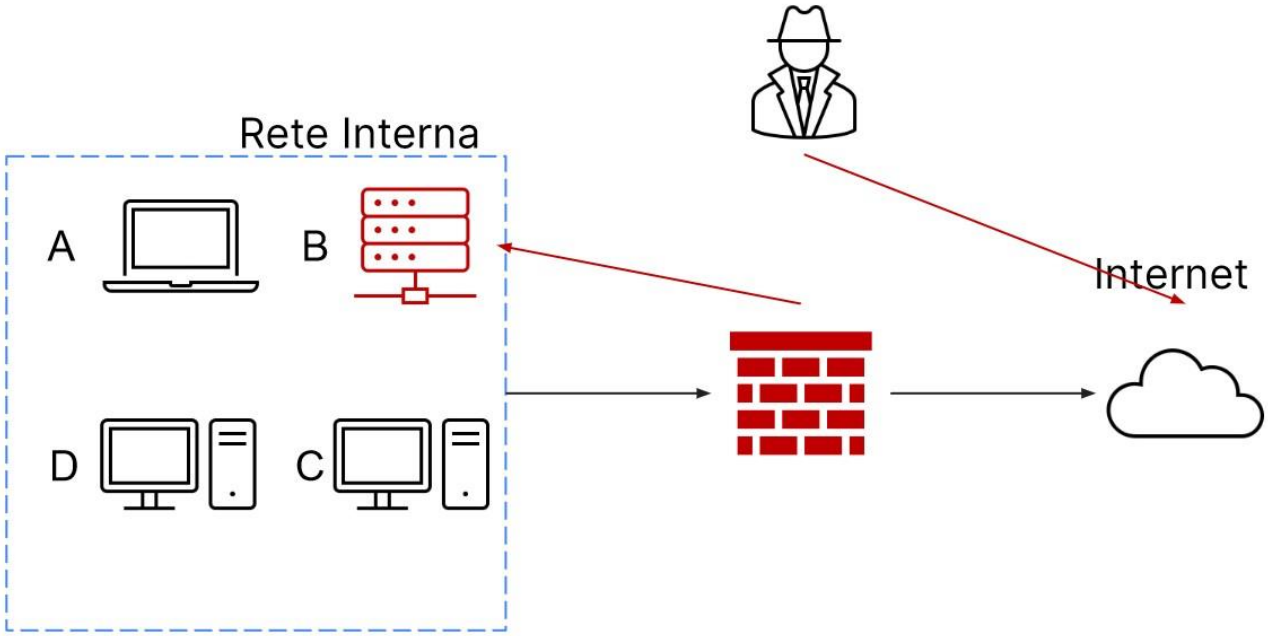
INCIDENT RESPONSE

Traccia:

Con riferimento alla figura, il sistema **B (un database con diversi dischi per lo storage)** è stato compromesso interamente da un attaccante che è riuscito a bucare la rete ed accedere al sistema tramite internet.

L'attacco è attualmente in corso e siete parte del team di CSIRT. Rispondere ai seguenti quesiti.

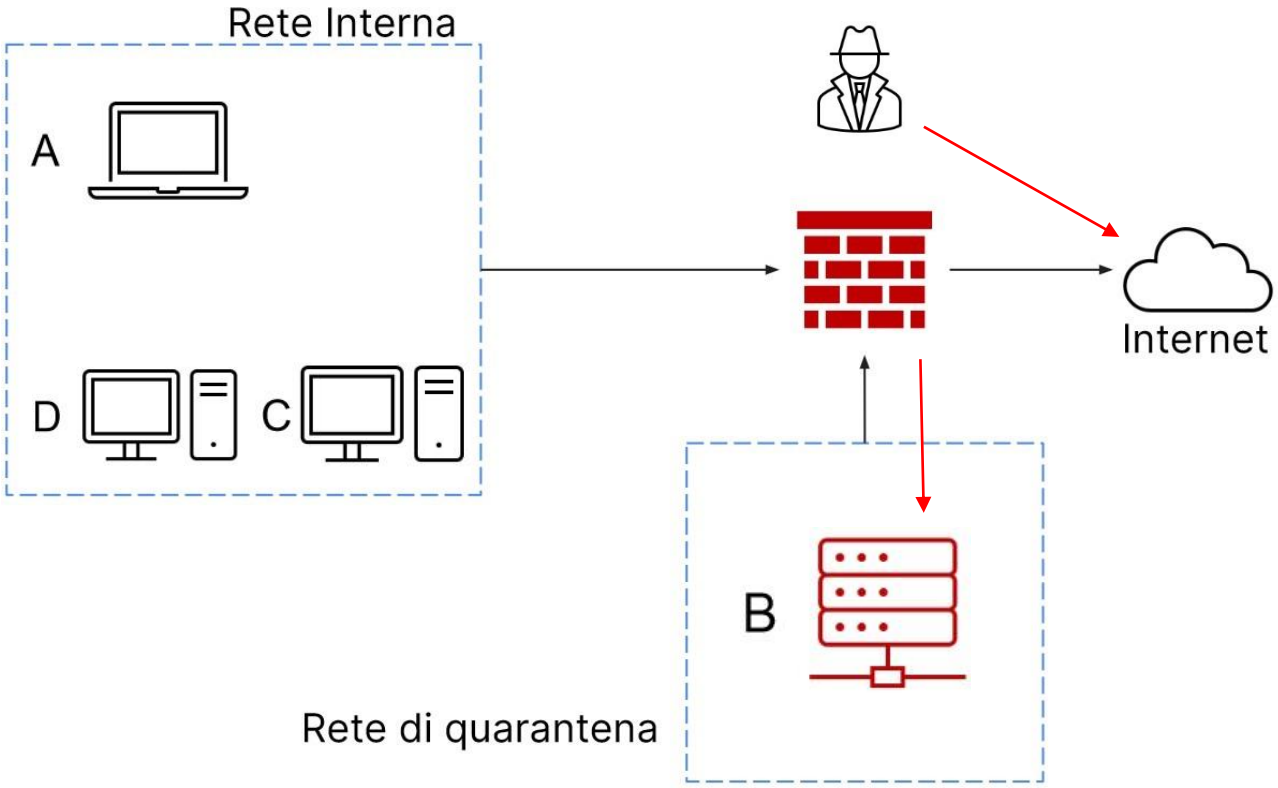
- Mostrate le tecniche di: I) Isolamento II) Rimozione del sistema **B infetto**
- Spiegate la differenza tra **Purge** e **Destroy** per l'eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi



