proofpoint

Proofpoint Threat Report

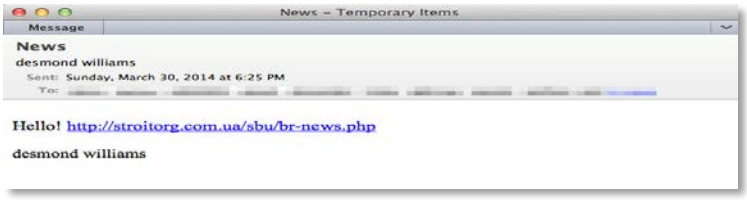
April 2014

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)

先進的手法を使ったスパム攻撃「News」

Proofpoint では最近 1 ヶ月以上にわたって、Targeted Attack Protection (TAP) をご利用頂いているお客様の多数のクリックを観測しています。これらのクリックの増加は特定の攻撃によるものと考えられ、私たちはその攻撃に「News」という名前を付けました。それは、この攻撃に使われる URL や件名に「News」という文字が高頻度で含まれているからです。以下がサンプルです。



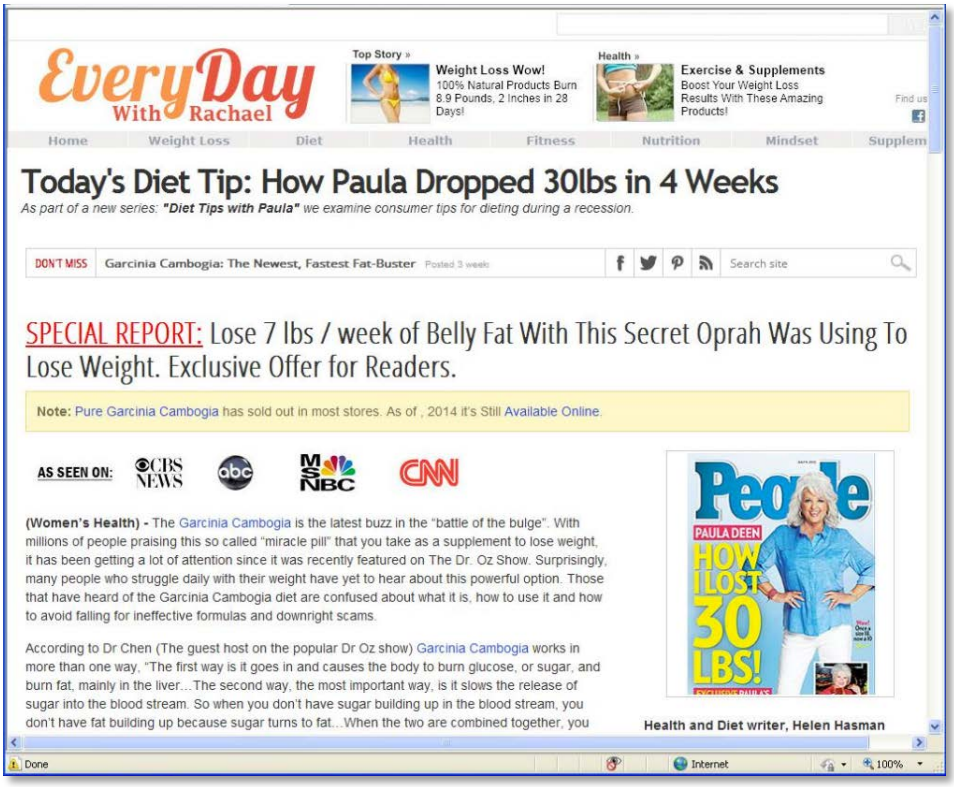
この攻撃で使われるメッセージは、ほとんどの場合非常にシンプルでコンテンツをほとんど含まないため、スパムとして検知したりブロックしたりするのが困難です。その結果、この攻撃では通常よりも多くのメッセージがエンドユーザーまで配信されてしまいます。

