proofpoint

Proofpoint Threat Report

March 2013

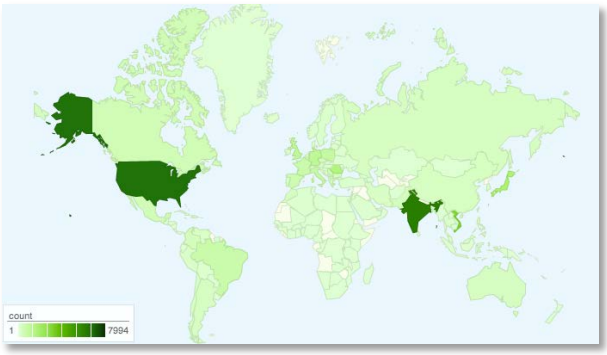
本レポートは、Proofpoint が注目し、お客様および一般企業に対して注意を喚起したいと考えている脅威に関する情報、詳細、トレンドなどをまとめたものです。

Threat Models (手法)

インターネットの分散アーキテクチャを利用した攻撃

フィッシング攻撃の手法は進化を続けており、より多くのリソースを活用し始めています。単一のフィッシング攻撃により、数百万通のメールが数万の IP アドレスから送信され、数百の侵害されたサイトに誘導するのです。

例えば Proofpoint では最近、いくつかの特徴を持った攻撃を確認しました。まず、このフィッシング攻撃では 53,578 個の送信者 IP アドレスを使っています。以下の地図に送信元 IP アドレスの分布を示します。



Proofpoint では、より多くのアドレスを使うことができる IPv6 が普及すると、このタイプの攻撃はさらに増えると予想しています。送信元 IP アドレスの分布図を見ると、インドとアメリカに集中していますが、これはこのレポートの最後に掲載しているスパム発信源のランキングと一致します。

さらに、攻撃の初期段階で、狙われた受信者は 569 台の侵害された Web サーバーに誘導されます。単一の攻撃の中で使われるサーバーの数が多くなると言うことは、レピュテーションなどの指標を使う従来型のセキュリティソリューションでは攻撃を検知できる可能性が低くなることを示しています。さらに、この攻撃は古いけれども効果的な手法も利用しています。480 万通のメッセージを

配信するのに 470 万もの送信者アドレスを使っているのです。攻撃者はインターネットのアーキテクチャを効果的に利用し、攻撃の分散化を進めているのです。

ドライブバイダウンロードにおける URL の仕組み

ドライブバイダウンロードでは、よく似た URL が使われます。Proofpoint が観測した二つの攻撃がこれを裏付けています。

最初の攻撃は同じドメインを使い、URL の最後を変えています。以下はその一部です。

<domain>/August.html
<domain>/barn.html
<domain>/cage.html
<domain>/camera.html
<domain>/cap.html
<domain>/certain.html
<domain>/check.html
<domain>/disappear.html
<domain>/essential.html
<domain>/familiar.html

