Process: (7740) WINWORD.EXE Operation: write 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]	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033 Name: TM03328986
(PID) Process: (7740) WINWORD.EXE Operation: write 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]	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033 Name: TM03328884
(PID) Process: (7740) WINWORD.EXE Operation: write 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]	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033 Name: TM03328990
(PID) Process: (7740) WINWORD.EXE Operation: write 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]	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033 Name: TM03328935
(PID) Process: (7740) WINWORD.EXE Operation: write 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]	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\WordDocBibs\1033 Name: TM02851223
(PID) Process: (7740) WINWORD.EXE Operation: write 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]	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\WordDocBibs\1033 Name: TM02851225
(PID) Process: (7740) WINWORD.EXE Operation: write 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]	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033 Name: TM03328972
(PID) Process: (7740) WINWORD.EXE Operation: write 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]	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\WordDocBibs\1033 Name: TM02851217
(PID) Process: (7740) WINWORD.EXE Operation: write 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]	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033 Name: TM03328908
(PID) Process: (7740) WINWORD.EXE Operation: write 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]	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033 Name: TM03328932
(PID) Process: (7740) WINWORD.EXE Operation: write 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]	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033 Name: TM03328925
(PID) Process: (7740) WINWORD.EXE Operation: write 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]	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\WordDocParts\1033 Name: TM02835233
(PID) Process: (7740) WINWORD.EXE Operation: write Value: [A:TM02851218][F:gjb][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]	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\WordDocBibs\1033 Name: TM02851218
(PID) Process: (7740) WINWORD.EXE Operation: write 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]	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033 Name: TM03328998
(PID) Process: (7740) WINWORD.EXE Operation: write	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\WordDocBibs\1033 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: (7740) 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: (7740) 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: (7740) 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: (7740) 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: (7740) 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: (7740) 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: (7740) 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: (7740) 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: (7740) 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: (7740) 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: (7740) 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: (7740) 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: (7740) 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: (7740) WINWORD.EXE	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033	
Operation: write	Name: NextUpdate	
Value: 2077BD4C4243DC01		
(PID) Process: (7740) WINWORD.EXE	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\SmartArt\1033	
Operation: write	Name: LastUpdate	
Value: 47533619EB41DC01		
(PID) Process: (7740) 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: (7740) WINWORD.EXE	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\WordDocBibs\1033	
Operation: write	Name: NextUpdate	
Value: 2077BD4C4243DC01		
(PID) Process: (7740) WINWORD.EXE	Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCCache\WordDocBibs\1033	
Operation: write	Name: LastUpdate	
Value: 47533619EB41DC01		
(PID) Process: (7740) 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: (7740) 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:	(7740) WINWORD.EXE	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCache\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:0][O:24]			
(PID) Process:	(7740) WINWORD.EXE	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCache\WordDocParts\1033
Operation:	write	Name:	NextUpdate
Value: 2077BD4C4243DC01			
(PID) Process:	(7740) WINWORD.EXE	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCache\WordDocParts\1033
Operation:	write	Name:	LastUpdate
Value: 0C646819EB41DC01			
(PID) Process:	(7740) WINWORD.EXE	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCache\Themes\1033
Operation:	write	Name:	NextUpdate
Value: 2077BD4C4243DC01			
(PID) Process:	(7740) WINWORD.EXE	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0\Common\LCache\Themes\1033
Operation:	write	Name:	LastUpdate
Value: 5DE9CE19EB41DC01			

Files activity

Executable files	Suspicious files	Text files	Unknown types
33	124	15	0

Dropped files

PID	Process	Filename	Type
7740	WINWORD.EXE	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\E2C6CBAF0AF08CF203BA74BF0D0AB6D5_0FB9553B978E7F00C6B2309507DEB64A MD5: 24776CB21F0741472407E5F02CF56532SHA256: 0B3C03AF86732CEE7DCC504300D89E3A62E01D117787D91BB12E06C7E4DCA8C2	binary
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\~\$mple.doc.docx MD5: 04206C1807866CC11A6741331E80CDA SHA256: B1EBEB4C139ED76F86E3A6C5412D18F47FD9A10DCFBEDFA12F59D7FD9FAB6B5C	binary
7740	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\~\$Normal.dotm MD5: 6745CC7A2B443A25AE384A864CFECE9B SHA256: AC872350FF0BD8382A1C7D35D95F8436A80886677048014D6CB70BA7F295CA4	binary
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Office\16.0\AddInClassifierCache\OfficeSharedEntities.bin MD5: CC90D669144261B198DEAD45AA266572SHA256: 89C701EEFF939A44F28921FD85365ECD87041935DCD0FE0BAF04957DA12C9899	text
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Office\16.0\Personalization\Governance\Anonymous\floodgatecampaigns.json MD5: AD94E3B45351B59212252DEE3E4D18D0 SHA256: DF43EE1C8BE01DCBF2BE714CA11FE105BA12498FABBA832DA0CD9E7643F04069	binary
7740	WINWORD.EXE	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\E2C6CBAF0AF08CF203BA74BF0D0AB6D5_CBDCCBE4F7A916411C1E69BDD97BB04 MD5: 9CDC604D15F0BDD7D6205EB2EDCEE009SHA256: BAF7BC53994541C071B733411725BBCCB493A3681463C0683F52A843EDEA21BB	binary
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Office\16.0\AddInClassifierCache\OfficeSharedEntitiesUpdated.bin MD5: 0AB288A31398051808909FCD76A9EC1E SHA256: 9C0026495F71F6F0644540AFAB782658F6215E18B24D06EE49B264AF1C76BE82	text
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Office\16.0\Personalization\Governance\Anonymous\floodgatecampaigns.json.tmp MD5: AD94E3B45351B59212252DEE3E4D18D0 SHA256: DF43EE1C8BE01DCBF2BE714CA11FE105BA12498FABBA832DA0CD9E7643F04069	binary
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\FontCache\4\PreviewFont\flat_OfficeFontsPreview_4_42.ttf MD5: 8BDF396FED21EED0F788CB9A23775A1E SHA256: BD6575CBCF808C13421BF03886E008624B85B6CE23651949BCFBD10EBD8452BE	binary
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\FontCache\4\Catalog\ListAll.Json MD5: 7C5578BC58BDE6DC855D5C929CF54232SHA256: A48ACBE81F33E5918B096A6B89687E505DA0E79196F74DC48B6E068708378A3F	binary
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\TokenBroker\Cache\089d66ba04a8cec4bdc5267f42f39cf84278bb67.tbres MD5: 9BCB95F25DEF697E7755D4BE389B706 SHA256: 5C650A33FF512A5A70E7897F1B6A55FE64C282345D66DF66BA89ACEB70C31318	binary
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\TokenBroker\Cache\56a61aeb75d8f5be186c26607f4bb213abe7c5ec.tbres MD5: C27168D4A87EAA19585C2D33DAB07ED SHA256: 2682FD44CF02C81FDA4EFA62E968F165147BFE7D5DA3BA823EFD7CA76CDD4F8E	binary
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\821E54C0-B244-4330-91FD-30145CBE6EE6 MD5: 509A5266FD9A6830F8EBA341E71EE394SHA256: 6E570AF75638671867252E3C5364C0E565833B1A604E53EB685D59D93A59C48	xml
7740	WINWORD.EXE	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\E2C6CBAF0AF08CF203BA74BF0D0AB6D5_0FB9553B978E7F00C6B2309507DEB64A MD5: 75D47E3CFD08E5FBBB4E019A7F673671SHA256: FEB86F0F03B7BC38E9D779EFF1F29C12588E28E207BC7DEADE7DCDC016F02ED6	binary
7740	WINWORD.EXE	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\E2C6CBAF0AF08CF203BA74BF0D0AB6D5_CBDCCBE4F7A916411C1E69BDD97BB04 MD5: 84991D23D1B88B40F3DE21EC6CD834CF SHA256: DAFF912EB65830FA29FEF4FE5100E7E235B17FD5C74B2CDE261E416F33EFC A16	binary
7740	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\fb3b0dbfee58fac8.customDestinations-ms	binary