見た目が野暮ったいため、私たちはクリック率は高くないだろうと思っていました。しかし、実際には配信されたメールのうち、実に 7%がクリックされています。これはかなり高いクリック率ということができ、私たちはこの 1 ヶ月間で数千件のクリックを観測しました。

このグループのもう一つの特徴は、15,000 以上の異なる侵害された Web サイトを使っていることです。大規模なボットネットを使って大量のメールを配信し、膨大な Web サイトの蓄積を使って URL をランダム化することにより、ボリュームベースの検知メカニズムを迂回することに成功して

いるのです。特定の Web サイトに紐付けられたメッセージ数は、1 時間当たりひとつかふたつでした。これは非常に少ない数です。

PC あるいは Mac でこの URL をクリックすると、ダイエットスパムのサイトに誘導されます。以下がサンプルです。



この攻撃のトラフィックは、すべてが TDS (Traffic Distribution System) レイヤーでルーティングされているという洗練されたもので、このためにこの攻撃は先進的スパム (advanced spam) に分類されます。(この場合でも TAP により URL は検知できます。) この仕組みにより、攻撃者はエンドユーザーに表示するコンテンツを時間や日付、地域、デバイスの種類などによって変化させることができます。あるユーザーはスパムサイトに誘導され、他のユーザーはそれとは違う、もっと悪意のあるサイトに誘導されるかもしれないのです。

この機能を使うと、例えばユーザーが Android デバイスでこの URL をクリックした場合に、PC 向けのスパムサイトではなく、Andorid デバイス用の他のサイトに誘導し、そこで Android のマルウェアをダウンロードさるといったことができます。(ところで、もし貴方が Android 用のアンチウイルスソフトウェアをお探しだとしても、アプリストアのナンバーワンアプリを選んではいけません。これは完全な詐欺アプリだからです。)

これらの特徴を見てみると、この攻撃がなぜ「先進的」なのか、ご理解頂けるでしょう。以下のような洗練された手法が使われています。

- ひとつの IP あたりのメッセージ数が少ないにも関わらず、大量のメッセージを配信することができる、巨大なボットネットを使っている。
- 大量の URL を使うために、ハックされた Web サイトを潤沢に確保している。
- シンプルでランダム化されたテンプレートにより、検知しづらく高いクリックレートを実現している。

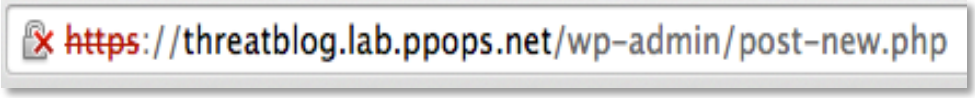
- プログラム可能な TDS レイヤーにより、様々な条件でクリックのトラフィックを生成でき、それを入札にかけて最も高い価格を付けた入札者に販売している。

特別に手の込んだフィッシング

フィッシングの URL を見分けるためのアドバイスとして良く聞くのは、以下の様なものです。

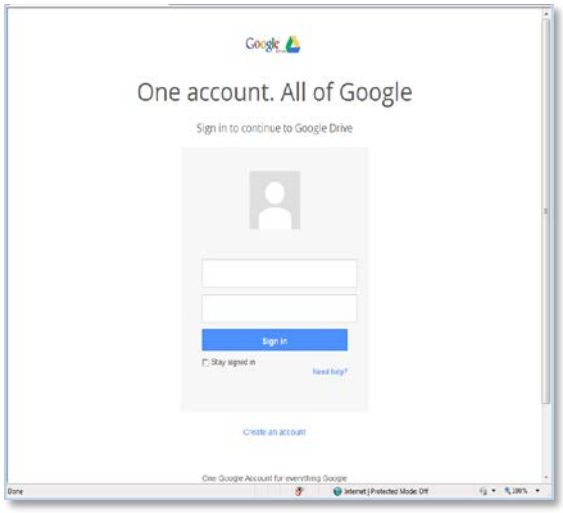
1. クリックする前に、URL 中のドメインが実在のサイトと一致しているかどうかを確認する。
2. サイトが SSL を使っている場合、証明書を確認する。

