EPICODE

ESERCIZIO W20D1

INCIDENT RESPONSE

Mungiovì Fabio

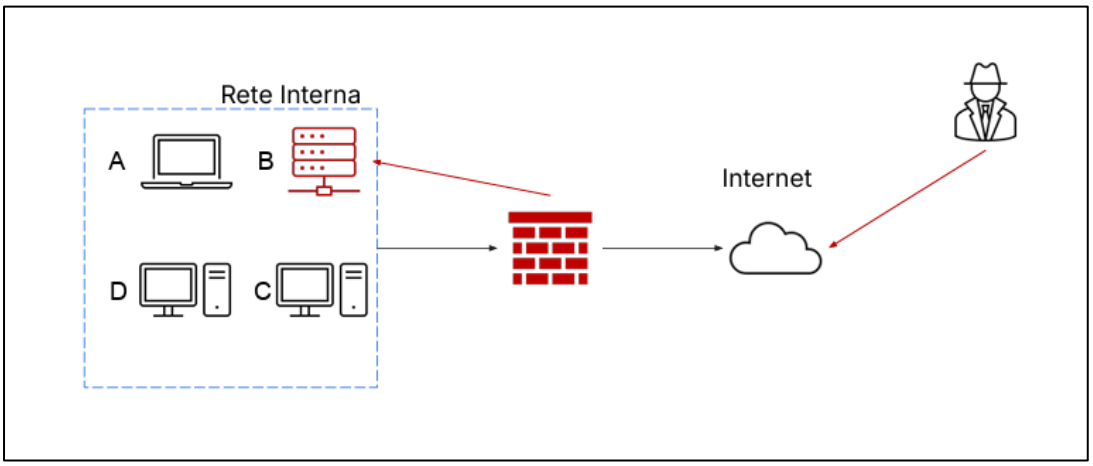
TASK

Con riferimento alla figura, 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 e 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:
  - Isolamento
  - 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



Facoltativo:

In una grande azienda, due utenti segnalano problemi sui loro computer e chiedono assistenza al reparto CSIRT/SOC (che siamo noi)

Analizzare i seguenti link e fare un piccolo report di quello che si scopre relativo alla segnalazione dell'eventuale attacco:

https://tinyurl.com/linklosco1

https://tinyurl.com/linklosco2

ESECUZIONE

Un sistema, chiamato sistema B, è stato compromesso e un attaccante è riuscito ad accedervi tramite Internet, bucando la rete.
Attualmente, l'attacco è in corso e facciamo parte del team CSIRT (Computer Security Incident Response Team).

Ci vengono chieste diverse cose per gestire questa situazione di sicurezza.

Tecniche di Isolamento

Per isolare un sistema compromesso come il sistema B, immaginiamo di voler creare una barriera per impedire che il problema si diffonda.
In questo caso, l'isolamento mira a contenere l'attacco e prevenire ulteriori danni o la diffusione del malware ad altri sistemi della rete interna.

Possiamo usare diverse tecniche:

- **Disconnessione dalla rete:** La soluzione più immediata è staccare fisicamente il sistema B dalla rete interna.
  Questo significa scollegare i cavi di rete o disabilitare l'interfaccia di rete.
- **Segmentazione della rete**: Se non si può disconnettere completamente, si può spostare il sistema B in una rete isolata, una "zona quarantena".
  Questo si fa configurando i firewall o i router per bloccare tutto il traffico da e verso il sistema B, tranne quello strettamente necessario per l'analisi.
- **Blocco tramite firewall**: Si possono aggiungere regole al **firewall** per bloccare tutto il traffico in entrata e in uscita dal sistema B, specialmente quello proveniente da Internet. Questo agisce come un guardiano che impedisce comunicazioni non autorizzate.

Rimozione del sistema infetto

Una volta isolato, il passo successivo è **rimuovere** la minaccia dal sistema B. Questo significa eliminare l'attaccante e qualsiasi traccia della sua presenza.

- **Analisi forense e identificazione del malware:**
  Prima di agire, dobbiamo capire cosa è successo.
  Si analizza il sistema per identificare il tipo di attacco, i malware presenti e le vulnerabilità sfruttate.
- **Eliminazione del malware:** Si usano strumenti antivirus e anti-malware per rimuovere qualsiasi software malevolo installato dall'attaccante.
- **Ripristino da backup sicuri:** Se l'attacco ha compromesso gravemente i dati o il sistema operativo, la soluzione più sicura è ripristinare il sistema B da un **backup** pulito e verificato, risalente a prima dell'attacco..
- **Patching e hardening:** Una volta pulito, è fondamentale applicare tutte le patch di sicurezza e aggiornamenti per correggere le vulnerabilità che l'attaccante ha sfruttato.
  Si rafforzano le configurazioni di sicurezza (hardening) per rendere il sistema più difficile da attaccare in futuro.

