OS X Backdoor

Using msfvenom

- Tool made by metasploit to generate payloads.
- Can be used to generate payloads for all operating systems.
- Even Veil uses it to generate its payloads.

PS: We will cover how to use msfvenom to generate an OS X backdoor but the same method can be used to generate backdoors for other operating systems.

OS X Backdoors

- Fat Rat and Empire can both generate OSX payloads.
  - Select OS X option in from menu 01 in Fat Rat.
  - Or use a stager that starts with osx in Empire.

PS: setting and using the backdoor is the same weather it is a Windows backdoor or an OS X backdoor.

Creating a Trojan For OS X

→ Configure evil file to download & execute a normal file (image, book, song ...etc).

→ Compile trojan & change its icon.

→ Configure trojan to run silently.

PS: No need to use any extensions in Mac or Linux machines.

Creating a Trojan For OS X

→ Configure evil file to download & execute a normal file (image, book, song ...etc). ✓

→ Compile trojan & change its icon.

→ Configure trojan to run silently.

PS: No need to use any extensions in Mac or Linux machines.

Creating a Trojan For OS X

→ Configure evil file to download & execute a normal file (image, book, song ...etc). ✓

→ Compile trojan & change its icon. ✓

→ Configure trojan to run silently.

PS: No need to use any extensions in Mac or Linux machines.

Trojans in Microsoft Office Docs

- Microsoft Office documents can run VBA code.
- VBA can be used to download & execute files.

–> Create a normal document with VBA code to download & execute evil files.