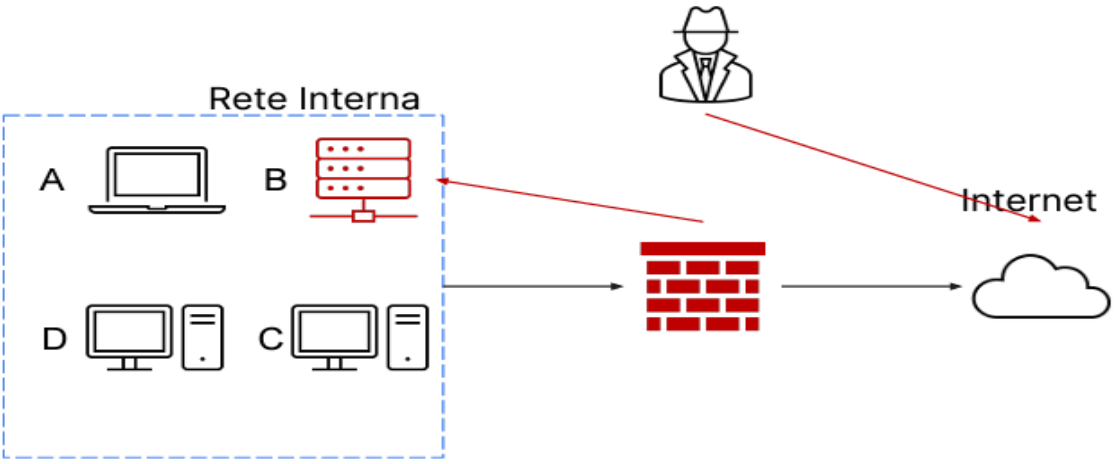
Traccia:

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.

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



Isolamento:

Disconnessione fisica: Se possibile, andremo a disconnettere il dispositivo infetto dalla rete rimuovendo il cavo di rete o spegnendo il Wi-Fi. Questo impedisce al malware di comunicare con altri dispositivi sulla rete e di diffondersi ulteriormente.

Isolamento virtuale: Se la disconnessione fisica non è un'opzione, è possibile utilizzare un firewall o altre misure di sicurezza per isolare il dispositivo infetto dalla rete. Questo può essere fatto configurando regole firewall per bloccare il traffico in entrata e in uscita dal dispositivo infetto.

Rimozione:

In questa fase lo scopo è eliminare tutte le attività, le componenti, i processi che restano dell'incidente all'interno della rete o sui sistemi. Questa attività può includere ad esempio rimuovere eventuali backdoor installate da un malware, oppure ripulire dischi e chiavette USB compromesse.
La fase di rimozione dipende molto da che tipo di incidente di sicurezza è in corso. Una lista dettagliata delle attività da seguire per macro-casistica deve essere elencata nei «playbooks».

Tecniche dettagliate da utilizzare in questa fase:

Scansione antivirus/anti-malware: Utilizzare software antivirus o anti-malware aggiornati per eseguire una scansione completa del sistema infetto. Questo può aiutare a identificare e rimuovere il malware presente sul dispositivo.

Modalità provvisoria: Avviare il dispositivo infetto in modalità provvisoria (safe mode) per limitare l'avvio di programmi e servizi non essenziali. In questa modalità, eseguire una scansione antivirus/anti-malware per individuare e rimuovere il malware senza l'interferenza di processi dannosi in esecuzione.

Analisi manuale dei processi e dei servizi: Utilizzare il Task Manager (Windows) o il Monitoraggio attività (macOS) per individuare processi sospetti o non riconosciuti in esecuzione sul sistema infetto. Terminare manualmente i processi sospetti e disabilitare i servizi non necessari.

Rimozione manuale dei file dannosi: Identificare i file dannosi o sospetti sul sistema infetto e rimuoverli manualmente. Questo può essere fatto utilizzando l'Esplora file (Windows) o il Finder (macOS) per individuare e eliminare i file dannosi.

Modifica delle impostazioni di avvio: Verificare che non ci siano voci di avvio dannose nel registro di sistema o nelle configurazioni di avvio del sistema operativo. Utilizzare strumenti come MSCONFIG (Windows) o launchd (macOS) per modificare le impostazioni di avvio e rimuovere eventuali voci sospette.

Controllo dei browser e delle estensioni: Verificare i browser installati sul sistema infetto per individuare estensioni dannose o non autorizzate.

Rimuovere le estensioni sospette e ripristinare le impostazioni del browser se necessario.

Pulizia dei registri di sistema: Utilizzare strumenti di pulizia del registro di sistema per rimuovere voci dannose o obsolete dal registro di sistema. Ciò può aiutare a ripulire il sistema e migliorare le prestazioni.

Verifica dell'integrità del sistema operativo e dei file di sistema: Utilizzare strumenti di verifica dell'integrità del sistema operativo come System File Checker (Windows) o Verify Disk (macOS) per verificare e riparare eventuali file di sistema danneggiati o compromessi.

Monitoraggio post-rimozione: Dopo aver eseguito la rimozione del malware, monitorare attentamente il sistema per individuare eventuali segni di infezione o attività sospetta. Assicurarsi di mantenere aggiornato il software antivirus/anti-malware e di eseguire scansioni periodiche per garantire che il sistema rimanga sicuro.

Backup e ripristino dei dati: Se i dati sono stati danneggiati o compromessi dall'infezione, ripristinarli da backup sicuri una volta completata la rimozione del malware. Assicurarsi di utilizzare backup puliti e di verificare che i dati ripristinati non contengano malware residuo.

2. Purge, Destroy e Clear

- **Clear: 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 più e più volte o si utilizza la funzione di «factory reset» per riportare il dispositivo nello stato iniziale.**
- **Purge: si adotta non solo un approccio logico per la rimozione dei contenuti sensibili, come visto nel caso di clear, ma anche tecniche di rimozione fisica come l'utilizzo di forti magneti per rendere le informazioni inaccessibili su determinati dispositivi.**
- **Destroy: è l'approccio più netto per lo smaltimento di dispositivi contenenti dati sensibili. Oltre ai meccanismi logici e fisici appena visti, si utilizzano tecniche di laboratorio come disintegrazione, polverizzazione dei media ad alte temperature, trapanazione. Questo metodo è sicuramente il più efficace per rendere le informazioni inaccessibili ma è anche quello che comporta un effort in termini economici maggiore.**