CONSEGNA 21 MARZO S9L

L'obbiettivo di oggi, nel contesto di un'attacco ad un sistema di database con diversi dischi per lo storage, è quello di rispondere ai seguenti quesiti:

- Mostrare le tecniche di 1) isolamento 2)rimozione del sistema B infetto
- Spiegare la differenza tra Pure, Destroy e Clear per l'eliminazione delle informazioni sensibili.

La rete si presenta com in Fig.1, il database B è stato compromesso interamente da un'attaccante che è riuscito a bucare la rete ed accedere al sistema tramite internet.

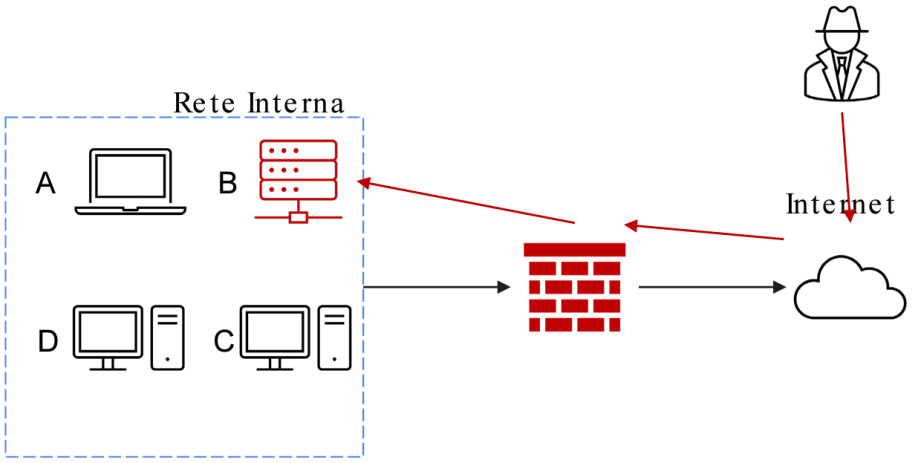

Fig.1

Tecnica dell'isolamento:
Quando necessitiamo di contenere un sistema compromesso, si utilizza la tecnica dell'isolamento, che consiste nella completa disconnessione del sistema infetto della rete, per restringere ancora maggiormente l'accesso alla rete interna da parte dell'attaccante. In uni tipo di scenario del genere, l'attaccante ha ancora l'accesso all sistema, ormai in quarantena, attraverso internet. Fig.2

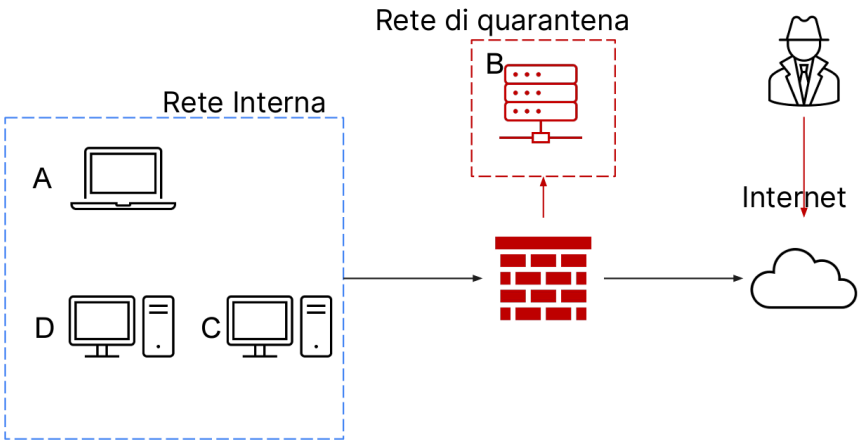

Fig.2

Tecnica di rimozione:
In questo caso si procede con una tecnica di contenimento molto stringente, dove avviene la completa rimozione del sistema infetto dalla rete, sia internet che intranet. In questo caso l'attaccante non avrà né accesso alla rete interna, né al sistema infetto.

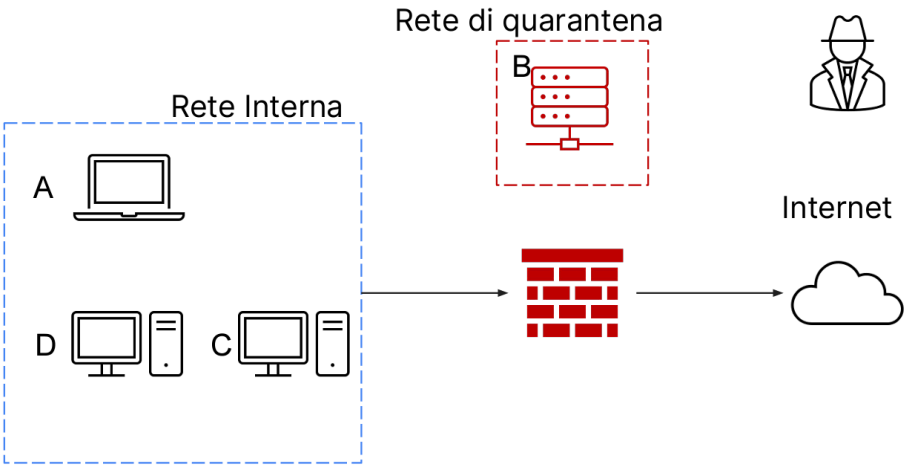

Fig.3

Durante la fesa di recupero, quando il sistema infetto è stato isolato o rimosso, dovremmo gestirne lo smaltimento o il riutilizzo. In questo caso bisogna accertarsi che le informazioni all'interno di esso siano completamente inaccessibili prima di smaltirlo o riutilizzarlo.
Possiamo individuare tre opzioni per le gestione dei dati contenuti in esso:

-**Purge**: Si riferisce a un processo di eliminazione dei dati che mira a rendere le informazioni irrecuperabili utilizzando metodi avanzati di cancellazione, sovrascrittura o crittografia. Il suo obiettivo è impedire il recupero delle informazioni da parte di terze parti.

-**Destroy**: Destroy implica la distruzione fisica dei dispositivi o dei supporti di memorizzazione contenenti dati sensibili. Questo metodo è estremamente sicuro in quanto rende fisicamente impossibile il recupero dei dati

-**Clear**: si riferisce a un processo di eliminazione dei dati che rimuove le informazioni dalla vista immediata senza renderle irrecuperabili. Questo può includere la cancellazione dei file, la formattazione del disco o la reimpostazione delle impostazioni di fabbrica. Tuttavia, le informazioni possono ancora essere recuperate utilizzando strumenti di recupero dati specializzati.