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.
Analyzing Malicious Office Documents

Offvis

OfficeMalScanner
Analyzing Malicious Office Documents

olevba
Analyzing Malicious Office Documents

oledump

http://didierstevens.com/workshop-maldoc-1.zip
Analyzing Malicious Office Documents

Python 2

@DidierStevens – Senior Analyst, NVISO
Analyzing Malicious Office Documents
Analyzing Malicious Office Documents
Analyzing Malicious Office Documents