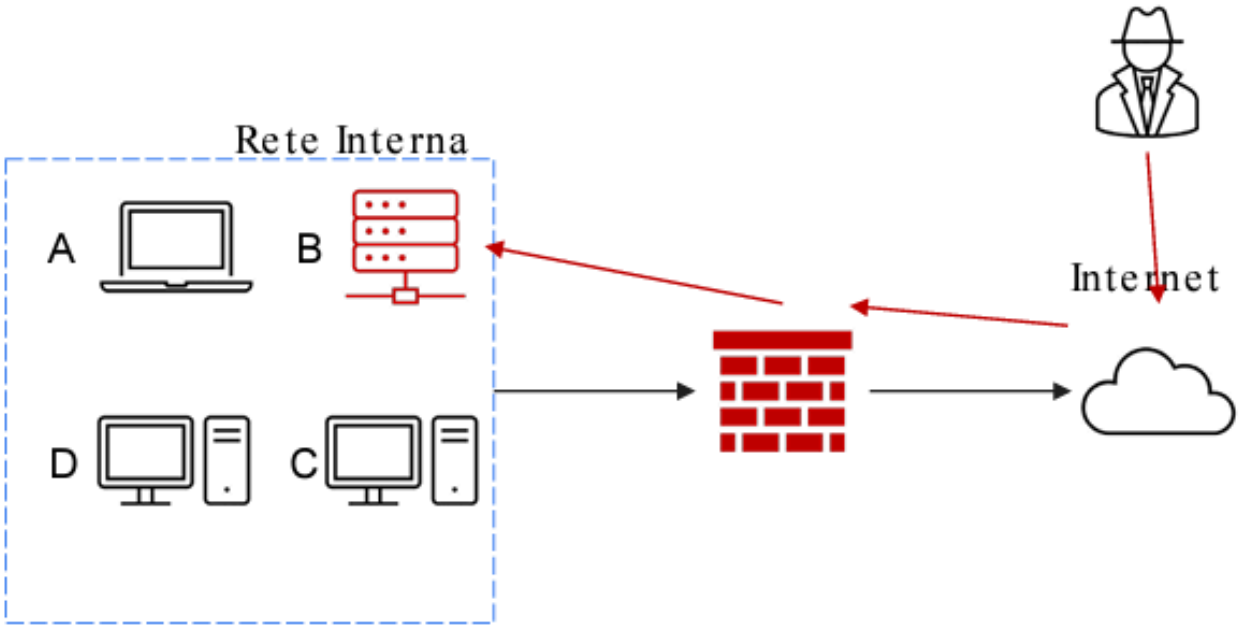
# Report di incident response

## Sistema B compromesso

## Schema di rete attuale




## Introduzione

Il giorno 6/06/2024, il nostro team ha ricevuto una segnalazione riguardante una compromissione del sistema B, un database con diversi dischi per lo storage, da parte di un attaccante esterno che è riuscito a infiltrarsi tramite Internet, l'attacco era in corso e necessitava di una risposta immediata per contenere e mitigare l'incidente.

**Per contenere e mitigare l'incidente sono state eseguite le seguenti azioni:**

1

Isolamento del sistema infetto, isolare il sistema è stato il primo passo cruciale per impedire la propagazione dell'attacco ad altri sistemi all'interno della rete interna e per contenere l'incidente.

Utilizzando strumenti di monitoraggio della rete, tra cui IDS (Intrusion Detection Systems) e SIEM (Security Information and Event Management), abbiamo indentificato il sistema B compromesso. Questi strumenti ci hanno aiutato a rilevare traffico anomalo e attività sospette.

2

Abbiamo scollegato fisicamente il sistema B dalla rete interna staccando il cavo di rete, la disconnessione fisica è un metodo diretto per interrompere immediatamente qualsiasi comunicazione tra il sistema infetto e il resto della rete.

3

Dopo la disconnessione fisica, abbiamo configurato il firewall hardware per bloccare tutto il traffico in entrata e in uscita dal sistema B. Questo passaggio ha garantito che, anche se il sistema venisse riconnesso accidentalmente, non potesse comunicare con altri sistemi o con l'esterno.

