REPORT

INCIDENT RESPONSE

PRESENTATION

Alejandro Cristino

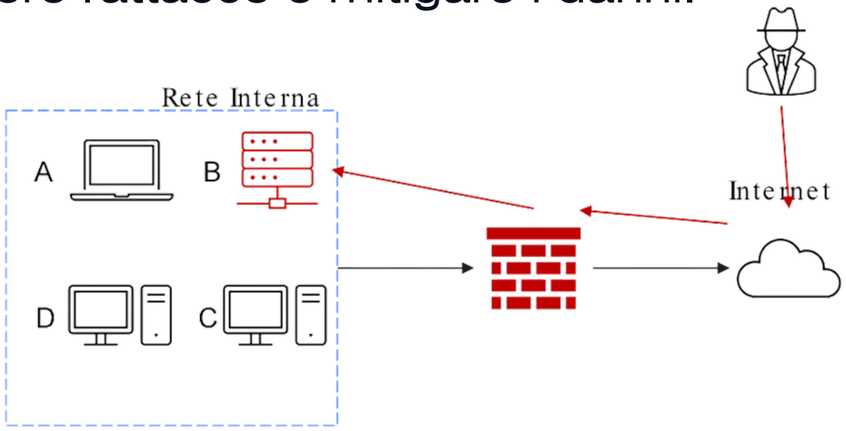
S9-L4

Report di Incident Response: Compromissione del Sistema B

1. Introduzione

Il Sistema B, un database con diversi dischi per lo storage, è stato compromesso da un attaccante che ha ottenuto accesso tramite Internet. L'incidente è attualmente in corso e il nostro compito, come parte del CSIRT, è contenere l'attacco e mitigare i danni.

Obiettivo della traccia



Mostrare le tecniche di:

I) Isolamento

II) Rimozione del sistema B infetto

Spiegare la differenza tra Purge e Destroy per l'eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi. Indicare anche Clear.

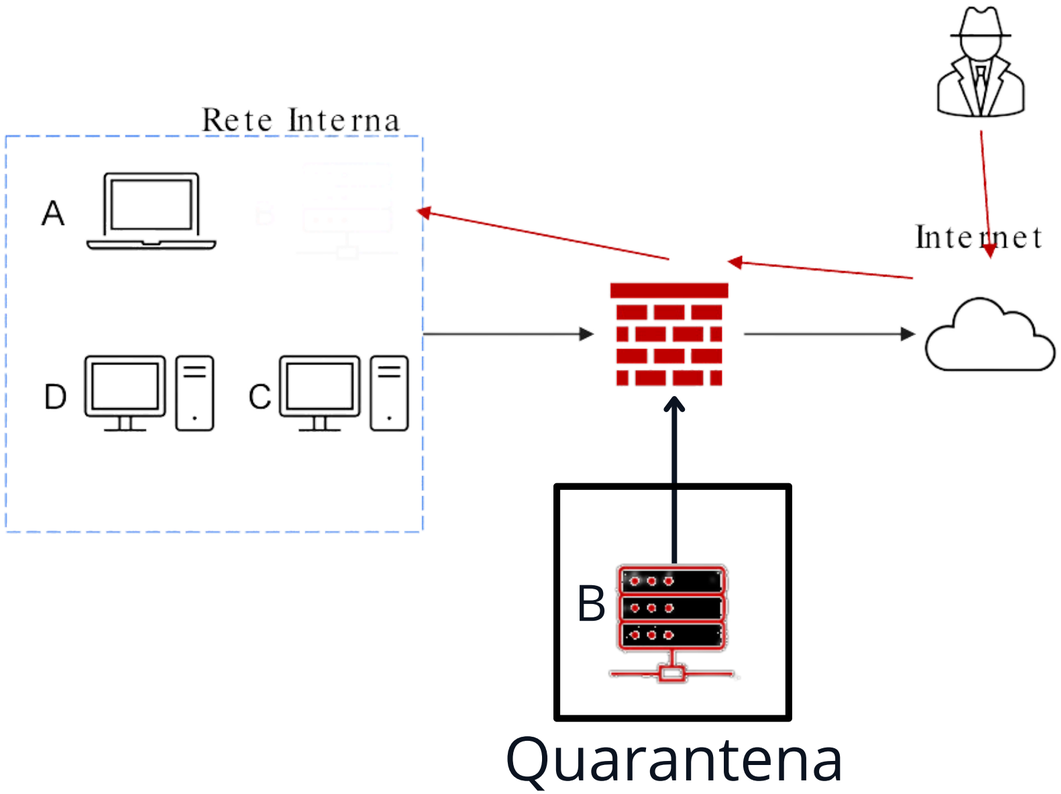
2. Contenimento del Danno

L'obiettivo primario del contenimento è isolare l'incidente per impedire la diffusione ad altri sistemi o reti. Questo processo deve iniziare il prima possibile dopo la rilevazione dell'incidente.