このアドバイスは、いくつかのブラウザでは URL の表示部分にも組み込まれています。例えば Google Chrome では、このブログの URL は以下のように (ブログ執筆時点では) 表示されます。

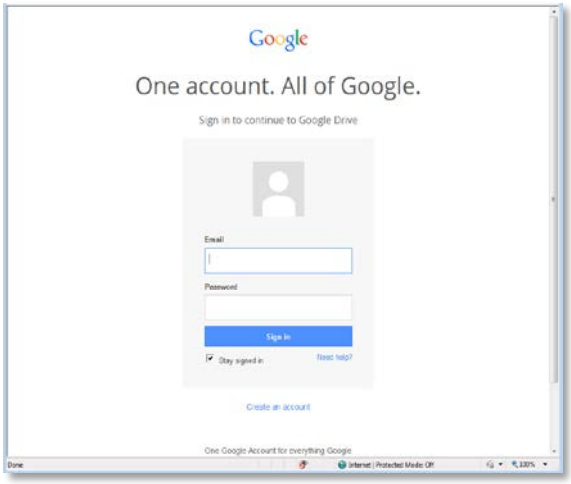


証明書とホスト名が一致していないため、赤い文字で警告が出て、SSL に問題があることを伝えてくれています。さらに、URL 中のホスト名部分を黒く、その他の部分をグレーで色分けして、ドメインが見分けやすくなっています。

つい最近、私たちはあるフィッシング URL を見つけましたが、それは上で述べたアドバイスを無価値にするものでした。その URL は正規のドメイン (googledrive.com) を示しており、完全に合法な SSL 証明書を持っていたのです。これは Google Drive がユーザーに対してコンテンツをアップロードできるようにしているために可能になったことで、これにより完全に模倣された Google のログインフォームをアップロードできるのです。以下がサンプルです。

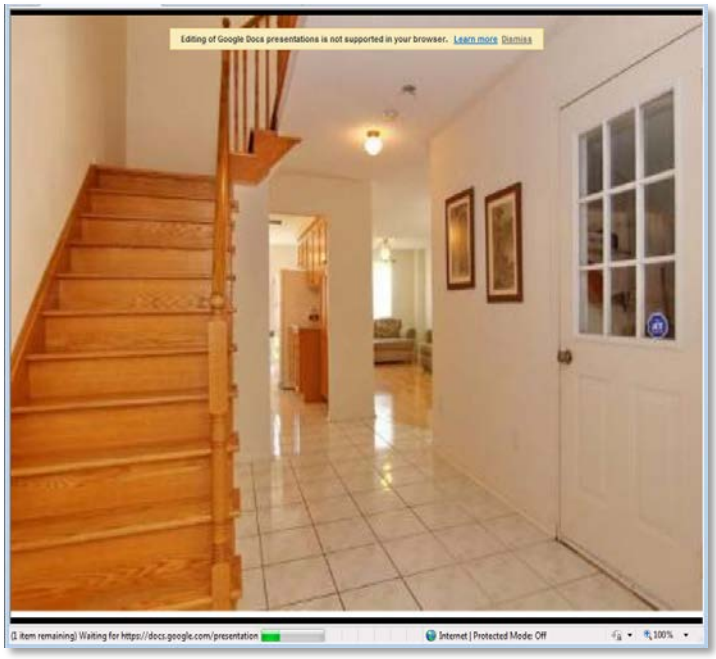


Google Drive のコンテンツを見ようとしているユーザーにとって、上のイメージには何ら怪しい点はありません。ホスト名は正しく、SSL 証明書もチェックされ、コンテンツは Google のログインフォームに非常に似ています。以下は、「正規の」Google のログインページです。



最初のイメージをフィッシングサイトだと見抜くことができるでしょうか? これが本物の Google のログインフォームではないことを確認するためには、ページのソースコードを確認する必要があります。フォームの設定を確認し、データがポストされた URL を見る以外に方法はありません。そのような作業を、一般のユーザーに期待するのは不可能です。

