proofpoint

Proofpoint Threat Report

April 2013

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)

大規模「はえ縄型」攻撃

4 月 15 日の週、ボストンマラソンの爆弾事件とテキサス肥料工場の爆発事件を餌として使った非常に大規模なフィッシング攻撃が観測されました。攻撃の中でも最大のものは Kelihos ボットネットを使ったもので、Proofpoint がこれまで観測したものの中でも最大の規模でした。詳細は以下の通りです。

# メッセージ数	2 億 8,700 万通
# 送信者 IP	249,257
# 悪意のあるドメイン	46
エクスプロイトキット	Redkit
マルウェアペイロード	Kelihos bot

使われたドメインはそれほど多くはありませんが、メッセージ数と送信者 IP アドレスの数が非常に多いことにご注目下さい。典型的なマルウェア攻撃のおよそ 10 倍の規模です。次頁の図 1 では今回の攻撃と、同時に見られた典型的な規模の攻撃(紫色)との比較を見ることができます。

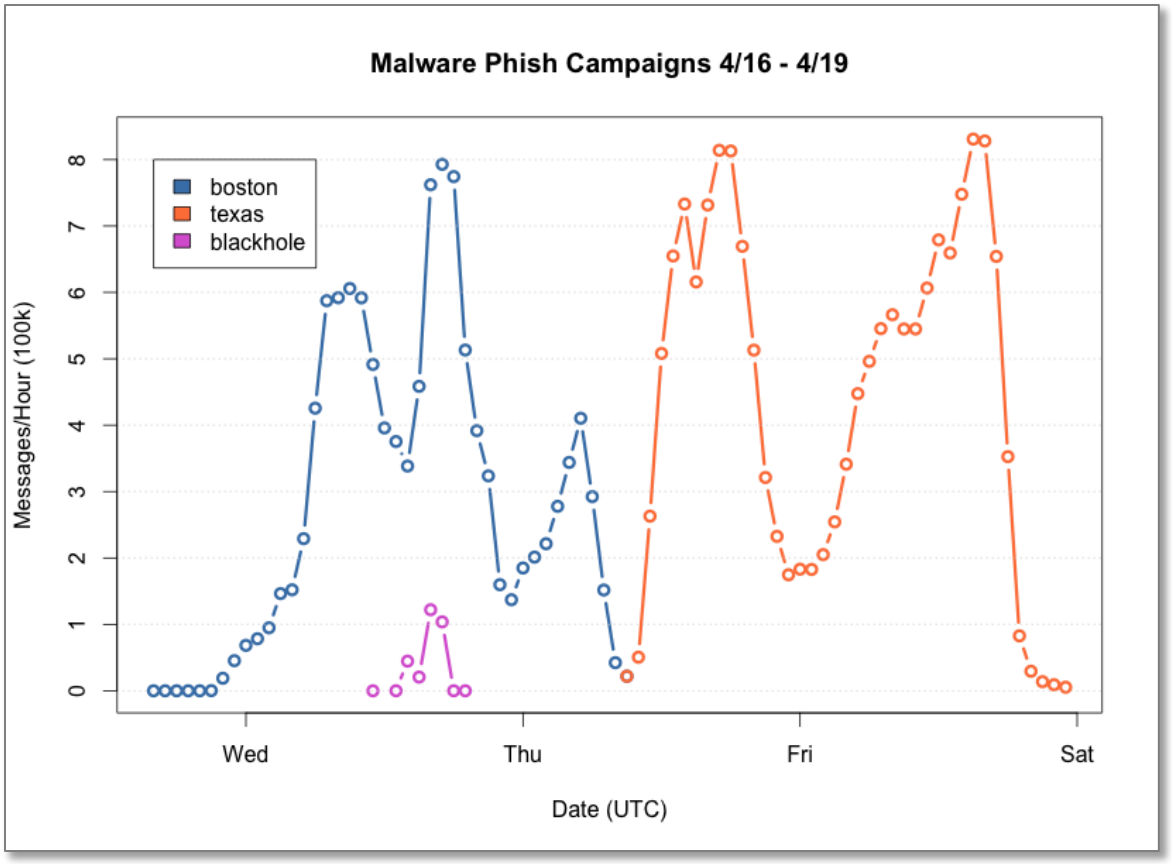


図 1: Kelihos（青・オレンジ）と Blackhole フィッシング攻撃（紫）の規模の比較。Blackhole 攻撃は典型的な攻撃の規模。

攻撃は 17 日水曜日の早朝にボストンマラソンの爆弾事件を餌として始まりました。この攻撃によるメッセージ数は最大で 80 万通/時に達し、使われた URL は「boston.html」と「news.html」でした。メールのテンプレート（図 2）は URL 以外に何のコンテンツも無いシンプルなものです。