また、その逆に同じランディングページを使ってドメインを変えるやり方もあります。

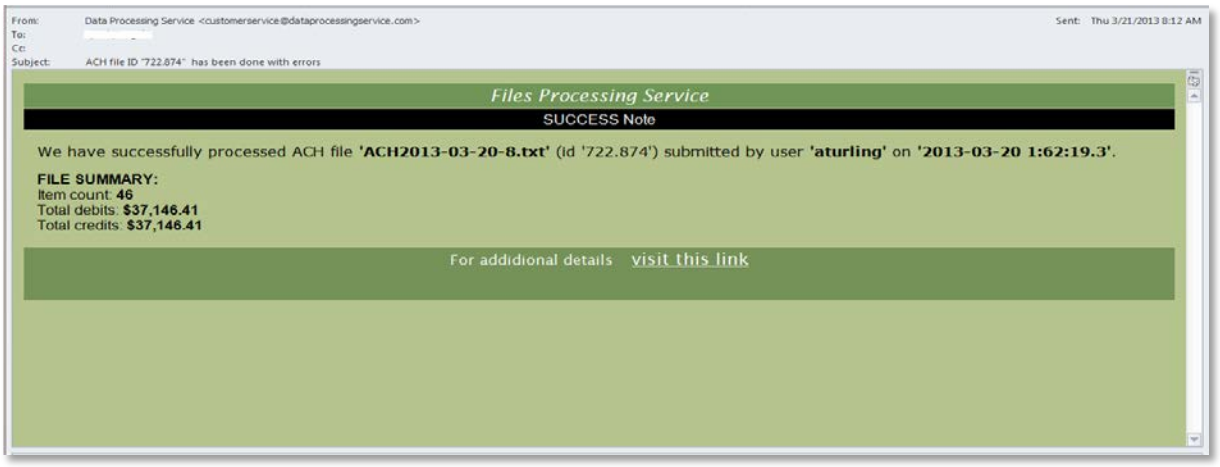
www.scmoju.<tld>/page2-highres.<ext>
bracodimitrijevic.<tld>/page2-highres.<ext>
startup.<tld>/page2-highres.<ext>
hecpcb.<tld>/page2-highres.<ext>
rr911.<tld>/page2-highres.<ext>
hello06.<tld>/page2-highres.<ext>
kennethclarke.<tld>/page2-highres.<ext>
moose.themaloneygroup.<tld>/page2-highres.<ext>
lorahtech-ng.<tld>/page2-highres.<ext>
3aym.<tld>/page2-highres.<ext>
www.camelieantiche.<tld>/page2-highres.<ext>
maadimessenger.<tld>/page2-highres.<ext>
hertzequip.<tld>/page2-highres.<ext>
olgino.<tld>/page2-highres.<ext>

この攻撃では 148 個の異なるドメインが使われています。どれにも含まれる page2-hires.<ext>がユーザーを悪意のあるサイトに誘導します。攻撃者は攻撃スタイルや経路を頻繁に変えます。これらの二つの攻撃はその実例です。“page2-highres“はドライブバイダウンロードをホスティングしており、二つの pdf エクスプロイトと一つの Java エクスプロイトを狙ってトロイの木馬をインストールしようとするものです。このマルウェアの解析から、アンチウイルスエンジンの 41%しか pdf エクスプロイトを検知できず、トロイの木馬は 20%でした。Java のセキュリティホールに至っては 9%の従来型アンチウイルスしかエンドユーザーを守ることができませんでした。

様々な URL と異なるドライブバイダウンロードにより、攻撃者はゲームを有利に運んでいます。Proofpoint の Targeted Attack Protection (TAP) はこれらの攻撃からユーザーを守ることができます。

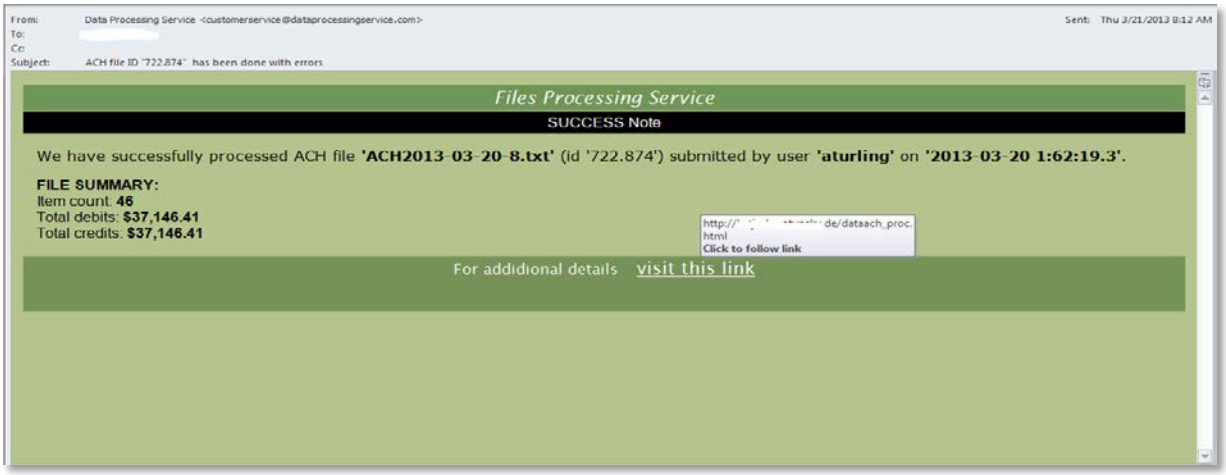
ソーシャルエンジニアリングの実例

エンドユーザーにリンクをクリックさせようとするのは、伝統的なスピアフィッシングの手口です。そして、メールを本物らしく見せかけるテクニックは常に進化を続けています。このメッセージをご覧ください。



