proofpoint

Proofpoint Threat Report

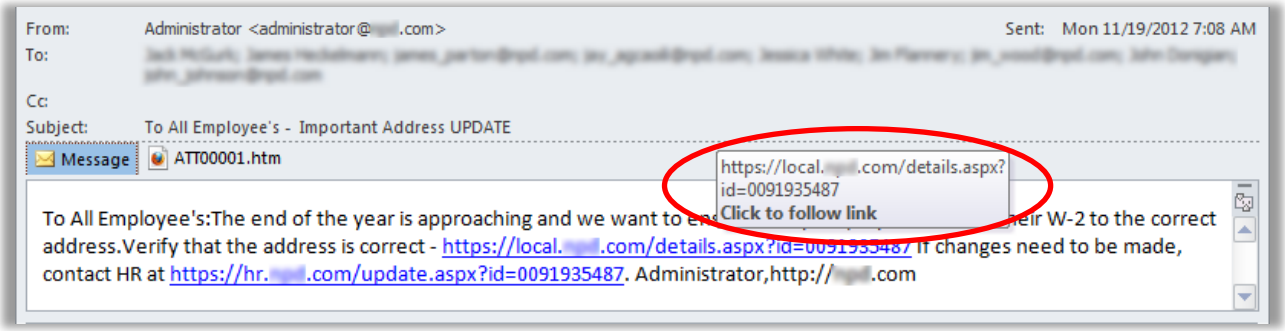
November 2012

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)

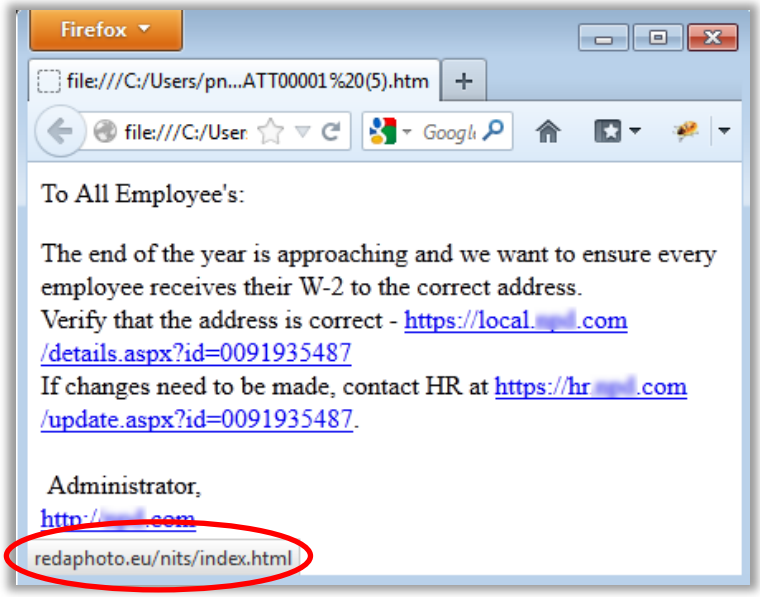
W-2 Verification (悪意のある HTML アタッチメント – 悪意の無いメッセージ中の URL)

11 月はハッカー達がブラックフライデイやサイバーマンデイの売り出しを装ったメールを出す月です。11 月はまた、ソーシャルエンジニアリングと年末の活動や告知などを組合わせて、より洗練された攻撃を仕掛ける時でもあります。一例として、従業員に年末向けの W-2 様式の税務申告書類 (他に W-1 や W-3、またはその他の W-x 様式もあります)に関する偽の住所確認通知を送りつけるものがあります。これらは非常に洗練されており、メッセージ中に表示されている URL の上にマウスを持って行った時にポップアップ表示される URL が外部の URL や悪意のあるサイトには見えず、社内の正規な URL に見えるのです。



