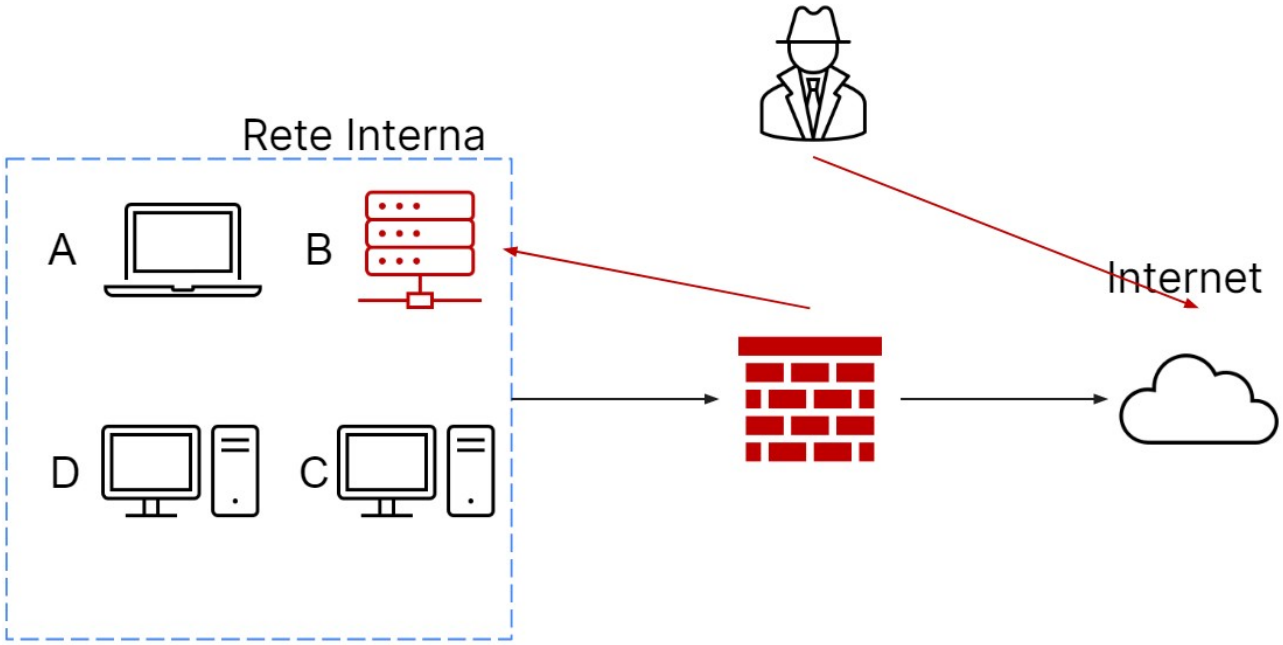
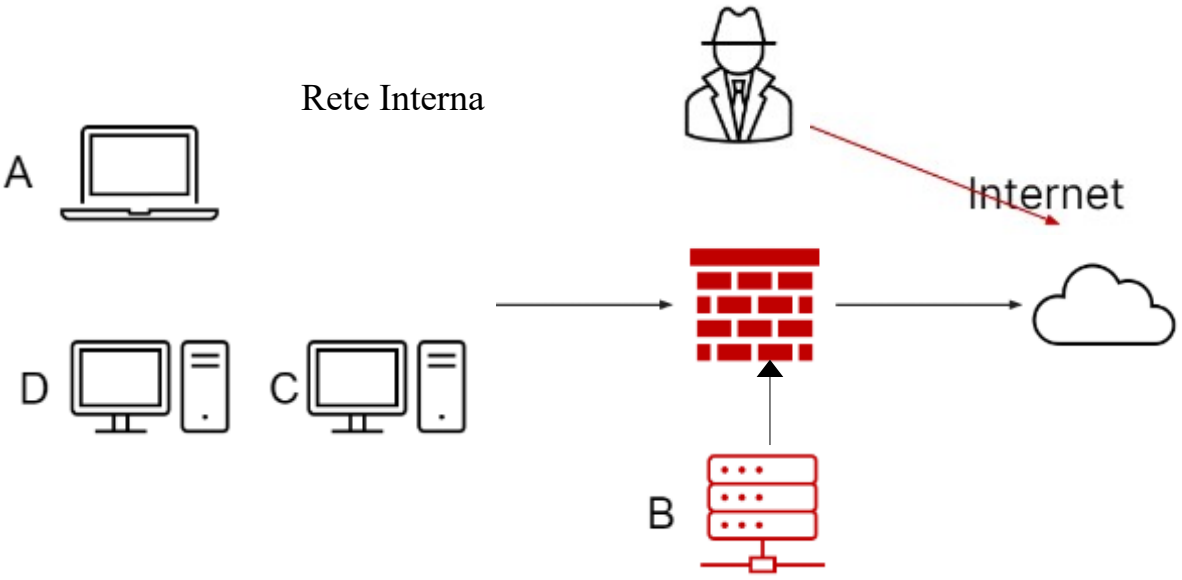
**Alaimo Alessandro**
**22/12/2022**