この偽サイトで Google のログイン情報を入力すると、ユーザーは正規の Google ドキュメントにリダイレクトされますから、操作とその結果についてなんら疑問を持つことはありません。このケースでは、ユーザーは新しい家の写真にアクセスしたかったと考えられ、目的のコンテンツが表示されています。



最初から最後まで、考え抜かれたフィッシング攻撃で、コンテンツについてユーザーが疑問を持つ余地はありません。

Threat News (ニュース)

ビジネスがデータ流出に関して政治的圧力に直面

Target や Experian などの注目を集めたデータ流出事件を受け、米連邦取引委員会 (FTC: Federal Trade Commission) は、消費者保護のため、米連邦議会に対して、国家レベルでの侵害通知に関する法律 (national breach notification legislation) の成立を強力に働きかけています。これは、多くのビジネスに大きな影響を与える可能性があります。詳細は以下でご覧ください。

http://www.csoonline.com/article/2140211/security-leadership/businesses-face-rising-political-pressure-from-data-breaches.html.

最悪のフィッシング年

先頃香港で行われた Anti-Phishing Working Group で、最新の APWG Global Phishing Survey が発表されました。このサーベイは 2013 年後半に観測された世界的なフィッシング問題についての詳細な分析です。Illumintel, Inc.の Greg Aaron と Internet Identity の Rod Rasmussen によって作成されました。

一言で言えば、状況は良くありません。

この期間に、世界で少なくとも 115,565 件のユニークなフィッシング攻撃がありました。このチームが調査を開始した 2007 年以来、最悪の結果となっています。

詳細は以下でご覧ください。いくつか良いニュースもあります。

http://www.circleid.com/posts/20140409_a_bad_year_for_phishing/.

データ流出インシデントに対する連邦政府の訴訟権を支持

データ流出インシデントへの対応を怠った企業を訴える権利について、米連邦取引委員会 (FTC: Federal Trade Commission) の申し立てが、ニュージャージー州の連邦裁判所に支持されました。

Wyndham Worldwide, Inc.はデータ流出事故に関して 2012 年に FTC から訴訟を起こされています。数十万件のクレジットカードおよびデビットカードのデータが流出し、被害額は 1,060 万ドルに上ります。詳細は以下でご覧ください。

http://www.fiercecio.com/story/feds-right-sue-data-breach-incidents-upheld/2014-04-14.

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.

貴方の PDF には Gamarue Trojan は潜んでいませんか?

Proofpoint の研究者は先頃、悪意のある PDF 攻撃を観測しました。限られた顧客に 590 通以上のメールが配信されました。ちなみに、狙われた企業の産業別構成は ThreatInsight に先日公開したエントリ (Are you being targeted?) でご紹介した内容と一致しています。このメールは、新しいセキュリティアップデートについてのお知らせを装っていますが、実際にはユーザーに悪意のある PDF 添付ファイルを開かせるためのものでした。詳細は以下でご覧ください。

http://www.proofpoint.com/threatinsight/posts/whats-in-your-pdf.php.

1 クリックで 1 億 1 千万件のクレジットカード情報: はえ縄型攻撃が米 Target, Inc.を狙った手法とは

調査型レポーターの Brian Krebs の最近のレポートによると、Target の侵害は HVAC (Heating, Ventilation, and Air Conditioning: 暖房、換気、および空調) のコントラクタに送られたフィッシングメールから始まったのではないか、ということです。

しかし、この指摘は驚くべきものではありません。研究者達は標的型攻撃や APT 攻撃の 95%がフィッシングによって引き起こされると指摘しています。また、IT セキュリティおよび運用スタッフの 76%が、過去 12 ヶ月間のうちに IDS やアンチウイルスソリューションを迂回したエクスプロイトやマルウェアに攻撃を受けたと言っています。

