Malware

Facendo una scansione con virustotal del file malware.exe(vedi foto) ho riscontrato che 53 su 72 antivirus hanno trovato il malware ma cambiando il formato da exe a raw con il secondo file malware2.exe (vedi foto) virustotal ha riscontrato solamente 12 su 61 antivirus.

Possibili migliorie:

- Aumento dell'offuscamento utilizzando altri encoder o utilizzarne più di uno
- Riducendo la Visibilità con Packing utilizzando Veil o Hyperion
- Implementando una Falsa Estensione o Modifica i Metadati
- Crittografando il payload usando CryptCat
- Randomizzando i parametri e le stringhe ad esempio cambiando indirizzo ip e porte in ascolto ogni volta che si genera un nuovo malware
- Modificando il flusso di Esecuzione Ad esempio, eseguire il malware da una **shell reversa** potrebbe renderlo più difficile da rilevare rispetto a un processo diretto