proofpoint

# Proofpoint Threat Report

## July 2014

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様々な脅威に関する情報、詳細、トレンドなどをまとめたものです。

## Threat Models (手法)

### 巨大ボットネットによる大規模な医薬品スパム攻撃

過去数週間にわたり、Proofpoint のスパム対策チームは医薬品スパム攻撃が拡大するのを監視してきました。これは、先月の本レポートでお伝えした株式売買のスパムに似たものです。医薬品スパムはそれに比較するとまだ影響は大きくないですが、ユーザーにとっての脅威であることに変わりはありません。Proofpoint は通常通り、繰り返される攻撃毎にスパム定義を更新し、検知ルールの作成を続けています。

この攻撃のサンプルをご紹介します。

**Campaign #1**

2014 年 7 月 10 日木曜日の午前 7 時 33 分 (米太平洋標準時) に、大規模なボットネット攻撃が Proofpoint のスパムトラップにより検知されました。使われたメッセージの全てが「v」で始まるアドレスから発信されているように見えますが、実際のアドレスは以下の様に様々です。

1. From: venita.a@email-discounts[.]com <numerator@flora.waw[.]pl>
2. From: vera.schuster@championoffers[.]com <vlsnf@bizjunction[.]com>
3. From: veralinss@net-submissions[.]com <marek.wrzoskowicz@howden[.]pl>
4. From: ve@ticmail[.]net <euroauton@toquero[.]com>
5. From: veils539@nyetmail[.]com <m.gajda@grand-hotel[.]pl>
6. From: vrx4xclo@wittyhenrys[.]us <seagonzo@globalcrossing[.]net>

件名は、以下の様に医薬品に関連しています。

1. Subject: Int///ernaational me///dst0re o///ni|ne
2. Subject: Int///ern@tional me///sdtore o///nliine
3. Subject: Int///ernatioonal me///d$tore 0///nl1ne
4. Subject: Int///ernaitonal me///dst0re 0///nl|ne
5. Subject: Int///ernaational md///estore o///nlnie
6. Subject: Int///ernaational me///dst0re 0///n1ine

(本レポートがスパムとして検知されないよう、スラッシュ (/) を追加しています)

使われている URL は、以下の様なものです。

- hxxp://doctorswmb.cn[.]com/?[randomstring]
- hxxp://doctorswmb.cn[.]com/?[randomstring]

この攻撃が始まってから数分後にスパム定義が更新され、この攻撃はブロックされました。

**サンプルメッセージ**

Internaitonal medstroe onilne hxxp://doctorswmb.cn[.]com/?jhjgffdsh

**Campaign #2**

2 番目の攻撃(亜種)は同じ日の午前 7 時 50 分に発見されました。これも大規模なボットネット攻撃でした。この攻撃で使われたメッセージは全て送信元が“VIP PfizerClub”になっていますが、実際にはランダムなアドレスから送られたものです。

1. From: “VIP PfizerClub” <gamed1376@bell[.]ca>
2. From: “VIP PfizerClub” <ynchuck846@business.telecomitalia[.]it>
3. From: “VIP PfizerClub” <stleigh.sheeksc6c@advico[.]co.uk>
4. From: “VIP PfizerClub” <chuck1f07@co[.]za>
5. From: “VIP PfizerClub” <fadamsnn37@82-198-197-167.briteline[.]de>
6. From: “VIP PfizerClub” <bernadetted76@dialog{.}net.pl>

様々な件名が使われています。

1. 5 h///ot days of ab///solutely fan///tastic SALE
2. Per///fect sa///ving s///olution! Onl///ine sh///opping!
3. Sav///ing and sh///opping is the b///est this week!
4. Wis///e fu///nds d///istribution inc///ludes SA///LE s///hopping!
5. We sel///l all pr///oducts o///nline at lea///st tw///ice c///heaper!
6. The bes///t on///line o///ffer of the mon///th!  75///% d///iscounts!