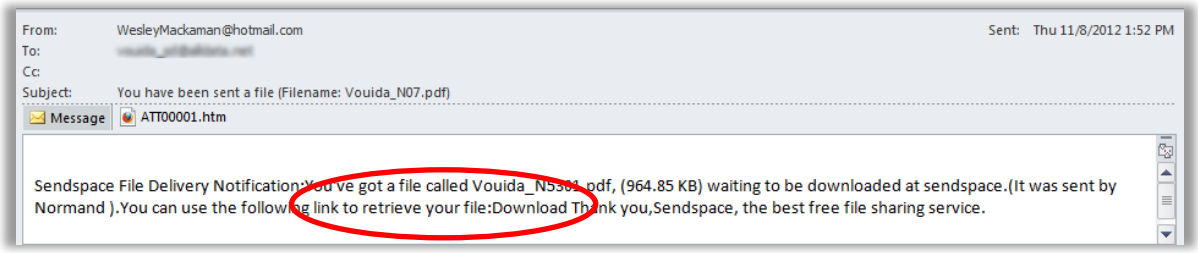
しかしこの URL は存在しないか、W-2 に関する情報を含んでいないため、ユーザーは添付の HTML を開いてしまい、そこから悪意のある活動が始まります。添付 HTML の中のリンクを解析したところ、そのリンクはヨーロッパのサイトにリダイレクトされるようになっており、そのサイトは複数のブラックリストに載っているものでした。

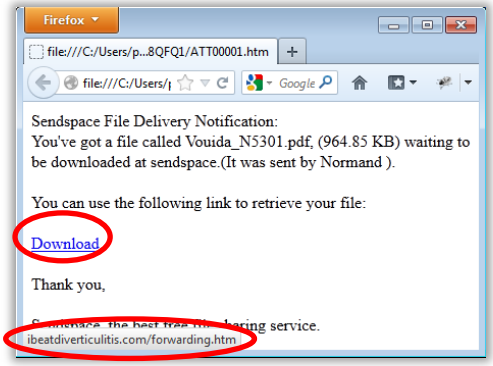
Proofpoint では複数のお客様がこの攻撃を受けていることを把握しており、ほとんどの場合、市や州、政府機関が狙われています。中小の企業やエンタープライズを狙ったものも数件ありました。Proofpoint Targeted Attack Protection を導入しているお客様では、疑わしい URL はメッセージ本文か添付 HTML かに関わらず全て書換えられるため、安全です。さらに、脅威が確認された段階でエンドユーザーがその URL をクリックしても全て自動的にブロックされ、攻撃から効果的に守ります。Proofpoint Enterprise Protection を導入しているユーザーも、これらのメールが脅威であると確認された後は保護されます。



File Share Notification (悪意のある HTML アタッチメント – メッセージに URL は含まれ無い)

エンドユーザーが日々の業務において IT 部門の許可無しに様々なコンシューマ向けサービスや個人のデバイスを使うケースが増加しています。これは、コンシューマライゼーション、あるいは BYOD (Bring Your Own Devices) と呼ばれています。コンシューマ向けサービスには Box.net、 Dropbox、YouSendIt



