proofpoint

Proofpoint Threat Report

January and February 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。

Industry Trends (全体のトレンド)

2013 年は大規模なマルチチャンネル攻撃で幕を開け、フォーチュン 500 企業のいくつかが被害を受けたといわれています。攻撃には乗っ取られた LA Times のサイトやマルウェアに侵害された NBC.com サイトなどへのリンクが含まれており、これらのサイトは Adobe Acrobat や Oracle Java のような一般的なデスクトップアプリケーションのゼロデイ脆弱性を標的にしています。「ハッキング」という言葉がメディアに取り上げられるため、被害を自演する企業まで現れました。

従来の非標的型の大規模攻撃から小規模なスピアフィッシング攻撃への移行は進んでおり、この点を重視した Proofpoint は最近、複数のフォーチュン 1,000 企業において数週間にわたる調査を行い、10 億通以上の電子メールを分析しました。この調査結果をホワイトペーパーとしてまとめた「はえ縄型フィッシング攻撃～大規模標的型攻撃の誕生～」の中で Proofpoint の研究者は、大規模で静的な攻撃から、標的毎には小規模ながら全体としては大規模で高度に動的な(送信 IP や URL、マルウェアのホスティングサイトを変化させる)攻撃への移行を解説しています。

標的となった組織の内外での攻撃者と受信ユーザーの行動について Proofpoint の製品である Targeted Attack Protection の追跡記録を使って解析した結果、以下の事が判明しました。

- 境界保護型のセキュリティソリューションをくぐり抜けたメールに埋め込まれた悪意のある URL を、受信者の 1/10 以上(11%)がクリックしてしまい、攻撃者を組織内に呼び込んでしまいました。
- これらの URL の多くは見た目には判別できませんでした。(Web ページにしか見えなかったり、ページの読み込み中に見えたりしました)

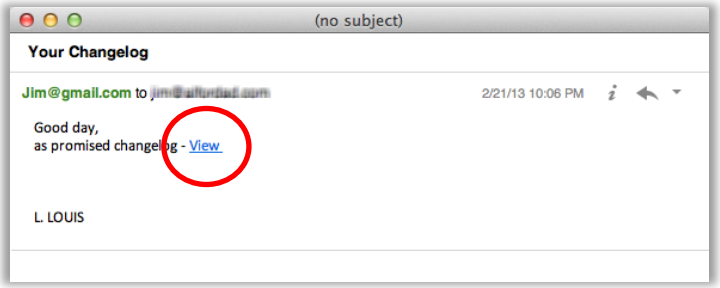
- スパムとして判定されたメールのうち 1/4 以上（27%）が悪意のある URL を含んでいました。
- 悪意のある URL をクリックしたうちの 1/5 近く（19%）が「ネットワーク外」（企業の境界保護の外）からのものでした。これは従業員が自宅から、あるいは外出先からモバイルデバイス経由でアクセスした場合を指します。
- 悪意のある URL のうち 1/7（14%）は標的となった企業のうち一社にのみ送られていました。平均して、ほとんどの URL は 5 つ以上の組織には送られておらず、既存のシグネチャベースの手法による検知や遮断を非常に難しくしています。

このホワイトペーパーをダウンロードし、この新しい脅威の詳細と防御方法をご確認下さい。

Threat Models（手法）

はえ縄型攻撃の仕組み

この攻撃の実例を見てみると、このタイプの攻撃がいかに動的で防御しにくいかがわかります。Proofpoint では、お客様の一部について 2 月 21 日からのメールトラフィックを解析し、700 ものお客様に送られた合計 100 万通におよぶ活発な攻撃を確認しました。



これら悪意のあるメッセージは 148 の別々のドメイン、33,000 もの異なる送信者から交互に送られており、一般的な防御システムをすり抜けるため、30,000 におよぶユニークな IP アドレスを使っていました。これらの特徴はすべて、特定ドメインや IP のブラックリスト化などの従来型のアンチスパム手法の限界を示しています。

Proofpoint の様々なレピュテーションおよびスコアリングシステムを使えば、96%以上のメッセージは遮断でき、残りのほとんどのメッセージが含む URL は Proofpoint にリダイレクトされ、遮断することができます。

攻撃者の狙いは、PDF や Java の様々な脆弱性を狙ったトロイの木馬のようなマルウェアをダウンロードさせるための URL を送り込むことです。ユーザーが脆弱性を残した Adobe Reader や Java をインストールしていた場合、このトロイの木馬に感染してしまうのです。

