Incident response

Sommario

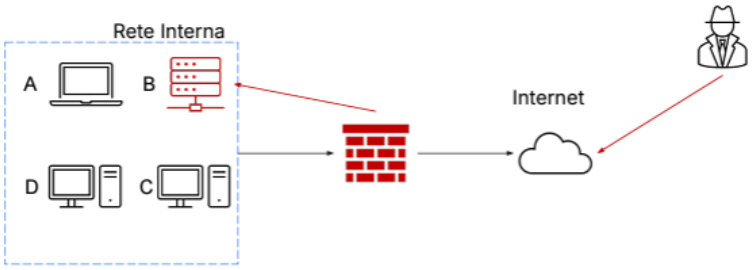
Traccia esercizio principale

Con riferimento alla figura nella prossima slide, 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:
  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**



Traccia esercizio facoltativo

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

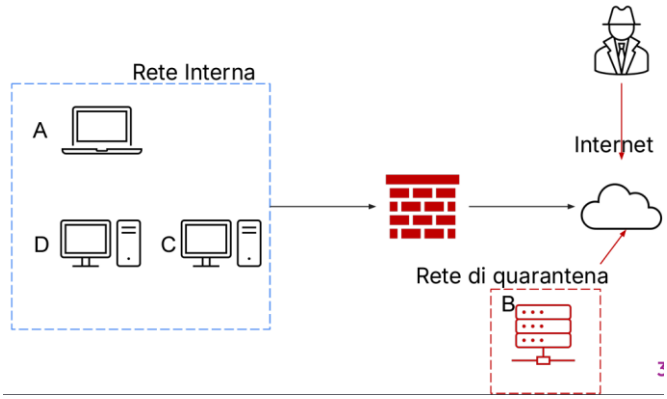
Analizzare i seguenti link e fare un **piccolo report** di quello che si scopre relativo alla segnalazione dell'eventuale attacco:

https://tinyurl.com/linklosco1 e https://tinyurl.com/linklosco2

Svolgimento esercizio principale

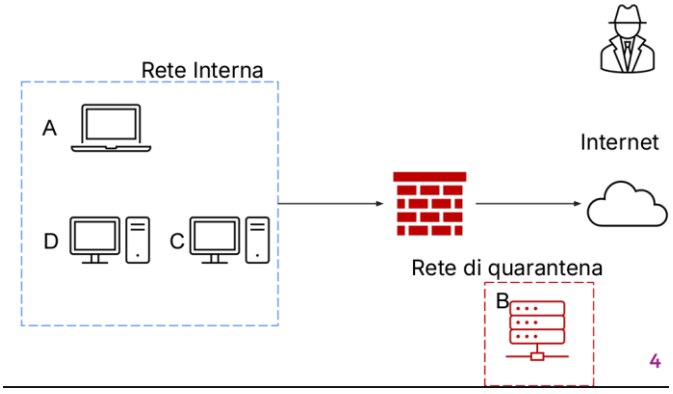
Isolamento

La tecnica di isolamento permette di isolare un sistema infetto restringendo l'accesso dell'attaccante alla rete interna. Tuttavia il sistema infetto sarà ancora accessibile dall'attaccante via internet



Rimozione

La tecnica di Rimozione elimina completamente il sistema dalla rete, di fatto rendendolo inaccessibile sia da rete interna che da internet. Questo approccio restringe l'accesso alla rete interna da parte dell'attaccante che non avrà nemmeno più accesso al sistema infetto.



Purge

Per quest'approccio si adottano sia misure logiche che misure fisiche per l'eliminazione permanente dei dati su un disco / dispositivo di storage. Le tecniche fisiche utilizzate tuttavia non sono invasive, e non implicano la distruzione dell'hardware

Destroy

Utilizza tecniche fisiche molto invasive per rendere inaccessibili i dati su un disco / dispositivo di storage. Alcune delle tecniche prevedono la distruzione a livello di hardware di fatto rendendo non recuperabile l'hardware e le relative informazioni salvate su di esso. È il metodo preferito quando si vuole smaltire un disco non riutilizzabile, ma è anche quello che costa di più.

Svolgimento esercizio facoltativo

https://tinyurl.com/linklosco1

Report di Analisi Malware

Informazioni Generali

L'analisi si riferisce al file **DNS_Changer.ps1**, con un verdetto di attività sospetta. L'analisi è stata eseguita il 29 Giugno 2023 su un sistema operativo **Windows 7 Professional SP1**.

