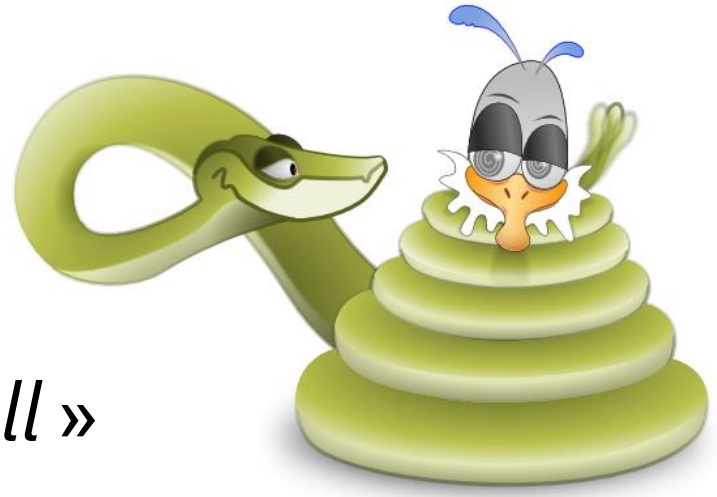
OpenOffice Macro in python : *« for Fun and for Profit »*

iAWACS 2010

Guillaume FAHRNER, gfahrner@lexsi.com

Context

- OpenOffice ships with the python scripting language
- AV handle MS Office macro but not OO one
- Same issue for macro security configuration
- One code to « *pown them all* »



Methods to avoid detection

- Cryptanalysis
- Decryption / Encryption
- Polymorphism

Viral ransomware : algorithm

1. Hide user interface
2. Bruteforce key on a known plaintext
3. Load decrypted code
4. Generate new encryption key and new known plaintext
5. Infection of all drives (local and network) for MS OS and from « / » on UNIX OS. For each ODT file found :
    1. Code obfuscation (file, variable and function name)
    2. Generate new encryption key and new known plaintext
    3. Encrypt new code with the new key
    4. Infecting file with the new code
6. Launch payload
7. Close OpenOffice

Viral ransomware : payload

1. Archive the HOME directory (with a unique filename)
2. Encrypt the arhive with AES 256 (not implemented yet)
3. Delete the HOME directory
4. HTTP POST request to send the AES key and the filename on a webserver
5. Drop AES key ☺ and let a message for the user

Questions

Thank you for your attention,

Any questions ?