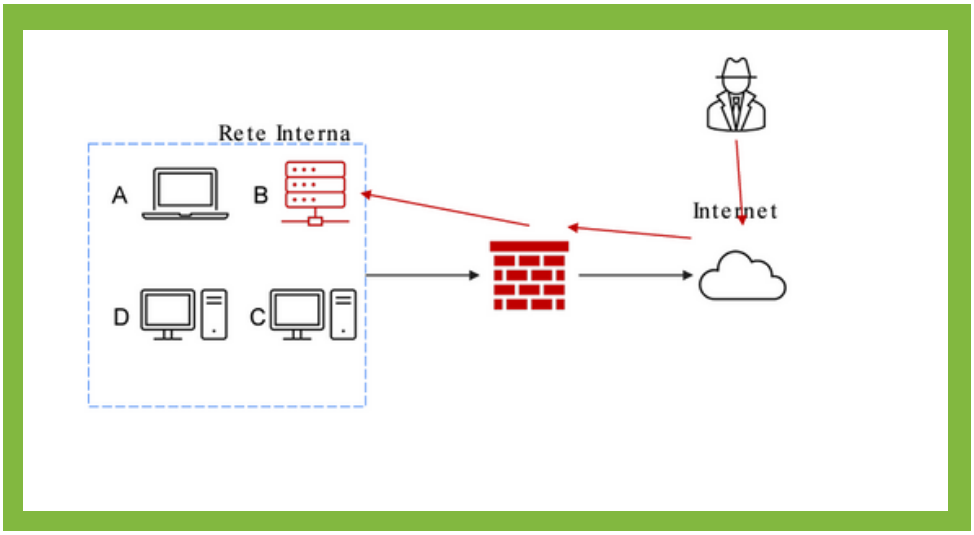
Incident Response

Prepared by
Alessandro Marasca

Presented to
Epicode - CS0124
S9L4

TRACCIA



Con riferimento alla figura sopra, 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. Indicare anche Clear

Tecniche di

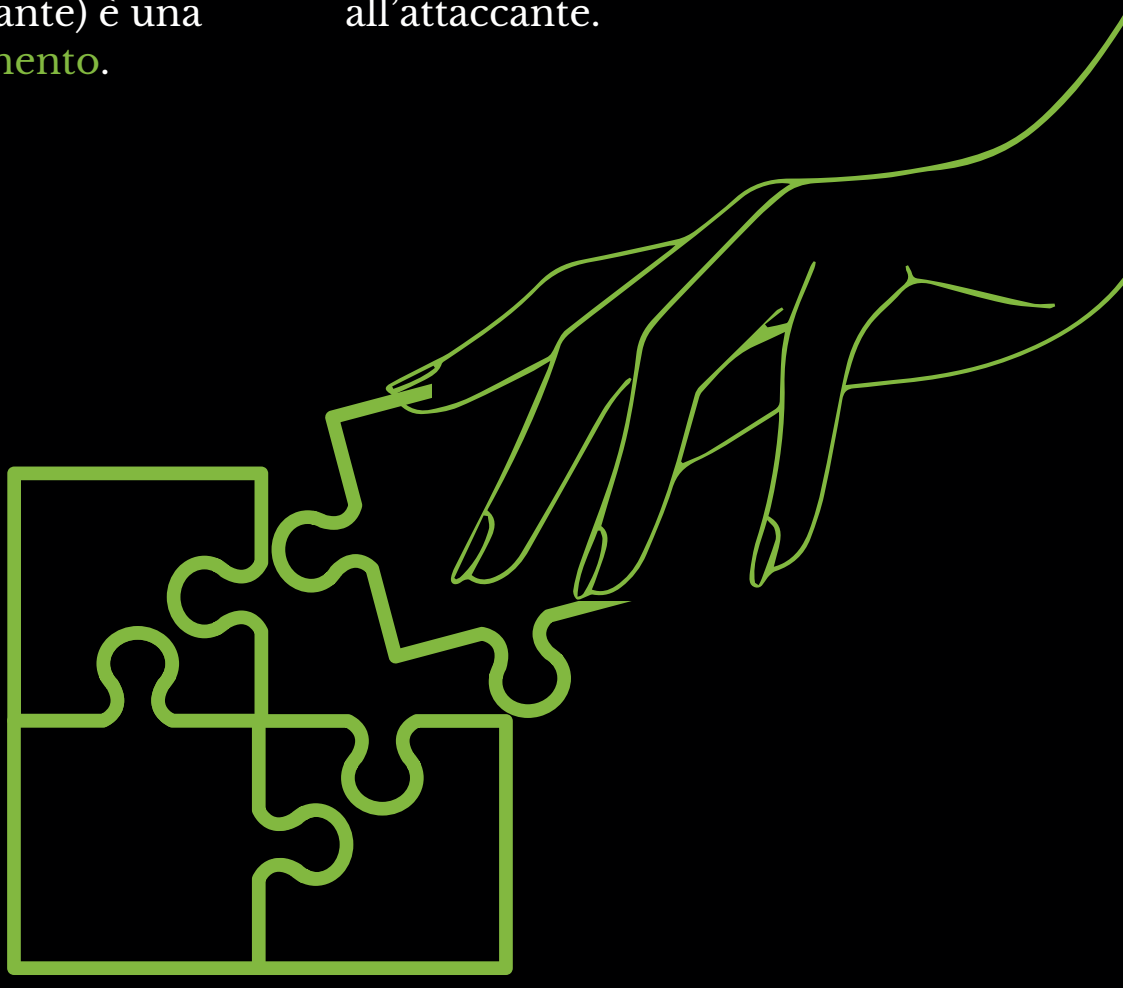
ISOLAMENTO E RIMOZIONE DEL SISTEMA B INFETTO