そしてこの攻撃は、極めて少数のアンチウイルスベンダーでしか検知できなかったのです。

- PDF は 41%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。
- Java のエクスプロイトは 9%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。
- トロイの木馬は 20%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。

攻撃の規模の大きさから、攻撃者あるいはそのグループは巨大なインフラを構築していると考えられます。

- Proofpoint のお客様が数多く攻撃されていることから、包括的なリストを保持している
- 送信者の数から見て 3 万台以上の規模のボットネットを構築している
- フィッシュメールの URL として 120 以上の侵害されたサイトを用意している
- ペイロードを配信し、セキュリティ解析を回避するゲートキーパーとして機能する洗練されたサーバーを保有している

この攻撃者はこのインフラを、自分のマルウェアを拡散したいと考えている人々に貸し出していると考えられます。このため、毎日のように新たなマルウェアを使った攻撃が行われていると考えられます。手口は毎日同じですが、細かい部分が微妙に異なっており（違うサーバーや違うパスネームなど）、従来型のアンチスパムエンジンで検知しにくくなっています。この点こそが、Proofpoint が Targeted Attack Protection を開発した理由であり、この新しく広範囲におよぶ脅威を発見し、その情報をスコアリングおよびレピュテーションエンジンに送って残りのお客様を保護します。

Docusign マルウェア（様々な手法）

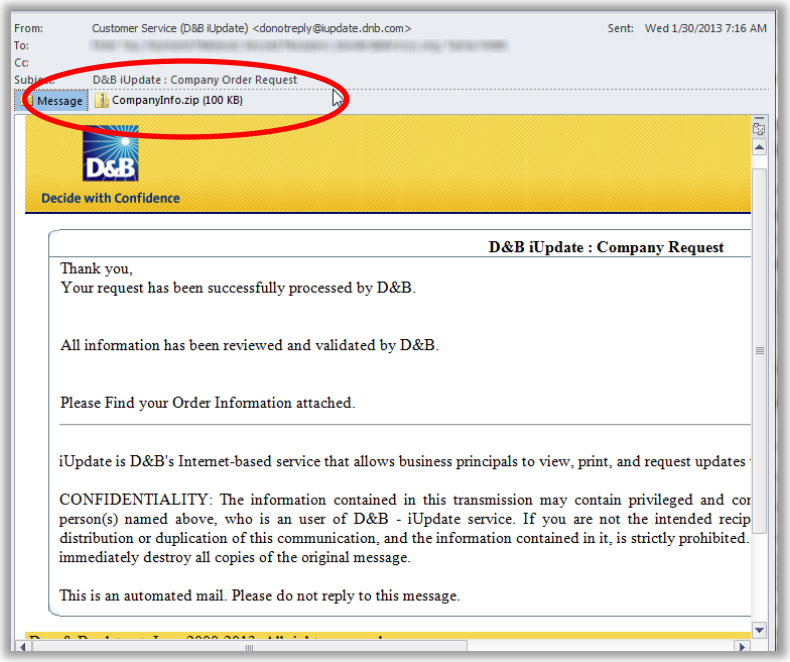
プロシューマ向けのサービスである Docusign が大規模ななりすまし攻撃に遭い、攻撃者がサイトユーザーに偽の通知を送りました。Proofpoint はこの攻撃についていくつかの亜種を確認しており、それには HTML のボタンを含むものや ZIP ファイル中にペイロードを含んでいるものがあります。

この通知では、攻撃者は Web ベースのマルウェアを使って PC に感染します。ZIP ファイルを使った攻撃は標的型に近く、ユーザーがトロイの木馬に感染したファイルを開くと隠されたアプリケーションが起動し、

- メールクライアントや Web ブラウザに保存されたログイン情報を盗み出し、
- RDP（Remote Desktop Protocol）を使ってパスワード強度の弱い他のマシンにログインを試み、
- 多くの場合、Zeus や Zbot のような悪名高い追加のマルウェアをダウンロード・インストールし、サーバー名、ポート番号、ログイン ID、FTP クライアント、クラウドストレージプログラムに関する情報を収集します。