Krebs は、攻撃者が最初から HVAC 企業あるいは小売業者を狙ったのかどうかについて考察していますが、ひょっとすると、少なくとも最初のうちは狙ってはいなかったのかもしれない、と述べています。「このタイプの攻撃の多くは、最初は広範囲にメールをばらまくショットガンタイプの攻撃です。クリックした被害者のリストができた後に、内容を詳細にチェックし、籾殻から小麦を見つけるように、興味を惹く標的を拾い集めるのです。」

いずれにせよ、Target の事例は過去最大級の成功した「はえ縄型攻撃」であると言えるでしょう。詳細は以下でご覧ください。

http://www.proofpoint.com/threatinsight/posts/how-longlining-likely-compromised-target-inc.php.

死と税は逃れられない…そしてクリックも

アメリカでは税金に関連したフィッシングメールが、プロ野球開幕や花粉症、税務申告などと並んで春の風物詩となっています。IRS (Internal Revenue Service: 米国税庁) はフィッシングメールに関する Web サイトを立ち上げ、メディアは納税者に対して IRS を名乗るメールに注意するよう呼びかけています。

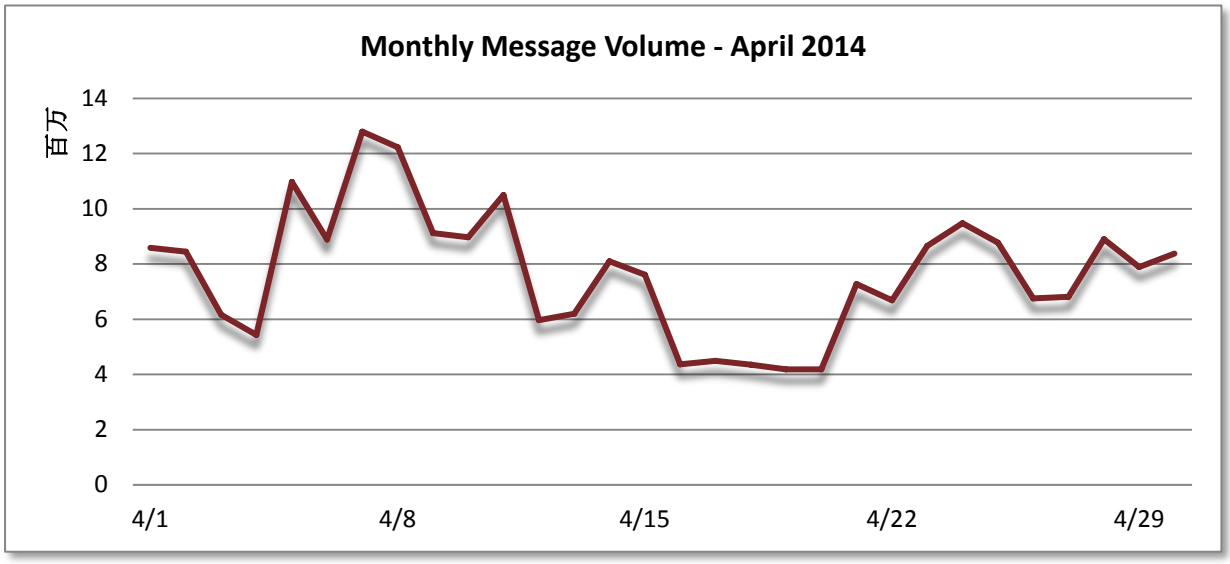
これだけの注意喚起がなされているにも関わらず、これらのフィッシングメールに騙される受信者が後を絶たないのは不思議なことです。コンシューマへの啓蒙はある程度功を奏すでしょうが、ビジネスユーザーについては、団体としての行動、あるいは大数の法則が支配的となり、怪しいメールをクリックしないようエンドユーザーを教育しても、その効果が徐々に薄れていくことが問題なのでしょう。詳細は以下でご覧ください。