		MD5: E4A1661C2C886EBB688DEC494532431C	SHA256: B76875C50EF704DBBF7F02C982445971D1BBD61AEBE2E4B28DDC58A1D66317D5	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\TokenBroker\Cache\5475cb191e478c39370a215b2da98a37e9dc813d.tbres		binary
		MD5: 05088C3FFC56274ED9EC003519D4176	SHA256: CBEE6917A2FDC866C73F8D71BA38704FE681591265874FE1A2362D9899CF412B	
7740	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\OFFIO658M9GQJKA624RY.temp		binary
		MD5: E4A1661C2C886EBB688DEC494532431C	SHA256: B76875C50EF704DBBF7F02C982445971D1BBD61AEBE2E4B28DDC58A1D66317D5	
7740	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\fb3b0dbfee58fac8.customDestinations-ms~RFF7728.TMP		binary
		MD5: 4FCB2A3EE025E4A10D21E1B154873FE2	SHA256: 90BF6BAA6F968A285F88620FBF91E1F5AA3E66E2BAD50FD16F37913280AD8228	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Office\16.0\UsageMetricsStore\FileActivityStoreV3\Word\ASkwMDAwMDAwMC0wMDAwLTAwMDAtMDAwMC0wMDAwMDAwMDAwMDAwMDBTnVsbAA.S		binary
		MD5: 8436B195C1EB2D30B3F6CEA99EFDAC52	SHA256: 0256B654E9F517DF720169DF07DAD6C7D8DDFC844EA730D79C8F64C408FB387	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab131E.tmp		compressed
		MD5: 92A819D434A8AAEA2C65F0CC2F33BB3A	SHA256: 5D13F9907AC381D19F0A7552FD6D9FC07C9BD42C0F9CE017FFF75587E1890375	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab131C.tmp		compressed
		MD5: ABBF10CEE9480E41D81277E9538F98CB	SHA256: 557E0714D5536070131E7E/CDD18F0EF23FE6FB12381040812D022EC0FEE7957	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab1322.tmp		compressed
		MD5: 89A9818E6658D73A73B642522FF8701F	SHA256: F747DD8B79FC69217FA3E36FAE0AB417C1A0759C28C2C4F8B7450C70171228E6	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab131F.tmp		compressed
		MD5: 4EFA48EC307EAF2F9B346A073C67FCFB	SHA256: 3EE9AE1F8DAB4C498BD561D8FCC66D83E58F11B7BB4B2776DF99F4CDA4B850C2	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab1338.tmp		compressed
		MD5: C455C4BC4BEC9E0DA67C4D1E53E46D5A	SHA256: 40E9AF9284FF07FDB75C33A11A794F533712BAA4A6CF82FA529FBAF5AD0FED0	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab1335.tmp		compressed
		MD5: 51804E255C573176039F4D5B55C12AB2	SHA256: 3C6F66790C543D4E9D8E0E6F476B1ACADF0A5FCDD561B8484D8DDADDFD8134B	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab1324.tmp		compressed
		MD5: D3C9036E4E1159E832B1B4D2E9D42BF0	SHA256: 434576EB1A16C2D14D666A33EDDE76717C896D79F45DF56742AFD90ACB9F21CE	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab131D.tmp		compressed
		MD5: E033CCBC7BA787A2F824CE0952E57D44	SHA256: D250EB1F93B43EFB7654B831B4183C9CAEC2D12D4EFEE8607FEE70B9FAB20730	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab1321.tmp		compressed
		MD5: 91AADBEC4171CFA8292B618492F5EF34	SHA256: 7E1A90CDB2BA7F03ABCB4687F0931858BF57E13552E0E4E54EC69A27325011EA	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab1323.tmp		compressed
		MD5: 205AF51604EF96EF1E8E60212541F742	SHA256: DF3FFF163924D08517B41455F2D06788BA4E49C68337D15ECF329BE48CF7DA2D	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab133E.tmp		compressed
		MD5: F913DD84915753042D856CEC4E5DABA5	SHA256: AA03AFB681A76C86C1BD8902EE2BBA31A644841CE6BCB913C8B5032713265578	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab133B.tmp		compressed
		MD5: 62863124CDCDA135ECC0E722782CB888	SHA256: 23CCFB7206A8F77A13080998EC6EF95B59B3C3E12B72B2D2AD4E53B0B26BB8C3	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab133A.tmp		compressed
		MD5: 69EDB3BF81C99FE8A94BBA03408C5AE1	SHA256: CEBE759BC4509700E3D23C6A5DF8D889132A60EBC92260A74947EAA1089E2789	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab133D.tmp		compressed
		MD5: E3C64173B2F4AA7AB72E1396A9514BD8	SHA256: 16C08547239E5B969041AB201EB55A3E30EAD400433E926257331CB945DFF094	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab1339.tmp		compressed
		MD5: 53EE9DA49D0B84357038ECF376838D2E	SHA256: 9E4688BA0BAD6E534AF33015C86396C33C5088D3AE5389217A5E90BA68252374	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab1337.tmp		compressed
		MD5: DA3380458170E60CBEA72602FDD0D955	SHA256: 6F8FB225F3B8C7ADE31A17A02F941FC534E4F7B5EE678B21CD9060282034701	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab1320.tmp		compressed
		MD5: F10DF902980F1D5BEEA96B2C66840A7	SHA256: E0100320A4F63E07C77138A89EA24A1CBD69784A89FE3BF83E35576114B4CE02	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab133C.tmp		compressed
		MD5: 1D6F8E73A0662A48D332090A4C8C898F	SHA256: 8077C92C66D15D7E03FBFF3A48BD9576B80F698A36A44316EABA81EE8043B673	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab134F.tmp		compressed
		MD5: C47E3430AF813DF8B02E1CB4829DD94B	SHA256: F2DB1E60533F0D108D5FB1004904C1F2E8557D4493F3B251A1B3055F8F1507A3	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab1336.tmp		compressed
		MD5: 6D787B1E223DB6B91B69238062CCA872	SHA256: DA2F261C3C82E229A097A9302C8580F014BB6442825DB47C008DA097CFCE0EE4	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab1393.tmp		compressed
		MD5: 486CBCB2238873132FFAF4B8AD0AD044	SHA256: B217393FD2F95A11E2C594E736067870212E3C5242A212D6F9539450E8684616	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab1381.tmp		compressed
		MD5: D30AD26DBB6DECA4FDD294F48EDAD55D	SHA256: 6B1633DD765A11E7ED26F8F9A4DD45023B3E4AD8B903C934DF3917D07A3856BFF	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab13C3.tmp		compressed
		MD5: 21A4B7B71631C2CCDA5FBB6A63751F0D2	SHA256: AE0C5A2C8377DBA613C576B1FF73F01AE8EF4A3A4A10B078B5752FB712B3776C	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab13C4.tmp		compressed
		MD5: E532038762503FFA1371DF03FA2E222D	SHA256: 5C70DD1551EB8B9B13EFAFEAEAF70F08B307E110CAEE75AD9908A6A42BBCCB07E	