Proofpoint では、こういった攻撃が多くのお客様組織内の少数のユーザーに対して行われていることを確認しています。

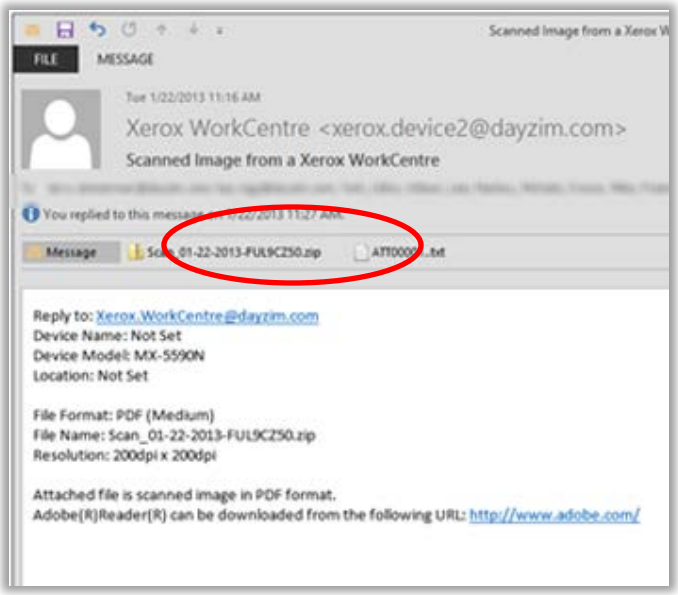
トロイの木馬を含む Zip 添付 – 複数の攻撃



金融サービス企業は標的として狙われる他、攻撃の餌として利用されることもよくあります。攻撃の餌とはマルウェアに感染したサイトに誘導するためのリンクをファイル内に持ってユーザーにクリックさせようとするものです。

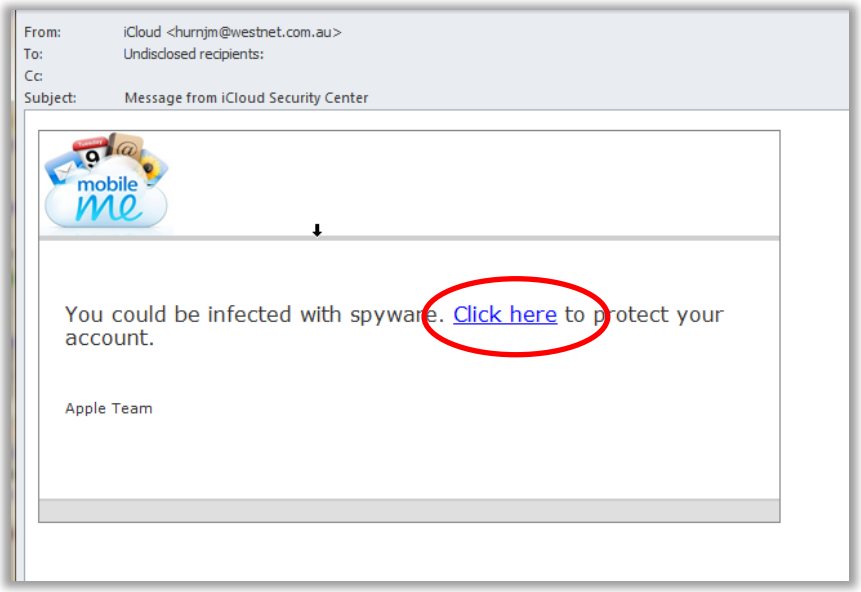
標的型攻撃でよく見られるように、攻撃者は攻撃手法や経路を変化させます。Proofpoint や他社はいくつかのバージョンを確認しており、異なる業種のいくつかの企業が攻撃を受けています。

これに関連する別の攻撃ではもっと踏み込んだ言葉が使われており、Wells Fargo を名乗る攻撃では、送金時の残高不足を警告するものもあります。Xerox を使った別の攻撃はさらに説得力があり、Xerox の WorkCenter アプリケーションのスキャンによりユーザーマシンにトロイの木馬が見つかったと通知するものがあります。（下図参照）



