ESA の SenderBase はもう 1 つの DNS RBL ですか。

目次

質問

SenderBase も DNSBL の 1 つですか。

SenderBase は通常の DNSBL ではありません。 アンチスパム コミュニティには、DNS ベースのブラックリストが多数あります。 DNS ベースのブラックリストは、大規模に分散されたデータベースに標準化された API (アプリケーション プログラミング インターフェイス) を追加する手法として、10 年以上前に開発されました。 メール サーバなどのネットワーク デバイスには一貫して DNS クライアント アプリケーション (「リゾルバ」と呼ばれることもあります) が組み込まれることから、DNS を使用して IP アドレスに関する情報を参照するのは、ほとんどのシステムにとって非常に自然な動作です。 DNS ベースのブラックリストの概念は、広く分布しているユーザのコミュニティに、データベース レプリケーション、認証、あるいは複雑な API について懸念することなく効率的に IP 指向のリストをクエリできる簡単な手段を提供するというものです。

大半の DNS ベースのブラックリストでは、ブラックリストの説明 (たとえば、「オープン リレーとして既知のシステム」) を記述した上で、誰もがそのリストをクエリして当該 IP アドレスがそこに含まれているかどうかを確認できるようにするという戦略をとっています。 アドレスがリストに含まれる場合、リストの所有者はその IP アドレスがブラックリストへの追加対象であることをアサートします。 つまり、DNS ベースのブラックリストは「はい/いいえ」式のリストです。---IP アドレスはリストに含まれるか含まれないかのどちらかです。

DNS ベースのブラックリストは一般に、ボランティアによって管理されています (ただし、有料のサブスクリプションに基づいて利用できるものもいくつかあります)。 このことから、非常に特異な方法で運用される傾向もあります。 これらはボランティアが運営するプロジェクトとして、スパムの問題を極めて深刻に懸念する個人またはグループによって運用されるため、慎重を期して正当なメールでもブロックしがちです。 DNS ベースのブラックリストを使用することを選択した企業は、これらのリストがスパムを削減するのに最小限の効果しかないという印象を受けるか (つまり、IP アドレスがなかなかブラックリストに追加されず、リストがタイムリーに更新されない)、あるいは誤検出率が極めて高いという印象を受けるか (つまり、IP アドレスがあまりにも安易にブラックリストに追加される) のいずれかです。

SenderBase は、DNS ベースのブラックリストの特異な振る舞いを軽減する目的、そしてネットワーク管理者がどれだけ保守的に、あるいはどれだけ積極的にリストを使用するか決定できるようにする目的で作成されました。 SenderBase を ESA のスロットリング機能と併せて適切に利用することで、誤検出率を大幅に低下できると同時に、スパムの大半を企業ネットワークから締め出すことができます。