7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab1380.tmp	compressed
		MD5: EF9CB8BDFBC08F03BEF519AD66BA642F	SHA256: 93A2F873ACF5BEAD4BC0D1CC17B5E89A928D63619F70A1918B29E5230ABEAD8E
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab13E7.tmp	compressed
		MD5: 0EBC45AA0E67CC435D075438371F948	SHA256: 3744BFA286CFCFF46E51E6A68823A23F55416CD6619156B5929FED17778F1C7
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab1417.tmp	compressed
		MD5: 65828DC7BE8BA1CE61AD7142252ACC54	SHA256: 849E2E915AA61E2F831E54F337A745A5946467D539CCBD0214B4742F4E7E94FF
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab13C5.tmp	compressed
		MD5: EE0129C7CC1AC92BBC3D6CB0F653FCAE	SHA256: 345AA5CA2496F975B7E33C182D5E57377F8B740F23E9A55F4B2B446723947B72
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab1350.tmp	compressed
		MD5: 66C5199CF4FB18BD4F9F3F2CCB074007	SHA256: 4A7DC4ED098E580C8D623C51B57C0BC1D601C45F40B60F39BBA5F063377C3C1F
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab1429.tmp	compressed
		MD5: 97F5B7B7E9E1281999468A5C42CB12E7	SHA256: 1CF5C2D0F6188FFFF117932C424CC55D1459E0852564C09D7779263ABD116118
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab13D6.tmp	compressed
		MD5: B9A6FF715719EE9DE16421AB983CA745	SHA256: E3BE3F1E341C0FA5E9CB79E2739CF0565C6EA6C189EA3E53ACF04320459A7070
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab13D7.tmp	compressed
		MD5: 8B29FAB506FD65C21C9CD6FE6BBBC146	SHA256: 773AC516C9B9B28058128EC9BE099F817F3F90211AC70DC68077599929683D6F
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab137F.tmp	compressed
		MD5: 7C645EC505982FE529D0E5035B378FFC	SHA256: 298FD9DADF0ACEBB2AA058A09EEBFAE15E5D1C5A8982DEE6669C63FB6119A13D
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab1392.tmp	compressed
		MD5: 7BF88B3CA20EB71ED453A3361908E010	SHA256: E555A610A61DB4F45A29A7FB196A9726C25772594252AD534453E69F05345283
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab1487.tmp	compressed
		MD5: 1C12315C862A745A647DAD546EB4267E	SHA256: 4E2E93EBAC4AD3F8690B020040D1AE3F8E7905AB7286FC25671E07AA0282CAC0
7740	WINWORD.EXE	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\696F3DE637E6DE85B458996D49D759AD	binary
		MD5: 12C0EE8AF57572FEB466D3A856649F3C	SHA256: 632C595F9C26336140ED13FA4E19F95F2998EE23F2B3EB31278C9E217DD5731
7740	WINWORD.EXE	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\37C951188967C8EB88D99893D9D191FE	binary
		MD5: 0BDDE46202CFA7F50640CD952AE0D6FF	SHA256: 7A615A41A8C4390078223C7C53A25093080C100434794E47952715200B93D09
7740	WINWORD.EXE	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\696F3DE637E6DE85B458996D49D759AD	binary
		MD5: 6872FAE8288DB34207D9E7EE350157F4	SHA256: 50795B027E2BC566D3B7ACB89913F8EFD23B70615C9DB9BF5B23323AD3132A7D
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab1418.tmp	compressed
		MD5: 26BEAB9CCEAFE4FBF0B7C0362681A9D2	SHA256: 217EC1B6E00A24583B166026DEC480D447FB564CF3BCA81984684648C272F767
7740	WINWORD.EXE	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\7396C420A8E1BC1DA97F1AF0D10BAD21	binary
		MD5: DA6311707878C59B687118C0656CF7F3	SHA256: FA4F39EABD01A3ED112B7D04CD6786C5CD7FB3F9B11D35982FF8CBD38961AAC
7740	WINWORD.EXE	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\37C951188967C8EB88D99893D9D191FE	binary
		MD5: 1F39D616E912A4269CC718A3B6D423EC	SHA256: AEA9C91AC573821FB0A42F7E21C39E8D2B3778892FFAE759870A8B2A833BC39
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD1565.tmp\APASixthEditionOfficeOnline.xsl	xml
		MD5: 5632C4A81D2193986ACD29EADF1A2177	SHA256: 06DE709513D7976690B3DD8F5FDF1E59CF456A2DFBA952B97EACC72FE47B238B
7740	WINWORD.EXE	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\C0018BB1B5834735BFA60CD063B31956	binary
		MD5: 69AC7DD08F3CD9BA14E9ADDE7459BF77	SHA256: 10E2B1980CB31FDCDEA070916500BE9AB509806FD87E49912DB53A05726740B9
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD1567.tmp\ThemePictureGrid.glox	compressed
		MD5: 031C246FFE0E2B623BBBD231E414E0D2	SHA256: 2D76C8D1D59EDB40D1FBBC6406A06577400582D1659A544269500479B6753CF7
7740	WINWORD.EXE	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\C0018BB1B5834735BFA60CD063B31956	binary
		MD5: FD7A77644034C2EB5820F914F47D5BD9	SHA256: 749B4F58137BDD25F5FAC367F1517FD27E4AF9393ADE0EA729F2458F5EE0D4BE
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD1564.tmp\gostname.xsl	xml
		MD5: 9888A214D362470A6189DEFF775BE139	SHA256: C64ED5C2A323C00E84272AD3A701CAEBE1DCCEB67231978DE978042F09635FA7
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD1565.tmp\Content.inf	text
		MD5: C3216C3FC73A4B3FFFE7ED67153AB7B5	SHA256: 7CF1D6A4F0BE5E6184F59BFB1304509F38E480B59A3B091DBDC43B052D2137CB
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD1564.tmp\Content.inf	text
		MD5: 8D9B02CC69FA40564E6C781A9CC9E626	SHA256: 1D4483830710EF4A2CC173C3514A9F4B0ACA6C44DB22729B7BE074D18C625BAE
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD1567.tmp\Content.inf	text
		MD5: 6F8FE7B05855C203F6DEC5C31885DD08	SHA256: B7F58DF058C938CCF39054B31472DC76E18A3764B78B414088A261E44A0870175
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD1563.tmp\ThemePictureAlternatingAccent.glox	compressed
		MD5: 2F8998AA9CF348F1D6DE16EAB2D92070	SHA256: 8A216D16DEC44E02B9AB9BBADF8A11F97210D8B73277B22562A502550658E580
7740	WINWORD.EXE	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\7396C420A8E1BC1DA97F1AF0D10BAD21	binary
		MD5: E07178901A4EAAC2816BB238EC3A80DB	SHA256: EEBD04C1272661E1091084108083CE44F7C961013791892D866B2F92EE3DED48
7740	WINWORD.EXE	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\F90F18257CBB4D84216AC1E1F3BB2C76	binary
		MD5: E95AF9B03513D729D28FD890CFF4EBE9	SHA256: B19F80A59705427F1E1728CDEE5D4534598329BA22FABF58BD2280EBD6BA629
7740	WINWORD.EXE	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\F90F18257CBB4D84216AC1E1F3BB2C76	binary

