proofpoint

Proofpoint Threat Report

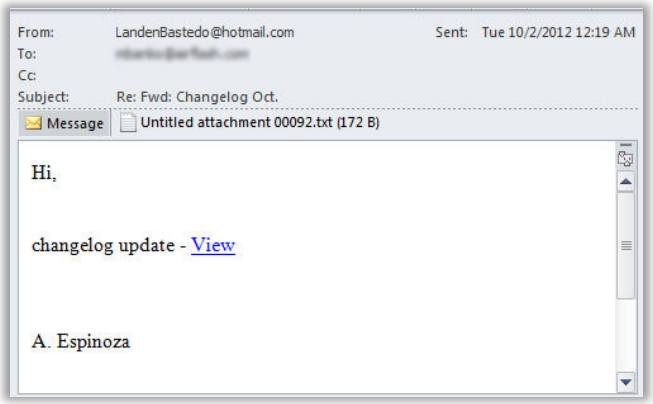
October 2012

本レポートは、Proofpoint が注目し、お客様および一般企業に対して注意を喚起したいと考えている脅威に関する情報、詳細、トレンドなどをまとめたものです。

Threat Models（手法）

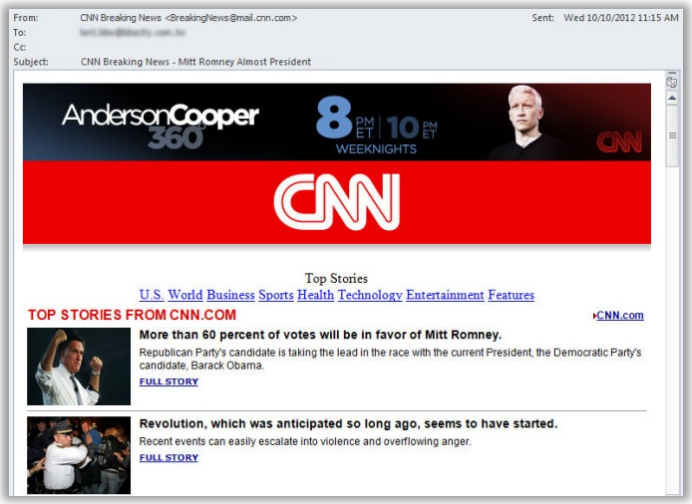
Changelog Javascript Exploit

Proofpoint では 9 月に最初に観測されたこの大規模な攻撃が再開されたことを、10 月 2 日に観測しました。今回の攻撃は前回よりも大規模で、100 近くの組織を狙って 500 通近いフィッシングメールが送られました。これらのメールは 3 万の異なる IP、3 万 5 千もの送信者アドレスから送られています。



この攻撃では、メール受信者は自動ダウンロードを起動させる不正な Javascript を仕込んだ 20 あまりの独立した Web サイトに誘導されます。このマルウェアは、既に感染済みのマシンへのリモートアクセスも試みます。この複合型の脅威は非常に短時間のうちに行われるため、既存の境界防衛型のセキュリティをすり抜けてしまいます。Proofpoint Targeted Attack Protection を利用していたお客様のサイトでは、これらの URL は自動的に書換えられ、エンドユーザーがそれらをクリックした場合でもアクセスは自動的にブロックされました。

CNN Breaking News

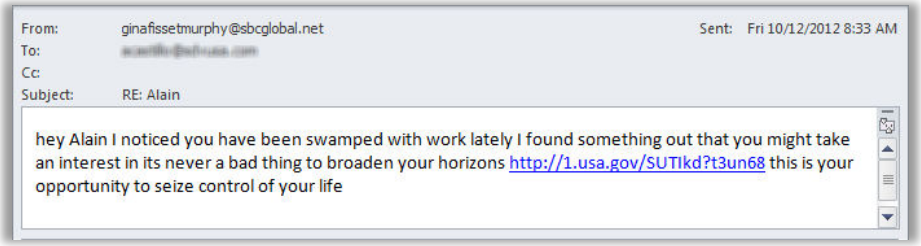


11 月の米大統領選には誰もが興味を持っており、ハッカー達はこれを利用しようとしています。10 月 10 日にはすでに Proofpoint は CNN Breaking New のテンプレートを使ったフィッシングメール検知し、ブロックし始めました。CNN の選挙情報ページの代わりに BlackHole コードを使った不正なサイトにリンクされています。解析により、これらのサーバーはドイツとロシアにあることがわかりました。