いくつかの項目が目につきます。1) お金。大金です。2)「差出人」アドレスは正規のものに見えます。3) メッセージの内容も日付と時間にふさわしいものに見えます。(多くの場合、送金は営業時間外に行われます) 多分、このメールの作成者は受信者のことを調査し、LinkedIn で彼または彼女が営業職であることを知り、コミッションやボーナスの支払いが予定されていると考えたのでしょう。これらのことを考え合わせると、受信者がリンクをクリックする可能性は高いと考えられます。

もう少し、詳しく見てみましょう。

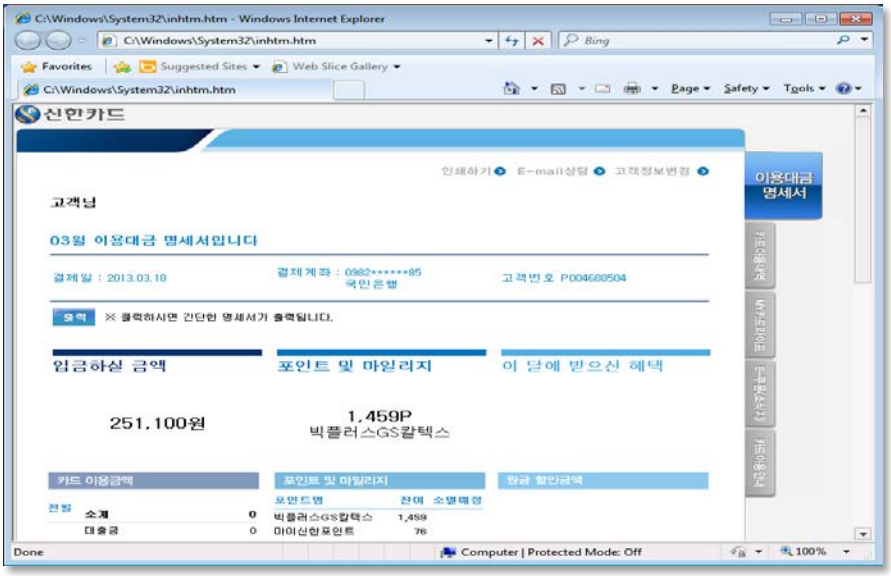


このマルウェアの作者は二つの間違いを犯しています。第一に、“For addidional details”のスペルが間違っています。第二に、リンクされた URL のラベルが明らかに疑わしいことです。(上図ではぼかしを入れてあります) この事例は、ソーシャルエンジニアリングについての勉強用としてご活用下さい。

Threat News（ニュース）

韓国の“wiper”攻撃に標的型メール攻撃の特徴

アンチウイルスソリューションの大手で、Proofpoint のパートナーでもある F-Secure は、この攻撃が標的型スピアフィッシングの特徴を備えていることを発見しました。最初のアーカイブには非常に長いファイル名が使われており、以下の画像のように偽の html ページがバックグラウンドでのマルウェアのダウンロードを隠しています。これはまた、マルウェアの作者は乗っ取ったシステムを、実際に攻撃を行うプラットフォームとして使おうとしていることを示しています。詳細はこちらをご覧ください。



Google Docs はフィッシングサービスなのか？

SophosLabs の研究者が Google Docs をプラットフォームとして利用したソーシャルエンジニアリングベースの攻撃を二つ発見しました。どちらもオンラインフォームでログイン情報を要求します。最初の例は ANZ（オーストラリアの金融サービス会社）で、オンラインバンキングのユーザーを、二つ目は北米の教育機関のポータルサービスのユーザーを狙ったものです。Google Docs の利用時と google.com ドメインは要求に対して簡単な認証を行います。これらは非常に巧みなソーシャルエンジニアリングです。

