Incident response

Traccia

Ipotizzando di avere un attacco attualmente in corso dove un attaccante ha bucato la rete ed ha accesso a un database tramite internet rispondere ai seguenti quesiti:

- Mostrare tecniche di Isolamento e Rimozione del sistema infetto
- Spiegare differenza fra Purge e Destroy prima di smaltire i dischi e indicare cosa si intende per Clear

Svolgimento

Per Isolamento si intende la completa disconnessione del sistema infetto dalla rete interna, questo impedisce la diffusione del malware agli altri dispositivi presenti nella rete interna. In questo caso il sistema infetto è ancora collegato ad internet.

Per Rimozione si intende uno scollegamento totale del sistema infetto, sia dalla rete interna che da internet. Possiamo quindi procedere con la rimozione di tutte le attività, componenti, processi relativi all'incidente sulla rete o sui sistemi.

Questo può comportare rimozione di backdoor o pulizia di dischi/chiavette USB compromesse.

La differenza fra Clear, Purge e Destroy sta nel modo in cui vengono eliminati i dati.

Nel caso di Clear i dati vengono cancellati sovrascrivendoli con informazioni casuali o con zeri attraverso programmi come Eraser.

Nel caso di Purge i dati vengono trattati come nel caso di Clear e in più vengono usate alcune tecniche di rimozione fisica come l'utilizzo di potenti magneti.

Nel caso di Destroy viene distrutto il supporto di archiviazione fisico, perforandolo, triturandolo o bruciandolo per garantire che i dati diventino totalmente inaccessibili.