詳細については SCmagazine の記事をご覧ください。

1.usa.gov への URL リダイレクト

tinyurl.com や bit.ly のような URL 短縮サービスは、元々マーケティングや SNS キャンペーンを効果的・効率的に行えるよう考えられたものです。しかしハッカー達は、これを不正な Web サイトを隠蔽するためや、レピュテーションベースのアンチスパムエンジンによる検知をすり抜けるために利用することをすぐに思いつきました。URL 短縮サービスにも不正サイトのフィルタリングおよびブロッキング機能は組込まれていますが、最近ではこのサービスを使った攻撃が増えつつあります。



10 月末になって、ハッカー達が米政府系の URL 短縮サービスを使って 2 万人のユーザーを不正な Web サイトに誘導したと報じられました。この大規模攻撃は open-redirect vulnerability を使ってユーザーを 2 回リダイレクトします。まず政府の Web サイトへ、次に偽の CNBC ニュース記事にリダイレクトされ、Money Making の広告が表示されます。Proofpoint はこれらの短縮 URL を全て解析しました。これらのタイプの攻撃は 10 月 3 日にはブロックされており、10 月 12 日の類似の攻撃でもブロックできたことを確認しました。

Threat News (ニュース)

miniFlame

2012 年 5 月、Kaspersky は「Flame」と呼ばれる新たなサイバー スパイ ワームを発見しました。Flame マルウェアについての継続的な調査の結果、最近になって、類似しているが完全に別のマルウェアである「miniFlame」を発見しました。miniFlame はデータを盗み感染したシステムにアクセスするツールとしては類似の機能を持っていますが、広範な対象にスパイを仕掛けるわけではなく、極めて限定された対象に絞ったコンパクトな攻撃ツールであるという点で異なっています。もちろん単体でも機能しますが、Flame や Gauss などの他のスパイツールと連携することもできます。詳細については wired.com の記事もご覧ください。

RAaaS (Remote Access-as-a-Service)

サイバー犯罪の世界では、個人情報や財務情報を含むあらゆるタイプのデータが有償で取引されてきましたが、この 10 月に新たな動きがありました。Blackhat が「少なくとも 17,000 台のハッキング済みマシンへのリモートアクセス」の販売を始めたのです。 その中には少なくとも 1 社のフォーチュン 500 企業のマシンが含まれています。ハッキング済みマシンへのリモートアクセスには RDP: Remote Desktop Protocol (ネットワークから仮想デスクトップへのアクセスを可能にするプロトコルおよびサービスで、Microsoft Windows でサポートされています)が使われます。仮想接続に利用可能なクライアントは広く存在しており、Windows XP、Vista、7 そして Mac にもその機能は搭載されています。

US-CERT が DKIM ベリファイアの脆弱性について警告

E メールアドレスのなりすまし(Spoofing)は、サイバー詐欺やハッキングにおいては最もよく使われる手法のひとつです。なりすましを防ぐためには、暗号鍵を使ってヘッダー内のドメイン名を検証する DKIM などの認証技術が有効です。

10 年前は、512 ビットの暗号鍵(DKIM の鍵など)を解読するために世界中の組織が協力しなければなりませんでした。しかし現在では、Amazon などのクラウドを使えば、72 時間で解読できてしまいます。これはセキュリティ上の問題を引き起こします。なぜならばいくつかの企業は未だに 512 ビットの DKIM 鍵を使っており、よく知られたブランド(Yahoo, Amazon, Google など)でも、なりすましに対して脆弱であることがあるからです。US-CERT (United States Computer Emergency Readiness Team)は警告を出し、512 あるいは 764 ビットの鍵は全て 1,024 ビットに置き換えるよう推奨しています。

Proofpoint のサービスを利用してアウトバウンドメールを送信しているお客様で DKIM を利用している場合には、お客様に代って Proofpoint が 2,048 ビットの鍵を生成していますから安全です。Proofpoint では既存の DKIM 鍵のインポートも認めていますが、事前に鍵長をチェックすることをお薦めしております。