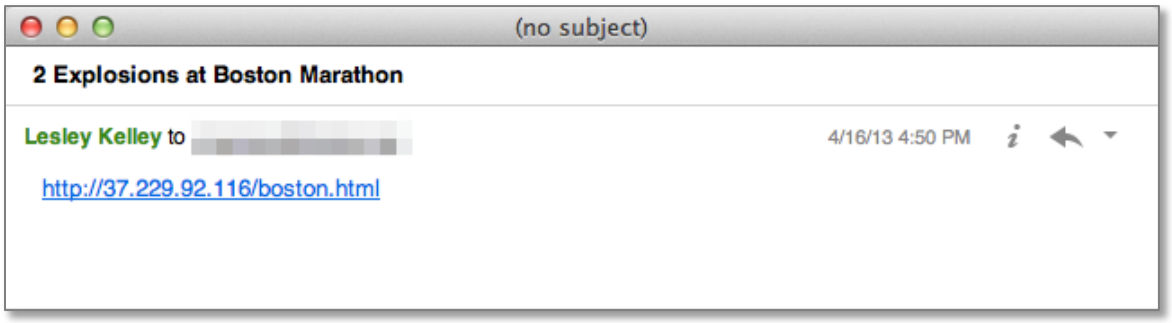


図 2: Boston フィッシングメール

これらの URL は最初、4 本のビデオを含むボストン爆弾事件の Web サイトを、後には肥料工場爆発のサイトを指し示していました。サイトには iflame が隠されており、エクスプロイトキットの Redkit をロードします。ブラウザに Java がインストールされている場合にはそれを検知して様々な Java のエクスプロイトを送り込みます。この Java エクスプロイトは、攻撃の初期には 46 種類中 3 つ（7%）のアンチウイルスエンジンでしか検知できませんでした。攻撃の終盤にはこの数は 46 種類中 14（30%）に上がりました