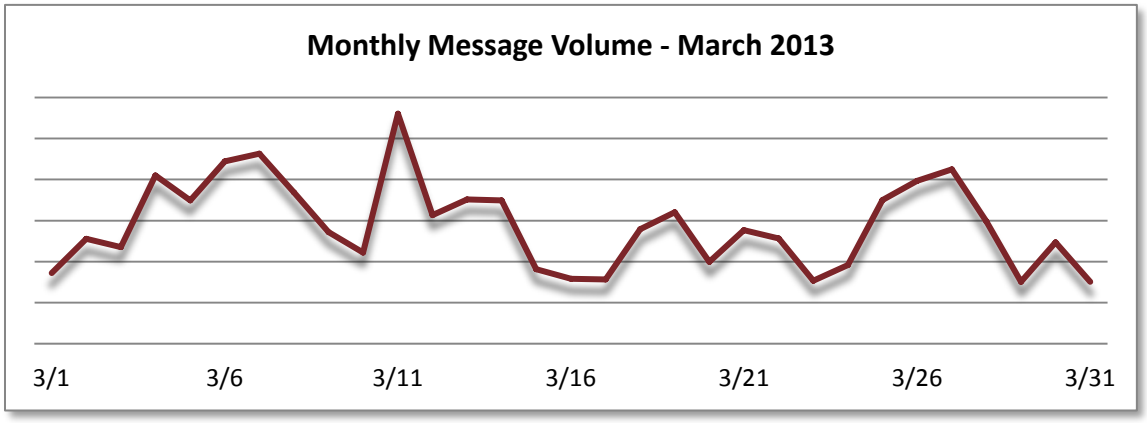
セキュリティ研究者でも騙されることがあります

セキュリティ研究家として名高い Brian Krebs のブログは本 Threat Report でも何回か紹介していますが、先頃自らの間違いを認めました。Darkode.com のソーシャルエンジニアリングされた投稿に騙され、「新しい Java エクスプロイトを購入者あたり$5,000 で販売」という記事を書きました。しかし後に、これは Krebs が使っていたユーザー名を特定するために管理者が仕込んだ罠だったことが判明しました。

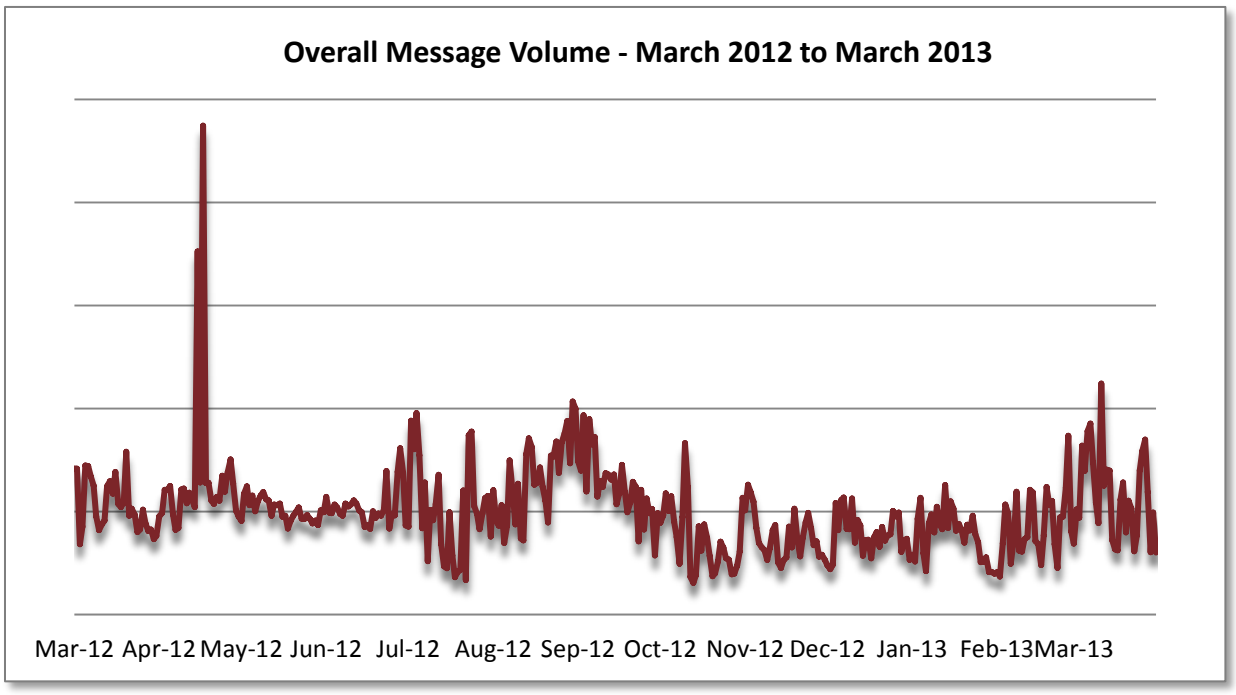
Threat Trends (トレンド)

