Cisco E メール セキュリティ アプライアンス（ESA）を通り抜けて組織に入り込むスパム

内容

概要

このドキュメントでは、スパム メールが組織に入り込む可能性がある 5 つの仕組みについて説明します。

方式

1.正当なメッセージ/マーケティングメール

正当なメッセージは、ユーザが事前に送信を許可しているか、ユーザの名前が別の組織に売られていることを意味します。前者の場合、ユーザが購読を解約してリストから削除されるための手続きを取る必要があります。後者の場合、スパム対策の定義をグローバルに更新して ESA の全体的スパム キャプチャ率を向上させるために、メッセージを spam@access.ironport.com に再送信してください。受信メール ポリシーでマーケティング メールを有効にすると、このメッセージを「スパム」ではなく「マーケティング」として認識させるのに役立つ場合があります。

2.アンチスパムが正しく更新されていない

スパム対策が無効にされているか、ライセンス キーの有効期限が切れています。スパム対策が更新されているかどうかを確認するには、**[GUI] > [Security Services] > [IronPort Anti-Spam]に移動します。**このパネルには、過去6時間以内にルールセットまたはエンジンの更新が表示されます。また、このタブの最上部から、スパム対策サービスが有効にされていることを確認できます。ライセンス キーのステータスを調べるには、[System Administration] タブから [Feature Key] に移動して、スパム対策キーのステータスを確認します。

3.メールポリシーまたはメッセージフィルタ

顧客のメール ポリシーに従って特定の送信者または受信者に対してスパム対策セキュリティ エンジンが無効にされていると、スパムが組織に入り込む可能性があります。 スパム フィルタリングをスキップするには、メッセージ フィルタ（CLI：**filters コマンド）を使用するという手段もあります。**

4.メールフローポリシー

ICID を使用してメッセージを分類すると、スパム対策セキュリティ機能がオフにされて、メール ポリシーがオーバーライドされる可能性があります。これを確認するには、メール ログを調べます。ログ内では最初に ICID を確認して、メッセージがどの SenderGroup に分類されているかを理解する必要があります。それを基に、関連するメール フロー ポリシーを確認します。
AllowListに大量のエントリがある場合は、AntiSpamエンジンによってスキャンされたかどうかを確認するために、受信しているメッセージの一部を確認する必要があります。メッセージのヘッダーを表示して、ヘッダー X-IronPort-Spam の有無を調べます。このヘッダーがあれば、メッセージはスパム対策エンジンによって処理されたことになります。

5.メッセージはスパムです

これは、実際にスパム メッセージが使用されるという手段です。メッセージ トラッキング機能を使用してスパム対策エンジンによってメッセージがスキャンされたことを確認した結果 (メッセージ トラッキングで「CASE」を検索します)、 ケースの判定が否定的であり、メッセージがスパムであると思われる場合は、元のメッセージを spam@access.ironport.com に報告してください。これは、新しくリリースされたスパムの脅威である場合、あるいは設計し直された古い脅威である場合が考えられます。

スパムの報告は、自動プロセスおよび手動プロセスの両方で処理され、その報告に関するフィードバックはありません。随時、Cisco TAC に連絡して評価と応答を要求できます。