が、従来型のシグネチャベースのアンチウイルスが最新型の攻撃に対抗する場合の限界を示す形となりました。

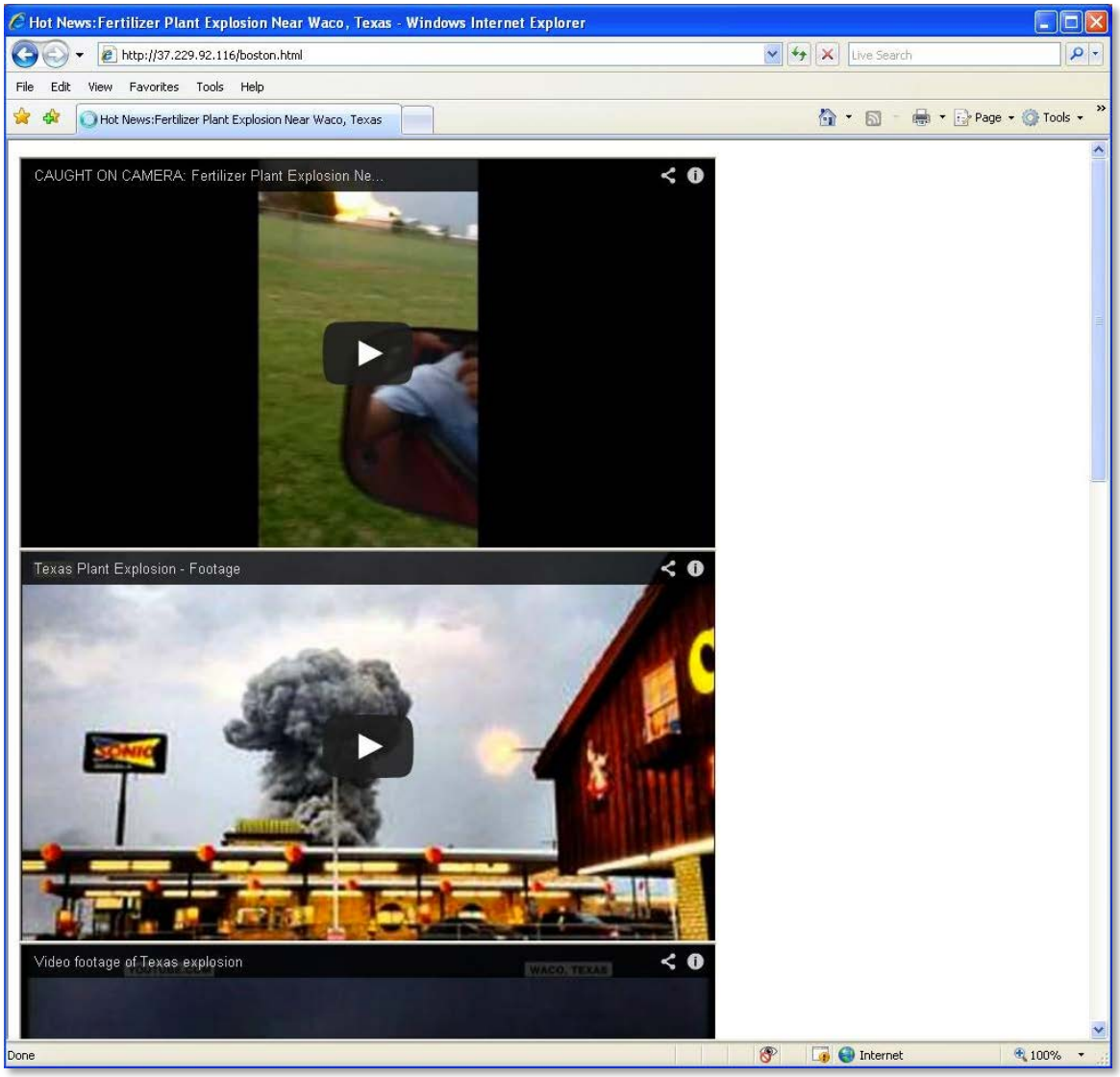


図 3.: ビデオのスクリーンショット

Boston/Kilihos 攻撃の間、ボストンマラソン爆弾事件を餌にした別の攻撃が開始され、これは Blackhole エクスプロイトキットに誘導されていました。この攻撃の規模は典型的な標的型のもので、4,725 の送信元 IP アドレスから 292,012 通のメッセージが配信されました。図 1 に見られるように、Blackhole 攻撃は Boston/Kelihos に比べて小規模なものです。

木曜日の昼までに Boston/Kelihos 攻撃は 1 時間ほど停止し、テキサス肥料工場爆発を餌に使った攻撃に変わって戻ってきました。この第 2 の攻撃で使われた URL は「texas.html」と「news.html」でした。この Texas 攻撃は最大で 83 万通/時を記録し、金曜日一杯続きました。Web サイト、エクスプロイトキットおよびペイロードは Texas と Boston で同じものが使われています。メッセージは Boston 同様シンプルで、アンチスパムソリューションを回避するようになっています。

