PHANTOM SRL

REPORT

RISPOSTA AGLI ATTACCHI

Prepared For :
IANNONE SRL

Liceria & Co.

SAN SEVERO, PROVINCIA
DI FOGGIA.

PHANTOM s.r.l
IMPOSSIBLE IS OUR TARGET

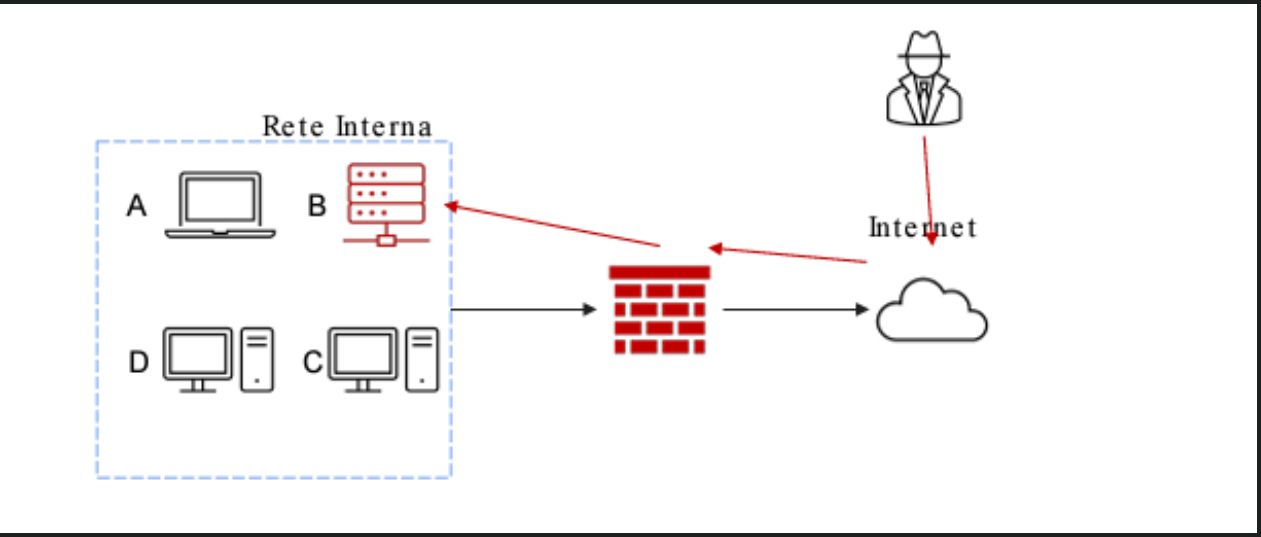
INDICE

REQUISITI

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 l'opzione Clear.



PROCEDURE

Procedura per isolare un database compromesso:

Identificazione dell'infezione: Prima di tutto, è essenziale rilevare quale parte del database è stata compromessa e in che modo l'infezione si è diffusa.

Disconnessione dal resto del sistema: Una volta identificata l'infezione, è importante interrompere immediatamente la connessione del database compromesso dal resto del sistema. Questo può essere fatto tramite la sospensione delle connessioni di rete o la disabilitazione dei servizi che accedono al database.

Creazione di una replica isolata: Per continuare ad operare con il database senza rischiare la diffusione dell'infezione, è consigliabile creare una replica isolata del database compromesso.
Questa replica deve essere separata dal resto del sistema e può essere configurata su un ambiente di test o su una rete isolata.

PHANTOM s.r.l
IMPOSSIBLE IS OUR TARGET

OPZIONE PURGA

La purga dei dati si riferisce al processo di eliminazione definitiva delle informazioni sensibili dai dispositivi di memorizzazione.
Durante la purga, i dati vengono sovrascritti con dati casuali o con zeri multiple volte.
L'obiettivo della purga è rendere le informazioni originarie irrecuperabili utilizzando tecniche di sovrascrittura multiple per eliminare qualsiasi traccia dei dati originali.
La purga è solitamente utilizzata quando si desidera riassegnare o riconsegnare un dispositivo di memorizzazione senza compromettere la sicurezza dei dati.

OPZIONE DESTROY

La distruzione dei dati è un processo più radicale che implica la distruzione fisica del dispositivo di memorizzazione.
Durante la distruzione, il dispositivo di memorizzazione viene fisicamente danneggiato in modo tale da rendere impossibile il recupero dei dati.
La distruzione può essere realizzata tramite metodi come la perforazione, la triturazione, la fusione o la degaussing (soprattutto per supporti magnetici).
L'obiettivo della distruzione è garantire che i dati non possano essere recuperati da nessun mezzo, nemmeno utilizzando tecniche avanzate di recupero dati.

DIFFERENZE

In breve, la purga si concentra sulla sovrascrittura sicura dei dati per renderli irrecuperabili, mentre la distruzione fisica distrugge completamente il dispositivo di memorizzazione per impedire qualsiasi possibilità di recupero dei dati. La scelta tra purga e distruzione dipende dalle esigenze specifiche di sicurezza e di conformità, nonché dalla sensibilità dei dati da eliminare.

OPZIONE CLEAR

Il "clear" si riferisce alla semplice eliminazione dei dati senza alcun processo di sovrascrittura o distruzione fisica del dispositivo di memorizzazione.
Durante il "clear", i dati vengono rimossi dal dispositivo di memorizzazione, ma non vengono sovrascritti con dati casuali o zeri.
Questo metodo lascia spazio vuoto sul dispositivo di memorizzazione, consentendo potenzialmente il recupero dei dati utilizzando strumenti di recupero dati specializzati, anche se il processo di eliminazione può rendere la maggior parte dei dati difficilmente accessibili tramite metodi convenzionali.
Il "clear" è solitamente utilizzato in situazioni in cui la sicurezza dei dati non è una preoccupazione critica o in cui i dati non sono particolarmente sensibili.
In sintesi, il "clear" consiste semplicemente nell'eliminare i dati senza ulteriori misure per rendere irreperibili le informazioni. Questo metodo è meno sicuro rispetto alla purga e alla distruzione e può lasciare dati recuperabili sul dispositivo di memorizzazione, sebbene possa essere sufficiente per scopi meno critici o per dati meno sensibili. Tuttavia, per dati sensibili, è consigliabile utilizzare metodi più sicuri come la purga o la distruzione.

	Purge	Clear	Destroy
Type of Sanitisation	Physical and logical sanitisation	Logical sanitisation	Physical sanitisation
Device Useful For	Floppy disks, hard disk drives, flash media	Floppy disks, disk drives, ATA hard drives	Floppy disks, hard disk drives, optical disks
Level of Protection	High	Moderate	Highest

POST-INCIDENTE

È obbligatorio un incontro di feedback e valutazione che coinvolga il team IR, le autorità dell'azienda e ogni individuo coinvolto nell'incidente di sicurezza per annotare le lezioni apprese e analizzare l'efficacia e le strategie del piano Incident Response in ogni sua fase.
Ecco alcuni punti su cui riflettere durante la fase di valutazione:

- La causa principale dell'incidente e dove si è verificato
- Se l'incidente si sarebbe potuto evitare
- La performance del piano IR e del team IR
- L'efficacia delle strategie ad ogni fase
- Attività che possono essere passate inosservate
- Qualsiasi step che avrebbe funzionato meglio se fatto diversamente
- Rilevamento della minaccia per evitare simili incidenti in futuro

GRAZIE

BY

PHANTOM SRL

Prepared For :
IANNONE SRL

Liceria & Co.

SAN SEVERO, PROVINCIA
DI FOGGIA.