攻撃そのものは ZIP ファイル中に置かれており、ユーザーにこれをクリックさせます。ファイル名は「Receipt」や「CompanyInfo」などの無害に見えるものです。実行プログラム自体は従来型のシグネチャベースのソリューションでは検知できないもので、感染したマシンにトロイの木馬型 rootkit をセットアップします。送信者は一般のブロードバンドユーザーで、知らぬ間にボットネット（感染した大量のマシン）に組込まれたものと見られます。これらの攻撃は特定の企業を狙ったものでは無く、少なくとも 1 種は Proofpoint の複数のお客様から見つかっています。

iCloud セキュリティセンターからのメッセージ



2 月に起きた他の攻撃に隠れてしまいましたが、Apple がまた、ブラックリストに記載された様々な悪意のあるサイトにユーザーを誘導するためのスパムの餌として利用されました。同様の、しかしもっと手の込んだ攻撃は 2011 年にもありました。偽の Web サイトに誘導し、請求明細をチェックさせるものです。

Proofpoint は複数のお客様でこの攻撃を確認しました。主に教育機関ですが、政府・州・市の機関も含まれています。Proofpoint Enterprise Protection はこの攻撃を検知したため、お客様はこの攻撃の被害を受けていません。

Threat News (ニュース)

Java のゼロデイ脆弱性を狙う一連の攻撃がメディアの注意を引き、Java 削除の動きへ

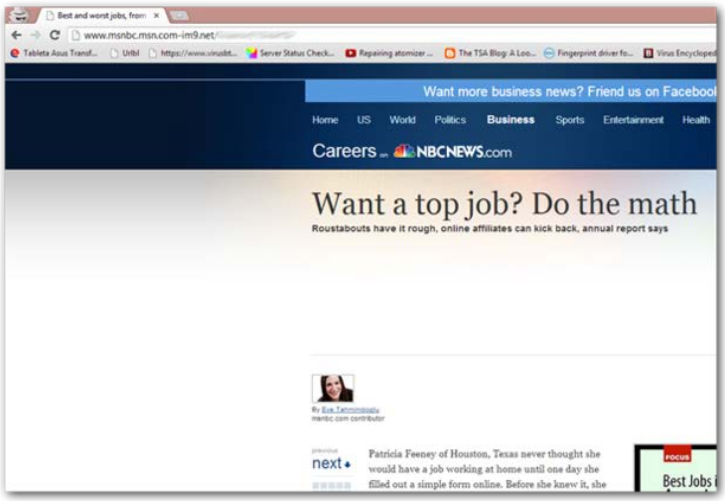
Threat Report の 2012 年 11 月版で取り上げたように、Oracle Java には非常に危険な脆弱性が多数見つかっています。Bloomberg News は、少なくとも 40 社が東欧のグループによると見られるマルウェア攻撃の標的となり、Reuters は中国からの攻撃を示唆する専門家のコメントを掲載しています。

Apple は Java のアップデートを作成しましたが、同時に iOS 上の Java プラグインを無効化しました。複数の OS に影響を及ぼす脆弱性は IT 管理者の注意を喚起し、多くのユーザーシステムから Java を完全に削除しました。

MSNBC サイトのなりすましとフィッシングによる Yhoo Mail の侵害

攻撃者は 1 ヶ月にわたって様々な手法による攻撃を行い、WordPress に見つかった脆弱性を使って Yahoo のクッキーにアクセスし、ユーザーのメールボックスにアクセスすることに成功しました。

最初に Bitdefender が報じたように、攻撃は以下のように行われました。



1) ユーザーに送られるメールには一件正常に見える MSNBC サイトへの短いリンク（www.msnbc.msn.com.xxx.net のような）が含まれていました。Whois 情報を調べると、このドメインはウクライナで登録されており、キプロスの首都ニコシアのデータセンターでホスティングされていることがわかります。

2) このリンクは MSNBC を模倣したサイトを指しており、悪意のある JavaScript コードを含んでいます。これに感染すると Yahoo! Mail にログインするためのブラウザクッキーが読み取られます。

