SenderBaseはCisco Eメールセキュリティアプライアンス(ESA)のもう1つのDNS RBLですか。

内容

質問

SenderBaseはCisco Eメールセキュリティアプライアンス(ESA)のもう1つのDNSリアルタイムブラックホールリスト(RBL)にありますか。

応答（Answer）

SenderBaseは通常のDNS RBLではありません。アンチスパムコミュニティには、DNSベースのブロックリストが多数存在します。長年にわたって開発された技術であるDNSベースのブロックリストは、広く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）を追加する方法を提供します。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ベースのブロックリストの概念は、広く分散しているユーザのコミュニティが、データベースの複製、認証、またはより複雑なAPIを心配することなく、IP指向のリストを効率的に照会する簡単な方法を提供することです。

ほとんどのDNSベースのブロックリストの戦略は、ブロックリストの説明（「オープンリレーとして知られているシステム」など）を記述し、リストにIPアドレスが含まれているかどうかを誰でも確認できるようにすることです。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ベースのブロックリストは「はい/いいえ」の回答で、リストに登録しているか、そうでない場合があります。

一般に、ボランティアはDNSベースのブロックリストを管理します（ただし、有料のサブスクリプションでは利用できるブロックリストはほとんどありません）。 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。ボランティア運営プロジェクトとして、スパムの問題に強く感じる個人やグループが運営しており、通常は正当なメールをブロックする側で エラーを起こす傾向があります。DNSベースのブロックリストを使用することを選択した企業は、スパムを減らすのに最小限の効果しか見つけることができません（つまり、リストに載せるのは困難で、リストの更新がタイミングが悪いです）。また、リストに載るのは簡単です。

SenderBaseは、DNSベースのブロックリストの特異な動作を減らし、ネットワークマネージャがリストの保守的な方法や積極的な使用方法について独自の決定を行えるように作成されました。SenderBaseをESAのスロットリング機能と組み合わせて適切に使用すると、誤検出率を大幅に低下させることができます。同時に、スパムの大部分は企業ネットワークから除外されます。

関連情報

- SenderBase の動作の仕組み
- テクニカル サポートとドキュメント – Cisco Systems