ISOLAMENTO

La completa disconnessione del sistema infetto dalla rete (restringere maggiormente l'accesso alla rete interna da parte dell'attaccante) è una tecnica di isolamento.

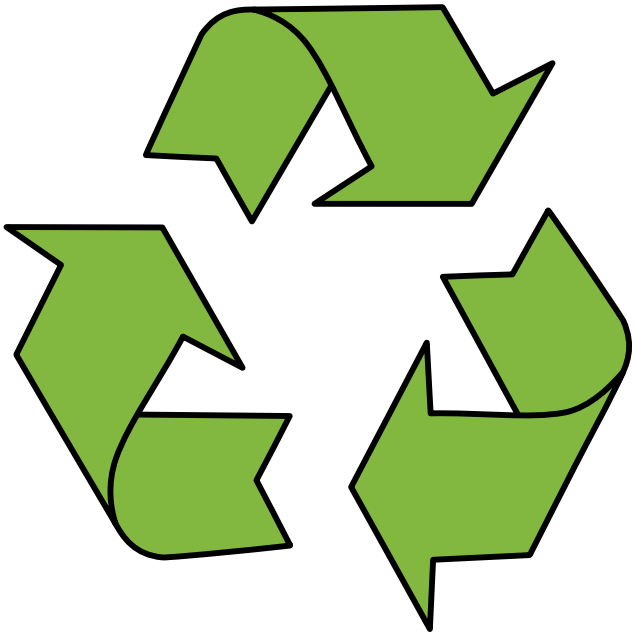
RIMOZIONE

Il sistema viene rimosso dalla rete sia interna sia internet, in modo tale da garantire l'inaccessibilità all'attaccante.



PURGE

Per gestire lo smaltimento o il riutilizzo di un disco o un sistema di storage di un sistema compromesso, posiamo ricorrere a diverse tecniche, vediamo qui il **PURGE** (bisogna accertarsi che le informazioni presenti sul disco/componente siano inaccessibili prima di smaltire o riciclare disco): utilizzo di forti magneti per rendere le informazioni inaccessibili su determinati dispositivi



DESTROY

si utilizzano, oltre alle tecniche di purge, tecniche di laboratorio come disintegrazione, polverizzazione dei media ad alte temperature, trapanazione.

Tecnica di

CLEAR

Tecnica «logica». 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;

GRAZIE

Incident Response

Prepared by
Alessandro Marasca

Presented to
Epicode - CS0124
S9L4