ESA のスプーフィング メールのフィルタリング

目次

概要

この資料はスパムおよび詐欺的な電子メールがネットワークに入るとき Cisco E メール セキュリティ アプライアンス（ESA）で直面する問題を記述したものです。

問題

電子メールに扮する詐欺師試み。 電子メールは（からある趣旨）会社担当者のメンバーに扮するとき、特に当てにならない場合もあり、混合を引き起こす可能性があります。 会社（スプーフィングされたメール）内から起きるようであるこの問題を解決するために、電子メール管理者は受信 メールをブロックするように試みるかもしれません。

ドメイン名で会社リターン アドレスがあるインターネットからの受信 メールをブロックすれば、それは問題を解決することは論理的なようであるかもしれません。 メールをこのようにブロックするとき残念ながら、それはまた正当 な電子メールを同時にブロックできます。 これらの例を参照して下さい:

- ISP メール サーバに透過的に Simple Mail Transfer Protocol （SMTP）トラフィックすべてをリダイレクトする従業員は旅し、ホテル インターネットサービスプロバイダー （ISP）を使用します。 メールが送信されるとき、それは企業に渡される前に企業 SMTP サーバを直接フローするが、サード パーティ SMTP サーバによって実際に送信 されることにようであるかもしれません。

- 従業員は電子メール説明リストを定期講読します。 メッセージが電子メールリストに送られるとき、発信元からすべてのサブスクライバに、外見上戻ります。

- 外部 システムは実際に目に見えるデバイスのパフォーマンスか到達可能性を監察するために使用されます。 アラートが発生するとき、電子メールにリターン アドレスで会社 ドメイン名があります。 サード パーティ サービスプロバイダーは、WebEx のような、これをかなり頻繁にします。

- 一時的 な ネットワーク 設定 エラーが理由で、会社の内側からメールは送信リスナーよりもむしろ受信リスナーによって、送信されます。

- 会社の外の誰かはオリジナルヘッダーよりもむしろ使用新しいヘッダー ラインをそのメール ユーザ エージェント（MUA）を持つ会社に再びそのメッセージをそれら転送します受け取り

ます。

- Federal Express **配布ページ**または Yahoo **電子メール**のようなインターネット ベース アプリケーションは、会社に戻ってリターン アドレスで**この技術情報**ページ、正当 な メールをそのポイント作成します。 メールは正規ので、が会社の送信元アドレスが内側からあります、内側から起きません。

これらの例はドメイン 情報に基づいて受信 メールをブロックすれば false positive という結果に終る場合があることを示します。

解決策

このセクションはこの問題を解決するために行う必要がある推奨 処置を記述します。

フィルタを加えて下さい

正当 な 電子メール メッセージの損失を避けるために、ドメイン 情報に基づいて受信 メールをブロックしないで下さい。 その代りそれらがメッセージは可能性としては造られることを受信者に示すネットワークに入ると同時に、これらのメッセージ の タイプの件名をタグ付けできます。 これはメッセージ フィルターまたはコンテンツ フィルターによって達成することができます。

これらのフィルタ用の基本的な戦略は逆方向先の尖ったボディ ヘッダー ライン (データ**から最も**重要のあります) 、また RFC 821 エンベロープ 送信側をチェックすることです。 これらのヘッダー ラインは MUAs で最も一般に示され、詐欺的な人によって造られる可能性が高い物です。

次 の 例のメッセージ フィルターは可能性としては人格化されるメッセージをどのようにタグ付けできるか示します。 このフィルタは複数の操作を行います:

- 件名がそれで既に**「{可能性のある造られる}」**持っている場合、別のコピーはフィルタによって追加されません。 これはメッセージ スレッドが完了する前に応答がメッセージフローに含まれている、件名はメールゲートウェイを通って移動するかもしれません数回とき重要であり。

- このフィルタはエンベロープ 送信側をまたはドメイン名 **@yourdomain.com** でそのアドレスが端あるヘッダ**から**捜します。 mail-from 検索が自動的に大文字と小文字を区別しないが、から-ですことに注意することは重要ヘッダ検索はそうではないです。 ドメイン名がどちらの位置でもある場合、フィルタは件名の端**に**「**{可能性のある造られる}」**挿入します。

フィルタの例はここにあります:

```
MarkPossiblySpoofedEmail:

   if ( (recv-listener == "InboundMail")       AND
        (subject != "\\{Possibly Forged\\}$") )
   {
       if (mail-from == "@yourdomain\\.com$") OR
          (header("From") == "(?i)@yourdomain\\.com")
       {
           strip-header("Subject");
           insert-header("Subject", "$Subject {Possibly Forged}");
       }
   }
```

追加手段

正当 な メールからのスプーフィングされたメールを識別する単純な方法がないので問題を完全に除去する方法がありません。 従って、Cisco は効果的に詐欺的なメール（phishing）またはスパムを識別し、肯定的にブロックする IronPort 反スパム スキャン（IPAS）を有効に することを推奨します。 この反スパム スキャナーの使用は正当 な電子メールの損失なしで、前のセクションに説明があるフィルターによってつながれたとき最もよい結果を提供します。

ネットワークに入って来る詐欺的な電子メールを識別する必要があったら、ドメイン キーによって識別されるメール（DKIM）テクノロジーの使用を考慮して下さい; それはより多くのセットアップを必要としますが、phishing、詐欺的な電子メールに対してよいメジャーです。

> **注:** メッセージ フィルターに関する詳細については、Cisco E メール セキュリティ アプライアンス サポートページの **AsyncOS ユーザガイドを**参照して下さい。