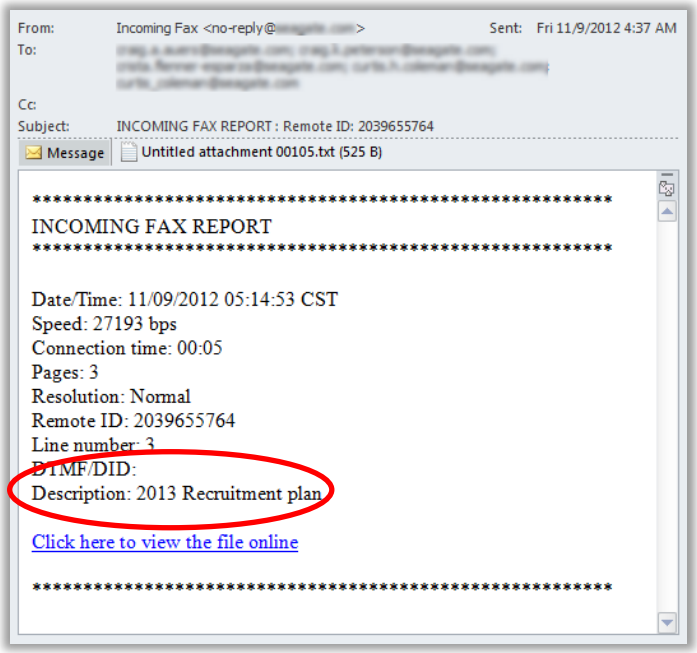


あるいは Sendspace などがあり、ユーザーはビジネス用にもこれらを使ってファイル共有を行っています。これらのサービスは広く使われているため、ここ数年ハッカーがこれらのサービスからの通知を装ったフィッシングメールを配信しています。しかし、この 11 月に Proofpoint はこれらのフィッシングメールの配信方法に興味深い変化を見つけました。

上に表示した通知メールは、ユーザーにファイルをダウンロードする必要があると言っていますが、クリックできる URL はメッセージ中に含まれておらず、ただ HTML アタッチメントが添付されているだけです。(下に表示) 前項の W-2 通知と同様、この HTML を開いた場合にのみ悪意のある URL にアクセスします。HTML アタッチメント中の URL をクリックすると、マルウェアをインストールしようとするサイトに導かれます。

電子 Fax 受信通知および 2013 採用計画

電子 Fax サービスもまた、IT 部門の承認無しに広く使われているコンシューマ向けサービスです。これらのサービスからの通知を装った偽の受信通知を使う手口は古くからあり、珍しいものではありません。11 月、ハッカー達は偽の受信通知にさらに詳細な内容やサブジェクトを組合せる手法を始めました。一例を挙げておきますが、年末のこの時期を狙って 2013 年の予算計画を装い、Description に「2013 Recruitment plan (2013 年採用計画)」などと表示することによって受信者の興味を引くという手口です。


From: Incoming Fax <no-reply@ > Sent: Fri 11/9/2012 4:37 AM
To:
Cc:
Subject: INCOMING FAX REPORT : Remote ID: 2039655764
Message Untitled attachment 00105.txt (525 B)

****
INCOMING FAX REPORT
****

Date/Time: 11/09/2012 05:14:53 CST
Speed: 27193 bps
Connection time: 00:05
Pages: 3
Resolution: Normal
Remote ID: 2039655764
Line number: 3
DTMF/DID:
Description: 2013 Recruitment plan

Click here to view the file online

****

2011 年 4 月の RSA Secure ID 漏洩事件で使われたフィッシングメールのサブジェクトが「2011 Recruitment Plan」、アタッチメントが「2011 Recruitment Plan.xls」だったことを思い出して下さい。

こういったメールは未知のスパムソースから送られるため、ほとんどがブロックされます。ハックされたメールアドレスから送られるものも少数ありますが、マルウェアをホストするサイトや他サイトからファイルをダウンロードさせるサイトなどへのURLを含んでいるため、これらもブロックされます。

Threat News (ニュース)

Windows 8 および Windows Surface のセキュリティ問題

CSO/CIO にとって、IT のコンシューマライゼーションや BYOD に関わる新たな問題が追加されました。Windows8 を搭載した Windows Surface タブレットは、IT 部門の管理下に無いままに企業ネットワーク内で利用される可能性のあるデバイスをまたひとつ増やしたのです。

Microsoft は November Security Bulletin の一部として 4 つの「クリティカル」なパッチをリリースしました。そのうちの 2 つは、その前の月にリリースされたばかりの Windows Surface タブレットの脆弱性に対応するためのものと報道されています。今はホリデイシーズン真っ盛りですから、Windows タブレット(やその他のデバイス)を購入する人が増え、IT 部門に管理されず、脆弱性を持つかも知れないデバイスが企業内に持ち込まれる可能性が増しています。