Firefox 16 の脆弱性

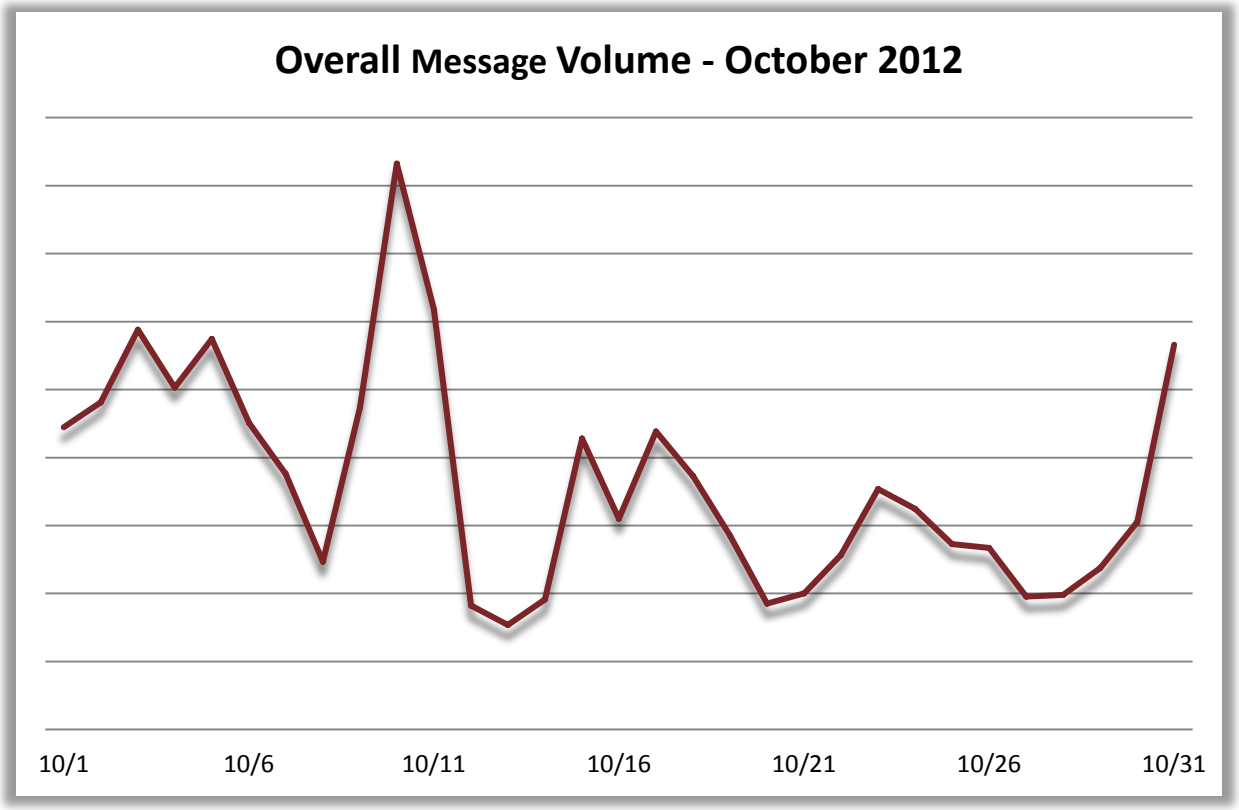
Web ブラウザとして Chrome を使う人は増え続けており、Internet Explorer のシェアは低下しています。一方で Firefox のシェアは 20%付近で落ち着いており、Firefox を使い続けているユーザーは月一回の定期的なアップデートに慣れてしまっています。

10 月、Firefox 16 へのアップグレードにセキュリティ上の問題が発見され、Web サイトから削除 されました。Mozilla のセキュリティ情報によると、この脆弱性は「悪意のあるサイトによって、ユーザーが訪れたことのあるサイトの URL や URL パラメータを判別される潜在的可能性がある」ということです。URL パラメータがユーザー名やパスワードを含む事があるということで、問題が解決するまでの間、ユーザーは Firefox 15 に主導でダウングレードするよう推奨しています。

