如何通過思科郵件安全裝置允許模擬網路釣魚平台活動

目錄

簡介

本檔案介紹思科電子郵件安全裝置(ESA)上的配置步驟，以成功模擬網路釣魚平台活動。

必要條件

需求

思科建議您瞭解以下主題：

- 在ESA上建立消息和內容過濾器。
- 主機存取表(HAT)的組態。
- 瞭解思科ESA傳入的電子郵件管道。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

模擬網路釣魚平台允許管理員將網路釣魚活動作為週期的一部分來管理，從而利用電子郵件系統作為社會工程攻擊媒介，從而管理最大的威脅之一。

問題

當ESA沒有準備好進行此類模擬時，其掃描引擎會停止網路釣魚活動消息，從而導致模擬失敗或降低模擬的有效性，這種情況並不少見。

解決方案

注意：在此配置示例中，選擇*TRUSTED*郵件流策略，以允許ESA通過更大的模擬網路釣魚活動，而不會有任何限制。持續進行大量網路釣魚活動可能會影響電子郵件處理效能。

為確保網路釣魚活動消息不會被任何安全元件阻止，需要將ESA配置中的安全元件安裝到位。

1. 建立新的發件人組：**GUI > Mail Policies > HAT Overview**，並將其繫結到*TRUSTED* mail flow policy(GUI > Mail Policies > Mail Flow Policies（郵件策略）>郵件流策略)。
2. 將模擬網路釣魚平台的傳送主機或IP新增到此發件人組。如果模擬網路釣魚平台具有大範圍的IP，則可以新增部分主機名或IP範圍（如果適用）。
3. 在*BLOCKLIST* Sender Group上方對發件人組進行排序，以確保靜態匹配而不是SBRS。
4. 在**GUI > Mail Policies > Mail Flow Policies > TRUSTED**下，禁用*TRUSTED*郵件流策略的所有安全功能（或新建立的郵件流策略）：

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.提**交這些更改並提交。**

先前的AsyncOS v.14

注意：在此配置示例中，選擇*TRUSTED*郵件流策略，以允許ESA通過更大的模擬網路釣魚活動，而不會有任何限制。持續進行大量網路釣魚活動可能會影響電子郵件處理效能。

為確保網路釣魚活動消息不會被任何安全元件阻止，需要將ESA配置中的安全元件安裝到位。

1. 建立新的發件人組：**GUI > Mail Policies > HAT Overview**並將其繫結到*TRUSTED郵*件流策略。
2. 將模擬網路釣魚平台的傳送主機或IP新增到此發件人組。如果模擬網路釣魚平台具有大範圍的IP，則可以新增部分主機名或IP範圍（如果適用）。
3. 在*BLOCKLIST* Sender Group上方對發件人組進行排序，以確保靜態匹配而不是SBRS。
4. **提交這些更改並提交。**
5. 導航到CLI並新增新的消息過濾器、**CLI >過濾器**，複製並修改語法並新增過濾器。

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. 在清單中將郵件過濾器向上排序，以確保其上方的另一個郵件過濾器（包括跳過過濾器操作）不會跳過該郵件過濾器。
8. 按Enter鍵導航回到AsyncOS的主命令提示符，然後發出命令「**commit**」提交更改。（請勿按一下CTRL+C — 它將清除所有更改）。
9. 導航到**GUI>**「郵件策略」(**Mail Policies)>「傳入內容過濾器」(Incoming Content Filters)**
10. 建立條件設定為「***Other Header***」的新傳入內容過濾器，以查詢在郵件過濾器中配置的自定義報頭「**x-sp**」及其uniquevalue，並配置操作Skip Remaining Content Filters(Final Action)。
11. 將內容過濾器排序為「1」，以確保其他過濾器不會對模擬的網路釣魚郵件執行操作。
12. 導航到**GUI > Mail Policies > Incoming Mail Policies**，然後將內容過濾器分配給所需的策略。
13. **提交和提交更改。**
14. 運行模擬網路釣魚平台活動，並監控mail_logs/Message Tracking以驗證流和策略規則匹配。