その他のデバイスも例外ではありません。CNET の記事によると、Android デバイスの実に 50%以上がパッチをあてられることなく利用されており、脆弱性を抱えたままであるということです。

Adobe Reader のゼロデイエクスプロイト (攻撃コード)

最初に Krebs on Security、後に Network World が、Adobe は Adobe Reader 10 および 11 のゼロデイエクスプロイト (攻撃コード) について調査中であると報じました。このエクスプロイトは現在$50,000 で売りに出されています(深刻なエクスプロイトであるほど高い値段が付きます)。それはこのエクスプロイトが、Adobe が Adobe Reader 11 と共に 2010 年に発表した「Sandbox」機能を回避できるためです。

「Snadbox」技術は Adobe Reader を隔離された環境で動作させる技術で、Microsoft および Google の専門家の助けを借りて開発されました。これに似た機能は他のアプリケーションでも採用されており、システム情報の書き換え、ファイルのインストールや削除などの一般的にエクスプロイトが行いそうな危険な操作を阻止します。11 月 30 日時点で Adobe の Product Security Incident Response ブログはこの脆弱性について否定も肯定もしていません。

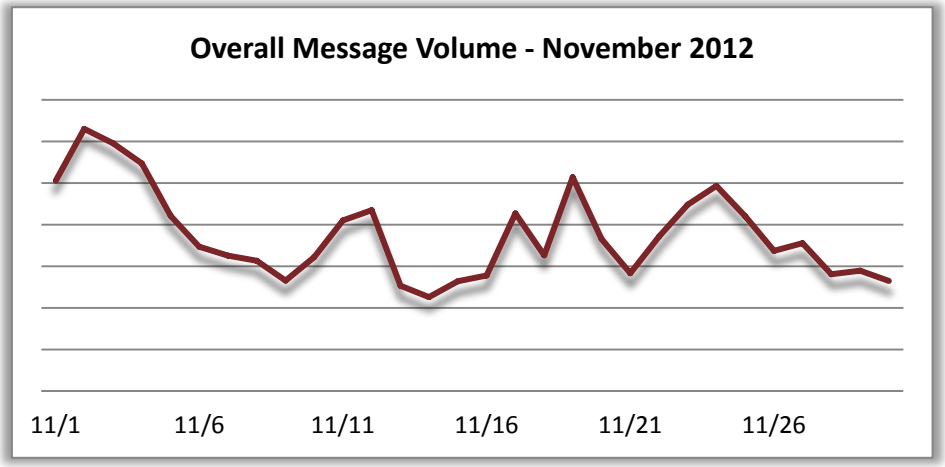
Java の新しいゼロデイエクスプロイト - 8 月以降 3 回目

3 ヶ月前、Java の二つの深刻なゼロデイエクスプロイトが発見され、Windwos、Mac OS X、Linux を採用した様々なデバイスが危険にさらされました。11 月最後の週、これらとは別のエクスプロイトが売りに出されたという噂が広がりました。売り主によると、このエクスプロイトは Firefox または InternetExplorer を搭載した Windows7 デバイスで確実に実行できるとのことです。この新たなエクスプロイトについてはまだ確認されたわけでは無く、対象も狭いですが、絶対必要でない限り、Java を無効化しておくのが望ましいでしょう。