Differenza tra Clear, Purge e Destroy per l'eliminazione delle informazioni sensibili

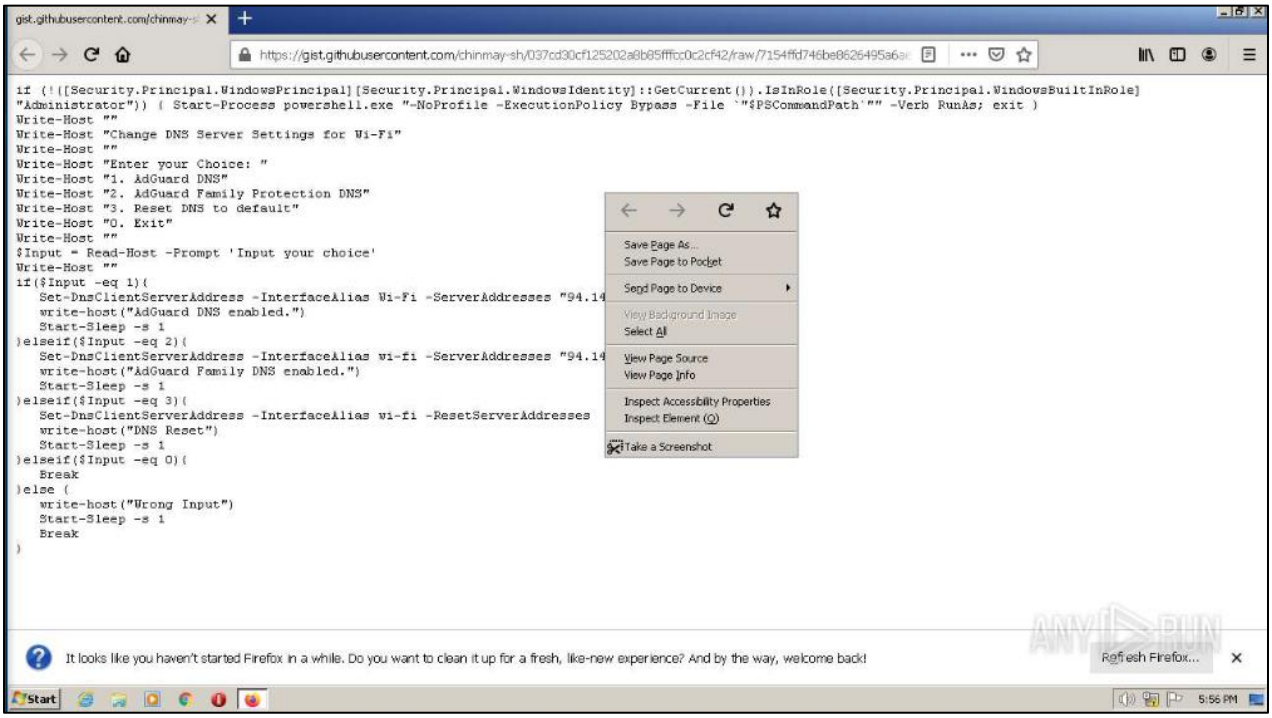
Quando si parla di eliminare informazioni sensibili, specialmente da dischi compromessi, ci sono diversi livelli di sicurezza.
Immaginiamo di voler eliminare un disegno da un foglio di carta: possiamo cancellarlo con una gomma (Clear), strappare il foglio (Purge) o bruciarlo (Destroy).
Ogni metodo ha un diverso livello di irrecuperabilità.

- **Clear (Cancellazione):** Questa tecnica serve a rendere i dati illeggibili con metodi standard, ma potenzialmente recuperabili con strumenti sofisticati. Si sovrascrive il disco una o più volte con dati casuali o zeri.
- **Purge (Pulizia):** Questo metodo mira a rendere i dati irrecuperabili anche con tecniche di recupero avanzate.
  Si utilizzano algoritmi specifici che sovrascrivono i dati più volte, spesso con schemi complessi, per eliminare qualsiasi residuo magnetico o elettronico.
- **Destroy (Distruzione):** Questo è il metodo più sicuro, che rende i dati assolutamente irrecuperabili attraverso la distruzione fisica del supporto di memorizzazione.
  Questo può includere la triturazione, la fusione, l'incenerimento o la perforazione dei dischi.