## Rimozione del sistema B infetto

La rimozione del sistema infetto dalla rete aziendale era necessario per prevenire ulteriori compromissioni ed eseguire un'analisi forense accurata in un ambiente controllato.

Come prima azione abbiamo spento il sistema B in modo sicuro per interrompere qualsiasi attività malevola in corso, utilizzando i comandi di spegnimento del sistema operativo.

Successivamente abbiamo creato un'immagine di backup completa del sistema B, questo passaggio è stato cruciale e necessario per l'analisi forense, permettendoci di esaminare il sistema per comprendere come l'attacco è avvenuto e quale tipo di dati sono stati compromessi.

# Smaltimento dei dati compromessi

Dopo l'isolamento e la rimozione del sistema B infetto, è stato fondamentale smaltire correttamente i dischi compromessi per garantire che le informazioni sensibili non possano essere recuperate.

## 1 Clear

Abbiamo eseguito una cancellazione sicura sui dischi compromessi utilizzando i comandi di cancellazione integrati, questo passaggio garantisce che i dati non vengano recuperati tramite mezzi normali.

Questo tipo di cancellazione sicura è stato il primo passo per rendere i dati meno accessibili e pronti per le successive azioni.

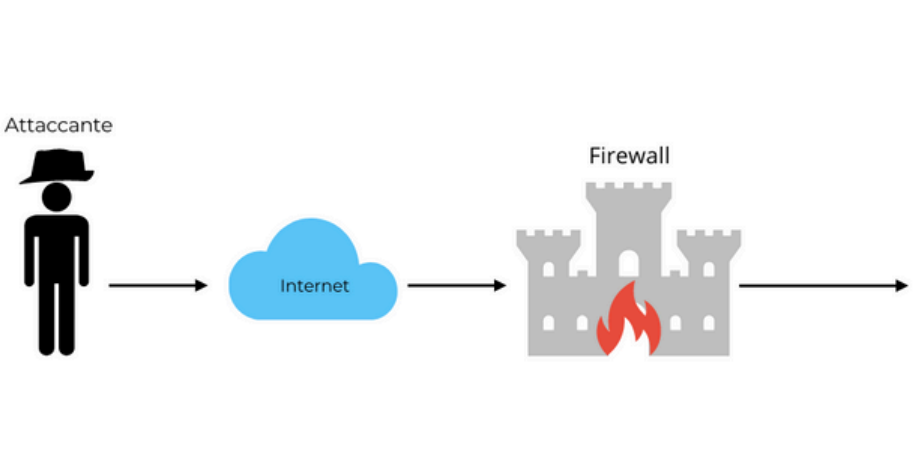
## 2 Purge

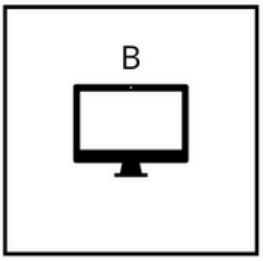
Abbiamo utilizzato software specializzati per sovrascrivere i dischi con dati casuali più volte, questo processo rende i dati originali irrecuperabili anche con mezzi più avanzati.

## 3 Destroy

Come ultimo passaggio abbiamo distrutto fisicamente i dischi compromessi. Questa azione garantisce che nessun dato possa essere recuperato in alcun modo.

# Schema di rete attuale dopo le azioni effettuate




Sistema B temporaneamente isolato e scollegato dalla rete interna per analisi e risoluzione.
Connessione temporaneamente disabilitata.

# Differenze tra i metodi principali di smaltimento dei dati compromessi

## Clear:

Il dispositivo viene completamente ripulito dal suo contenuto con tecniche, 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

In questo metodo si adottano le metodologie del clear ma anche tecniche di rimozione fisica come l'utilizzo di forti magneti per rendere le informazioni inaccessibili su determinati dispositivi.

## Destroy

E' il metodo più netto per lo smaltimento di dispositivi contenenti dati sensibili, oltre ai meccanismi logici e fisici si usano metodi come la disintegrazione, polverizzazione e trapanazione, è il metodo più efficacie ma comporta spese economiche più alte in quanto questi metodo devono essere eseguiti in laboratorio.