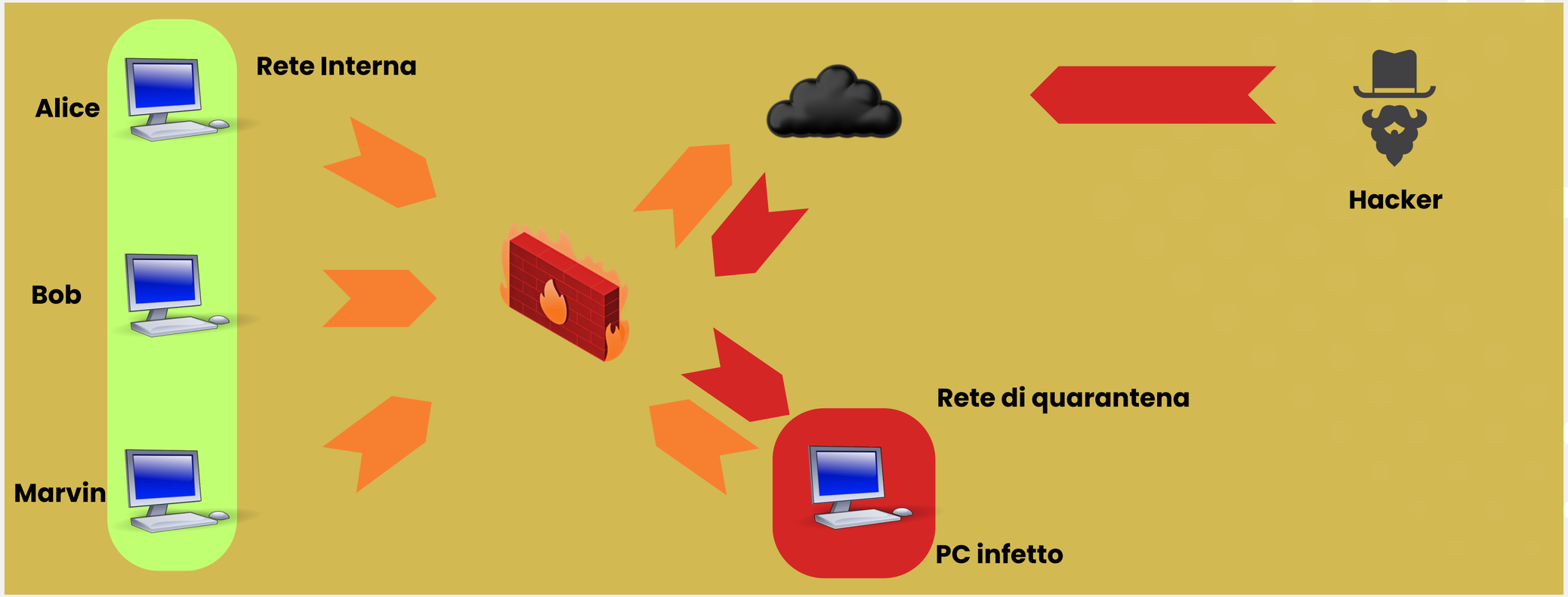
Consegna U3 S9 L4

Incident Response

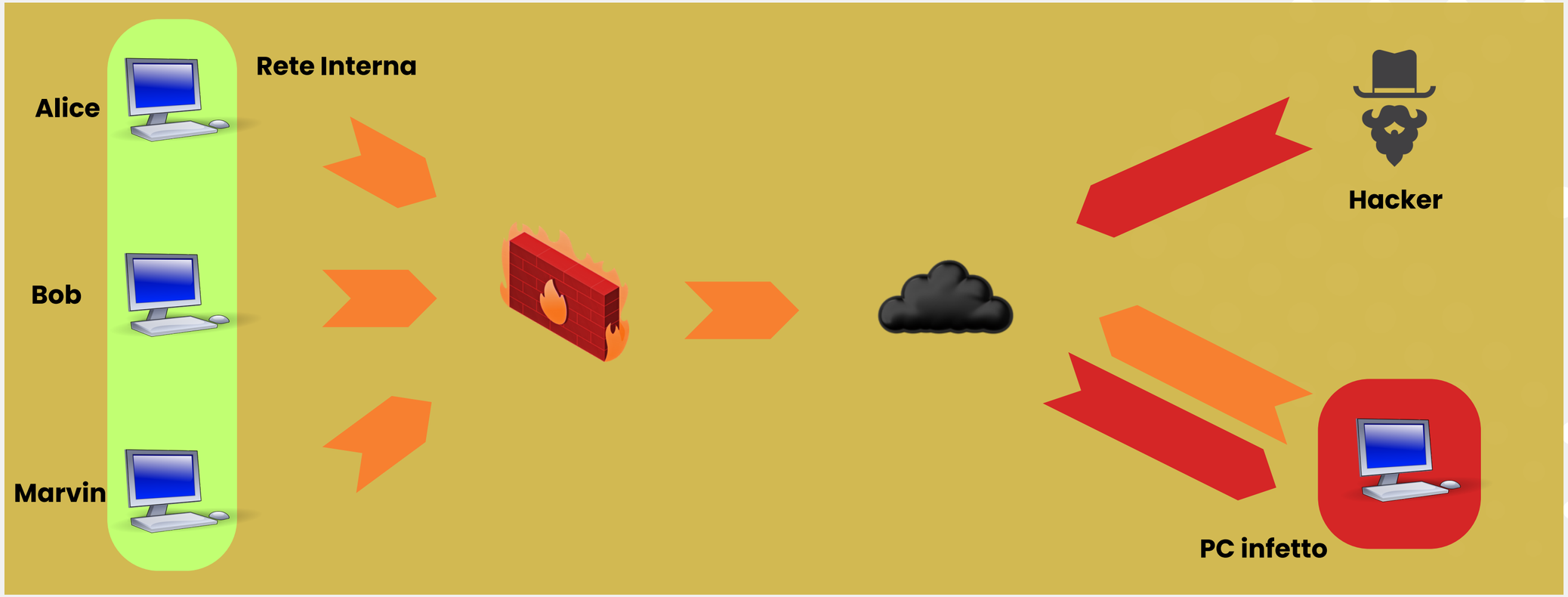
Rete di quarantena

In caso di macchina infetta da malware, la prima soluzione da adottare è quella della creazione di una sottorete, detta **rete di quarantena**, dove isolare il computer infetto per evitare che il malware si diffonda altrove nella rete interna. Dato che la macchina è ancora collegata ad internet, l'attaccante sarà ancora direttamente in contatto con il computer vittima dell'attacco.



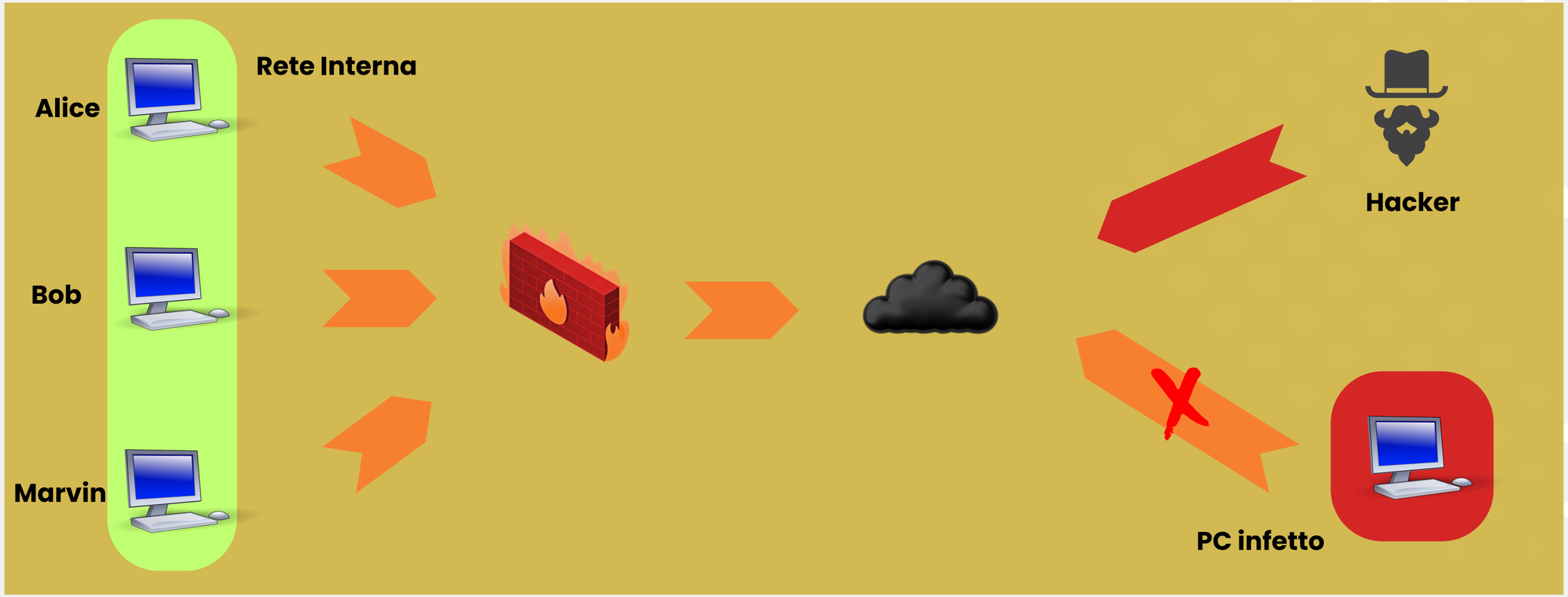
Tecnica di isolamento

Se la tecnica precedente si dovesse rivelare troppo debole, occorre isolare la macchina infetta per renderla innocua rispetto alle altre. Si procede quindi a disconnetterla dalla rete interna ma si continua a mantenerla connessa ad internet, quindi chi ha lanciato l'attacco a quel determinato computer manterrà ancora l'accesso via internet ad esso.



Tecnica di rimozione

Quando l'isolamento non è abbastanza, si procede all'effettivo distacco della macchina infetta dalla rete internet per scongiurare qualsiasi altro tentativo, da parte dell'attaccante, di creare ulteriori disservizi.



Smaltimendo dischi compromessi

Se non si è intervenuti repentinamente per salvare le macchine sotto attacco, servirà poi smaltire correttamente ed in modo sicuro i sistemi di storage ormai compromessi. Esistono diverse tecniche:

- **Clear:** la tecnica consiste nell'effettuare numerose e ripetute sovrascritture dei dati presenti sul disco oppure al ripristino di fabbrica del dispositivo per riportarlo al suo stato iniziale.
- **Purge:** è previsto l'uso di potenti magneti per danneggiare i file memorizzati sui piattelli magnetici del disco per renderli irrecuperabili.
- **Destroy:** oltre alle tecniche sopracitate, si procede alla totale distruzione del supporto di memoria portandolo ad alte temperature, per far sì che i campi magnetici sui piattelli vengano totalmente distrutti. Poi si puo procedere ulteriormente alla trapanazione del supporto di memorizzazione.

Grazie

Gianluca Sansone