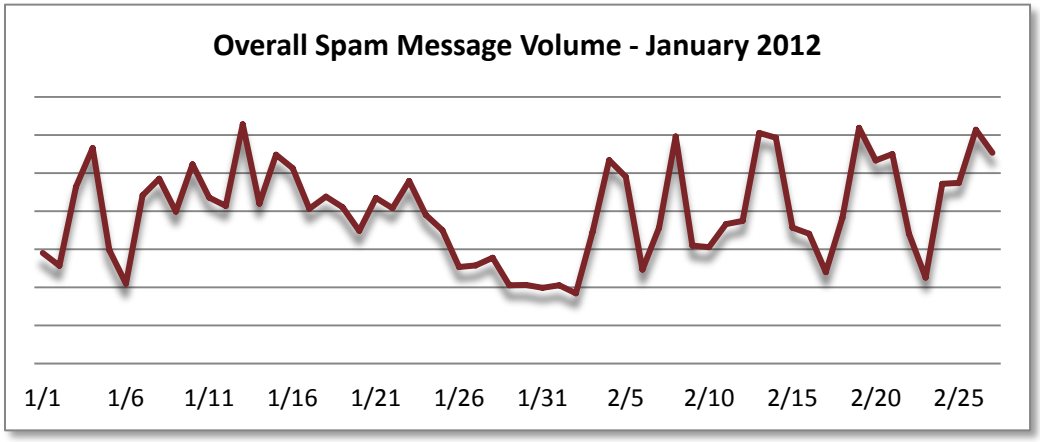
3) 攻撃者は盗んだクッキーを使って被害者の Yahoo!メールボックスにアクセスしました。Bitdefender の記事によると、Yahoo Developer のブログシステムは WordPress を使っており、2012 年 4 月以降パッチが当てられていないため、メールボックスへのアクセスが可能になったと言うことです。この脆弱性によりハッカーは yahoo.com ドメイン全体のセッションクッキーにアクセスすることができ、その情報を彼ら自身に送りました。

影響を受けたユーザー数は分かっていませんが、この攻撃により、攻撃者が一見関連性の無い脆弱性も利用する守備範囲の広さを持っていることを教えてくれます。

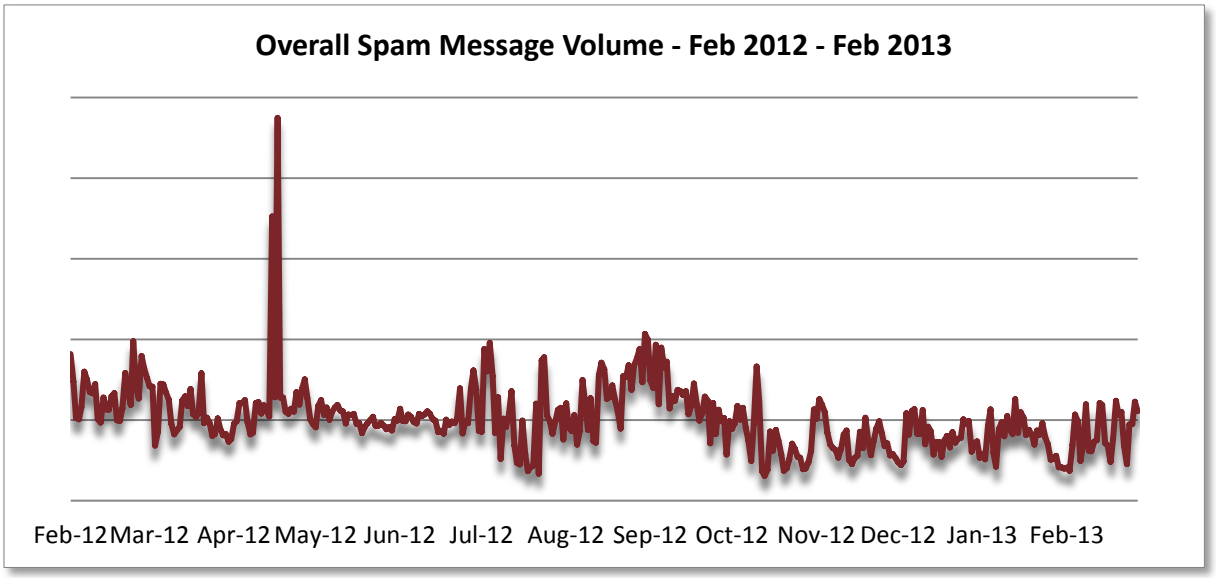
Threat Trends (トレンド) – January 2013

Spam Volume Trends (スパム量のトレンド)

