ANY RUN
Interactive malware hunting service

General Info

File name	ft3058_1.doc
Full analysis	
Verdict	**Malicious activity**
Analysis date	3/3/2020, 09:49:08
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Tags:	**macros** **macros-on-open** **generated-doc** **maldoc-8**
Indicators:	
MIME:	application/vnd.openxmlformats-officedocument.wordprocessingml.document
File info:	Microsoft Word 2007+
MD5	F3AD208C650931002564411825F05D78
SHA1	077029B266C33C173A0E4443F4D26C7AC5E8D0EB
SHA256	62862A6B1C12B3C747698B53326EDDB871AC4E2DE216124C48479D43658BD740
SSDEEP	6144:B8GW+YB57DVQAIWK7KNPCDX/FBM5MBOFG2XYNDSXODCTB922FZUSSVTIDEK/KCK:BUDDVFIP7XN/TQRXV++FYMYVTI9KCK

Behavior activities

MALICIOUS	SUSPICIOUS	INFO
Starts CMD.EXE for commands execution • WINWORD.EXE (PID: 1348)	**Executes scripts** • cmd.exe (PID: 3356)	**Reads Microsoft Office registry keys** • WINWORD.EXE (PID: 1348)
Unusual execution from Microsoft Office • WINWORD.EXE (PID: 1348)		**Creates files in the user directory** • WINWORD.EXE (PID: 1348)

Static information

TRiD

.docm | Word Microsoft Office Open XML Format document (with Macro) (53.6%)
.docx | Word Microsoft Office Open XML Format document (24.2%)
.zip | Open Packaging Conventions container (18%)
.zip | ZIP compressed archive (4.1%)

EXIF

ZIP

ZipRequiredVersion:	20
ZipBitFlag:	0x0006
ZipCompression:	Deflated
ZipModifyDate:	1980:01:01 00:00:00
ZipCRC:	0xfefd9a9e
ZipCompressedSize:	482
ZipUncompressedSize:	2010
ZipFileName:	[Content_Types].xml

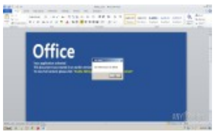
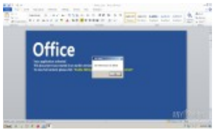
XMP

Title:	*null*
Creator:	*null*

XML

LastModifiedBy:	*null*
RevisionNumber:	1
CreateDate:	2020:01:13 01:40:00Z
ModifyDate:	2020:02:25 13:14:00Z
Template:	Normal.dotm
TotalEditTime:	*null*
Pages:	1
Words:	1
Characters:	7
Application:	Microsoft Office Word
DocSecurity:	None
Lines:	1
Paragraphs:	1
ScaleCrop:	No
HeadingPairs	*null* *null*
TitlesOfParts:	*null*
LinksUpToDate:	No
CharactersWithSpaces:	7
SharedDoc:	No
HyperlinksChanged:	No
AppVersion:	14

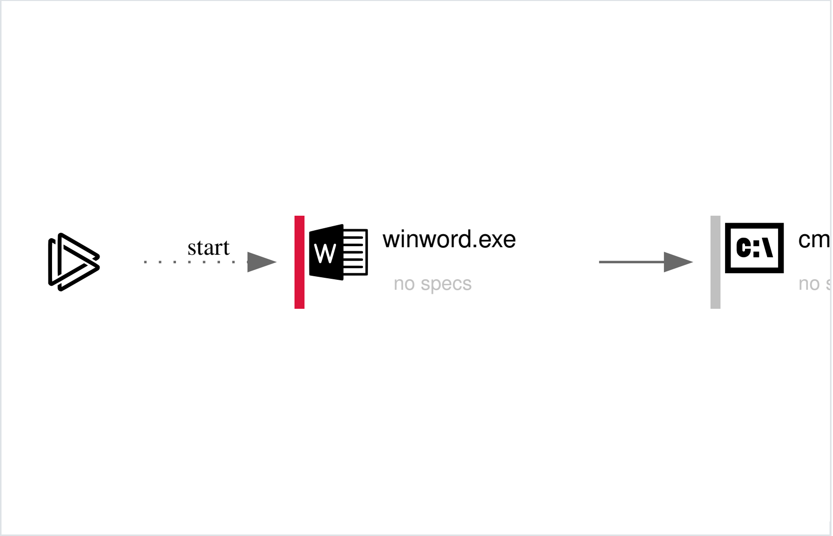
Screenshots

Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
38	3	1	0

Behavior graph



Registry activity

Total events	Read events	Write events	Delete events
1123	956	166	1

Modification events

PID	Process	Operation	Key	Name	Value
1348	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems	p91	7039310044050000010000000000000000000000
1348	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages	1033	Off
1348	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages	1041	Off
1348	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages	1046	Off
1348	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages	1036	Off
1348	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft	1031	Off

Files activity

Executable files	Suspicious files	Text files	Unknown types
0	0	2	3

Dropped files

PID	Process	Filename	Type
1348	WINWORD.EXE	C:\AprilReport\List1.jse	text
		MD5: 36254B3F04E27E6ECB138EB4DFE0...	**SHA256:** 8187C859F666
1348	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\~DF2D6E631F88D20F16.TMP	––
		MD5: ––	**SHA256:** ––
1348	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\~DF9AD41F3F659D34C8.TMP	––
		MD5: ––	**SHA256:** ––
1348	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\~DF79B5F916CD39B754.TMP	––
		MD5: ––	**SHA256:** ––
1348	WINWORD.EXE	C:\AprilReport\LogsTsg\LogsTsg7\LogsTsg8\List1.bat	text
		MD5: EF370F56174BD3E1D2ED1597AE9...	**SHA256:** 2F1D06C3EDF1
1348	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\VBE\MSForms.exd	tlb
		MD5: 9493686A47E362BC6502A2CA40A4...	**SHA256:** CE732DFBC5A7
1348	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\~$3058_1.doc	pgc
		MD5: D1B371A938777CF40D3B237C415...	**SHA256:** FE97B6426225
1348	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	pgc
		MD5: 79E75D269FD97A0359A2AF837AEE...	**SHA256:** 9CA4EAC61FC0
1348	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\CVR6970.tmp.cvr	––
		MD5: ––	**SHA256:** ––

Network activity

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

No network activity.

Debug output strings

No debug info.

Interactive malware hunting service ANY.RUN