		MD5: 30A6BDF1A29D68BEA8AB50F1A2BC31F1	SHA256: 464918543F985E161CC68AABED49F2FD7E769B069305348CF1FF03D073D67E42	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD1579.tmp\architecture.glox		compressed
		MD5: 8109B3C170E6C2C114164B8947F88AA1	SHA256: F320B4BB4E57825AA4A40E5A61C1C0189D808B3EACE072B35C77F38745A4C416	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab15E3.tmp		compressed
		MD5: 9A07035EF802BF89F6ED254D0B02AB0	SHA256: 6CB03CEBAB2C28BF5318B13EEEE49FBED8DCEDAF771DE78126D1BFEB9D81C674	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD1563.tmp\Content.inf		text
		MD5: 3D52060B74D7D448DC733FFE5892CB52	SHA256: BB980559C6FC38B703D1E9C41720D5CE8D00D2FF86D4F25136DB02B1E54B1518	
7740	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\SmartArt Graphics\1033\TM003328983\{fn=Theme Picture Alternating Accent}.glox		compressed
		MD5: 2F8998AA9CF348F1D6DE16EAB2D92070	SHA256: 8A216D16DEC44E02B9AB9BBADF8A11F97210D8B73277B22562A502550658E580	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD158D.tmp\VaryingWidthList.glox		compressed
		MD5: 6776FF48AF205B771B53AA2FA82B4F4	SHA256: 160D05B4CB42E1200B859A2DE00770A5C9EBC736B70034AFC832A475372A1667	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab15E4.tmp		compressed
		MD5: 84D8F3848E7424CBE3801F9570E05018	SHA256: B4BC3CD34BD328AAF68289CC0ED4D5CF8167F1EE1D7BE20232ED4747FF96A80A	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab15E1.tmp		compressed
		MD5: 93FA9F779520AB2D22AC4EA864B7BB34	SHA256: 6A3801C1D4CF0C19A990282D93AC16007F6CACB645F0E0684EF2EDAC02647833	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD1566.tmp\Text Sidebar (Annual Report Red and Black design).docx		document
		MD5: 5A53F55DD7DA8F10A8C0E711F548B335	SHA256: 66501B659614227584DA04B64F44309544355E3582F59DBCA3C9463F67B7E303	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD158B.tmp\PictureFrame.glox		compressed
		MD5: D32E93F7782B21785424AE2BEA62B387	SHA256: 2DC7E71759D84EF8BB23F11981E2C2044626FEA659383E4B9922FE5891F5F478	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD158D.tmp\Content.inf		text
		MD5: 63E8B0621B5DEFE1EF17F02EFBFC2436	SHA256: 9243D99795DCDAD26FA857CB2740E58E3ED581E3FAEF0C83781CBCD25FB4EE06	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD1568.tmp\Content.inf		text
		MD5: C1B36A0547FB75445957A619201143AC	SHA256: 4DFF7D1CEFD8D5CC73E1554D705FA6586A1FBD10E4A73EEE44EAABA2D2FFED9	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab15F6.tmp		compressed
		MD5: E29CE2663A56A1444EAA3732FFB82940	SHA256: 3732EB6166945DB2BF792DA04199B5C4A0FB3C96621ECBFDEAF2EA1699BA88EE	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab15E5.tmp		compressed
		MD5: 21437897C9B88AC2CB2BB2FEF922D191	SHA256: 372572DCBAD590F64F5D18727757CBDF9366DDE90955C79A0FCC9F536DAB0384	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD1566.tmp\Content.inf		text
		MD5: 2F7A8FE4E5046175500AFFA228F99576	SHA256: 1495B4EC56B371148EA195D790562E5621FDBF163CDD8A5F3C119F8CA3BD2363	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD158A.tmp\CircleProcess.glox		compressed
		MD5: 950F3AB11CB67CC651082FEBE523AF63	SHA256: 9C5E4D8966A0B30A22D92DB1DA2F0DBF06AC2EA75E7BB8501777095EA0196974	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab15E2.tmp		compressed
		MD5: E1101CCA6E3FEDB28B57AF4C41B50D37	SHA256: 69B2675E47917A9469F771D0C634BD62B2DFA0F5D4AF3FD7AFE9196BF889C19E	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD1591.tmp\TabList.glox		compressed
		MD5: 0A4CA91036DC4F3CD8B6DBF18094CF25	SHA256: E5A56CCB3B3898F76ABF909209BFA401B5DDCC88289AD43CE96B02989747E50	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD1589.tmp\rings.glox		compressed
		MD5: 6C24ED9C7C868DB0D55492BB126EAF8	SHA256: 48AF17267AD75C142EFA7AB7525CA48FAB579592339FB93E92C4C4DA577D4C9F	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD1568.tmp\pictureorgchart.glox		compressed
		MD5: 586CEBC1FAC6962F9E36388E5549FFE9	SHA256: 1595C0C027B12FE4C2B506B907C795D14813BBF64A2F3F65D71912D7E57BC40	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD158C.tmp\mlaseventheditionofficeonline.xml		xml
		MD5: 377B3E355414466F3E3861BCE1844976	SHA256: 4AC5B26C5E66E122DE80243EF621CA3E1142F643DD2AD61B75FF41CFEE3DFFAF	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD1591.tmp\Content.inf		text
		MD5: A6B2731ECC78E7CED9ED5408AB4F2931	SHA256: 6A2F9E46087B1F0ED0E847AF05C4D4CC9F246989794993E8F3E15B633EFD744	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD158B.tmp\Content.inf		text
		MD5: 69757AF3677EA8D80A2FBE44DEE7B9E4	SHA256: 0F14CA656CDD95CAB385F9B722580DE2F46F8622E17A63F4534072D86DF97C3	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD1579.tmp\Content.inf		text
		MD5: D79B5DE6D93AC06005761D88783B3EE6	SHA256: 96125D6804544B8D4E6AE8638EFD4BD1F96A1BFB9EEF57337FFF40BA9FF4CDD1	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD158E.tmp\HexagonRadial.glox		compressed
		MD5: 20621E61A4C5B0FFEEC98FFB2B3BCD31	SHA256: 223EA2602C3E95840232CACC30F63AA5B050FA360543C904F04575253034E6D7	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD1594.tmp\iso690.xml		xml
		MD5: FF0E07EFF133CDF9FC2523D323DB654	SHA256: 3F925E0CC1542F09DE1F99060899EAFB0042BB9682507C907173C392115A44B5	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD159D.tmp\InterconnectedBlockProcess.glox		compressed
		MD5: 08D3A25DD65E5E0D36ADC602AE68C77D	SHA256: 58B45B9DBA959F40294DA2A54270F145644E810290F71260B90F0A3A9FCDEBC1	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD158A.tmp\Content.inf		text
		MD5: D04EC08EFE18D1611BD89A5EC0CC00B1	SHA256: FA60500F951AF8FFDB6D1828456D60004AE1558E8E1364ADC6ECB59F5450C9	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD1596.tmp\Element design set.dotx		document
		MD5: 7CDFFC23FB85AD5737452762FA36AA0	SHA256: 68A8FBFBEE4C903E17C9421082E839144C20559AFE61338CBD83AF79F0D270	