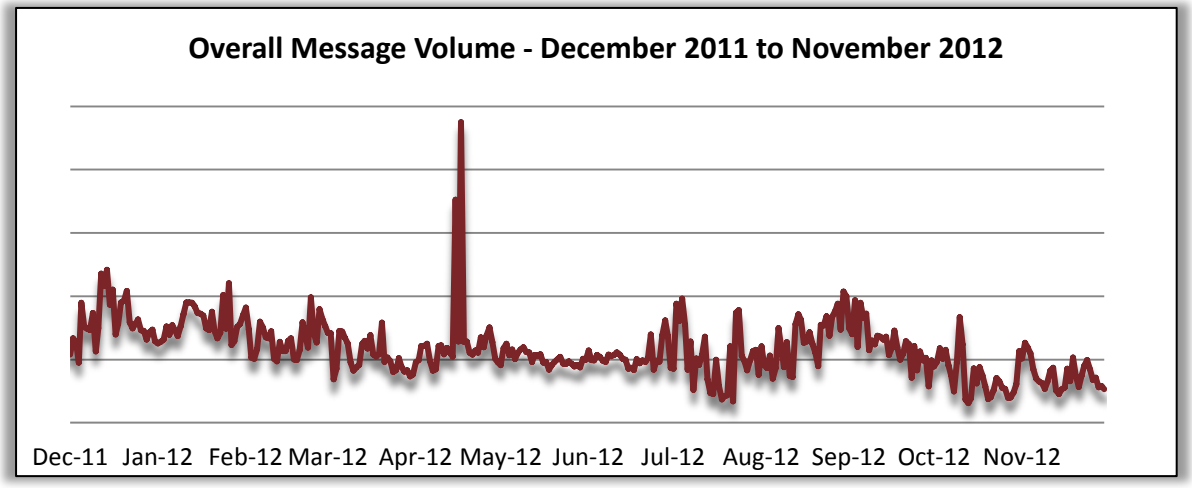
Threat Trends (トレンド)

Spam Volume Trends (スパム量のトレンド)

10 月から 11 月にかけてのスパム量は安定しており、3.27%しか増加していません。11 月のスパム量は今年 2 番目に少ない数値で、過去 24 ヶ月間を見ても 2 番目の低さです。