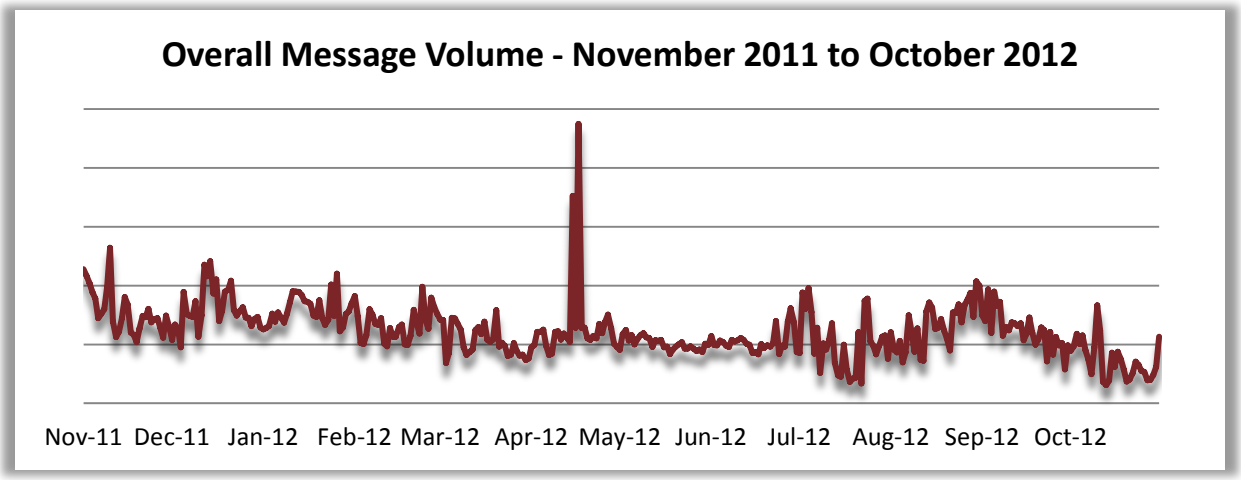
Threat Trends (トレンド)

Spam Volume Trends (スパム量のトレンド)

今年行われたボットネットの解体はここへ来て全体のスパム量に影響を及ぼしてきました。9 月から 10 月にかけて、スパム量は 40%も減少しました。ハッカーやスパマーはホリデイシーズンに備えているのかもしれません。10 月のスパム量は今年最低であるばかりか、過去 24 ヶ月間の中でも最低でした。