7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD158F.tmp\chicago.xml	xml
		MD5: 9AC6DE7B629A4A802A41F93DB2C49747	SHA256: 52984BC716569120D57C8E6A360376E9934F00CF31447F5892514DDCCF546293
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD1594.tmp\Content.inf	text
		MD5: 9B8D7FE8A69E41CDC2439C38FE59FAF	SHA256: 70042F1285C3CD91DDE8D4A424A5948AE8F1551495D8AF4612D59709BF69DF2
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD1590.tmp\ThemePictureAccent.glox	compressed
		MD5: 42A840DC06727E42D42C352703EC72AA	SHA256: 02CCE7D526F844F70093AC41731D1A1E9B040905DCBA63BA8BFFC0DBD4D3A7A7
7740	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\SmartArt Graphics\1033\TM03328986[[fn=Theme Picture Grid]].glox	compressed
		MD5: 031C246FFE0E2B623BBBD231E414E0D2	SHA256: 2D76C8D1D59EDB40D1FBBC6406A06577400582D1659A544269500479B6753CF7
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD159D.tmp\Content.inf	text
		MD5: 1309D172F10DD53911779C89A06BFB65	SHA256: C190F9E7D00E053596C3477455D1639C337C0BE01012C0D4F12DFCB432F5EC56
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD1590.tmp\Content.inf	text
		MD5: 6C489D45F3B56845E68BE07EA804C698	SHA256: 3FE447260CDCDEE287B8D01CF5F9F53738BFD6AAEC9FB9787F2826F8DEF1CA45
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD1589.tmp\Content.inf	text
		MD5: 2240CF2315F2EB448CEA6E9CE21B5AC5	SHA256: 0F7D0BD5A8CED523CFF4F99D7854C0EE007F5793FA9E1BA1CD933B0894BFBDD0
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD158E.tmp\Content.inf	text
		MD5: E8B30D1070779CC14FBE93C8F5CF65BE	SHA256: 2E90434BE1F6DCEA9257D42C331CD9A8D06B848859FD4742A15612B2CA6EFACB
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD158F.tmp\Content.inf	text
		MD5: 4A9A2E8DB82C90608C96008A5B6160EF	SHA256: 4FA948EEB075DFCB8DCA773A3F994560C69D275690953625731C4743CD5729F7
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD1595.tmp\gostitle.xml	xml
		MD5: F425D8C274A8571B625EE66A8CE06287	SHA256: DD7B7878427276AF5DBF8355ECE0D1FE5D693DF55AF3F79347F9D20AE50DB938
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD159C.tmp\RadialPictureList.glox	compressed
		MD5: CDC1493350011DB9892100E94D5592FE	SHA256: F637A67799B492FEFFB65632FED7815226396B4102A7ED790E0D9BB4936E1548
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD1599.tmp\turabian.xml	xml
		MD5: F079CE5E2CCB9CD4529673BCDFB90486	SHA256: 3B651258F4D0EE1BFFC7FB189250DED1B920475D1682370D6685769C3A9346DB
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD1596.tmp\Content.inf	text
		MD5: 0F98498818DC28E82597356E2650773C	SHA256: 4587CA0B2A60728FF0A5B8E87D35BF6C6FDF396747E13436EC856612AC1C6288
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD158C.tmp\Content.inf	text
		MD5: 333BA58FCE326DEA1E4A9DE67475AA95	SHA256: 66142D15C7325B98B199AB6EE6F35B7409DE64EBD5C0AB50412D18CBE6894097
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD15AE.tmp\gb.xml	xml
		MD5: 51D32EE5BC7AB811041F799652D26E04	SHA256: 6230814BF5B2D554397580613E20681752240AB87FD354ECECF188C1EABE0E97
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD1597.tmp\TabbedArc.glox	compressed
		MD5: E8308DA3D46D0BC30857243E1B7D330D	SHA256: 6534D4D7EF31B967DD0A20AFF092F8B93D3C0EFCBF19D06833F223A65C6E7C4
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD1592.tmp\BracketList.glox	compressed
		MD5: 5D9BAD7ADB88CEE98C5203883261ACA1	SHA256: 8CE600404BB3DB92A51B471D4AB8B166B566C6977C9BB63370718736376E0E2F
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD1597.tmp\Content.inf	text
		MD5: 16711B951E1130126E240A6E4CC2E382	SHA256: 855342FE16234F72DA0C2765455B69CF412948CFBE70DE5F6D75A20ACDE29AE9
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD1592.tmp\Content.inf	text
		MD5: 1A314B08BB9194A41E3794EF54017811	SHA256: 9025DD691FCAD181D5FD5952C7AA3728CD8A2CAFD20DEA14930876419BED9B379
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD1595.tmp\Content.inf	text
		MD5: A0D51783BFEE86F3AC46A810404B6796	SHA256: 47B43E7DBDF8B25565D874E4E071547666B08D7DF4D736EA8521591D0DED640F
7740	WINWORD.EXE	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\A583E2A51BFBDCE1E492A57B7C8325850	binary
		MD5: ED2BB2BDFC6E2A4019C6E42ED4B5F365	SHA256: 4C8F0F8B1DA4F336AA38A4012FCC37779B7E910BCD7548B276B384CA5E80A702
7740	WINWORD.EXE	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\A583E2A51BFBDCE1E492A57B7C8325850	binary
		MD5: 9A6C3A86296BEC3070824451A699B6E5	SHA256: 99E4AB8CC1CD4F8F371416A6D676AF0A4A864ED1BC7A7E48BA0CD40C1745FC2D6
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD159A.tmp\Content.inf	text
		MD5: 923D406B2170497AD4832F0AD3403168	SHA256: EBF9CF474825DDFE0F6032BA910D5250CBA2F5EDF9CF7E4B3107EDB5C13B50BF
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD1599.tmp\Content.inf	text
		MD5: C15EB3F4306EBF75D1E7C3C9382DEECC	SHA256: 23C262DF3AEACB125E88C8FFB7DBF56FD23F66E0D476AFD842A68DDE69658C7F
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD15AF.tmp\chevronaccent.glox	compressed
		MD5: 7BC0A35807CD69C37A949BBD51880FF5	SHA256: BD3A013F50EBF162AAC4CED11928101554C511BD40C2488CF9F5842A375B50CA
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD159C.tmp\Content.inf	text
		MD5: 52BD0762F3DC77334807DDFC60D5F304	SHA256: 30C20CC835E912A6DD89FD1BF5F7D92B233B2EC24594F1C1FE0CADB03A8C3FAB
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD159A.tmp\ConvergingText.glox	compressed
		MD5: C9F9364C659E2F0C626AC0D0BB519062	SHA256: 6FC428CA0DCFC27D351736EF16C94D1AB08DDA50CB047A054F37EC028DD08AA2
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD15AE.tmp\Content.inf	text
		MD5: 877A8A960B2140E3A0A2752550959DB9	SHA256: FE07084A41CF7DB58B06D2C0D11BCACB603D6574261D1E7EBADCF85F39AFB47
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD1598.tmp\Content.inf	text