# Report Incident Response

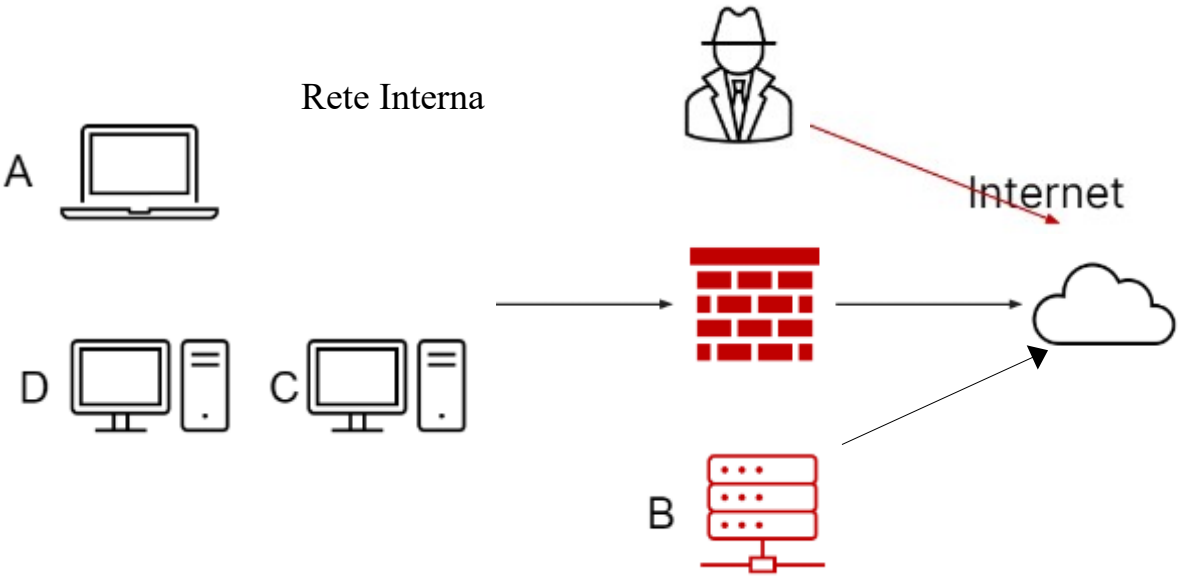
Prendendo in analisi la situazione nel seguente screenshot, iniziamo mostrando le tecniche di **Isolamento** e **Rimozione del sistema infetto B** per poi spiegare la differenza tra **Clear, Purge e Destroy.**




Vi sono due metodi per isolare il sistema infetto, di seguito abbiamo:
**Isolamento: Primo Metodo**

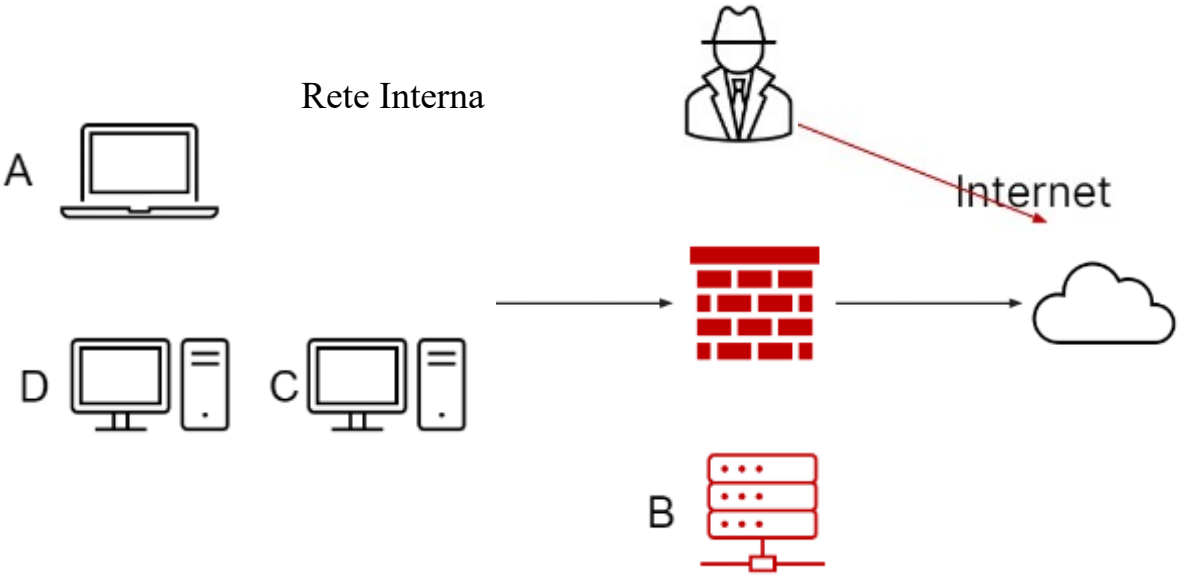


**Isolamento: Secondo Metodo**




L'ultimo metodo è quello di scollegare direttamente il sistema infetto, un esempio pratico è quello di scollegare direttamente il cavo e la configurazione sarebbe la seguente:

**Rimozione del sistema infetto**




Per concludere, la differenza sostanziale tra Clear, Purge e Destroy sta nel trattamento del dispositivo. Prendendo in analisi Clear, quello che si va ad effettuare un approccio read & write dove il contenuto viene sovrascritto più e più volte con un massimo di 7 volte oppure si utilizza la funzione di *factory reset*. Se invece si usa il Purge  si usa un approccio più logico come il Clear ma con anche tecniche fisiche, per esempio tramite l'uso di forti magneti per rendere inaccessibile le informazioni. Infine il metodo di Destroy, il dispositivo viene direttamente distrutto, per esempio tramite trapanamento. Sicuramente questo metodo è il più efficace per rendere inaccessibili i file ma comporta un effort maggiore in termini di costi.