Indicatori

Gli indicatori di compromissione includono i seguenti hash:

- **MD5:** 7CD193E2B99F15030CA538B924B4498C
- **SHA1:** 07A04D3C4279FFFE62968A4F76133B1AC71B490F
- **SHA256:** 3B9E727C56BFA9A16E5311F8D17472B9DCBE2F1E149FA2924EDA013611076D39

Attività Comportamentali

L'analisi ha rivelato comportamenti maliziosi, come il bypass della policy di esecuzione di PowerShell per eseguire comandi. Il processo **powershell.exe** ha avviato autonomamente diverse operazioni, tra cui la modifica delle impostazioni DNS e la lettura delle configurazioni di rete.

Inoltre, è stato osservato l'uso di PowerShell per gestire account locali e l'auto-avvio di **firefox.exe**, suggerendo che l'applicazione potrebbe essere stata scaricata o utilizzata in modo inappropriato.

Rischio di Attacco Phishing

È probabile che questo attacco sia di natura phishing. Modificando le impostazioni DNS, anche se l'utente digita un link legittimo, potrebbe essere reindirizzato a un sito malevolo che simula un sito autentico. In questo modo, le informazioni inserite potrebbero essere intercettate da aggressori.

Raccomandazioni

In via precauzionale, è fondamentale isolare immediatamente il PC infettato dalla rete. Questo passaggio impedirà la diffusione di eventuali minacce e proteggerà altri dispositivi collegati. Dopo aver isolato il sistema, controlla le impostazioni DNS e, se necessario, ripristinale a valori predefiniti o impostale su server DNS affidabili.

Esegui quindi una scansione approfondita del sistema utilizzando un software antivirus aggiornato. Questo aiuterà a identificare e rimuovere eventuali altre minacce. Dopo aver completato questi passaggi, monitora attentamente il sistema per segni di attività anomala e considera l'implementazione di misure di sicurezza aggiuntive.

Conclusioni

Il file **DNS_Changer.ps1** presenta comportamenti potenzialmente dannosi, con la capacità di alterare impostazioni di rete senza consenso. Si raccomanda di monitorare attentamente l'attività del sistema, isolare il PC infettato e intraprendere le azioni necessarie per garantire la sicurezza della rete. La consapevolezza riguardo ai rischi di phishing è fondamentale per prevenire futuri attacchi.

https://tinyurl.com/linklosco2

Report di Analisi Malware

Informazioni Generali

L'analisi si riferisce a un file scaricato da Google Drive, identificato come **DOCX_SENTENCIA_20230003001.tar**, con un verdetto di attività malevola. L'analisi è stata eseguita il 29 Giugno 2023 su un sistema operativo **Windows 7 Professional SP1**.

Indicatori

Gli indicatori di compromissione includono i seguenti hash:

- **MD5:** F227B42BC5D29AC82A82C40B6325B9E3
- **SHA1:** E5AA130B362D68AD2010540C0DE6BE3372DA3375
- **SHA256:** B24023DF44B0A1074B5DBB86AE6DA16FA4C10918C5C21E0100C4812CAE056C49

Attività Comportamentali

L'analisi ha rivelato attività maliziose e sospette. È stato identificato un **keylogger**, un tipo di spyware che registra ogni battitura sulla tastiera, consentendo agli aggressori di raccogliere informazioni personali, incluse le credenziali bancarie degli utenti. Inoltre, è stato rilevato un **Remote Access Trojan (RAT)**, specificamente **Remcos**, che consente il controllo remoto del sistema compromesso.

Comportamenti Maliziosi

- Il file è stato eseguito e ha avviato il compilatore C#.
- È stato utilizzato **Task Scheduler** per eseguire altre applicazioni.
- Sono stati rilevati tentativi di evasione delle difese tramite la creazione di un driver di sistema.

Comportamenti Sospetti

- Creazione di file con nomi simili a quelli di file di sistema.
- Lettura delle impostazioni di sicurezza di Internet Explorer e delle impostazioni dei certificati di sistema.
- Scrittura di file che potrebbero contenere registri del keylogger.
- Connessione a porte insolite, suggerendo attività di rete sospette.

Conclusioni e Raccomandazioni

Il file **DOCX_SENTENCIA_20230003001.tar** contiene componenti malevoli che possono compromettere seriamente la sicurezza del sistema. È fondamentale isolare il computer infettato dalla rete per prevenire ulteriori attacchi. Inoltre, è consigliabile eseguire una scansione approfondita con software antivirus aggiornati e ripristinare eventuali impostazioni di sicurezza compromesse.

Infine, si raccomanda di monitorare continuamente il sistema per rilevare eventuali segni di attività anomala e di educare gli utenti sulle minacce legate al phishing, che rappresentano un vettore comune per l'infezione da keylogger e RAT.