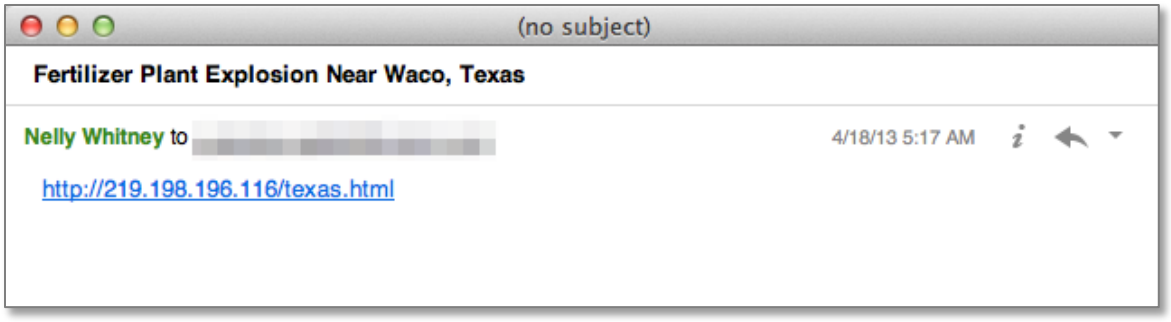


図 4: Texas フィッシングメール

25 万におよぶボストン爆弾およびテキサス爆発攻撃の送信元 IP を地図上に表示すると、以下の様になります。ベラルーシとカザフスタンが注目されます。

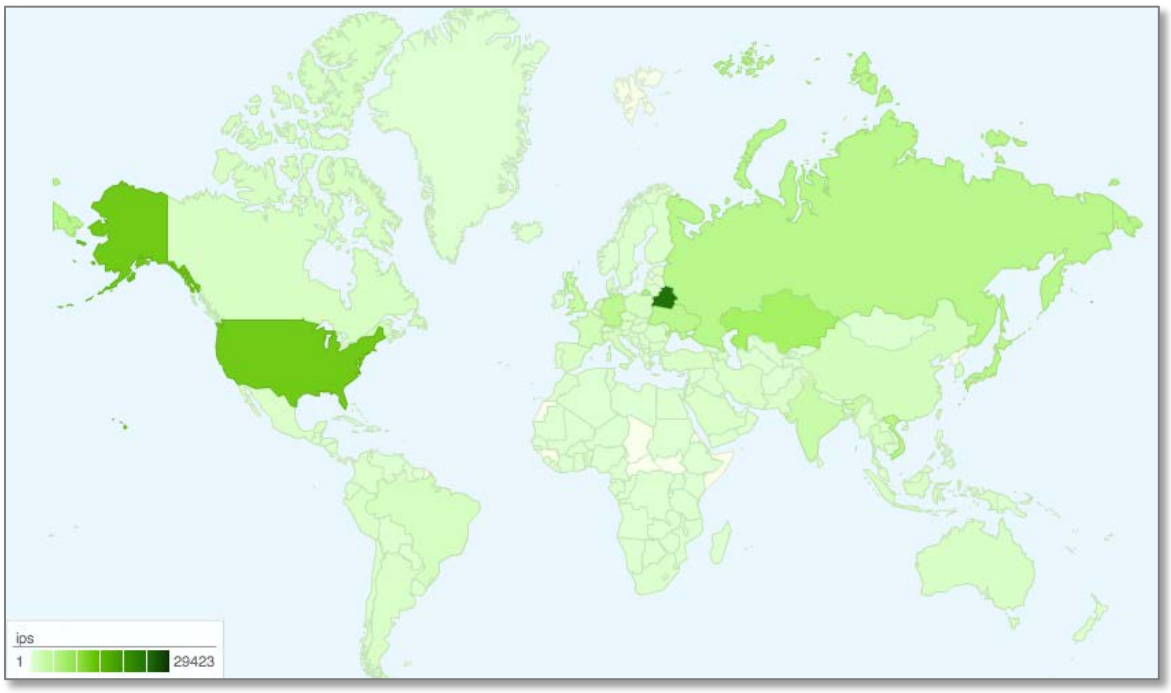
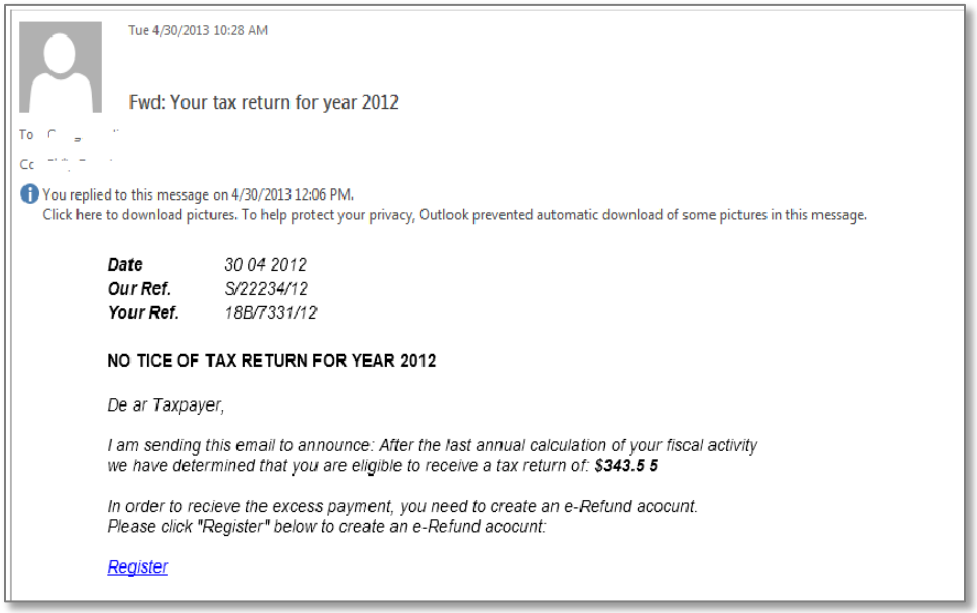


図 5: Boston および Texas 攻撃の送信元 IP の分布

毎年恒例の US Tax フィッシングの例

4 月 15 日の米税務申告の前後には、毎年毎年時計仕掛けのようにフィッシング攻撃が行われます。以下に典型的な例を 2 つご紹介します。



Tue 4/30/2013 10:28 AM

Fwd: Your tax return for year 2012

To

Cc

You replied to this message on 4/30/2013 12:06 PM.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Date *30 04 2012*
Our Ref. *S/22234/12*
Your Ref. *18B/7331/12*

NO TICE OF TAX RETURN FOR YEAR 2012

De ar Taxpayer,

I am sending this email to announce: After the last annual calculation of your fiscal activity we have determined that you are eligible to receive a tax return of: ***$343.5 5***

In order to recieve the excess payment, you need to create an e-Refund acocunt. Please click "Register" below to create an e-Refund acocunt:

Register

図 6: Tax フィッシング例 1

Tue 4/30/2013 11:12 AM

IRS <no-reply@

NOTICE OF TAX RETURN FOR YEAR 2012

To

You forwarded this message on 4/30/2013 1:19 PM.

