proofpoint

Proofpoint Threat Report

December 2012

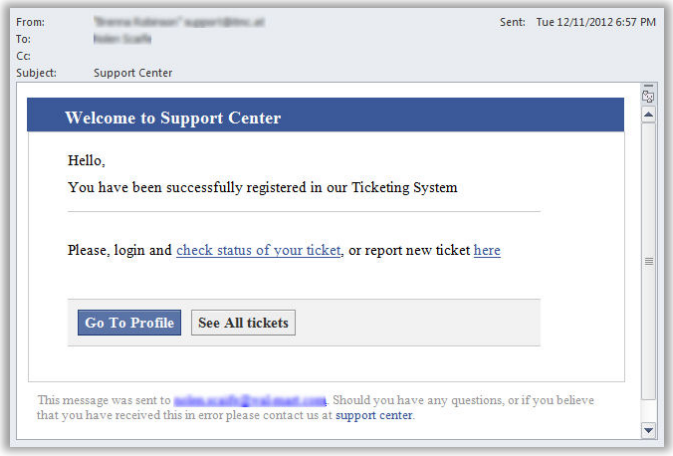
本レポートは、Proofpoint が注目し、お客様および一般企業に対して注意を喚起したいと考えている脅威に関する情報、詳細、トレンドなどをまとめたものです。

Threat Models（手法）

12 月の間、私たちは一つのフィッシング攻撃とその亜種に注目していました。この攻撃は私たちのお客様の多くに対して 3-5 日間にわたって行われたものです。この攻撃およびその亜種は新たに登録された URL を使っており、それらの URL は配信の時点では悪意を持っていない URL でした。Proofpoint Targeted Attack Protection を採用しているお客様は、たとえこの攻撃の亜種がフィルタリングを通り抜けて、これらの URL がクリックされたとしても安全です。

最初の攻撃 "Welcome To Support Center"

12 月 11 日、Proofpoint は新たなソースからのフィッシングメールを確認しました。このフィッシングメールには餌としてのコンテンツがほとんど含まれていませんでした。最初の解析で、これらのメールは 300 個ものユニークな IP アドレスから発信されており、それらの IP はそれまでスパムやフィッシングに関与していない – 別の言い方をすれば、いかなるブラックリストにも載っていない – IP だったことがわかりました。


From:
To:
Cc:
Subject: Support Center
Sent: Tue 12/11/2012 6:57 PM

Welcome to Support Center

Hello,

You have been successfully registered in our Ticketing System

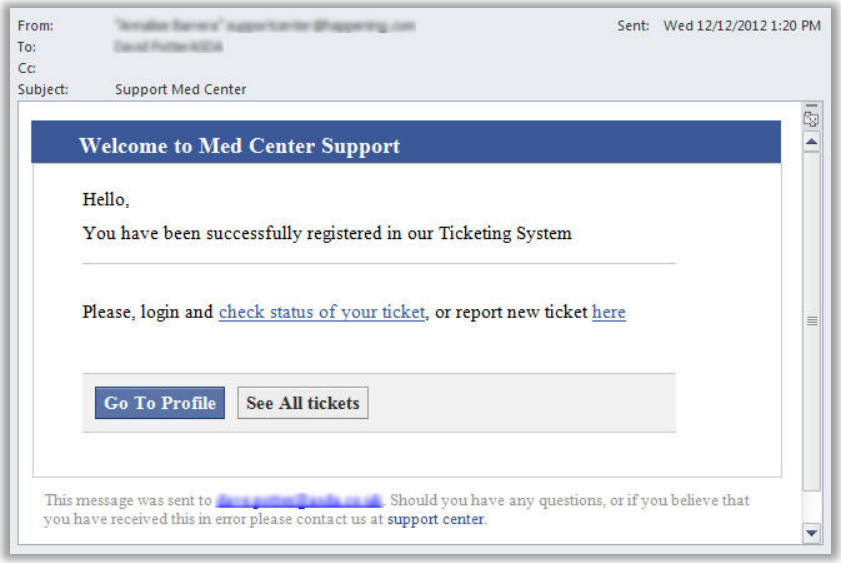
Please, login and check status of your ticket, or report new ticket here

Go To Profile | See All tickets

This message was sent to [redacted]. Should you have any questions, or if you believe that you have received this in error please contact us at support center.