Come prima cosa andremo ad analizzare il caso di **isolamento** e **rimozione** del sistema infetto.

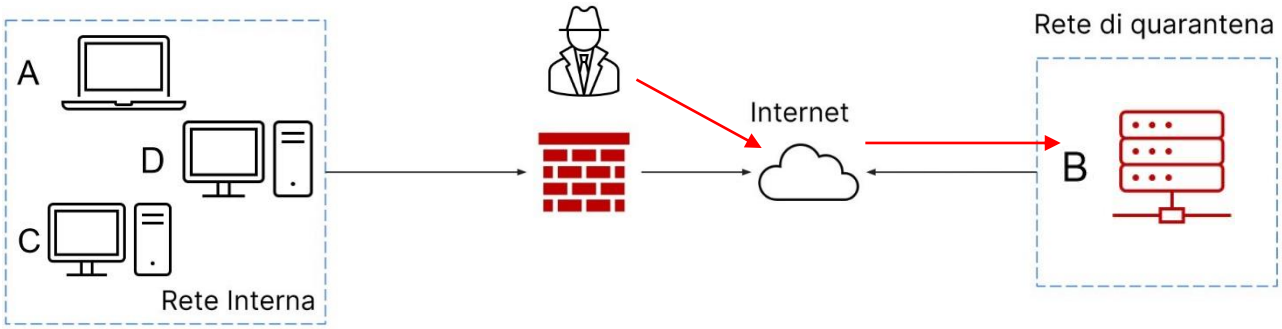
Una delle tecniche utili nella fase di contenimento di un incidente in corso è la **segmentazione**, cioè la divisione della rete in diverse LAN/VLAN.

Nel nostro caso il sistema B infetto potrebbe essere stato attaccato da un malware che potrebbe riprodursi ed infettare anche A, C, D. Andremo quindi a separare il sistema B dagli altri sistemi sulla rete creandone una nuova chiamata **rete di quarantena.**

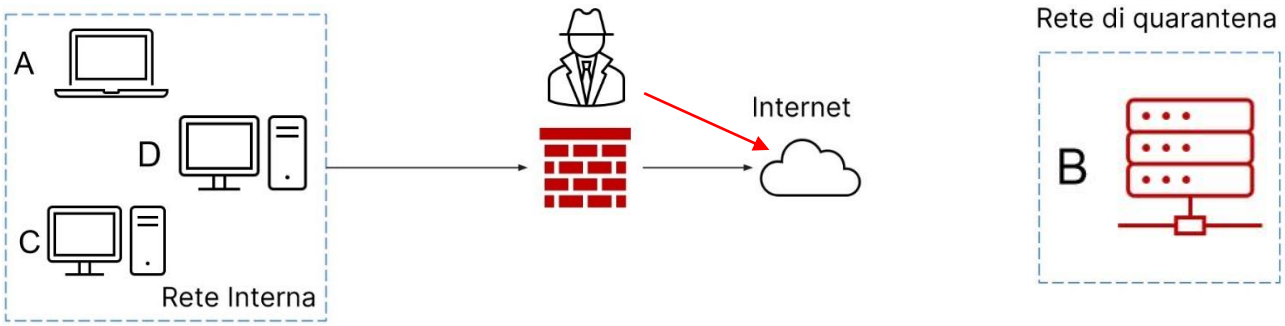


Con le giuste configurazioni network il malware dovrebbe così essere separato dal resto della rete ed incapace di riprodursi.

Se non fosse sufficiente, dato che il sistema B è ancora connesso al Firewall di rete, si utilizzerà la tecnica dell'**isolamento**, che consiste nella completa disconnessione del sistema infettato dalla rete, lasciando comunque la macchina connessa ad internet, per restringere ancora di più l'accesso alla rete interna da parte dell'attaccante.



Nei casi più estremi si può procedere con una tecnica di contenimento più stringente, cioè la **rimozione** completa del sistema dalla rete sia interna sia internet. In questo caso l'attaccante non avrà accesso né alla rete interna né al sistema infettato.



Prima di poter smaltire o riutilizzare il sistema B infettato bisognerà accertarsi che le informazioni presenti sul sistema e sui suoi dischi di storage siano completamente inaccessibili. Per la gestione dei media contenenti informazioni sensibili possiamo individuare le opzioni:

- **Purge**: nel quale per la rimozione delle informazioni sensibili si utilizzeranno tecniche logiche, come la sovrascrizione del contenuto o la factory reset (tecniche utilizzate anche nell'opzione **clear** per la gestione dei media), e tecniche di rimozione fisica, come l'utilizzo di forti magneti.
- **Destroy**: nel quale la rimozione delle informazioni sensibili ha un approccio più netto dove si utilizzano tecniche di disintegrazioni, polverizzazione, trapanazione dei media. Metodo sicuramente più efficace ma anche più dispendioso.