Internal Revenue Service
DEPARTMENT OF THE TREASURY

Date *30 04 2013*
Our Ref. *S/22234/13*
Your Ref. *18B/7331/13*

NOTICE OF TAX RETURN FOR YEAR 2012

Dear Taxpayer,

I am sending this email to announce: After the last annual calculation of your fiscal activity we have determined that you are eligible to receive a tax return of: ***$343.5 5***

In order to recieve the excess payment, you need to create an e-Refund acocunt. Please click "Register" below to create an e-Refund acocunt:

Register

図 7: Tax フィッシング例 2

これらのメッセージには二つの異なる「From」アドレスが使われています。例 2 では信憑性の高い「IRS」（米内国歳入庁）が使われています。この例では IRS のロゴも使われています。「Register」は二つの異なるサイトにリンクされています。37 ベンダー中 5 ベンダー（13.5%）だけがこれらのサイトを悪意のあるものとして特定しました。2 つめのメッセージで使われているリンクについては 37 ベンダー中 6 ベンダーでした。どちらも検知率は低く、エンドユーザーのメールボックスまで届けられてしまう可能性があります。

Threat News（ニュース）

Twitter アカウントの侵害と元になったスピアフィッシングメッセージ

200 万のフォロワーを持つ AP 通信のニュース速報用の Twitter アカウントがスピアフィッシング攻撃により乗っ取られ、ホワイトハウスが攻撃を受けているという偽のツイートを流しました。その結果、ダウ平均が 143 ポイントも下落したのです。Slate 誌によると、Syrian Electronic Army（SEA)が反抗を認めていると言うことです。SEA は以下のメッセージによって複数の AP 通信の社員を狙いました。（詳細部分は削除してあります）

Sent: Tue 4/23/2013 12:12 PM
From: [An AP staffer]
Subject: News

Hello,

Please read the following article, it's very important :

http://www.washingtonpost.com/blogs/worldviews/XX/2013/04/23/

[A different AP staffer]
Associated Press
San Diego
mobile [removed]

図 8: SEA のスピアフィッシングメッセージ

「From」フィールドには AP の社員名が書かれており、詳細は LinkedIn のような SNS サイトで簡単に見つけられるものでした。コンテクストに注目して下さい。ニュースソースは信頼性の高いワシントンポストで、内容は彼らの職業（ジャーナリスト）に直接関連するものです。さらなる詳細と事件の全貌はこちらにあります。

Android デバイスを狙ったトロイの木馬マルウェア

Dell のセキュリティ研究者達が Android を狙ったトロイの木馬「Stels」を発見しました。Dell は「Stels はマルチパーパスの Android 向けトロイの木馬で、被害者の住所録を盗み、SMS を送ったり受信したり、勝手に電話をかけ（有料サービスを含む）たり、別のマルウェアをインストールしたりします。」と報告しています。Stels は悪意のある URL を含んだフィッシングメールによって拡散します。以下に例を挙げます。

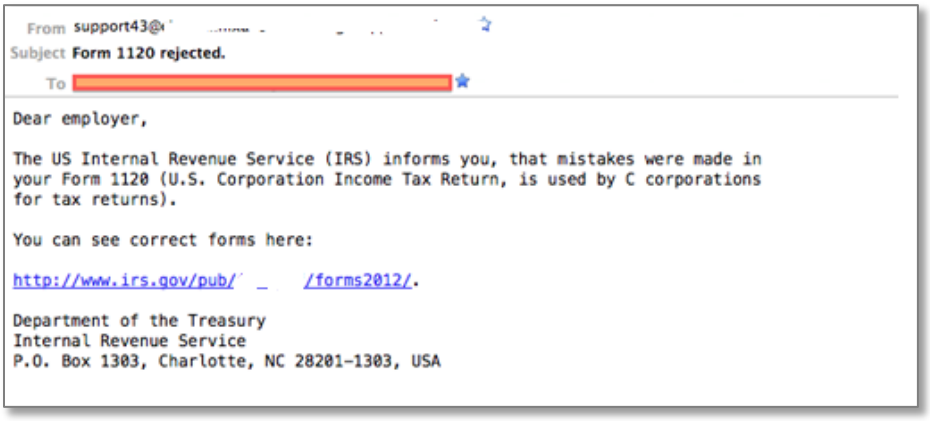


図 9: Android 向けトロイの木馬 Stels のスピアフィッシング

攻撃は非常に洗練されており、この URL にアクセスすると、ユーザーはデバイス（デスクトップかモバイルか）、OS あるいはブラウザに応じて様々なサイトに誘導されます。