その後の解析により、これらの初期の攻撃には乗っ取られた Web サイトへのリンクが含まれており、被害者のマシンに　はマルウェアがインストールされていたことがわかりました。

第 2 の攻撃 "Welcome to Med Center Support"



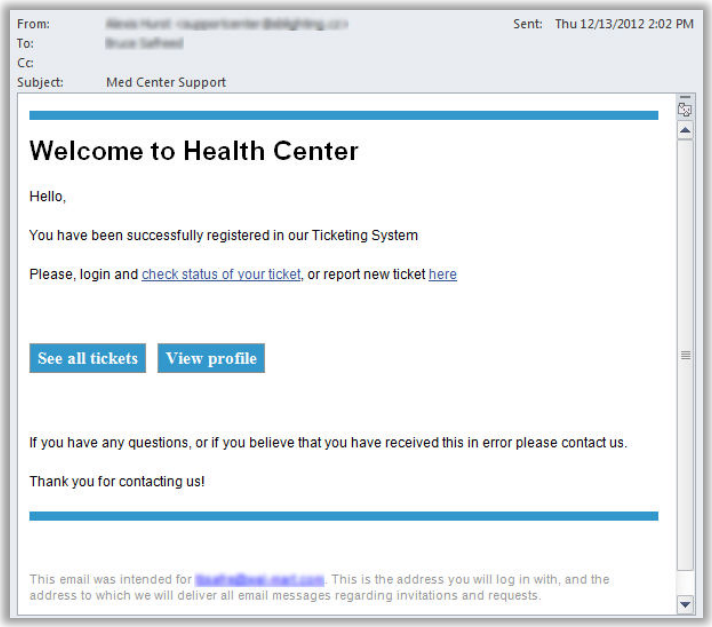
12 月 12 日に Proofpoint では上記”Support Center”攻撃の亜種による攻撃を確認しました。

リンク解析により、このフィッシングメールは被害者を新たに登録された Web サイトに誘導し、マルウェアをインストールしようとするものであることがわかりました。今回の攻撃では、Web サイトとドメインの多くは 12 月 10 日に登録された新しいものでした。

第 3 の攻撃 "Welcome to Health Center"

3 番目の（しかし最後ではない）亜種は、12 月 13 日にそれまで悪意のあるサイトとして認知されていなかった 72 個の IP アドレスから配信されました。

リンク解析により、このフィッシングメールもまた、被害者を新たに登録された Web サイトに誘導し、マルウェアをインストールしようとするものであることがわかりました。第 2 回の攻撃同様、Web サイトとドメインの多くは 12 月 11 日に登録された新しいものでした。



まとめ

この攻撃の間、Proofpoint のテクニカルアカウントマネージャは社内の脅威対策チームおよびお客様と協力して最新の保護と復旧を行えるよう活動しました。これら以外の亜種については現在ブロックされています。

Threat News（ニュース）

Internet Explorer のゼロデイ脆弱性

12 月 29 日、Microsoft の Web サイトでセキュリティアドバイザリ 2794220（日本語版はこちら）が公開されました。これには初期の Internet Explorer のゼロデイ脆弱性をマニュアルで回避するやり方が説明されています。この脆弱性は Internet Explorer の 6, 7 および 8 のみに影響を及ぼすもので、攻撃者がリモートシステム上でプログラムを実行させることができます。Internet Explorer の 9 と 10 には影響しませんが、あるレポートではこれら初期の Internet Explorer はデスクトップブラウザーのマーケットシェアの 1/4 から 1/3 を占めていると指摘されています。数日後、Microsoft はこの脆弱性をアニュアルで回避するためのやり方をナレッジベースの記事としても公開しました。

最初オンラインニュースサイトで、後に F-secure により報じられたように、この脆弱性は既に中国のハッカーによって悪用されています。そのうちの一つは公務員、メディア関係者や外交政策を扱う記者などがアクセスするサイトに悪意のあるソフトウェアを埋め込もうとしていました。未確認のレポートですが、この脆弱性はかつて 2009 年中頃に Google やその他の企業を狙った Aurora 攻撃に似ているとの指摘もあります。