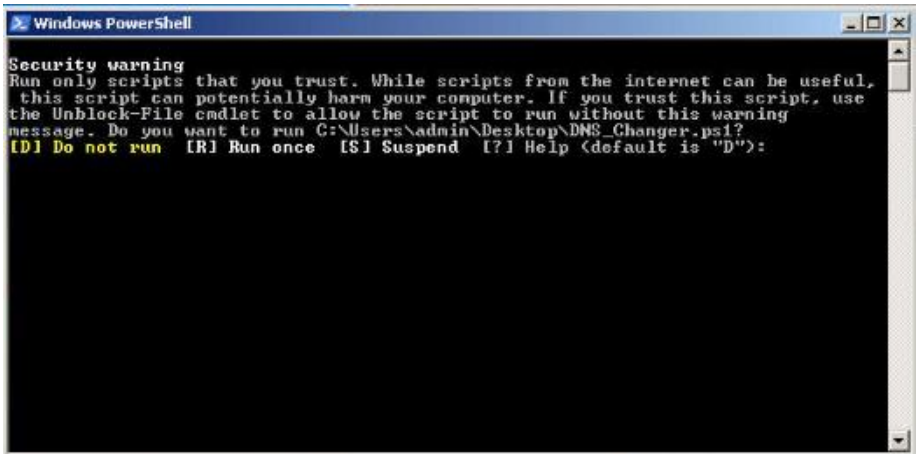
FACOLTATIVO

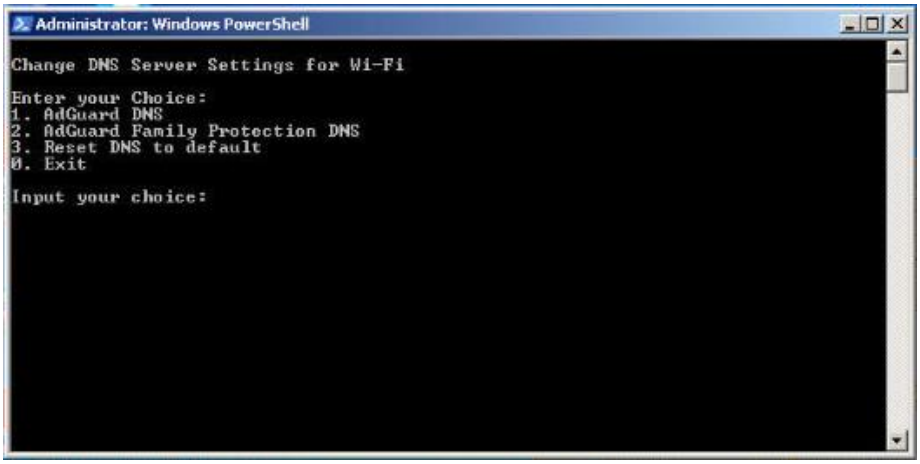
Scenario 1 - https://tinyurl.com/linklosco1

In questo primo scenario si nota che l'utente salva da una pagina web sconosciuta uno script PowerShell.



Una volta salvato lo script viene eseguito dall'utente che ignora il messaggio di sicurezza del sistema





