



Analyzing Malicious Office Documents

@DidierStevens – Senior Analyst, NVISO

Analyzing Malicious Office Documents

<http://didierstevens.com/workshop-maldoc-1.zip>

About Didier

I'm Didier Stevens and work as a senior analyst for NVISO. This includes malware analysis and incident response. I'm a Microsoft MVP and SANS Internet Storm Center Handler.



Offvis

OfficeMalScanner

Analyzing Malicious Office Documents



olevba



oledump

<http://didierstevens.com/workshop-maldoc-1.zip>



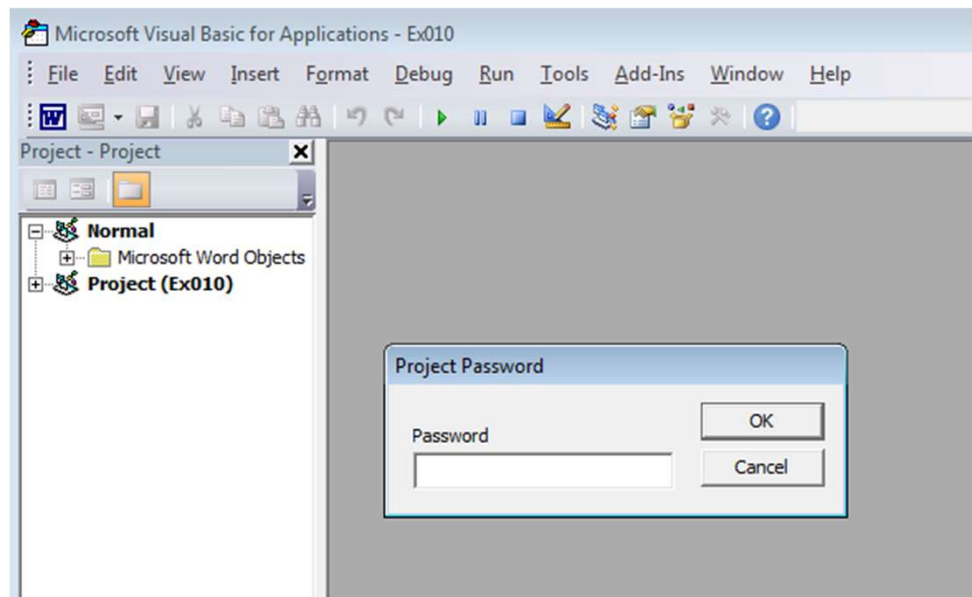
Python 2

Analyzing Malicious Office Documents

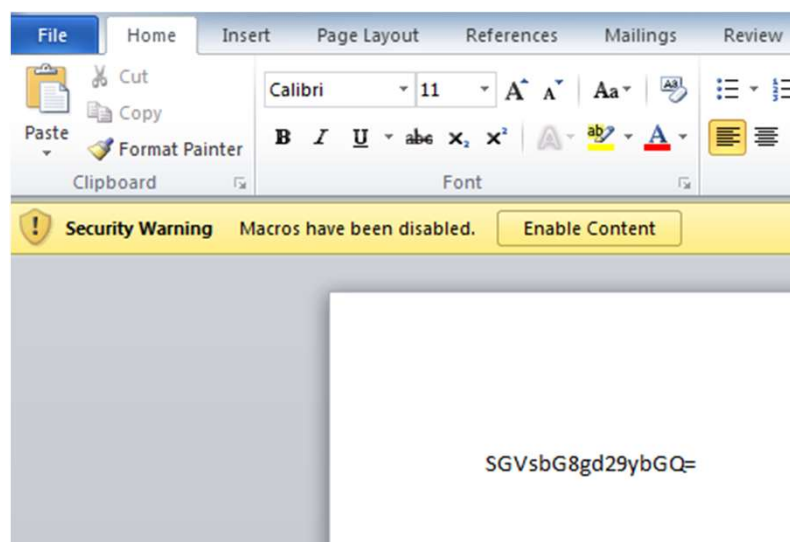


```
C:\Windows\system32\cmd.exe
C:\Workshop>oledump.py
This program requires module OleFileIO_PL.
http://www.decalage.info/python/olefileio
C:\Workshop>_
```


Analyzing Malicious Office Documents



Analyzing Malicious Office Documents





<http://blog.nviso.be>

<https://blog.DidierStevens.com>

<http://isc.sans.edu>

@DidierStevens – Senior Analyst, NVISO