SCaaS (Stolen Credentials as a Service)

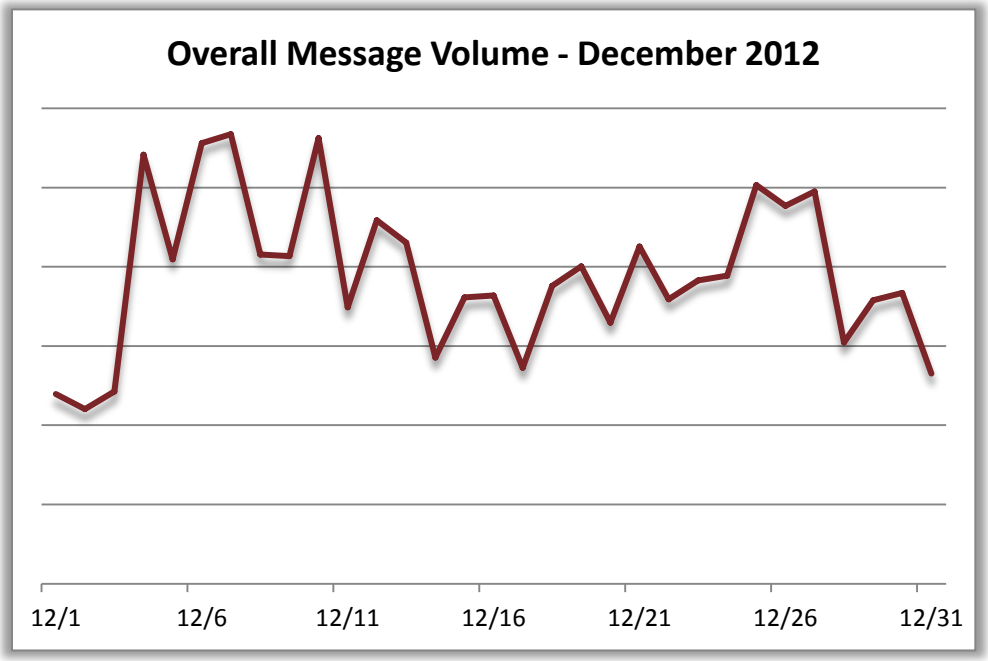
ハッカー及びスパマーは、スパム攻撃やその他の標的型攻撃を仕掛けるために、常に電子メールのログイン情報を狙っています。最近になって、配送や支払いに関連するビジネスサービスの Web サイトから流出した電子メールアドレスとパスワードの組合せがブラックマーケットで売り出されました。この記事によると、これらの盗み出されたパスワードの多くがハックされた PC からのものだそうです。その他、フィッシングメールによって偽の Web サイトでパスワードを入力させてだまし取られたものもあります。

FedEx、UPS あるいは Paypal のアカウント情報を狙うフィッシングメールは多く、よく知られていますが、その他のサイトも狙われていることが分かってきました。例えば、有名なオンラインショッピングサイトのクレジットカード情報などはブラックマーケットにとってより価値を持ちます。クレジットカード情報が隠されていたとしても、ハッカーはその情報を元にその個人や業務を狙った標的型攻撃を仕掛けるでしょう。最悪の場合にはアカウント情報が偽の注文や出荷指示に利用され、費用がアカウント保持者に請求されると言ったことがあるかもしれません。