Proofpoint の Targeted Attack Protection であれば、先進的な解析によりこの攻撃を検知し、エンドユーザーのデスクトップ環境および Android モバイルデバイスから URL へのアクセスをブロックしてユーザーを保護することができます。

強力でユニークなパスワードへの要求

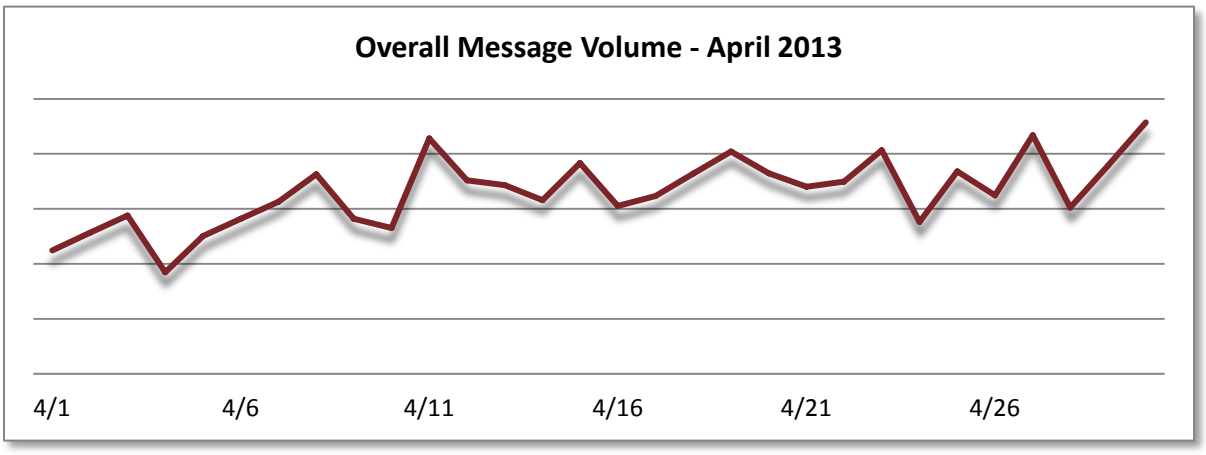
パスワードの強化については、ユーザーがいつも IT 部門から言われていることですが、今では Web サービスでも同じ事を言われるようになりました。Evernote、LinkedIn および LivingSocial（詳細はこちら）の侵害によってこの傾向が生まれました。

アカウントとプライバシーを守るためには、強力でユニークなパスワードが欠かせません。大文字と小文字を組合せたパスワードフレーズが効果的です。サービス毎に異なるパスワードを設定することも重要です。パスワードの使い回しは、たとえそれが強力なものであっても、複数のアカウントを危険にさらすことになります。攻撃者は、一つのアカウントの侵害に成功した場合、他のサービスでも同じユーザー名とパスワードの組合せが使えないか試してみるからです。ユーザーに対してパスワード強化の呼びかけを行う事は大変重要です。

