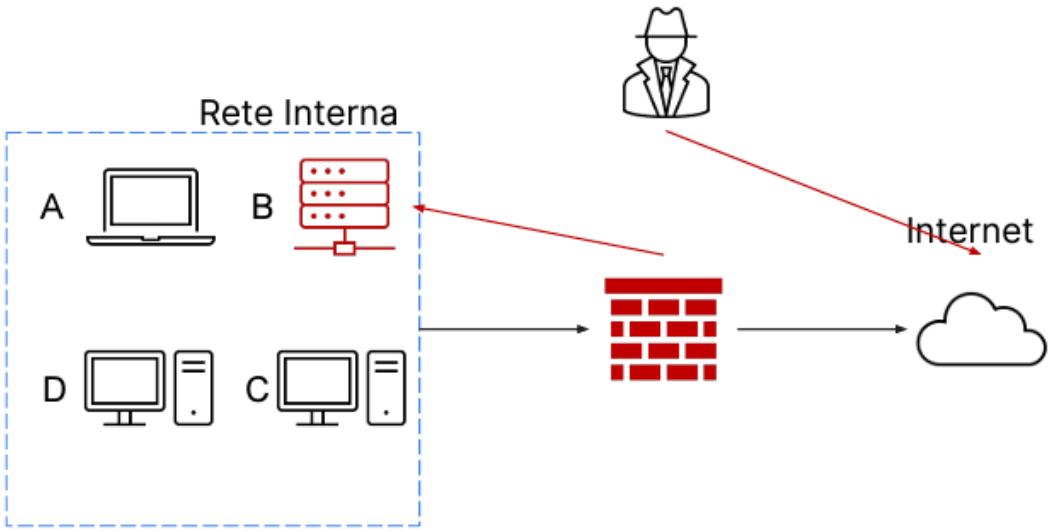
Incident response

Sommario

Introduzione

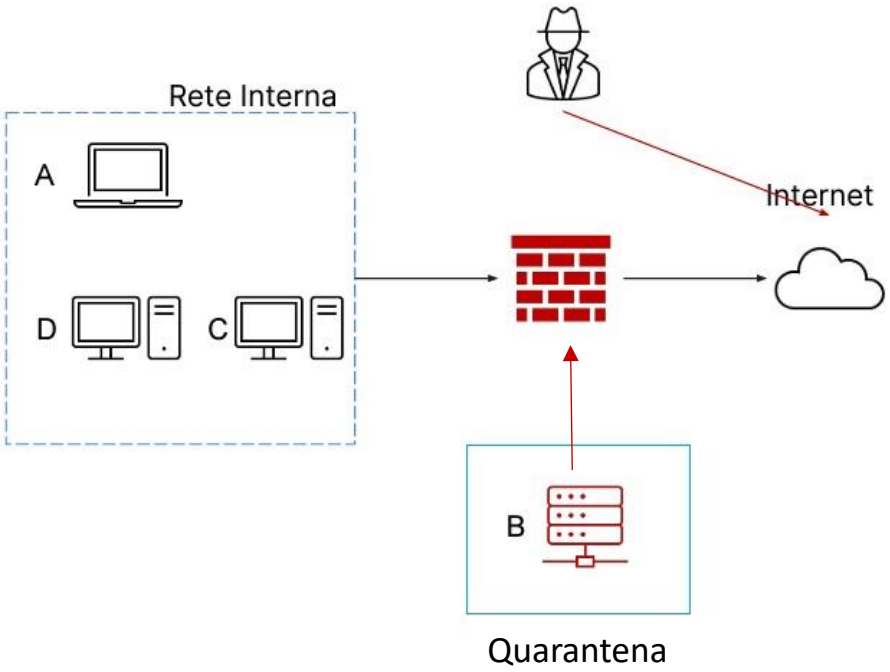
Il sistema B (un database con diversi dischi per lo storage) è stato compromesso interamente da un attaccante che è riuscito a bucare la rete ed accedere al sistema tramite internet.



L'attacco è attualmente in corso e sono parte del team di CSIRT (Computer Security Incident Response Team). Un Computer Security Incident Response Team (CSIRT) è una struttura responsabile di monitorare, intercettare, analizzare e rispondere alle minacce informatiche

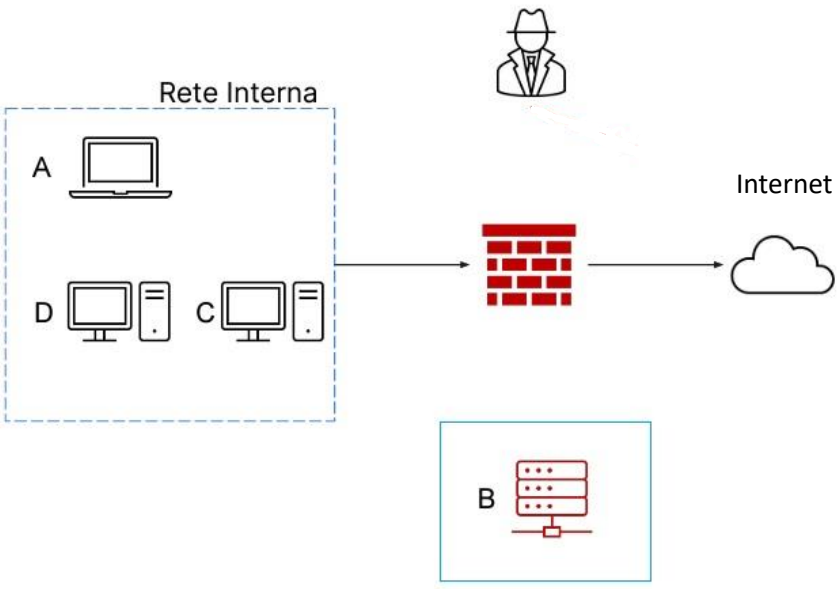
Isolamento del sistema B infetto

Grazie ad un processo di segmentazione il server infetto si può separare dalla rete interna e lo si confina in una rete di quarantena configurata con un'apposita VLAN e rete. Ad esempio: se la rete interna è 192.168.10.0/24 VLAN 10, la rete di quarantena potrebbe essere 192.168.20.0/24 VLAN 20. Questo non permetterà al malware di diffondersi e i bloccherà l'accesso all'hacker alla rete interna, ma non al server infetto.



Rimozione del sistema B infetto

Con questa tecnica si disconnette completamente il server sia da internet che dalla rete interna. In questo modo l'hacker non avrà più accesso neppure al sistema infetto.



Qual è la differenza tra Purge e Destroy?

Purge è un rende inaccessibili i dati presenti su un dispositivo di archiviazione. Durante il processo di purge, i dati vengono sovrascritti con informazioni casuali o con zeri, rendendoli irrecuperabili. Tuttavia, il dispositivo stesso rimane utilizzabile e può essere riutilizzato.

Destroy è un metodo più drastico. Durante il processo di distruzione, il dispositivo viene fisicamente danneggiato o distrutto in modo irreversibile. Ad esempio, i dischi rigidi possono essere perforati, frantumati o fusi. Questo metodo garantisce che i dati non siano più recuperabili e che il dispositivo non possa essere utilizzato nuovamente. È la scelta migliore quando si tratta di dati altamente sensibili o quando il dispositivo è fuori uso.