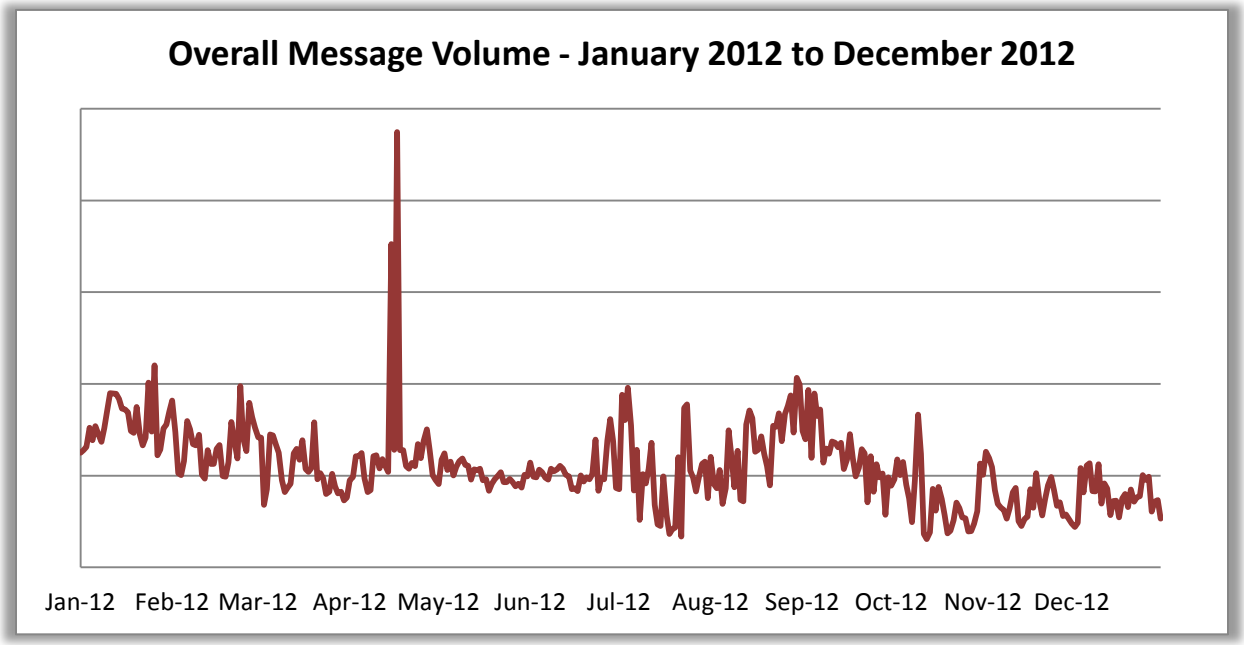
Threat Trends (トレンド)

Spam Volume Trends (スパム量のトレンド)

11 月から 12 月にかけてスパム量はわずかながら (4.85%) 増加しました。しかし 12 月のスパム量は 1 年を通じて 3 番目の少なさで、過去 24 ヶ月を見ても 3 番目の低さです。