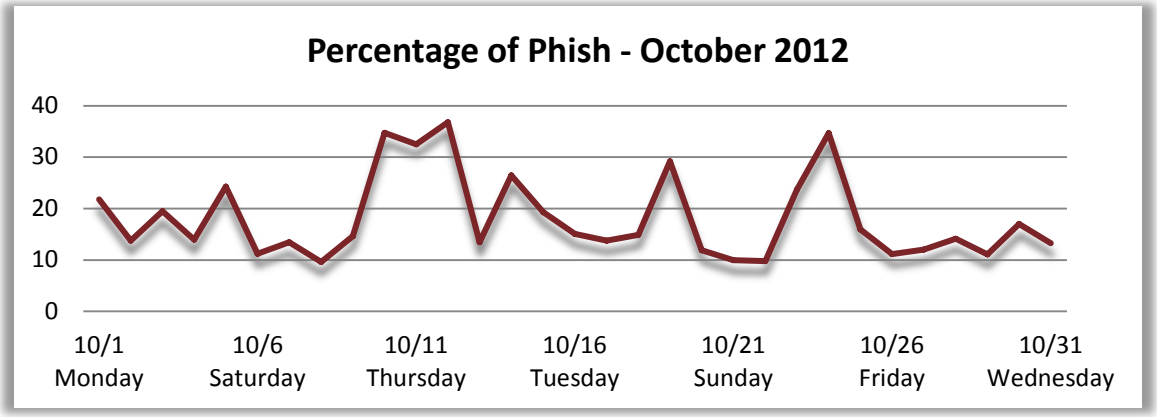


昨年同月比でも減少傾向は変らず、2011 年 10 月と比べてスパム量は 65%減少しています。

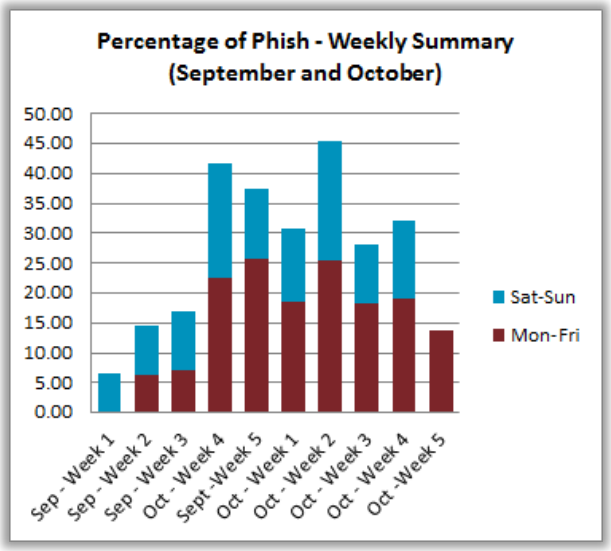


Phish Classification Trends（フィッシング分類のトレンド）

下のグラフは、Proofpoint MLX および Targeted Attack Protection によってスパム及びバルクメールの中からフィッシングに分類されたメッセージのパーセンテージです。グラフ中の数値は上位 10 ソースの平均を日次で集計したものです。

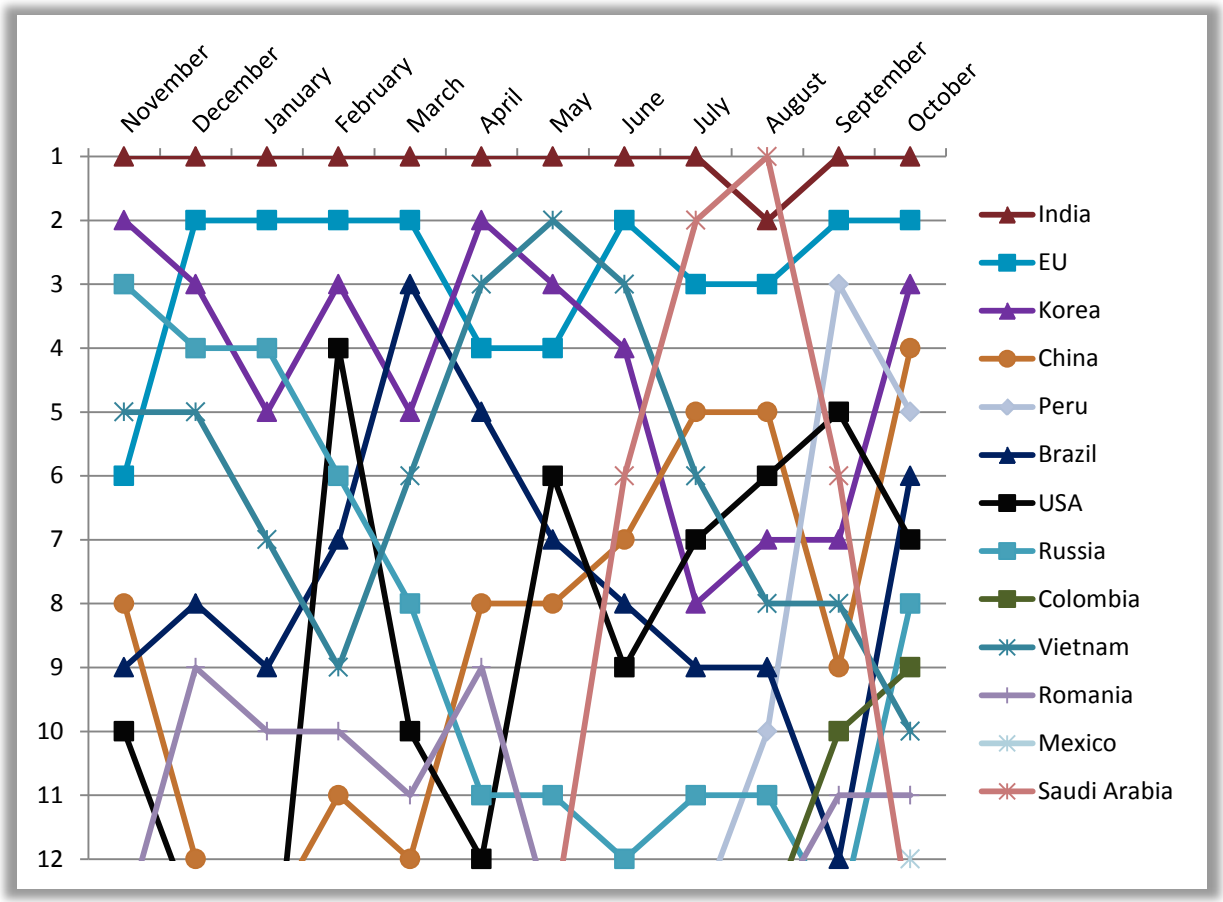


後半 2 週間に攻撃の増加が見られた 9 月とは違い、10 月は月間を通して増減が見られました。また、ウィークデイに比べてウィークエンドのフィッシングメッセージの量が少ないという特徴もありました。しかし、フィッシング攻撃自体は日によって大きな違いがあるわけでは無く、一週間を通じてランダムに発生しています。



