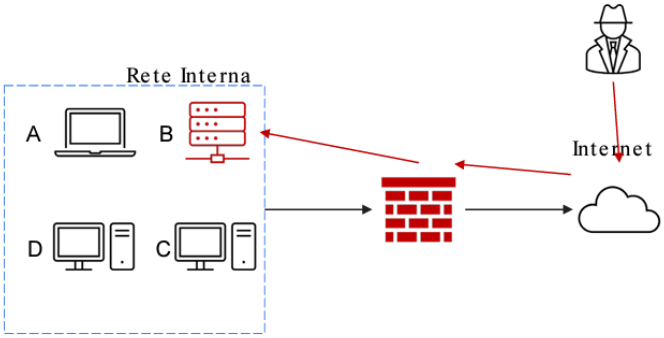
S9L4



Tecniche di isolamento:

- Disconnettere il sistema infetto dalla rete: Questo impedisce al malware di comunicare con altri sistemi sulla rete e di diffondersi ulteriormente.
- Disattivare connessioni esterne: Se il sistema infetto ha connessioni Bluetooth, Wi-Fi o altre connessioni esterne, disattivarle per prevenire la trasmissione del malware.
- Utilizzare un firewall: Configurare un firewall per bloccare il traffico dannoso in entrata e in uscita dal sistema infetto.
- Creare una rete separata: Se possibile, isolare completamente il sistema infetto creando una rete separata solo per quel dispositivo.

Tecniche di rimozione del sistema B infetto:

- Utilizzare software antivirus/antimalware: Eseguire una scansione completa del sistema utilizzando software antivirus o antimalware aggiornati per rilevare e rimuovere il malware.
- Rimuovere manualmente i file dannosi: Identificare manualmente i file dannosi e eliminarli dal sistema. Questa tecnica richiede una conoscenza approfondita dei file e delle cartelle del sistema operativo.
- Ripristinare da un backup pulito: Se possibile, ripristinare il sistema da un backup pulito effettuato prima dell'infezione da malware.
- Utilizzare strumenti di ripristino del sistema: Alcuni sistemi operativi offrono strumenti di ripristino integrati che consentono di tornare a uno stato precedente in cui il sistema non era infetto.

Differenza tra Purge e Destroy:
Purge: Il termine "purge" si riferisce al processo di eliminazione sicura dei dati sensibili da un dispositivo di archiviazione, come un disco rigido o un'unità flash, prima di smaltirlo o riciclarlo. Nella pratica, la purga dei dati può avvenire attraverso l'utilizzo di software specializzato progettato per sovrascrivere i dati esistenti sul disco

rigido con dati casuali o con zeri. Questo processo rende i dati originali irrecuperabili e inaccessibili per qualsiasi persona che tenti di recuperarli successivamente.

Destroy: Il termine "destroy" implica la distruzione fisica del dispositivo di archiviazione, come un disco rigido o un'unità flash. Questo può essere fatto utilizzando strumenti specializzati progettati per distruggere fisicamente il dispositivo, come trituratori industriali, piegatrici, o perforatrici. Distruggere fisicamente il dispositivo garantisce che non sia più possibile accedere ai dati memorizzati in esso, poiché il dispositivo stesso è reso completamente inutilizzabile.

La scelta, dipende dalle esigenze di sicurezza e privacy dell'organizzazione o dell'individuo, nonché dalle normative o dalle linee guida specifiche che possono regolare il trattamento dei dati sensibili prima dello smaltimento.