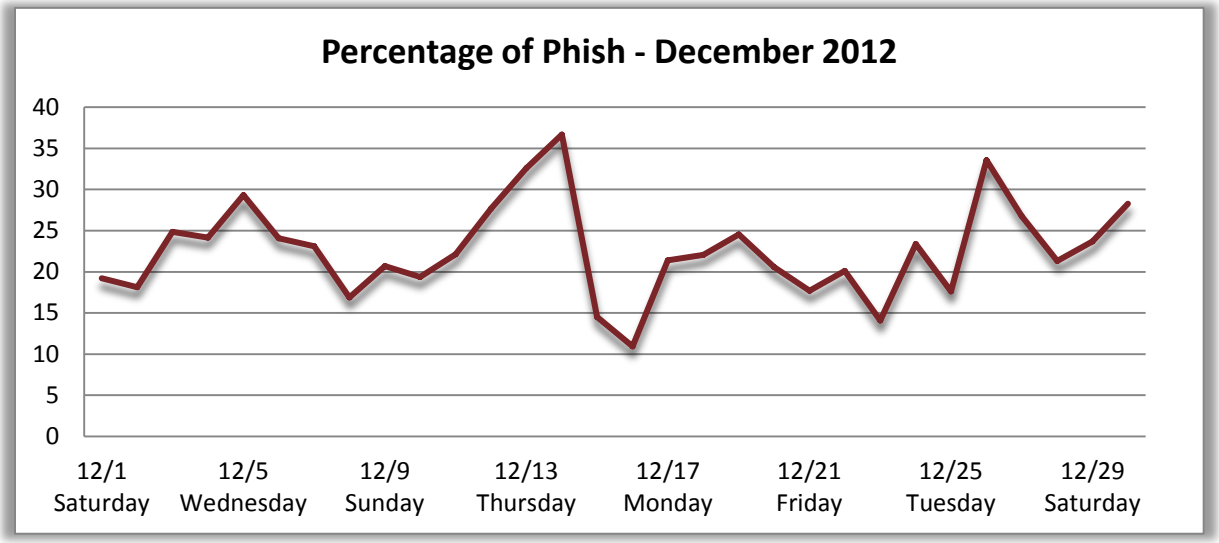


今年は毎月のスパム量が前年同月を下回りました。2012 年 12 月のスパム量は 2011 年 12 月のスパム量の約半分 (51%) です。

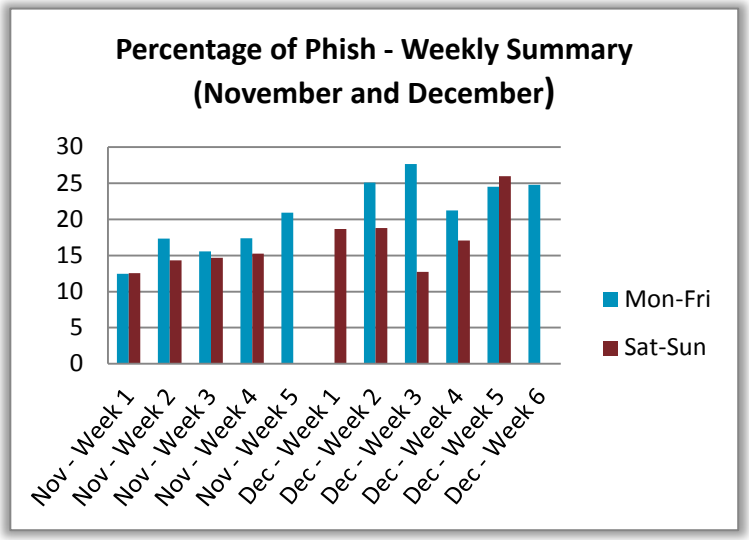


Phish Classification Trends（フィッシング分類のトレンド）

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。

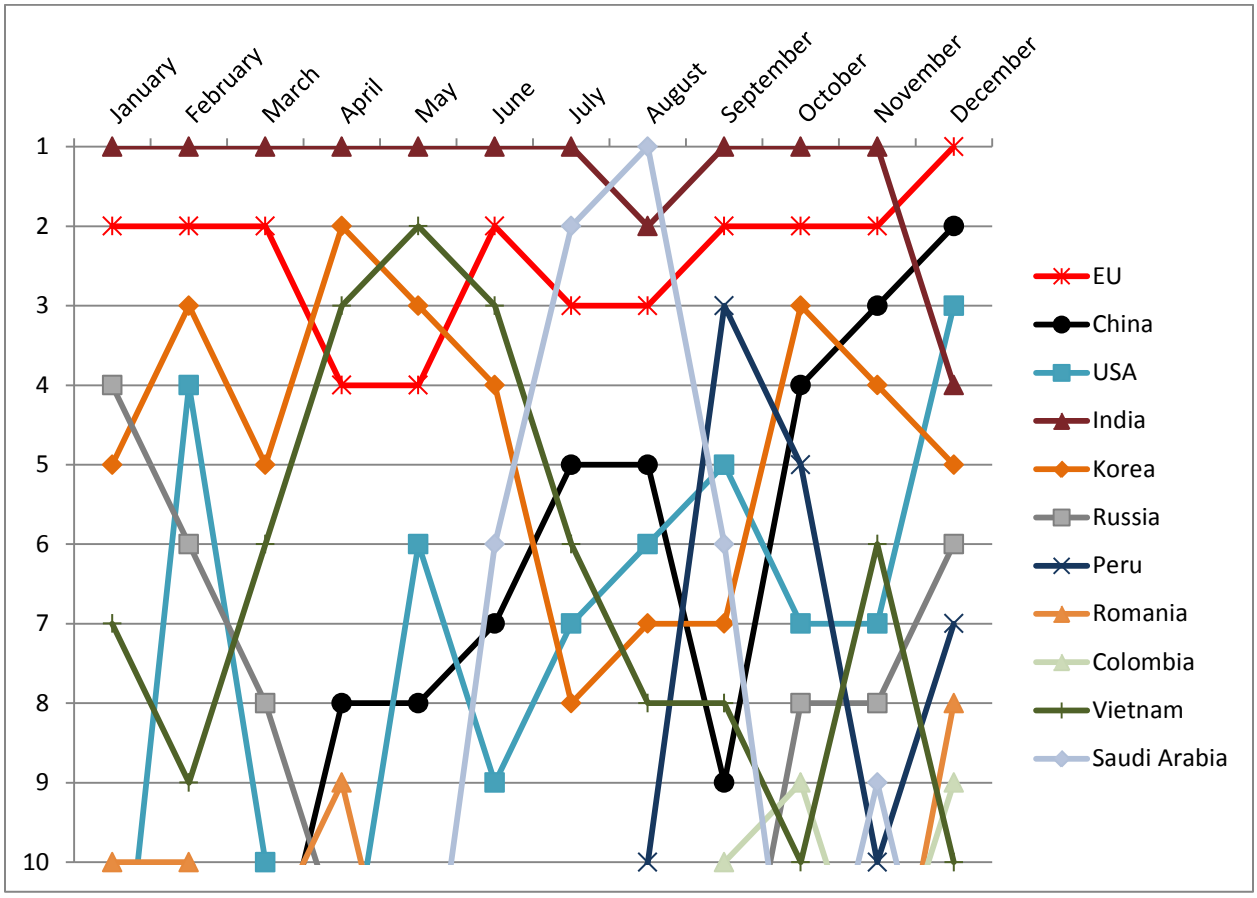


11 月中はフィッシング攻撃は一貫して増加していましたが、この傾向は 12 月の前半も続き、その後ばらつきました。フィッシング攻撃は週末よりもウィークデイのほうが多く、この傾向は月の前半で顕著でした。



Source of Spam（スパム発信源）

今年は第 2 位にいることの多かった EU が 12 月は首位でした。9 月に 9 位だった中国はじわじわと上昇し、12 月は第 2 位です。アジア諸国は上位 6 カ国のうち 4 カ国を占め、上位 10 カ国のうち 5 カ国を占めています。