		MD5: 93149E194021B37162FD86684ED22401	SHA256: 50BE99A154A6F632D49B04FCEE6BCA4D6B3B4B7C1377A31CE9FB45C462D697B2	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD1593.tmp\ieee2006officeonline.xsl		xml
		MD5: 0C9731C90DD24ED5CA6AE283741078D0	SHA256: ABCE25D1EB3E70742EC278F35E4157EDB1D457A7F9D002AC658AAA6EA4E4DCDF	
7740	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\SmartArt Graphics\1033\TM03328884[[fn=architecture]].glox		compressed
		MD5: 8109B3C170E6C2C114164B8947F88AA1	SHA256: F320B4BB4E57825AA4A0E5A61C1C0189D808B3EACE072B35C77F38745A4C416	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD15AF.tmp\Content.inf		text
		MD5: 4DD225E2A305B50AF39084CE568B8110	SHA256: 6F00DD73F169C73D425CB9895DAC12387E21C6E4C9C7DDCFB03AC32552E577F4	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD159B.tmp\iso690nmerical.xsl		xml
		MD5: 3BF8591E1D808BCCAD8EE2B822CC156B	SHA256: 7194396E5C833E6C8710A2E5D114E8E24338C64EC9818D51A929D57A5E4A76C8	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD1593.tmp\Content.inf		text
		MD5: F25AC64EC63FA98D9E37782E2E49D6E6	SHA256: 834046A829D1EA836131B470884905856DBF2C3C136C98ADEEFA0F206F38F8AB	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD15B1.tmp\sist02.xsl		xml
		MD5: F883B260A8D67082EA895C14BF56DD56	SHA256: EF4835DB41A485B56C2EF0FF7094BC2350460573A686182BC45FD6613480E353	
7740	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\SmartArt Graphics\1033\TM03328908[[fn=Circle Process]].glox		compressed
		MD5: 950F3AB11CB67CC651082FEBE523AF63	SHA256: 9C5E4D8966A0B30A22D92DB1DA2F0DBF06AC2EA75E7BB8501777095EA0196974	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD15B1.tmp\Content.inf		text
		MD5: 149948E41627BE5DC454558E12AF2DA4	SHA256: 1B981DC422A042CDDEBE2543C57ED3D468288C20D280FF9A9E2BB4CC8F4776ED	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD1598.tmp\Equations.dotx		document
		MD5: 2AB22AC99ACFA8A82742E774323C0DBD	SHA256: BC9D45D0419A08840093B0BF4DCF96264C02DFE5BD295CD9B53722E1DA02929D	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD15B0.tmp\Content.inf		text
		MD5: 4EC6724CBBAA516CF202A6BD17226D02C	SHA256: 18E408155A2C2A24D91CD45E065927FFDA726356AAB115D290A3C1D0B7100402	
7740	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\SmartArt Graphics\1033\TM03328935[[fn=Picture Organization Chart]].glox		compressed
		MD5: 586CEBC1FAC6962F9E36388E5549FFE9	SHA256: 1595C0C027B12FE4C2B506B907C795D14813BBF64A2F3F6F5D71912D7E57BC40	
7740	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\SmartArt Graphics\1033\TM03328990[[fn=Varying Width List]].glox		compressed
		MD5: 6776FF48AF205B771B53AA2FA82B4F4	SHA256: 160D05B4CB42E1200B859A2DE00770A9CE9BC736B70034AFC832A475372A1667	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD159B.tmp\Content.inf		text
		MD5: 9C00979164E78E3B890E56BE2DF00666	SHA256: 21CCB63A82F1E6ACD6BAB6875ABBB37001721675455C746B17529EE793382C7B	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD15B0.tmp\harvardanglia2008officeonline.xsl		xml
		MD5: 33A829B4893044E1851725F4DAF20271	SHA256: C40451CADF8944A9625DD690624EA1BA19CECB825A67081E8144AD5526116924	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab1645.tmp		compressed
		MD5: 748A53C6BDD5CE97BD54A76C7A334286	SHA256: 9AF92B1671772E8E781B58217DAB481F0AFBCF646DE36BC1BFFC7D411D14E351	
7740	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\SmartArt Graphics\1033\TM03328972[[fn=Tab List]].glox		compressed
		MD5: 0A4CA91036DC4F3CD8B6DBF18094CF25	SHA256: E5A56CCB3B3898F76ABF909209BFA401B5DDC88289AD43CE9B02989747E50	
7740	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\SmartArt Graphics\1033\TM03328932[[fn=Picture Frame]].glox		compressed
		MD5: D32E93F7782B21785424AE2BEA62B387	SHA256: 2DC7E71759D84EF8BB23F11981E2C2044626FEA659383E4B9922FE5891F5F478	
7740	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\Word Document Building Blocks\1033\TM03998158[[fn=Element]].dotx		document
		MD5: 7CDFFC23FB85AD5737452762FA36AAA0	SHA256: 68A8FBFBEE4C903E17C9421082E839144C05C559AFE61338CBD83AF79F0D270	
7740	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\SmartArt Graphics\1033\TM03328916[[fn=Converging Text]].glox		compressed
		MD5: C9F9364C659E2F0C626AC0D0BB519062	SHA256: 6FC428CAODCFC27D351736EF16C94D1AB08DDA50CB047A054F37EC028DD08AA2	
7740	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\SmartArt Graphics\1033\TM03328998[[fn=Rings]].glox		compressed
		MD5: 6C24ED9C7C868DB0D55492BB126EAF8	SHA256: 48AF17267AD75C142EFA7AB7525CA48FAB579592339FB93E92C4C4DA577D4C9F	
7740	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\SmartArt Graphics\1033\TM03328925[[fn=Interconnected Block Process]].glox		compressed
		MD5: 08D3A25DD65E5E0D36ADC602AE68C77D	SHA256: 58B45B9DBA959F40294DA2A54270F145644E810290F71260B90F0A3A9FCDEBC1	
7740	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\SmartArt Graphics\1033\TM03328940[[fn=Radial Picture List]].glox		compressed
		MD5: CDC1493350011DB9892100E94D5592FE	SHA256: F637A67799B492FEFFB65632FED7815226396B4102A7ED790E0D9BB4936E1548	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab1711.tmp		compressed
		MD5: 828F96031F40BF8EBCB5E52AAEEB7E4C	SHA256: 640AD075B555D4A2143F909EAFD91F54076F5DDE42A2B11CD897BC564B5D7FF7	
7740	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\Word Document Building Blocks\1033\TM01840907[[fn=Equations]].dotx		document
		MD5: 2AB22AC99ACFA8A82742E774323C0DBD	SHA256: BC9D45D0419A08840093B0BF4DCF96264C02DFE5BD295CD9B53722E1DA02929D	
7740	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\SmartArt Graphics\1033\TM03328905[[fn=Chevron Accent]].glox		compressed
		MD5: 7BC0A35807CD69C37A949BBD51880FF5	SHA256: BD3A013F50EBF162AAC4CED11928101554C511BD40C2488CF95842A375B50CA	
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab1712.tmp		compressed
		MD5: BF95E967E7D1CEC8EFE426BC0127D3DE	SHA256: 4C3B008E0EB10A722D8FEDB325BFB97EDAA609B1E901295F224DD4CB4DF5FC26	
7740	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\SmartArt Graphics\1033\TM03328893[[fn=BracketList]].glox		compressed