使われている URL は、以下の通りです。

- hxxp://[random username from *To:* address].homeherbsservice[.]ru/?[randomstring]
- hxxp://[random username from *To:* address].hotcurativemart[.]ru/?[randomstring]

この攻撃も、程なくスパム定義のアップデートによりブロックされました。

**サンプルメッセージ**

> The more you order the cheaper you get it. The faster you visit us the better is the choice!
> hxxp://[random username from *To:* address].homeherbsservice[.]ru/?[randomstring]

## フィッシングの教育？

あらゆる業種、規模の組織にとって、従業員の教育は重要です。熱心な経営者は、新しい、あるいは効果的な教育ツールを常に探しています。Proofpoint の研究者は先頃、企業向け教育ツールを提供する企業の Web サイトにマルウェアが隠されているのを発見しました。大手ヘルスケア組織の部長クラス宛てに送られたメールに含まれていた URL を経由したものです。


攻撃者側にとって、こういった「ウォータリングホール型攻撃」にはいろいろなメリットがあります。正規のメールを使うことにより、文法上の間違いを避けることができ、見た目もプロのようにできますから、フィッシングが見破られにくくなります。さらに、メール本文に銀行口座の話や登録リンク、SNS へのリンクなど、多くのフィッシングメールに共通する特徴が含まれていないため、高い成功率を期待できます。これらの特徴によって受信者の警戒心を解き、クリックする確率を高めるのです。

メールに含まれるリンクをユーザーがクリックしたことが分かったため、このサイトを解析したところ、このリンクはロシアの TDS (traffic direction system) を経由して Sweet Orange エクスプロイトキットにリダイレクトされていることがわかりました。この有償のエクスプロイトキットは、最新のエクスプロイトを幅広く取り入れると共に、クライアントやゲートウェイのアンチウイルスエンジンの検知から逃れるために、暗号化を用いた難読化も使っていました。さらにこのインスタンスはオンラインバンキングのログイン情報や暗号化証明書を盗み出す QBOT マルウェアを配信しており、ファイル共有機能を使って他のシステムに感染します。このマルウェアはキーロガー、バックドアの機能を持っており、将来別のマルウェアをダウンロードする機能も備えています。

現代の洗練されたフィッシング攻撃に対抗するためには従業員の教育が重要ですが、今回の攻撃の発見は、今日の脅威に追従していくことの難しさを示しています。ウォータリングホールを使った今回の標的型フィッシング攻撃から読み取れることは、攻撃者はフィッシング攻撃の効果を高めるために最新のエクスプロイトや技術を活用するだけで無く、企業や経営者のニーズも理解しようとして、常に進化し学習していることです。

## Threat News (ニュース)

### フィッシングの心理学

Proofpoint の EMEA (Europe, Middle East, and Africa) 担当ディレクターである Mark Sparshott が、以下のサイトでフィッシングの手法と心理学について分析しています。

フィッシングメールは、一般の利用者や組織にとって最も大きい脅威の一つです。攻撃者が数千通のメールを無作為に送りつけ、ほんのわずかな成功に満足していた「古き良き時代」は過ぎ去りました。退屈な作業ではありますが、今日のフィッシングメールは高度に標的を絞り込み、受信者を念頭に置いて作成されています。良くできたフィッシングメールは、努力に対して明らかにより多くのリターンを犯罪者にもたらします。

こちらをクリックして、サイバー犯罪の心理学を理解し、Proofpoint の「人的要因」調査の結果を読み、Mark の説明をご確認下さい。

http://www.net-security.org/article.php?id=2078.

### マレーシア航空機事故から数時間後に送られた悪意のある URL を含むツイート

大方の予想通り、サイバー犯罪者はマレーシア航空 17 便の悲劇に乗じて、悪意のあるツイッターのリンクをクリックさせようとする攻撃を起こしました。緊急のニュースやゴシップに乗じて不法な利益を得ようとする動きは、今回が初めてではありません。サイバー犯罪者はいつもこういった場合に最初に反応します。人々の好奇心を利益に変えるのです。

詳細はこちらからどうぞ: http://www.infosecurity-magazine.com/view/39391/cyber-fraudsters-tweet-malicious-mh17-urls-hours-after-incident/.

## Threat Insight Blog (ブログ)

Proofpoint のセキュリティブログである Threat Insight から、興味深い記事をピックアップしました。皆様も Threat Insight のディスカッションに是非ご参加ください。http://www.proofpoint.com/threatinsight.

### お祭り (Fiesta) はどこで?

クライムウェアのなかには時々、ユーモアを感じさせるものが紛れ込んでいます。

Proofpoint は、TexMex (メキシコ風アメリカ料理) Frito サラダのレシピを紹介した Web サイトへのリンクを含むメールを検知しました。サンドボックス解析によって、リンク先は侵害されたサイトであることがわかりました。この Web ページはさらに、Fiesta (NeoSploit) エクスプロイトキットにリダイレクトされていたのです。Fiesta はスペイン語で祭りを意味し、スペイン語圏の料理に関するサイトを侵害したエクスプロイトとしては気が利いています。

この例は多分偶然でしょうが、疑問も沸きます。こういった偶然は、攻撃者のユーモアを刺激するのでしょうか? そうだとすると、Fiesta ディナーウェアのサイトも攻撃候補になるのかもしれません。

詳細はこちらからどうぞ: http://www.proofpoint.com/threatinsight/posts/the-fiesta-exploit-kit.php.