Source of Spam（スパム発信源）

インドは、2 ヶ月前に一回だけ 2 位に落ちましたが、先月・今月とまたスパム発信量世界一の座を取り返しています。8 月に急伸してトップになったサウジアラビアは、今月は 12 位と圏外に落ちました。同じく急伸して 3 位になったペルーは 5 位に後退しました。先月とは違い、スパム量 1 位のインドは 2 位の EU よりも 50%多いだけで、上位 3 カ国のスパム量の違いは比較的少ないと言えます。



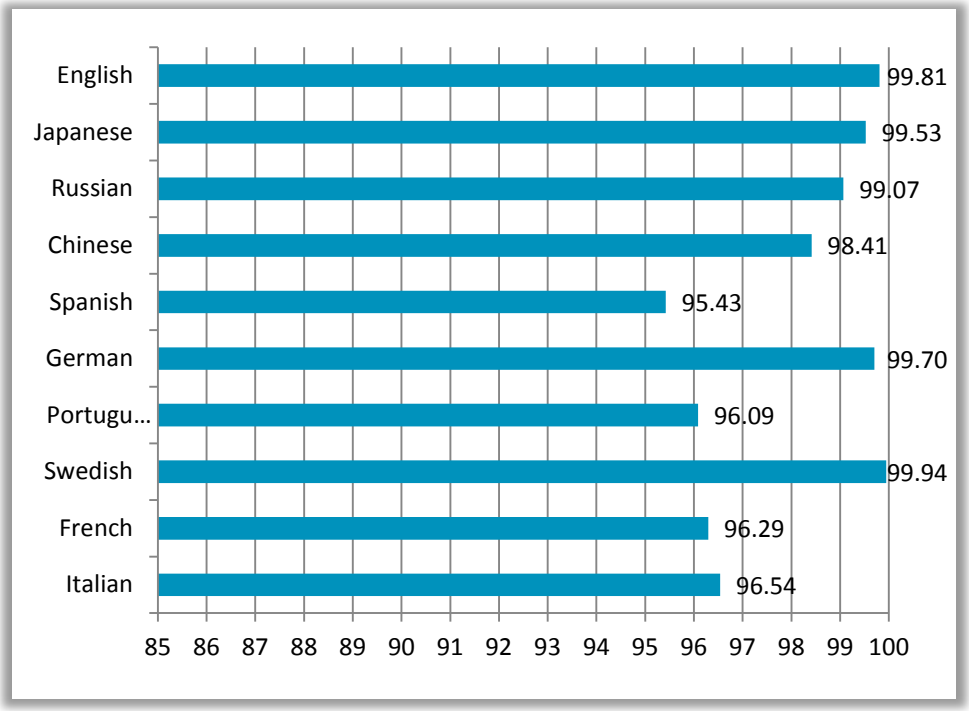
興味深い点として、ラテンアメリカの国々がスパムの主要な発信元となる傾向を引き続き示しています。今月、メキシコが第 12 位に初登場しました。（2 ヶ月前にペルーが初めて 10 位に登場し、先月はコロンビアが 10 位にランクインしています）ラテンアメリカからのスパムは上位 10 カ国のうち 30%、上位 12 カ国のうち 33%を占めています。

右側の表はスパム配信元 10 カ国の、全体に占めるパーセンテージおよびトップ 10 の中でのパーセンテージを示しています。

Rank	Country	% Overall	% Of Top 10
1	India	8.46%	18%
2	EU	7.37%	16%
3	Korea	6.05%	13%
4	China	5.62%	12%
5	Peru	4.10%	9%
6	Brazil	3.98%	8%
7	USA	3.36%	7%
8	Russia	2.83%	6%
9	Colombia	2.67%	6%
10	Vietnam	2.64%	6%

Language Effectiveness（言語別防御効果）

次のグラフは、Proofpoint ソリューションのスパム防御の有効性を言語毎に示したものです。



proofpoint

Proofpoint, Inc.
892 Ross Drive, Sunnyvale, CA 94089
Tel: +1 408 517 4710
www.proofpoint.com