**Traccia:**

Un giovane dipendente neo assunto segnala al reparto tecnico la presenza di un programma sospetto.
Il suo superiore gli dice di stare tranquillo ma lui non è soddisfatto e chiede supporto al SOC.
Il file "sospetto" è IEXPLORE.EXE contenuto nella cartella C:\Program Files\Internet Explorer (no, non ridete ragazzi)

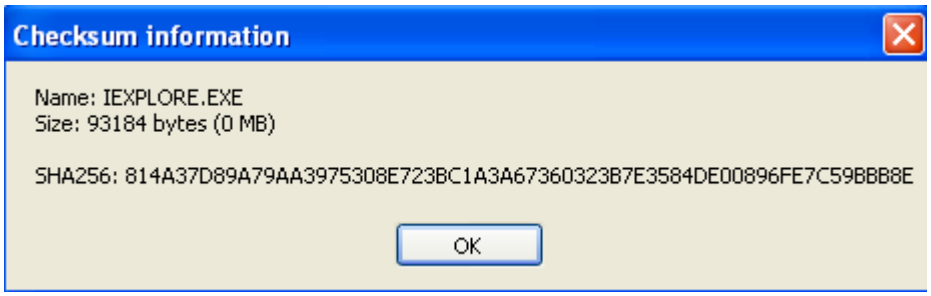
**Come membro senior del SOC ti è richiesto di convincere il dipendente che il file non è maligno.**

Possono essere usati gli strumenti di analisi statica basica e/o analisi dinamica basica visti a lezione.
No disassembly no debug o similari

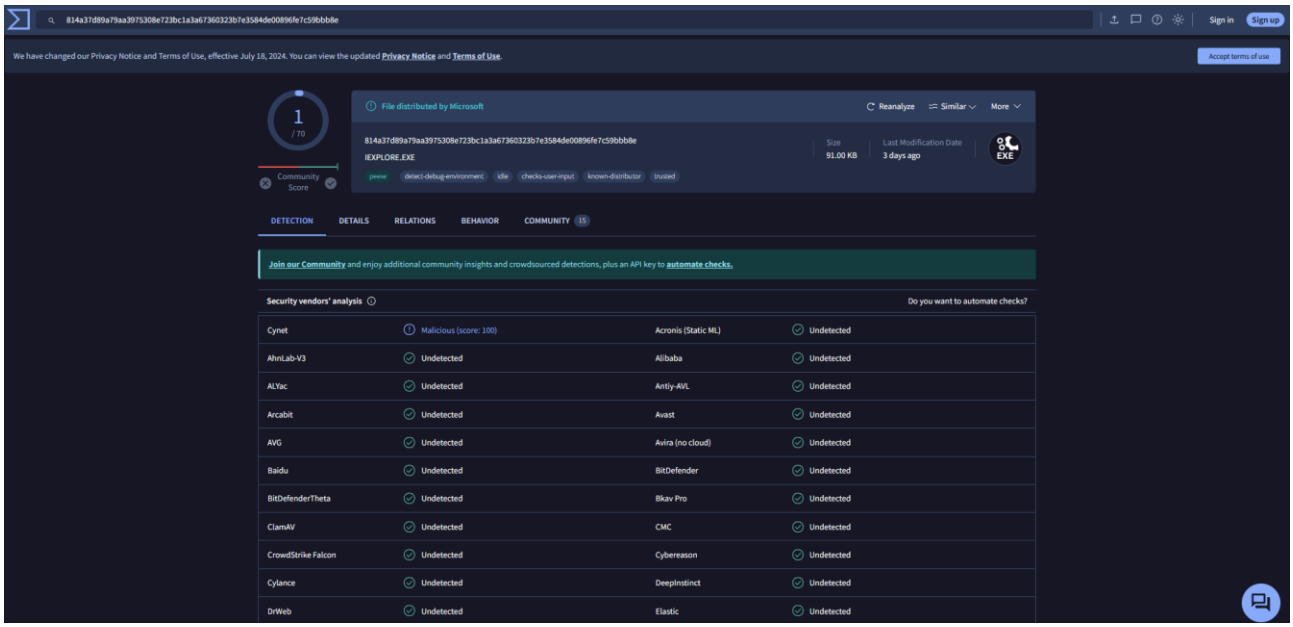
VirusTotal non basta, ovviamente
Non basta dire iexplorer è Microsoft è buono, punto.

3

Premessa, essendo questa una macchina virtuale, vecchia, mal tenuta e che sta in piedi per miracolo, usiamo un tool per calcolare l'hash sha256 del file "iexplorer.exe" della VM




Facendo una rapidissima ricerca su virustotal sullo sha256 estratto:




Si nota che il processo è un legittimo eseguibile di internet explorer pre installato con XP sp3