Spam Volume Trends (スパム量のトレンド)

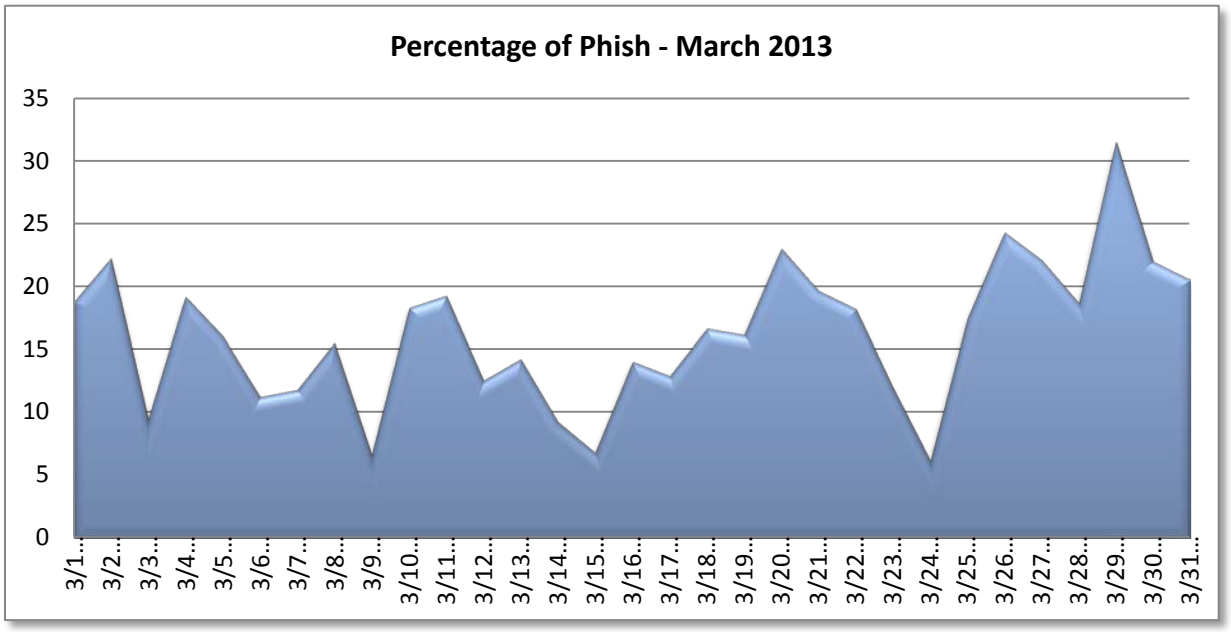
悪意のある、あるいはその他の攻撃を除いたスパム量は 2 月から 3 月にかけて大幅に増加し、前月比で 35.48%も増えました。最近の減少傾向に歯止めをかけ、2012 年 3 月と比べても 8.88%増加しています。



上のグラフで分かるように、過去数ヶ月間と同様、スパム量は月の中旬が最も多く、月末に書けて減少しています。月間のスパム量は増加し、2012 年中期の水準に戻っています。