3. Creazione di una Rete di Quarantena

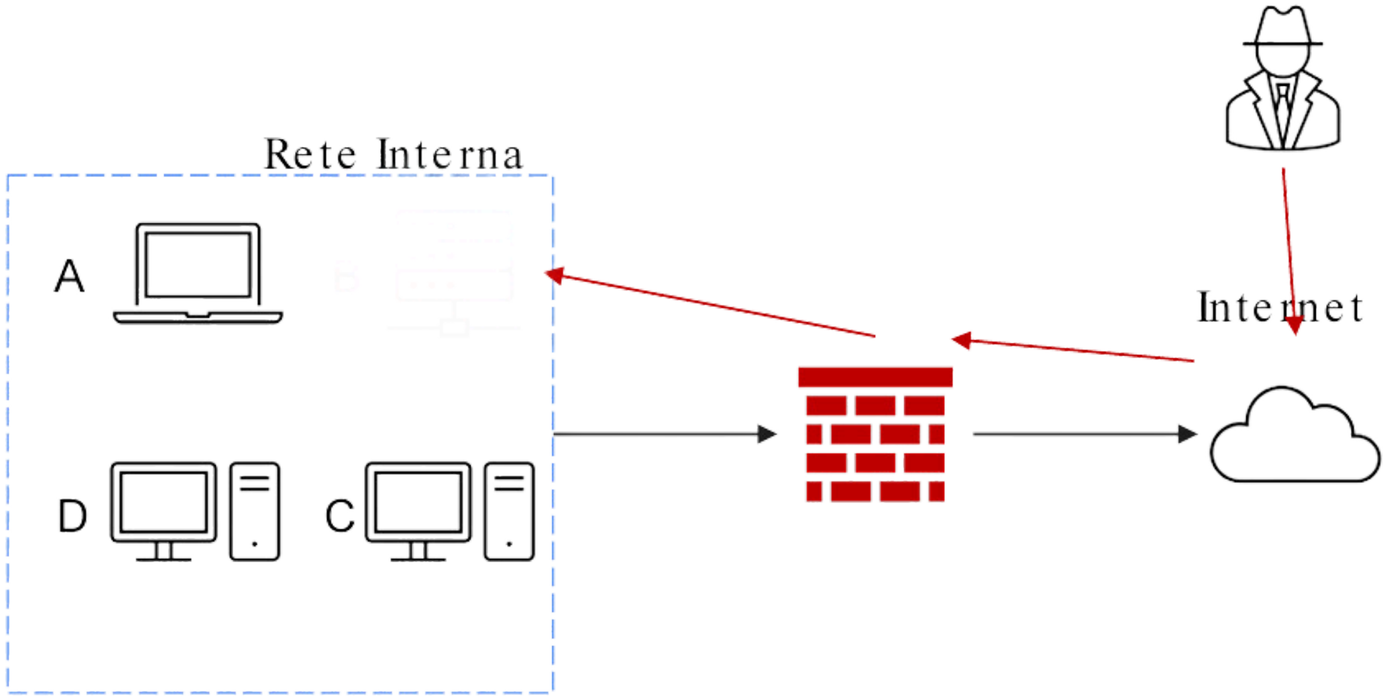
Creazione di una Rete di Quarantena

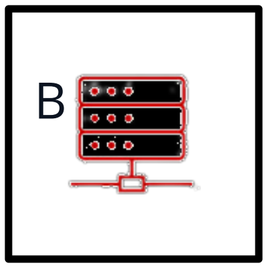
- Descrizione: Nel contesto di questo incidente, una rete di quarantena è stata creata per separare il sistema infetto dagli altri sistemi (A, C, D).
- Vantaggio: Questo impedisce la propagazione del malware e permette di contenere l'attacco in un ambiente controllato.



4. Isolamento Completo

In casi dove la quarantena non è sufficiente, l'isolamento completo del sistema infetto è necessario. Questo comporta la disconnessione fisica e logica del sistema dalla rete aziendale e da Internet.





Quarantena

5. Differenza tra Purge, Destroy e Clear

5.1 Clear (Pulizia Superficiale)

- Descrizione: Il dispositivo viene completamente ripulito dal suo contenuto con tecniche «logiche». Si utilizza ad esempio un approccio di tipo read and write dove il contenuto viene sovrascritto. Utilizzato per situazioni dove il livello di sicurezza richiesto è minimo.

5.2 Purge (Pulizia Profonda)

- Descrizione: Eliminazione dei dati sensibili tramite metodi che rendono il recupero dei dati significativamente più difficile, ma anche tecniche di rimozione fisica come l'utilizzo di forti magneti

5.3 Destroy (Distruzione)

- Descrizione: Distruzione fisica del supporto per garantire l'impossibilità di recupero dei dati. Attraverso la triturazione dei dischi, degaussing e fusione fisica dei supporti.