### フィッシング攻撃者はシンプルを好む

先頃私たちは、有効な SSL 証明書とほぼ完全な Google のログインページを組み合わせて Google ユーザーのログイン情報を盗み出すフィッシング攻撃について書きました。

Proofpoint の研究者はこの手法をさらに強化し、しかし少しひねくれた攻撃を発見しました。以前同様にユーザーはメールのログイン画面へ誘導されるメールを受け取ります。URL は受信者のメールアドレスとユーザー名を base64 でエンコードしたもので、個々のメッセージ毎にユニークで、動的に生成されます。

注目すべきは、これらのページをホストするドメインは、Proofpoint がこの攻撃を検知したその日の朝に作られたものだったことです。

詳細はこちらからどうぞ: http://www.proofpoint.com/threatinsight/posts/phishers-keep-it-simple.php.

### 寄付マルウェア: 侵害された旅行サイトに狙われる旅行者

Proofpoint の研究者は最近、多くの旅行関連サイトが侵害され、Nuclear エクスプロイトキットを配信していることを初めて発見しました。Proofpoint のユーザーが侵害されたページへのリンクを含むメールを受信したため、Proofpoint Targeted Attack Protection (TAP) がこれらのサイトを発見したのです。これはかなり効果があった攻撃とみられ、ユーザーが受信を許可した正規のメールを使うウォータリングホール型攻撃に見られる多くの特徴を備えています。

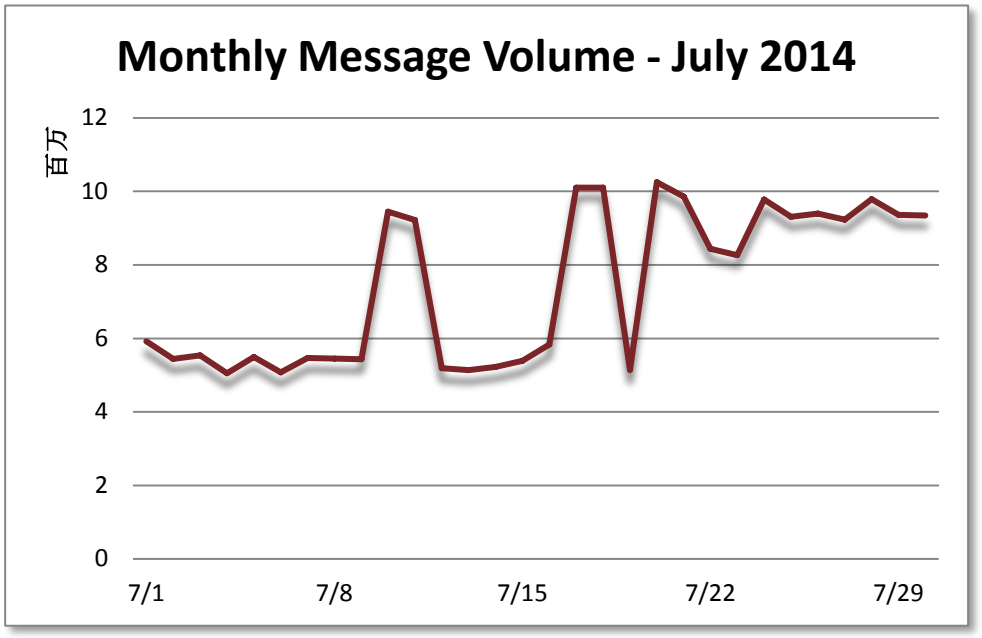
抜け目ないことに、いくつかのプロモーションメールは独立記念日の行事に関連づけられていました。攻撃者はメールの信憑性を増すために時期を見計らったのでしょう。しかし、他のほとんどのものは一般的な旅行関連の話題でした。

詳細はこちらからどうぞ: http://www.proofpoint.com/threatinsight/posts/travelers-targeted-by-infected-travel-websites.php.

