目次

質問

SenderBase はもう一つの DNSBL ですか。

SenderBase は通常の DNSBL ではないです。 反スパム コミュニティでは、多くの DNS ベース ブラックリストがあります。 前に 10 年に開発される手法は DNS ベース ブラックリスト広く追加する方法を分散型データベースへ標準化された API（アプリケーション プログラミング インターフェイス）を提供します。 ネットワークデバイスに、メール サーバのような、すべて DNS クライアントアプリケーション 組み込みが（時々「リゾルバ」と呼ばれる）あるので、DNS を使用して IP アドレスについての情報を調べることはほとんどのシステムのための非常に自然なオペレーションです。 DNS ベース ブラックリストの概念は効率的にデータベース複製、authentizcation、またはより複雑な API を心配しないで IP 指向リストを問い合わせるユーザの広く分散コミュニティに簡単な方法を提供することです。

ほとんどの DNS ベース ブラックリストのための戦略はブラックリスト（例えば知られている、「開いた中継」であるためにシステム）の説明を示し、次に IP アドレスがリストにあるかどうか見るためにリストを問い合わせるようにだれでもすることです。 アドレスが現われる場合、リスト オーナーは IP アドレスがリストであるために修飾に会ったことをアサートします。 すなわち、DNS ベース ブラックリストは「yes/no」返事です---リストにあります、またはありません。

DNS ベース ブラックリストはボランティアによって一般に（のため支払サブスクリプション基礎で利用可能である）少数があるが管理されます。 それらはまたオペレーションで非常に特有でありがちです。 ボランティア運営のプロジェクトとして、それらはスパムの問題について非常に強く感じ、一般に ブロッキング 正規の メールの側で誤りがちである個人またはグループ操作されます。 DNS ベースを使用するために選択した企業は最小限に見つけますそれらをスパムを（ブラックリストに載せます、リストで得ることは困難であり、リスト更新は時機を得ていませんか）減らすためにすなわち有効またはこれらのリストが非常に高い false positive 比率（すなわち、リストで得ることは余りにも容易です）を生成することが分ります。

SenderBase は両方に作る機会を提供するために積極的にリストをどのようににについての使用するか軽減します DNS ベース ブラックリストの特有動作の問題をネットワーク管理者に自身のデシジョンをどのように保守主義者または作成され。 SenderBase の適切な使用によって、ESA のスロットリング機能と共に、false positive の比率はスパムの大きい比率が社内ネットワークから保存されると同時に劇的に廃棄することができます。