http://www.proofpoint.com/threatinsight/posts/death-and-taxes-and-clicking.php

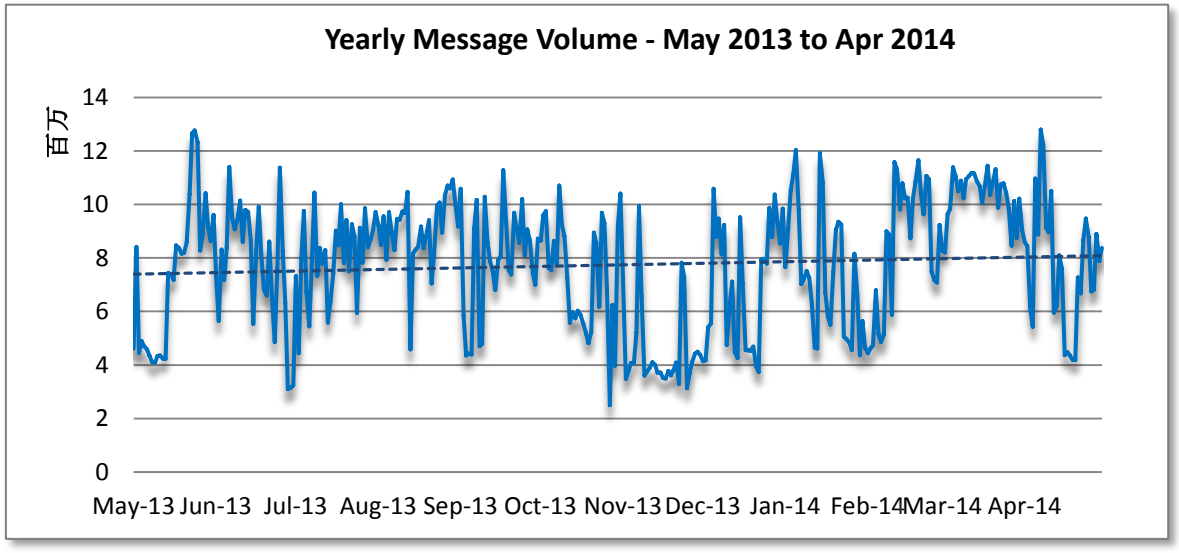
Threat Trends (トレンド)

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。4 月は異常な月でした。日々のスパム量は 1 日当たり 400 万通以下の日もあれば、1,200 万通を超える日もありました。スパム量は月初には中くらいでしたが、すぐに急減し、最初の週の終わりには月間のピーク値をマークしました。第 3 週に最大の落ち込みがあり、この落ち込みは最終週まで続きました。月末もまた異常でしたが、最初の週ほど動的ではありませんでした。最終日は最初の日と同じレベルで終っています。



スパム量は大幅に減少しており、3 月に比べて 25.09%減でした。対前年比も同様に減っており、16.33%減でした。



Spam Sources by Country (スパム発信源)

EU が独走を続け、アルゼンチンはアメリカを抜いて 2 位に浮上しました。アメリカは 3 位です。ロシアが 4 位、中国は 3 月にトップ 5 から落ちましたが、再度 5 位に返り咲きました。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。

		Nov '13	Dec '13	Jan '14	Feb '14	Mar '14	Apr '14
Rank	1st	EU	EU	EU	EU	EU	EU
	2nd	China	US	US	US	US	Argentina
	3rd	US	China	Argentina	Argentina	Argentina	US
	4th	Japan	Argentina	China	Russia	India	Russia
	5th	India	India	India	China	Mexico	China

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 39.98%で、引き続き世界のスパム量の大半を占めます。トップ 5 の残りの 4 カ国を足しても 19.59%で、EU の半分にも満たない数字です。

March 2014			April 2014		
1	EU	37.78%	1	EU	39.98%
2	US	6.98%	2	Argentina	7.64%
3	Argentina	4.36%	3	US	6.94%
4	India	2.98%	4	Russia	2.59%
5	Mexico	2.70%	5	China	2.42%

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