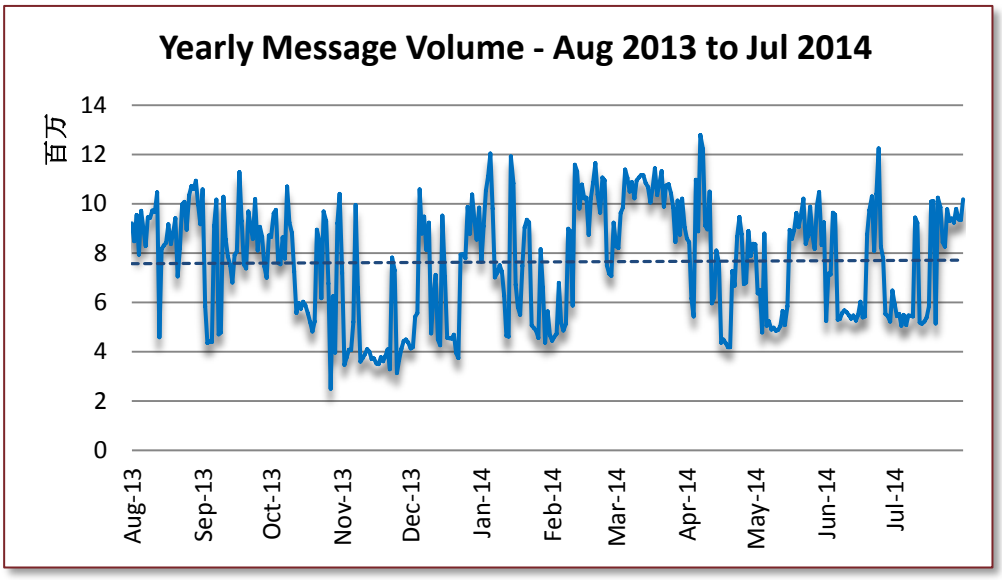
## Threat Trends (トレンド)

### Spam Volume Trends (スパム量のトレンド)

Proofpoint では、スパム量についてハニーポットを使って追跡していますが、この値は Proofpoint のお客様からの報告ともほぼ一致します。7 月の第 1 周は 6 月の傾向を引き継いで安定していましたが、第 2 週の初めから劇的な変化を始めました。600 万通/日からいきなり 900 万通/日に跳ね上がり、すぐに元の 600 万通/日を下回るレベルにまで落ち込みました。しかし、さらに大きな変化が待っていました。第 3 週の初めにそれまでの最高を超え、1,000 万通/日に達したのです。そしてまた 500 万通/日に落ち込み、すぐにまた 1,000 万通/日に戻しています。第 4 週は 900 万通/日前後で揺れ動きました。




比較すると、6 月よりも 7 月のほうが 8.12%スパム量が増えました。前年同月比だと 6.87%の減少です。



## Spam Sources by Country (スパム発信源)

EU は 7 月も強さを見せ、アメリカが 2 位に返り咲きました。中国は 3 位、アルゼンチンが 4 位に入り、ロシアは 5 位でした。以下は過去 6 ヶ月間のスパム配信量上位 5 カ国の表です。

| | | Feb '14 | Mar '14 | Apr '14 | May '14 | Jun '14 | Jul '14 |
|---|---|---|---|---|---|---|---|
| Rank | 1st | EU | EU | EU | EU | EU | EU |
| | 2nd | US | US | Argentina | US | Vietnam | US |
| | 3rd | Argentina | Argentina | US | Argentina | US | China |
| | 4th | Russia | India | Russia | Russia | China | Argentina |
| | 5th | China | Mexico | China | China | Russia | Russia |

以下の表は、各国が総スパム量に占める発信量の割合を示したものです。EU の数値は全加盟国を含んでおり、以前よりも正確に傾向をつかむことができます。EU は全体のスパム量の 38.13%を配信しており、トップです。トップ 5 の残りの 4 カ国は合わせて 20.32%で、EU の半分を少し上回る程度です。

| June 2014 | | | July 2014 | | |
|---|---|---|---|---|---|
| **1** | EU | 30.89% | **1** | EU | 38.13% |
| **2** | Vietnam | 5.91% | **2** | US | 6.94% |
| **3** | US | 5.53% | **3** | China | 5.19% |
| **4** | China | 5.25% | **4** | Argentina | 4.58% |
| **5** | Russia | 4.70% | **5** | Russia | 3.61% |


この他の情報については以下をご覧ください
www.proofpoint.com/threatinsight

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