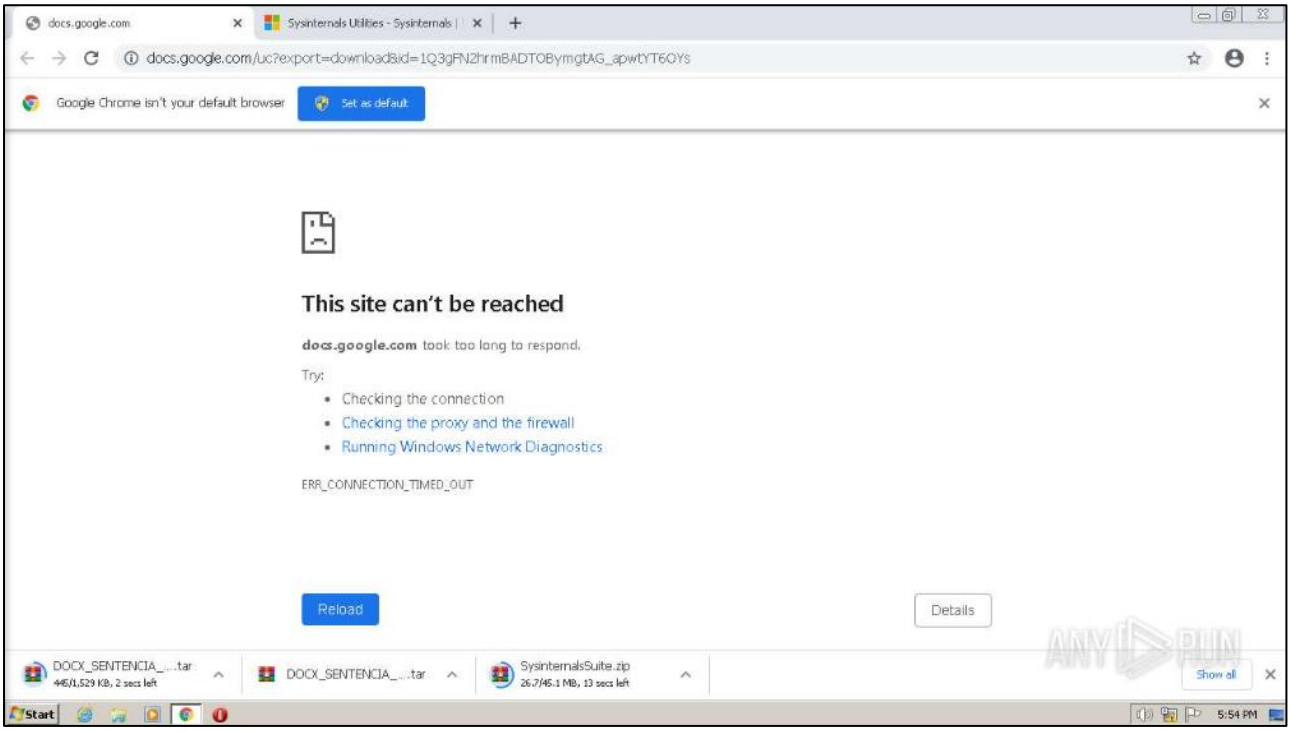
L'utente fortunatamente, avviato lo script non procede con l'utilizzo chiudendo la finestra.

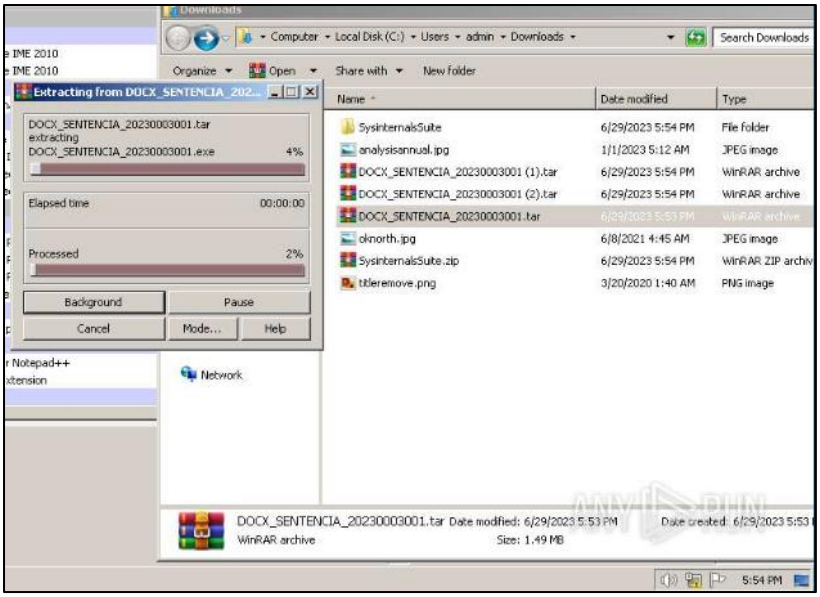
Lo script sembra avere la funzione di modificare le impostazioni DNS della macchina

Nonostante lo script non sia una minaccia diretta come un malware, rimane un comportamento rischioso.

Scenario 2 - https://tinyurl.com/linklosco2

Nel seguente scenario, notiamo come l'utente, collegato ad un link malevolo sconosciuto, sia vittima di più download automatici.





L'utente decomprime poi il file per analizzarlo

Questo comportamento è molto imprudente e rischioso, in quanto il file scaricato risulta essere un pericoloso eseguibile malevolo secondo le analisi dei processi.