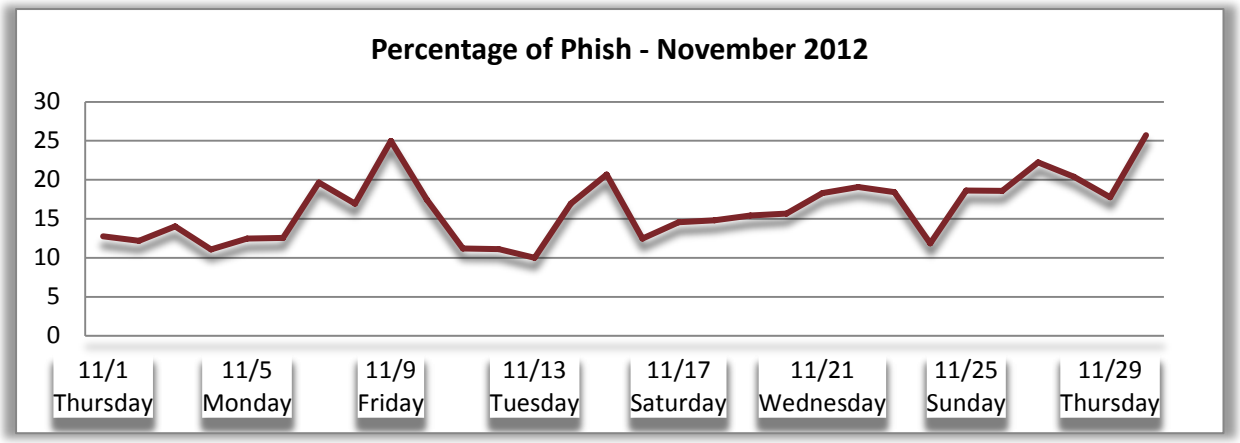


前年比でも減少傾向は続いており、2011 年 11 月と比べて 50%以上減っています。

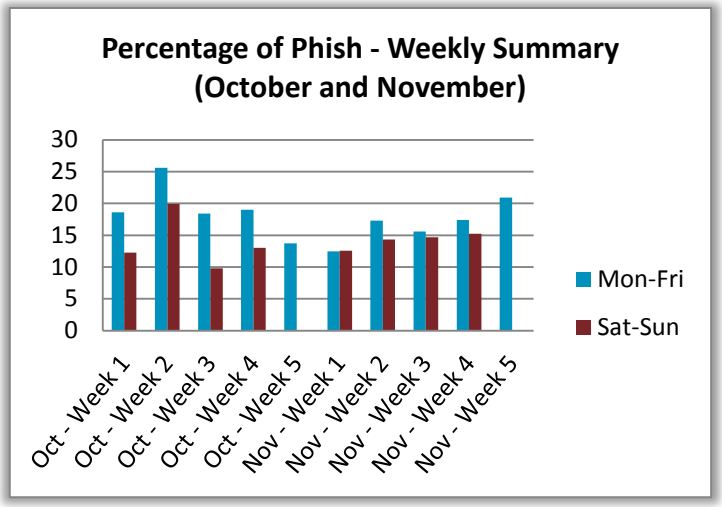


Phish Classification Trends（フィッシング分類のトレンド）

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。

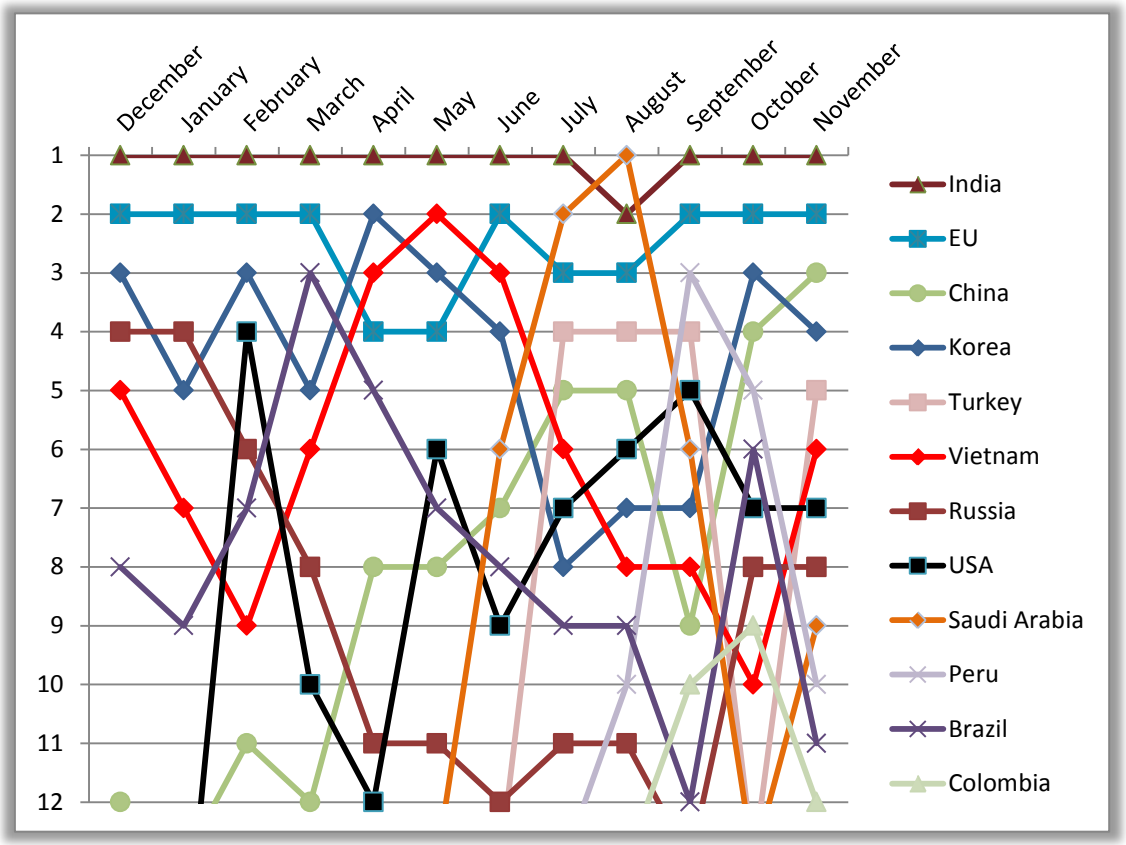


10 月中は不規則な増減を見せていたフィッシング攻撃ですが、11 月の後半 3 週間の攻撃数は一貫して増え続けています。また 9 月にも見られたように、フィッシング攻撃の数はウィークデイに多く、週末は少ないという傾向があります。特に 11 月最後の週はその傾向が顕著でした。



Source of Spam（スパム発信源）

インドはスパム発信量のランキングで 4 ヶ月前に 2 位に後退した後、3 ヶ月連続で首位の座にあります。EU もまた 3 ヶ月連続で 2 位です。中国は 3 位に上がり、代わりに韓国が 4 位に落ちました。ベトナムが 10 位から 6 位となり、アジア諸国はスパム発信国トップ 6 カ国の内 3 カ国を占めます。ペルーは 2 ヶ月間上位 5 位以内に入っていましたが、今月は 10 位に落ちました。南アメリカの国々は、先月はトップ 10 の 30%、トップ 12 の 33%を占めていましたが、今月は 10 以内に無く、ブラジルとコロンビアが 11 位と 12 位に入っています。