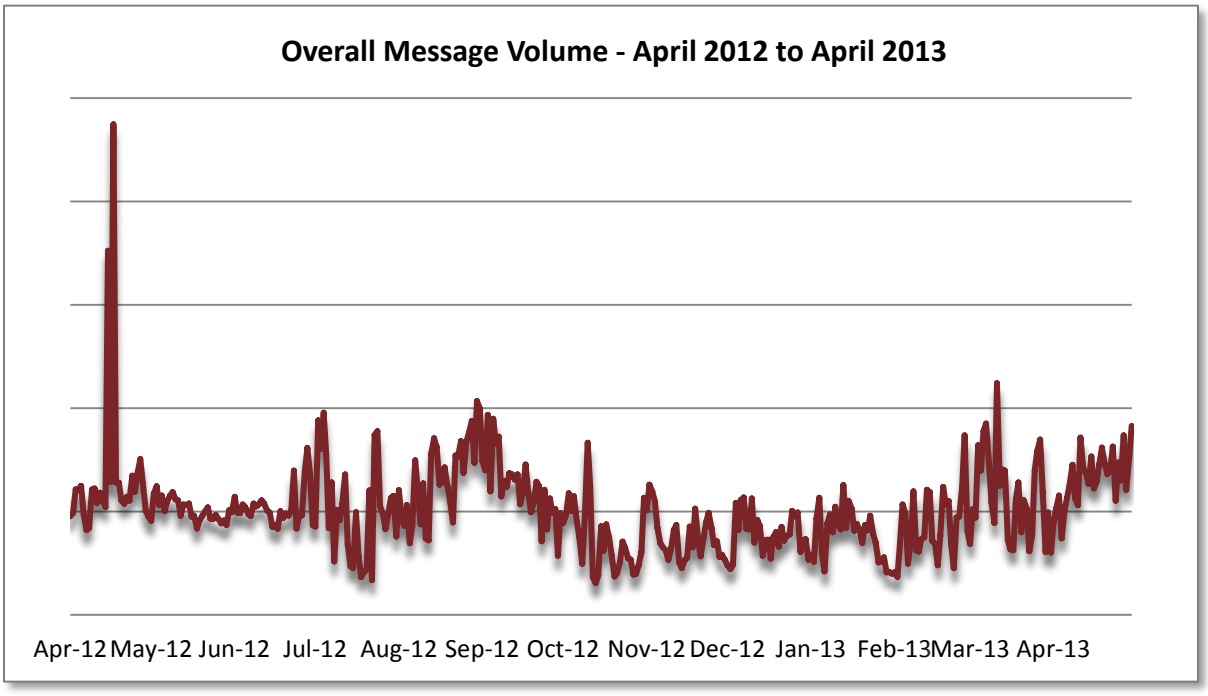
Threat Trends (トレンド)

Spam Volume Trends (スパム量のトレンド)

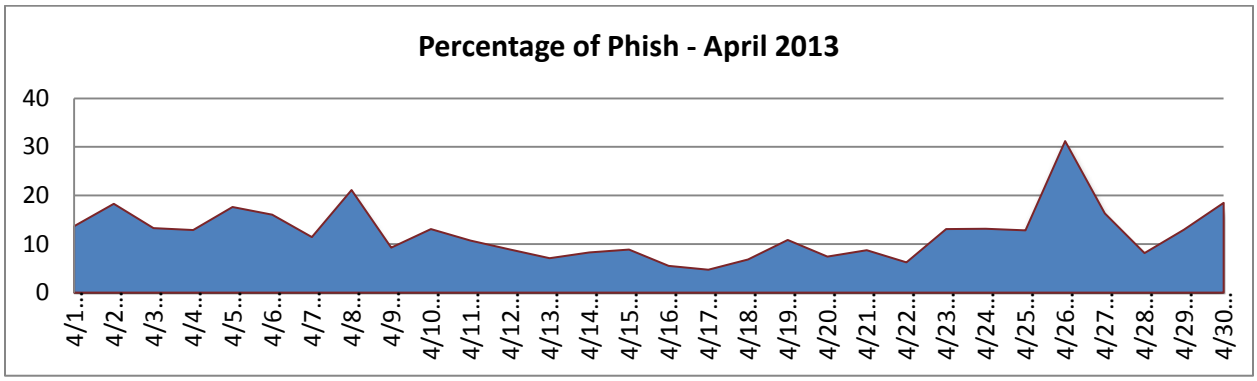
スパム量は悪意のある、またはその他のタイプのメッセージとは別に集計されますが、以下に見られるように一ヶ月間一貫して増えています。この傾向は月の中旬にピークがあって月末へ向けてスパム量が減っていた 2013 年の初めの頃と異なるパターンです。



全体的なスパム量は 4 月に再度増加し、2012 年の 8-9 月のレベルにあります。また 3 月から 4 月にかけてスパム量は 14.66%増加しました。3 月は前月比で 35.48%増加しており、増加率は落ちましたが、2013 年に入ってから増加傾向が続いています。一方で、2012 年 4 月と比べると全体のスパム量は 1.34%下落しています。



