

WINDOWS EVIL FILES

- Backdoors.
- Keyloggers.
- Password Recovery tools.
- Download & execute payloads
- And more !



VEIL - FRAMEWORK



- A backdoor is a file that gives us full control over the machine that it gets executed on.
- Backdoors can be caught by Anti-Virus programs.
- Veil is a framework for generating **Undetectable** backdoors.

THE FAT RAT

- Just like Veil, generates **Undetectable** Metasploit backdoors.
- Uses a **different** methods to evade AV programs.
- Generates executable binary backdoors for:
 - Windows.
 - Mac OS.
 - Linux.
 - And Android.



EMPIRE



- Generates **Undetectable** Metasploit backdoors.
- Uses a **completely different** approach to evade AV programs.
- Uses native listener.
- Generates backdoors for:
 - Windows.
 - Mac OS.
 - Linux.
 - And Android.

BYPASSING ALL AVS



- Av programs use database of signatures to detect malware.
- Modifying backdoor code will change its signature.
 - > What if we manually change backdoor code?
- Idea:
 - Open backdoor with text editor.
 - Make sure shellcode is not detect, if it then change payload settings or use a different one.
 - Remove all arguments, add them one by one to identify the one triggering AV programs
 - Remove / modify detectable code.

ZLOGGER

- Keylogger is a program that records keys pressed on the keyboard
- Runs in the **background** of target system.
- **Reports every key** pressed on the target machine to email.
- Starts with system **boot**.

LAZAGNE

- Post exploitation tool to retrieve **saved passwords** on local computer.
- Recovers saved passwords from lots of programs.
- Recovers passwords from **memory**.
- Works with Windows and Linux.
- Displays results on screen or store it on local machine.

WEAPONISING LAZAGNE

Problems:

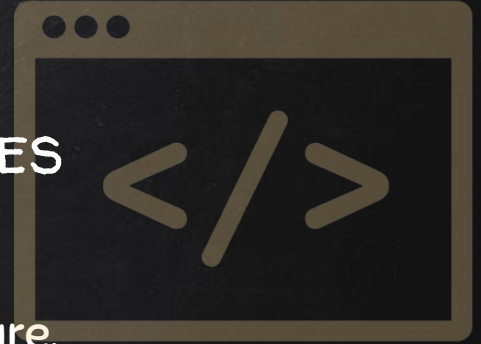
- LaZzne needs to be **executed on target computer**
- Displays logs on screen or store them in a **local** file.

Solution

-> Use a file that downloads LaZagne, execute it and send us an email with the result

BYPASSING ALL AVs

BY MODIFYING HEX VALUES



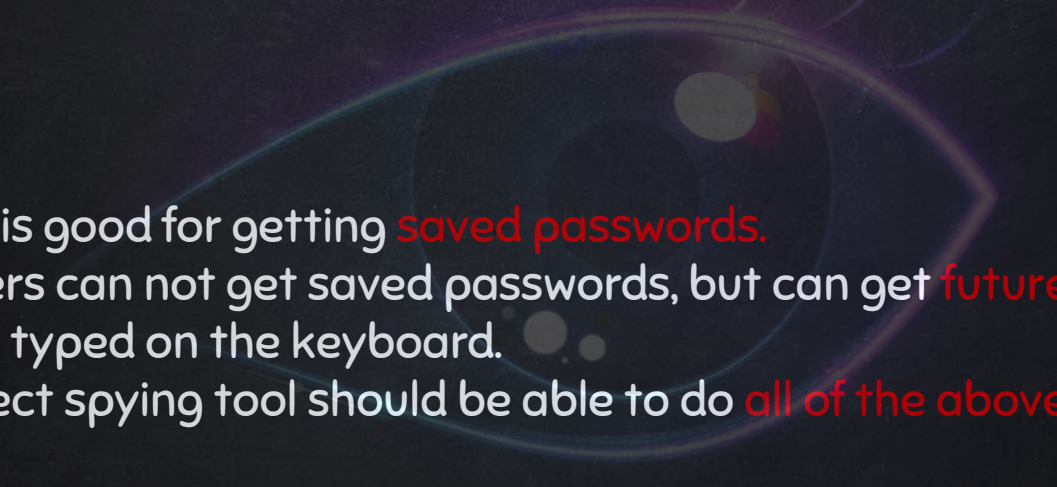
- Av programs use database of signatures to detect malware.
- Modifying backdoor code will change its signature.
 - How about changing parts of the code that do nothing?
- Idea:
 - Open file with hex editor.
 - Change values that don't affect code execution..
 - Save and test the file.

DOWNLOAD & EXECUTE PAYLOAD

- Generic executable that downloads & executes files.
- Ideas:
 - Download backdoor + keylogger.
 - Download keylogger + password recovery tool.
 - Download keylogger + password recover tool + backdoor.
 - Use it as a trojan -- evil file + a normal file.



THE PERFECT SPYING TOOL



Facts:

1. LaZagne is good for getting **saved passwords**.
2. Keyloggers can not get saved passwords, but can get **future passwords** + anything typed on the keyboard.
3. The perfect spying tool should be able to do **all of the above**

Problem: There is no such tool.

Solution: Use the download and execute payload to download and execute LaZagne + keylogger.

TROJANS



- A trojan is a file that looks and functions as a normal file (image, pdf, song ..etc).
- When executed :
 1. Opens the normal file that the user expects.
 2. Executes evil code in the background (run a backdoor/keylogger ..etc).

-> Therefore it is great to social engineer the target into running our evil code


CREATING A TROJAN



- Combine evil file with normal file (image, book, song ..etc).
- Configure evil file to run silently in the background.
- Change file icon.
- Change file extension.



CREATING A TROJAN



- Combine evil file with normal file (image, book, song ..etc). 
- **Configure evil file to run silently in the background.**
- Change file icon.
- Change file extension.

CREATING A TROJAN



- Combine evil file with normal file (image, book, song ..etc). 
- Configure evil file to run silently in the background. 
- **Change file icon.**
- Change file extension.




AUTOIT DOWNLOAD & EXECUTE PAYLOAD

- Generic executable that downloads & executes files.
- Advantages over the .bat download & execute payload:
 - Silent (doesn't show any popups).
 - No need to use a 3rd party software to change it to exe.



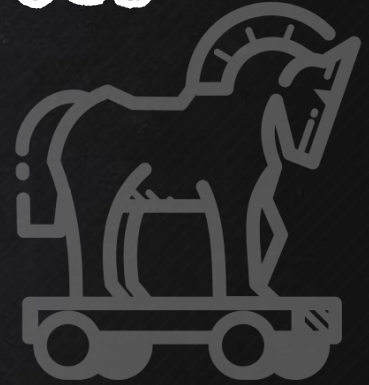
CREATING A TROJAN



- Combine evil file with normal file (image, book, song ..etc). 
- Configure evil file to run silently in the background. 
- Change file icon. 
- **Change file extension.**

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.