Come consentire le campagne sulle piattaforme di phishing simulate tramite Cisco Email Security Appliance

Sommario

Introduzione

In questo documento viene descritta la procedura di configurazione di Cisco Email Security Appliance (ESA) per simulare correttamente le campagne sulle piattaforme di phishing.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Creazione di filtri messaggi e contenuti sull'ESA.
- Configurazione della HAT (Host Access Table).
- Comprensione della pipeline di posta elettronica in arrivo dell'ESA Cisco.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Le piattaforme di phishing simulate consentono agli amministratori di eseguire campagne di phishing come parte di un ciclo per gestire una delle minacce più gravi che utilizza i sistemi di posta elettronica come vettore di attacchi di ingegneria sociale.

Problema

Quando l'ESA non è preparata per tali simulazioni, non è insolito per i suoi motori di scansione interrompere i messaggi della campagna di phishing, con conseguente fallimento o diminuzione dell'efficacia delle simulazioni.

Soluzione

> **Attenzione:** In questo esempio di configurazione, il criterio *TRUSTED* per il flusso di posta è selezionato per consentire all'ESA di passare attraverso campagne di phishing simulate di maggiori dimensioni senza alcuna limitazione. L'esecuzione di campagne di phishing continue di volume elevato può influire sulle prestazioni di elaborazione della posta elettronica.

Per garantire che i messaggi della campagna di phishing non vengano arrestati da nessuna componente di sicurezza della configurazione ESA, è necessario predisporre.

1. Crea un nuovo gruppo di mittenti: **GUI > Mail Policies > HAT Overview** e associarlo a *TRUSTED* mail flow policy (in alternativa è possibile creare un nuovo criterio con opzioni simili sotto **GUI > Mail Policies > Mail Flow Policies**).
2. Aggiungere gli host o gli IP di invio della piattaforma di phishing simulata al gruppo di mittenti. Se la piattaforma di phishing simulata dispone di un ampio intervallo di indirizzi IP, è possibile aggiungere nomi host parziali o intervalli IP, se applicabili.
3. Ordinare il gruppo di mittenti sopra il gruppo di mittenti *BLOCKLIST* per assicurarsi che venga confrontato in modo statico anziché in SBRS.
4. Disabilitare tutte le funzioni di sicurezza per il criterio flusso di posta *TRUSTED* in **GUI > Criteri di posta > Criteri flusso di posta > TRUSTED** (o il criterio flusso di posta appena creato):

Security Features	
Spam Detection:	○ Use Default (On) ○ On ◉ Off
AMP Detection	○ Use Default (On) ○ On ◉ Off
Virus Protection:	○ Use Default (On) ○ On ◉ Off
Sender Domain Reputation Verification:	○ Use Default (On) ○ On ◉ Off
Virus Outbreak Filters:	○ Use Default (On) ○ On ◉ Off
Advanced Phishing Protection:	○ Use Default (On) ○ On ◉ Off
Graymail Detection:	○ Use Default (On) ○ On ◉ Off
Content Filters:	○ Use Default (On) ○ On ◉ Off
Message Filters:	○ Use Default (On) ○ On ◉ Off

5. **Inviare le modifiche ed eseguire il commit.**

AsyncOS v.14 precedente

Attenzione: In questo esempio di configurazione, il criterio *TRUSTED* per il flusso di posta è selezionato per consentire all'ESA di passare attraverso campagne di phishing simulate di maggiori dimensioni senza alcuna limitazione. L'esecuzione di campagne di phishing continue di volume elevato può influire sulle prestazioni di elaborazione della posta elettronica.

Per garantire che i messaggi della campagna di phishing non vengano arrestati da nessuna componente di sicurezza della configurazione ESA, è necessario predisporre.

1. Crea un nuovo gruppo di mittenti: **GUI > Mail Policies > HAT Overview (Policy di posta)** e associarlo ai criteri di flusso di posta *TRUSTED*.
2. Aggiungere gli host o gli IP di invio della piattaforma di phishing simulata al gruppo di mittenti. Se la piattaforma di phishing simulata dispone di un ampio intervallo di indirizzi IP, è possibile aggiungere nomi host parziali o intervalli IP, se applicabili.
3. Ordinare il gruppo di mittenti sopra il gruppo di mittenti *BLOCKLIST* per assicurarsi che venga confrontato in modo statico anziché in SBRS.
4. **Inviare le modifiche ed eseguire il commit.**
5. Passare alla CLI e aggiungere un nuovo filtro messaggi, **CLI > filtri,** copiare e modificare la sintassi e aggiungere il filtro.
6.
```
skip_engines_for_simulated_phishing:
if (sendergroup == "name_of_the_newly_created_sender_group")
{
insert-header("x-sp", "uniquevalue");
log-entry("Skipped scanning engines for simulated phishing");
skip-spamcheck();
skip-viruscheck();
skip-ampcheck();
skip-marketingcheck();
skip-socialcheck();
skip-bulkcheck();
skip-vofcheck();
skip-filters();
}
.
```
7. Ordinare il filtro messaggi verso l'alto nell'elenco per assicurarsi che non venga ignorato da un altro filtro messaggi al di sopra di esso che include l'operazione skip-filters.
8. Premere Invio per tornare al prompt dei comandi principale di AsyncOS ed eseguire il comando "**commit**" per eseguire il commit delle modifiche. (non fare clic su CTRL+C: tutte le modifiche verranno cancellate).
9. Selezionare **GUI> Mail Policies > Incoming Content Filters** (Policy di posta > Filtri contenuti in arrivo)
10. Creare un nuovo filtro contenuti in arrivo con la condizione ***"Altra intestazione"*** impostata per cercare l'intestazione personalizzata **"x-sp"** e il relativo *valore univoco* configurato nel filtro messaggi e configurare l'azione ***Ignora filtri contenuti rimanenti (azione finale)***.
11. Ordinare il filtro contenuti su "1" per assicurarsi che altri filtri non eseguano azioni sul messaggio di phishing simulato.
12. Selezionare **GUI > Mail Policies > Incoming Mail Policies** (Policy di posta in arrivo) e assegnare il filtro contenuti al criterio richiesto.
13. **Inviare e confermare le modifiche.**
14. Eseguire la campagna per piattaforme di phishing simulate e monitorare mail_logs/Message

Tracking per verificare la corrispondenza tra flusso e regole dei criteri.