		MD5: 5D9BAD7ADB88CEE98C5203883261ACA1	SHA256: 8CE6004048B3DB92A51B471D4AB8B166B566C6977C9BB63370718736376E0E2F
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Low\Microsoft\CryptnetUrlCache\Content\4C7F163ED126D5C3CB9457F68EC64E9E	<div>binary</div>
		MD5: AA19435EDE4656C3E74B668CC6877589	SHA256: E922EF4A390E4ADD161F106F4212CA97EEADC39D191D2C96A92ED81B8DBF512B
7740	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\SmartArt Graphics\1033\TM03328919[[fn=Hexagon Radial]].glox	<div>compressed</div>
		MD5: 20621E61A4C5B0FFEEC98FFB2B3BCD31	SHA256: 223EA2602C3E95840232ACC30F63AA5B050FA360543C904F04575253034E6D7
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Low\Microsoft\CryptnetUrlCache\MetaData\4C7F163ED126D5C3CB9457F68EC64E9E	<div>binary</div>
		MD5: 23614343FB2F12CC265C79ACA1963568	SHA256: E5D0C58E6EF4CF171AA91972DD8FDAF79BD62C78679D01D4977C80959B245E52
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab1771.tmp	<div>compressed</div>
		MD5: BEB12A0464D096CA33BAEA4352CE800F	SHA256: A44166F5C9F2553555A43586BA5DB1C1DE54D72D308A48268F27C6A00076B1CA
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab1791.tmp	<div>compressed</div>
		MD5: 749C3615E54C8E6875518CFD84E5A1B2	SHA256: F2D2DF37366F8E49106980377D2448080879027C380D90D5A25DA3BDAD771F8C
7740	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\SmartArt Graphics\1033\TM03328951[[fn=Tabbed Arc]].glox	<div>compressed</div>
		MD5: E8308DA3D46D0BC30857243E1B7D330D	SHA256: 6534D4D7EF31B967DD0A20AFF092F8B93D3C0EFCBF19D06833F223A65C6E7C4
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab187F.tmp	<div>compressed</div>
		MD5: 53C5F45B22E133B28D4BD3B5A350FDBD	SHA256: 8AF4C7CAC47D2B9C7ADEADF276EDA830B4CC5FFE7E765E3C3D7B3FADCB5F273
7740	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\SmartArt Graphics\1033\TM03328975[[fn=Theme Picture Accent]].glox	<div>compressed</div>
		MD5: 42A840DC06727E42D42C352703EC72AA	SHA256: 02CCE7D526F844F70093AC41731D1A1E9B040905DCBA63BA8BFFC0DBD4D3A7A7
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab17F2.tmp	<div>compressed</div>
		MD5: 9C9F49A47222C18025CC25575337A965	SHA256: ADA7EFF0676D9CCE1935D5485F3DDE35C594D343658FB1DA42CB5A48FC3FC16A
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD17A1.tmp\Insight design set.docx	<div>document</div>
		MD5: 8BC84DB5A3B2F8AE2940D3FB19B43787	SHA256: AF1FDEEA092169BF794CDC290BCA20AEA07AC7097D0EFCAB76F783FA38FDACDD
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab17F1.tmp	<div>compressed</div>
		MD5: D4EAC009E9E7B64B8B001AE82B8102FA	SHA256: 8B0631DA4DC79E036251379A0A68C3BA977F14BCC797BA0EB9692F8BB90DDB4D
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\TCD17A1.tmp\Content.inf	<div>text</div>
		MD5: 55BA5B2974A072B131249FD9FD42EB91	SHA256: 13FFAAFFC987BAAEF7833CD6A8994E504873290395DC2BD9B8E1D7E7E64199E7
7740	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\Word Document Building Blocks\1033\TM03998159[[fn=Insight]].dotx	<div>document</div>
		MD5: 8BC84DB5A3B2F8AE2940D3FB19B43787	SHA256: AF1FDEEA092169BF794CDC290BCA20AEA07AC7097D0EFCAB76F783FA38FDACDD
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab19B9.tmp	<div>compressed</div>
		MD5: F256ACA509B4C6C0144D278C7036B0A8	SHA256: AD26761D59F1FA9783C2F49184A2E8FE55FCD46CD3C49FFC099C02310649DC67
7740	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\cab1A37.tmp	<div>compressed</div>
		MD5: 8867BDF5FC754DA9DA6F5BA341334595	SHA256: 42323DD1D3E88C3207E16E0C95CA1048F2E4CD66183AD23B90171DA381D37B58

Network activity

HTTP(S) requests

14

TCP/UDP connections

89

DNS requests

31

Threats

0

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
—	—	GET	200	96.16.241.23:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDI7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	unknown	—	—	<div>whitelisted</div>
—	—	GET	200	96.16.241.23:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTrrjydrYt%2BApF3GSPypfHBxR5XtQQUs9tlpPmxxdiuNkHMEWNPYim8S8YCEAI5PUjXAKJafLQcAAo18o%3D	unknown	—	—	<div>whitelisted</div>
7740	WINWORD.EXE	GET	200	184.25.102.141:80	http://crl.microsoft.com/pki/crl/products/MicTimStaPca_2010-07-01.crl	unknown	—	—	<div>whitelisted</div>
—	—	GET	200	96.16.241.23:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDI7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	unknown	—	—	<div>whitelisted</div>
7448	backgroundTaskHost.exe	GET	200	96.16.241.23:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Zt1%2Bz8SIPI7wEWVxDIQQUTiJUIBiV5uNu5g%2F6%2BrkS7QYXjzkCEAn5bsKVvY8kdJ6vHI3O1J0%3D	unknown	—	—	<div>whitelisted</div>
7740	WINWORD.EXE	GET	200	96.16.241.23:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Zt1%2Bz8SIPI7wEWVxDIQQUTiJUIBiV5uNu5g%2F6%2BrkS7QYXjzkCEAn5bsKVvY8kdJ6vHI3O1J0%3D	unknown	—	—	<div>whitelisted</div>
7740	WINWORD.EXE	GET	200	96.16.241.23:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Zt1%2Bz8SIPI7wEWVxDIQQUTiJUIBiV5uNu5g%2F6%2BrkS7QYXjzkCEApDqVcBaTUviZV57HlulA%3D	unknown	—	—	<div>whitelisted</div>