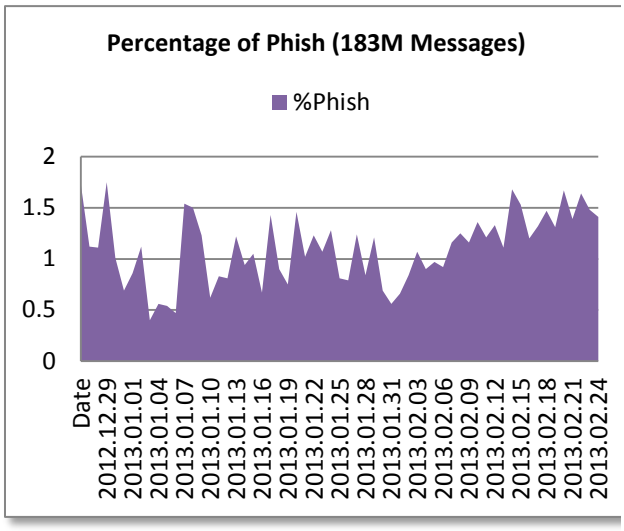
悪意のある攻撃を別にすると、12 月から 1 月にかけてのスパム量は比較的安定しており、2.31%下がっただけでした。1 月から 2 月では 7.64%増えています。この 2 ヶ月間のスパム量は過去 6 ヶ月間の傾向と同じで、前年同期に比べて約 40%減少しています。これは小規模で広範囲へ、というトレンドを反映しています。

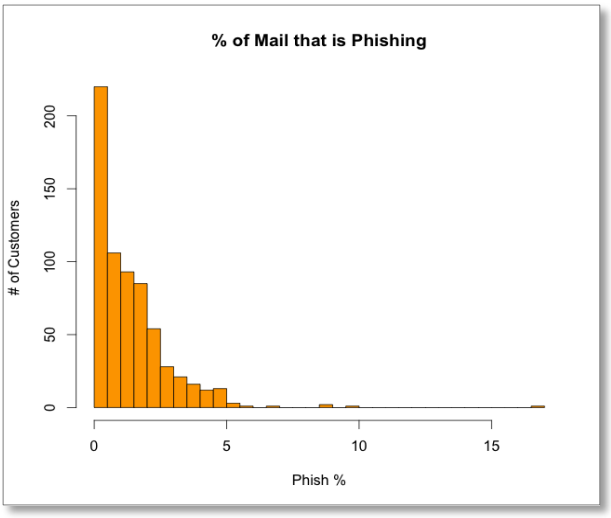


12 月と同様、スパム量は中旬にピークがあり、月末へ向けて減っています。月別のスパム量は 12 月から 2 月にかけて比較的安定しており、過去数ヶ月間のトレンドと同じです。



