Interactive malware hunting service

General Info

File name	pk-3215981491.doc
Full analysis	
Verdict	Malicious activity
Analysis date	3/2/2020, 10:32:40
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 64 bit)
Tags:	macros, macros-on-open, generated-doc, maldoc-42
Indicators:	
MIME:	application/msword
File info:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1251, Author: user, Template: Normal, Last Saved By: Windows User, Revision Number: 2, Name of Creating Application: Microsoft Office Word, Create Time/Date: Fri Feb 28 17:20:00 2020, Last Saved Time/Date: Fri Feb 28 17:20:00 2020, Number of Pages: 1, Number of Words: 0, Number of Characters: 1, Security: 0
MD5	81CD9B1F5D32E93A0B6730CDCD584558
SHA1	6766562AD5A1456404824CF36EEF73BF0EABD969
SHA256	9C15DFDA67A14BAAACB69FFB547509BB8516758628CD4286C4BED4F7D0E795FC
SSDEEP	3072:S/S1DIRZ4EEVUDCU/0GT0PZKQ5YWLZURHKPZZS4Q+ZDBX1VIBPRBGPU3VKUKANH3:RDI/XTRTOKZH/5/UC

Behavior activities

MALICIOUS	SUSPICIOUS	INFO
No malicious indicators.	**Creates files in the user directory** • powershell.exe (PID: 2360) **Reads the machine GUID from the registry** • powershell.exe (PID: 2360) **PowerShell script executed** • powershell.exe (PID: 2360) **Starts CertUtil for decode files** • powershell.exe (PID: 2360) **Executed via WMI** • powershell.exe (PID: 2360)	**Reads the machine GUID from the registry** • WINWORD.EXE (PID: 2876) **Reads Microsoft Office registry keys** • WINWORD.EXE (PID: 2876) **Creates files in the user directory** • WINWORD.EXE (PID: 2876)

Static information

TRiD

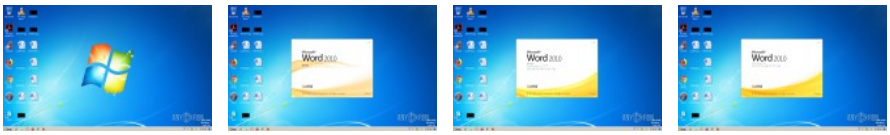
.doc | Microsoft Word document (38.3%)
.xls | Microsoft Excel sheet (alternate) (29.3%)
.doc | Microsoft Word document (old ver.) (22.7%)

EXIF

FlashPix

Title:	*null*
Subject:	*null*
Author:	user
Keywords:	*null*
Comments:	*null*
Template:	Normal
LastModifiedBy:	Windows User
RevisionNumber:	2
Software:	Microsoft Office Word
TotalEditTime:	*null*
CreateDate:	2020:02:28 17:20:00
ModifyDate:	2020:02:28 17:20:00
Pages:	1
Words:	*null*
Characters:	1
Security:	None
CodePage:	Windows Cyrillic
Company:	diakov.net
Lines:	1
Paragraphs:	1
CharCountWithSpaces:	1
AppVersion:	15
ScaleCrop:	No
LinksUpToDate:	No
SharedDoc:	No
HyperlinksChanged:	No
TitleOfParts	*null* *null*
HeadingPairs	*null* *null* *null* *null*
CompObjUserTypeLen:	32
CompObjUserType:	Microsoft Word 97-2003 Document

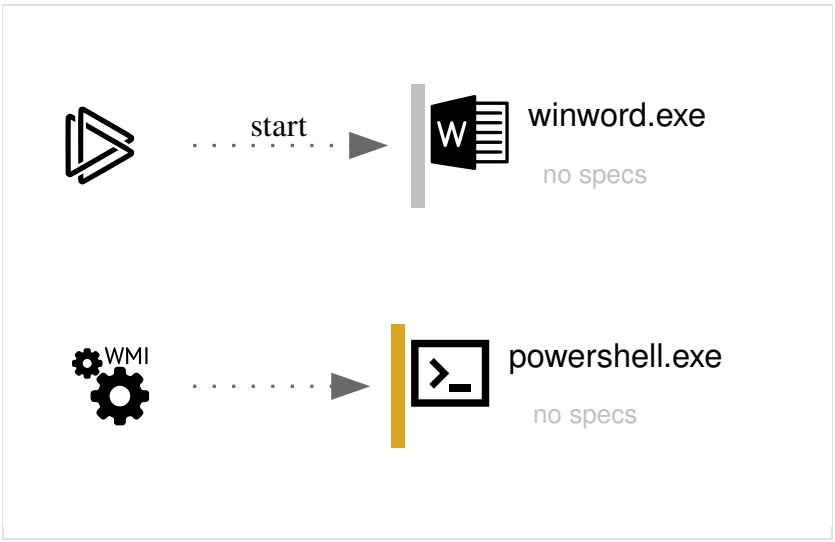
Video and screenshots



Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
40	3	0	1

Behavior graph



Registry activity

Total events	Read events	Write events	Delete events
1923	1246	615	62

Modification events

PID	Process	Operation	Key	Name	Value
2876	WINWORD.EXE	delete key	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems		
2876	WINWORD.EXE	delete key	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\12E0F3		
2876	WINWORD.EXE	delete key	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery		
2876	WINWORD.EXE	delete key	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency		
2876	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems	73>	37333E003C0B000001000000000000000000000000
2876	WINWORD.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\Enabled	1033	Off

Files activity

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

Dropped files

PID	Process	Filename	Type
2876	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{30FF04C6-CF38-4378-ADEA-DD4F92343A73}.tmp **MD5:** -- **SHA256:** --	--
2876	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{F821A5A6-C466-4894-B801-3D1E4930EE38}.tmp **MD5:** -- **SHA256:** --	--
2876	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\~DF94F6657CA73E2961.TMP **MD5:** -- **SHA256:** --	--
2360	powershell.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms~RF12ea1a.TMP **MD5:** 4E6AD0ECE45F8A679C9EC44CBA8... **SHA256:** 50D19BA8D1C7	binary
2360	powershell.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms **MD5:** 4E6AD0ECE45F8A679C9EC44CBA8... **SHA256:** 50D19BA8D1C7	binary
2360	powershell.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\M92XF8WPSN24UVIF54VT.temp **MD5:** -- **SHA256:** --	--
2876	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Office\Recent\pk-3215981491.doc.LNK **MD5:** 8B2461BC46698550FD70192AF299... **SHA256:** 90293CB9EABB	lnk
2876	WINWORD.EXE	C:\Users\admin\AppData\Roaming\Microsoft\Office\Recent\index.dat **MD5:** B9E6C47CF3A2B9B1B0312AD9E98... **SHA256:** C310BA149D76	text
2876	WINWORD.EXE	C:\Users\admin\Desktop\~$-3215981491.doc **MD5:** CB9B2CC6C7D675091BAA1E1986D... **SHA256:** E21D3DC6E031	pgc
2876	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\CVRD317.tmp.cvr **MD5:** -- **SHA256:** --	--

Network activity

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

HTTP requests

No HTTP requests.

Connections

No connections.

DNS requests

Domain	IP	Reputation
atest001.site	No response	malicious

Threats

No threats detected.

Debug output strings

No debug info.