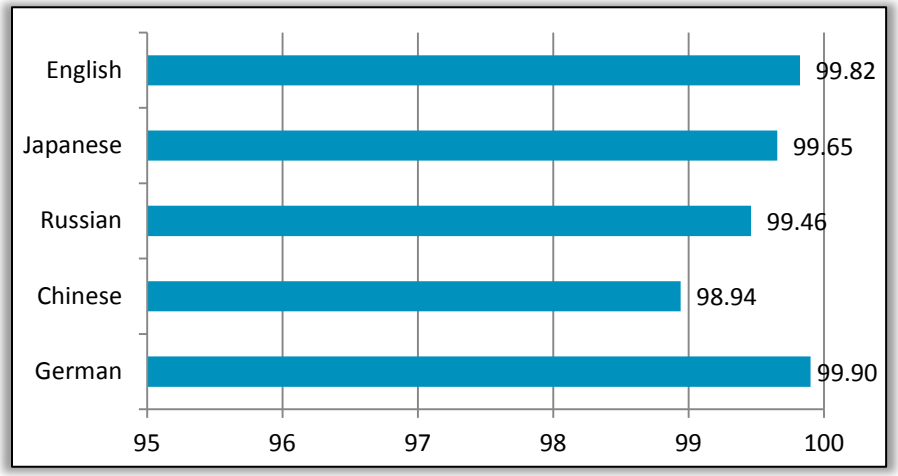


右の表はスパム発信国トップ 10 について、全体に占める割合とトップ 10 の総和に占める割合を示したものです。今月は 1 位のインドが 2 位の EU の 2 倍近いスパムを配信しています。2 位と 3 位を足したよりも 1 位のほうが多くなっています。また、アジア諸国からのスパム量は EU と USA を足したよりも多くなっています。

順位	国	全体 %	トップ 10 %
1	India	16.02%	27.31%
2	EU	8.55%	14.57%
3	Korea	6.10%	10.39%
4	China	5.43%	9.25%
5	Peru	4.90%	8.35%
6	Brazil	3.84%	6.55%
7	USA	3.18%	5.42%
8	Russia	2.69%	4.58%
9	Colombia	2.37%	4.04%
10	Vietnam	2.22%	3.79%

Language Effectiveness（言語別防御効果）

次のグラフは、11 月の 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。スパム量で上位 5 位までの国を示しています。



proofpoint

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