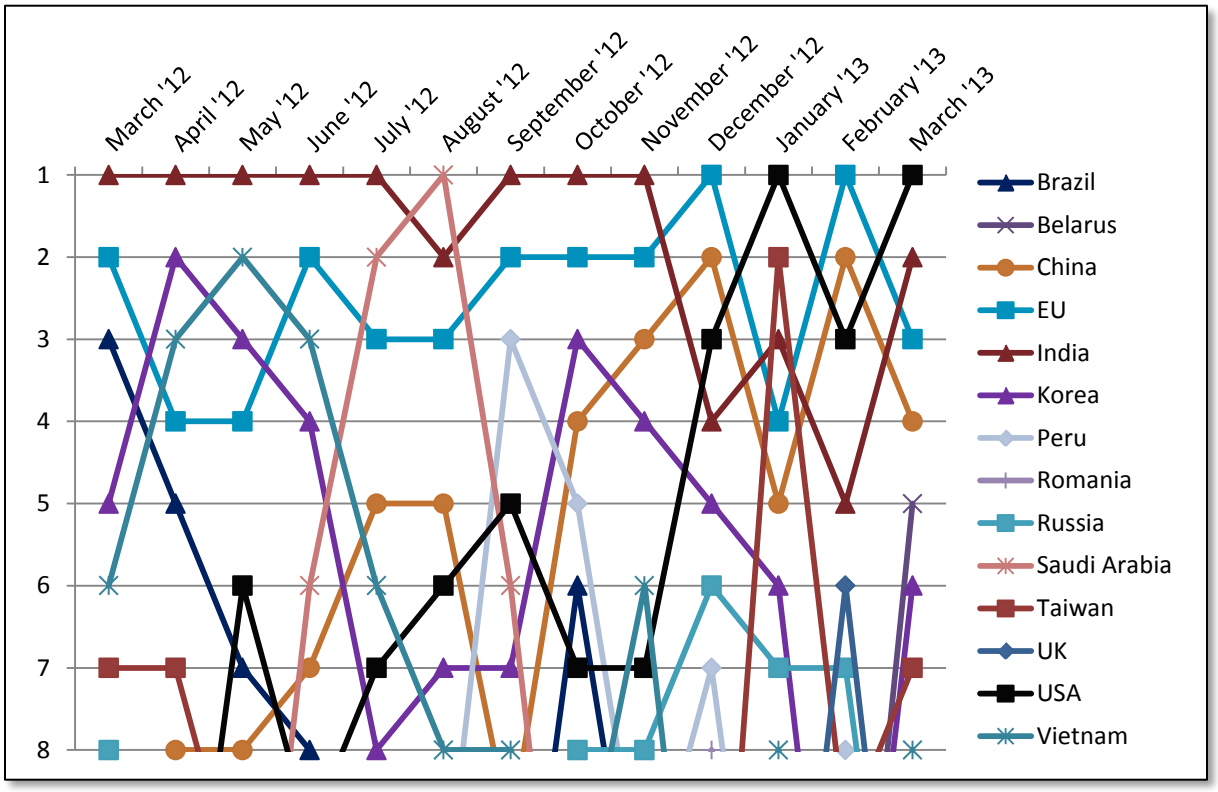
Phish Classification Trends (フィッシング分類のトレンド)



上のグラフは Proofpoint の MLX および Targeted Attack Protection によってフィッシングに分類(スパムやバルクメールではなく)されたメッセージの割合(パーセンテージ)を示しています。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。

Spam Sources by Country (スパム発信源)

2 月に 3 位に後退しましたが、3 月にまたアメリカがスパム発信源の首位に返り咲きました。インドも量と全体に占める割合(下の表を参照)の両方で 2 位に戻っています。ベラルーシが初めてランキングに登場し、5 位に入ったのが注目されます。



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 3 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。

February 2013			March 2013		
1	USA	10.01%	1	USA	9.70%
2	Taiwan	8.49%	2	India	8.72%
3	India	7.70%	3	EU	7.25%
4	EU	6.88%	4	China	5.16%
5	China	6.78%	5	Belarus	4.28%
6	Korea	6.31%	6	Korea	3.271%
7	Russia	3.12%	7	Taiwan	3.12%
8	Vietnam	2.97%	8	Vietnam	2.97%

proofpoint

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