2024

EPICODE

CS0124

REPORT

Week 10 Lesson 2

PREPARED BY : Bruno Falconi

Dopo Aver configurato la macchina virtuale ed aver avviato tutti gli strumenti necessari all'individuazione dei processi del malware ed aver effettivamente avviato l'exe malevolo è risultato impossibile avviare correttamente l'applicazione in quanto supportata da Windows Xp e non da Windows 7. Dopo aver provato varie volte a lanciare l'exe concedendogli permessi di amministratore ed usando lo strumento per la compatibilità come si può constatare il malware non viene lanciato con successo in quanto non riesce a portare a termine la sua esecuzione Tuttavia facendo una analisi statica del malware tramite CFF Explorer e virustotal possiamo dedurre che si tratti di un keylogger che proverà ad inviare i comandi eseguiti dall'utente.