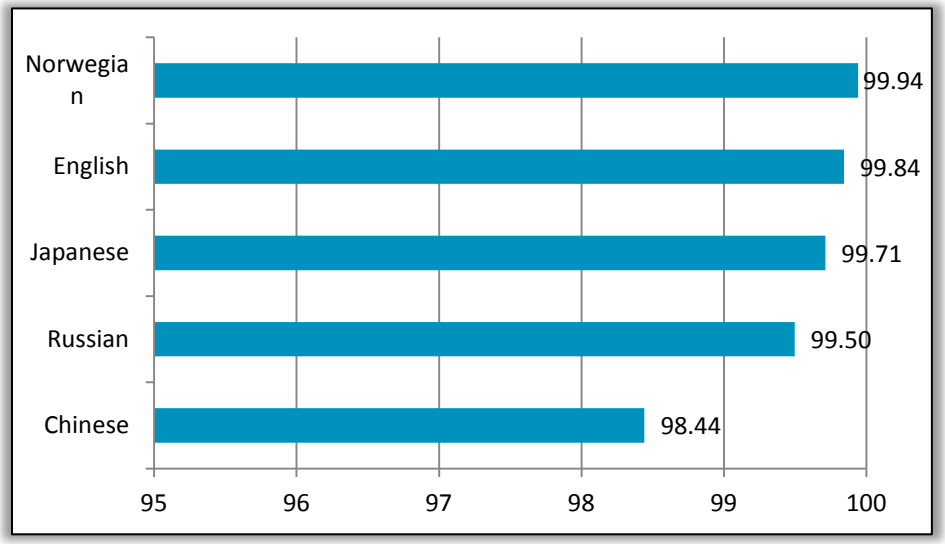


右の表はスパム発信国トップ 10 について、全体に占める割合とトップ 10 の総和に占める割合を示したものです。インドが 2 位までに入らないのは 12 ヶ月以上ぶりのことです。

Rank	Country	% Overall	% Of Top 10
1	EU	8.99%	27.31%
2	China	6.19%	14.57%
3	USA	5.75%	10.39%
4	India	5.04%	9.25%
5	Korea	3.69%	8.35%
6	Russia	3.11%	6.55%
7	Peru	3.07%	5.42%
8	Romania	2.22%	4.58%
9	Colombia	2.22%	4.04%
10	Vietnam	2.12%	3.79%

Language Effectiveness（言語別防御効果）

次のグラフは、12 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