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

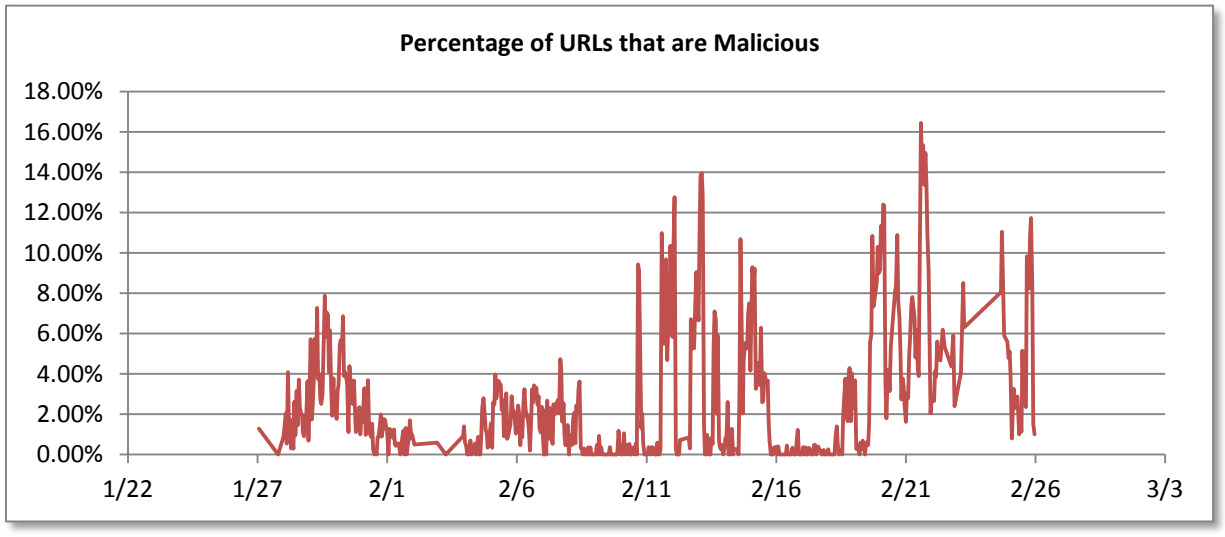




上のグラフは、Proofpoint MLX および Targeted Attack Protection によってスパム及びバルクメールの中からフィッシングに分類されたメッセージのパーセンテージです。全体的に見て、フィッシングに分類されるメールの割合は全体のメールの量に比べると少ないということができます。しかし、その少ないメールは標的型メッセージである傾向が強く、従来型のアンチスパム手法では検知が難しく、混乱は長く続きます。

URL vectors found in Phish emails (フィッシングメール中の URL)

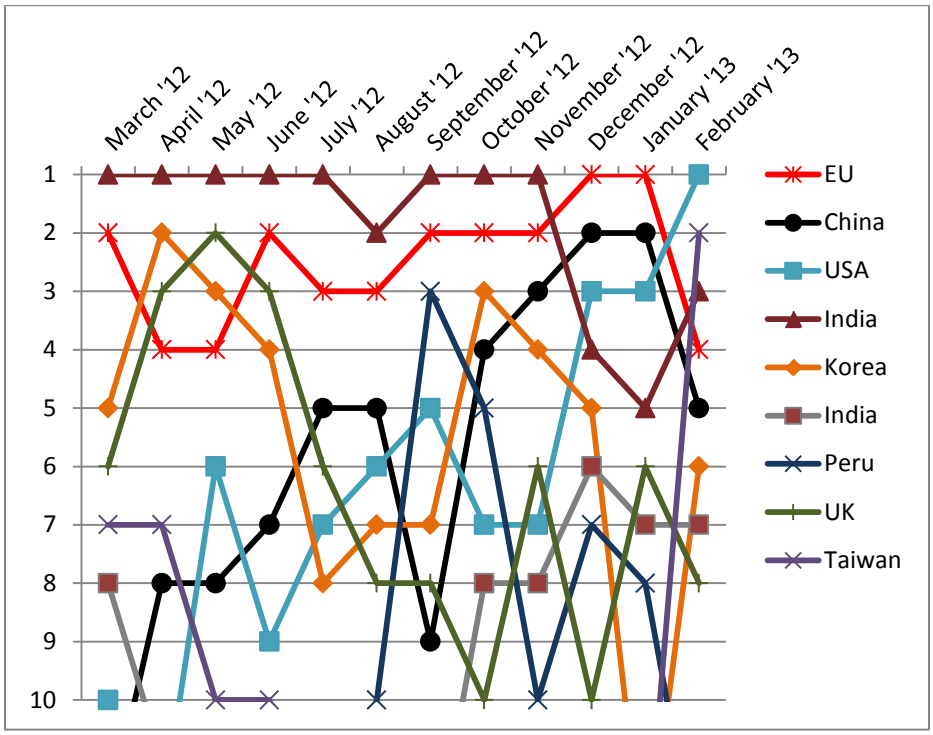
本項は今号の Threat Report から始まったもので、お客様のシステムを侵害しようとして Targeted Attack Protection により検知された悪意のある URL が全体に占める割合を示すものです。低いレベルから急激に増加する傾向があることに注目して下さい。検知を逃れるために増殖し変形する強力な攻撃が示されています。



Spam Sources by Country (スパム発信源)

スパム発信源として長らく 1 位の座にいたインドが昨年の 11 月以降は大きくスパム量を減らしています。インドからのスパム量の減少は全体に影響を与えており、8 位以下の国のスパム量は 1%以下に減少しました。

注目すべきは米国発のスパムが増え続けていることで、2 月にはついに 1 位の座を占めました。



上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 1 月と 2 月のスパム発信量(総数に対してのパーセンテージ)の上位 8 カ国です。

January 2013			February 2013		
1	EU	8.97%	1	USA	10.01%
2	China	7.58%	2	Taiwan	8.49%
3	USA	5.93%	3	India	7.70%
4	Korea	5.90%	4	EU	6.88%
5	India	5.80%	5	China	6.78%
6	Vietnam	4.41%	6	Korea	6.31%
7	Russia	3.91%	7	Russia	3.12%
8	Peru	1.76%	8	Vietnam	2.97%

proofpoint

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