1416	backgroundTaskHost.exe	GET	200	172.66.2.5:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGuAABQ50otx%2Fh0Zt1%2Bz8SiPI7wEWVxDIQUtIjUIBiV5uNu5g%2F6%2BrkS7QYXjzkCEAn5bsKVvV8kdJ6vHI301J0%3D	unknown	—	—	<div>whitelisted</div>
7740	WINWORD.EXE	GET	200	184.25.102.141:80	http://crl.microsoft.com/pki/crl/products/microsoftrootcert.crl	unknown	—	—	<div>whitelisted</div>
7740	WINWORD.EXE	GET	200	184.25.102.141:80	http://crl.microsoft.com/pki/crl/products/MicrosoftTimeStampPCA.crl	unknown	—	—	<div>whitelisted</div>
7740	WINWORD.EXE	GET	200	184.25.102.141:80	http://crl.microsoft.com/pki/crl/products/MicCodSigPCA_08-31-2010.crl	unknown	—	—	<div>whitelisted</div>
7740	WINWORD.EXE	GET	200	184.25.102.141:80	http://crl.microsoft.com/pki/crl/products/MicRooCerAut2011_2011_03_22.crl	unknown	—	—	<div>whitelisted</div>
7740	WINWORD.EXE	GET	200	2.22.57.219:80	http://www.microsoft.com/pkiops/crl/MicCodSigPCA2011_2011_07-08.crl	unknown	—	—	<div>whitelisted</div>
7740	WINWORD.EXE	GET	200	184.25.102.141:80	http://crl.microsoft.com/pki/crl/products/MicRooCerAut_2010-06-23.crl	unknown	—	—	<div>whitelisted</div>

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
5488	svchost.exe	40.127.240.158:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	<div>whitelisted</div>
4	System	192.168.100.255:137	—	—	—	<div>whitelisted</div>
6980	svchost.exe	40.126.32.74:443	login.live.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	<div>whitelisted</div>
5596	MoUsocoreWorker.exe	40.127.240.158:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	<div>whitelisted</div>
—	—	23.48.32.223:443	www.bing.com	Akamai International B.V.	US	<div>whitelisted</div>
—	—	96.16.241.23:80	ocsp.digicert.com	AKAMAI-AS	US	<div>whitelisted</div>
7416	backgroundTaskHost.exe	23.48.32.223:443	www.bing.com	Akamai International B.V.	US	<div>whitelisted</div>
3440	svchost.exe	172.211.123.248:443	client.wns.windows.com	MICROSOFT-CORP-MSN-AS-BLOCK	FR	<div>whitelisted</div>
7448	backgroundTaskHost.exe	20.223.35.26:443	arc.msn.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	<div>whitelisted</div>
7448	backgroundTaskHost.exe	96.16.241.23:80	ocsp.digicert.com	AKAMAI-AS	US	<div>whitelisted</div>
7740	WINWORD.EXE	52.109.32.97:443	officeclient.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	GB	<div>whitelisted</div>
7740	WINWORD.EXE	184.25.102.76:443	omex.cdn.office.net	Akamai International B.V.	US	<div>whitelisted</div>
4	System	192.168.100.255:138	—	—	—	<div>whitelisted</div>
7740	WINWORD.EXE	52.123.129.14:443	ecs.office.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	<div>whitelisted</div>
7740	WINWORD.EXE	52.109.76.243:443	roaming.svc.cloud.microsoft	MICROSOFT-CORP-MSN-AS-BLOCK	IE	<div>whitelisted</div>
7740	WINWORD.EXE	96.16.241.23:80	ocsp.digicert.com	AKAMAI-AS	US	<div>whitelisted</div>
7740	WINWORD.EXE	23.67.174.202:443	fs.microsoft.com	AKAMAI-AS	US	<div>whitelisted</div>
7740	WINWORD.EXE	52.111.243.8:443	messaging.engagement.office.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	<div>whitelisted</div>
5488	svchost.exe	51.104.136.2:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	<div>whitelisted</div>
7740	WINWORD.EXE	4.251.34.91:443	nleditor.osi.office.net	MICROSOFT-CORP-MSN-AS-BLOCK	US	<div>whitelisted</div>
7740	WINWORD.EXE	13.69.116.109:443	self.events.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	<div>whitelisted</div>
6980	svchost.exe	20.190.160.2:443	login.live.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	<div>whitelisted</div>
5596	MoUsocoreWorker.exe	51.104.136.2:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	<div>whitelisted</div>
1416	backgroundTaskHost.exe	20.223.35.26:443	arc.msn.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	<div>whitelisted</div>
5280	RUXIMICS.exe	51.104.136.2:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	<div>whitelisted</div>
1416	backgroundTaskHost.exe	172.66.2.5:80	ocsp.digicert.com	—	US	<div>whitelisted</div>
7740	WINWORD.EXE	184.25.102.28:443	metadata.templates.cdn.office.net	Akamai International B.V.	US	<div>whitelisted</div>
7740	WINWORD.EXE	184.25.102.84:443	binaries.templates.cdn.office.net	Akamai International B.V.	US	<div>whitelisted</div>
7740	WINWORD.EXE	184.25.102.141:80	crl.microsoft.com	Akamai International B.V.	US	<div>whitelisted</div>
7740	WINWORD.EXE	2.22.57.219:80	www.microsoft.com	AKAMAI-AS	FR	<div>whitelisted</div>
5308	SIHClient.exe	74.179.77.204:443	slscr.update.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	<div>whitelisted</div>
5308	SIHClient.exe	13.85.23.206:443	fe3cr.delivery.mp.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	<div>whitelisted</div>

DNS requests

Domain	IP	Reputation
settings-win.data.microsoft.com	40.127.240.158 51.104.136.2	whitelisted
login.live.com	40.126.32.74 20.190.160.2 40.126.32.140 40.126.32.136 40.126.32.138 20.190.160.66 20.190.160.5 20.190.160.65	whitelisted
google.com	142.250.186.174	whitelisted
www.bing.com	23.48.32.223 23.48.32.225 23.48.32.228 23.48.32.224 23.48.32.227 23.48.32.226 23.48.32.229 23.48.32.230 23.48.32.222	whitelisted
ocsp.digicert.com	96.16.241.23 172.66.2.5 162.159.142.9	whitelisted
client.wns.windows.com	172.211.123.248	whitelisted
arc.msn.com	20.223.35.26	whitelisted
fd.api.iris.microsoft.com	20.223.35.26	whitelisted
officeclient.microsoft.com	52.109.32.97	whitelisted
roaming.svc.cloud.microsoft	52.109.76.243	unknown
omex.cdn.office.net	184.25.102.76 184.25.102.75	whitelisted
ecs.office.com	52.123.129.14 52.123.128.14	whitelisted
fs.microsoft.com	23.67.174.202	whitelisted
messaging.engagement.office.com	52.111.243.8	whitelisted
messaging.lifecycle.office.com	52.111.243.8	whitelisted
nleditor.osi.office.net	4.251.34.91	whitelisted
self.events.data.microsoft.com	13.69.116.109 20.50.80.210	whitelisted
metadata.templates.cdn.office.net	184.25.102.28 184.25.102.15	whitelisted
binaries.templates.cdn.office.net	184.25.102.84 184.25.102.98	whitelisted
crl.microsoft.com	184.25.102.141 184.25.102.145	whitelisted
www.microsoft.com	2.22.57.219	whitelisted
slscr.update.microsoft.com	74.179.77.204	whitelisted
fe3cr.delivery.mp.microsoft.com	13.85.23.206	whitelisted
activation-v2.sls.microsoft.com	4.154.185.43	whitelisted

Threats

No threats detected

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.



Interactive malware hunting service ANY.RUN
© 2017-2025 ANY.RUN LLC. ALL RIGHTS RESERVED