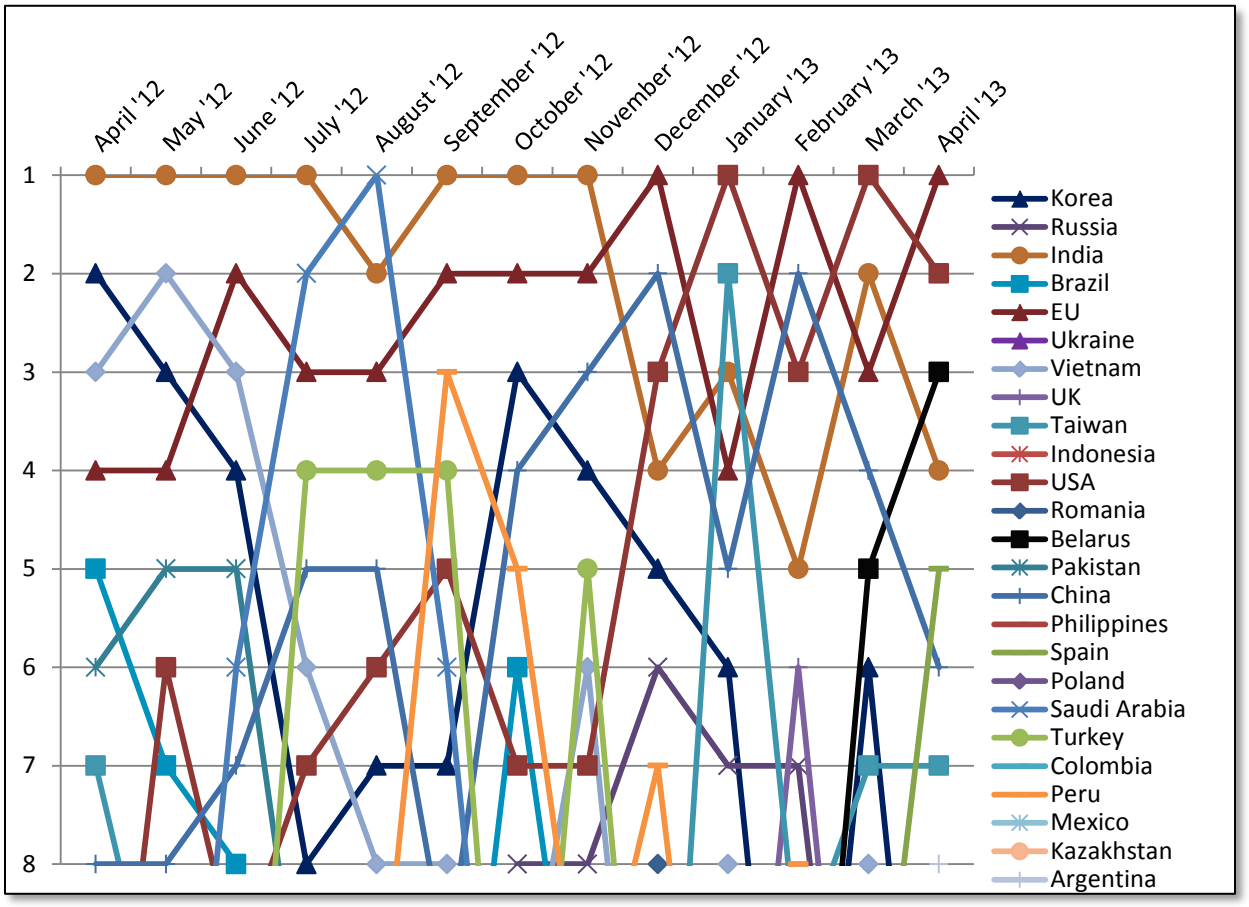
Phish Classification Trends（フィッシング分類のトレンド）



Proofpoint MLX および Targeted Attack Protection によってフィッシングに分類されたメッセージの割合は一貫して増えています。4 月には 2 つのピークがあります。最初のピークは全メッセージの 20%を占めました。2 番目のピークは 30%で、最高値を更新しました。

Spam Sources by Country（スパム発信源）

2013 年 4 月は EU がスパム発信元の第 1 位となりました。ベラルーシは増え続けて 3 月の第 5 位から第 3 位に上がり、アルゼンチンが 2 ヶ月連続で 8 位に入っています。



前頁のグラフは過去一年間のスパム発信量の上位の国を月ごとに示したものです。
下の表は 3 月と 4 月のスパム発信量（総数に対しての割合）の上位 8 カ国です。

March 2013			April 2013		
1	USA	9.70%	1	EU	8.60%
2	India	8.72%	2	USA	7.60%
3	EU	7.25%	3	Belarus	6.10%
4	China	5.16%	4	India	5.00%
5	Belarus	4.28%	5	Spain	4.00%
6	Korea	3.271%	6	China	3.70%
7	Taiwan	3.12%	7	Taiwan	3.60%
8	Vietnam	2.97%	8	Argentina	3.10%

proofpoint

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