proofpoint

Proofpoint Threat Report

November 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)

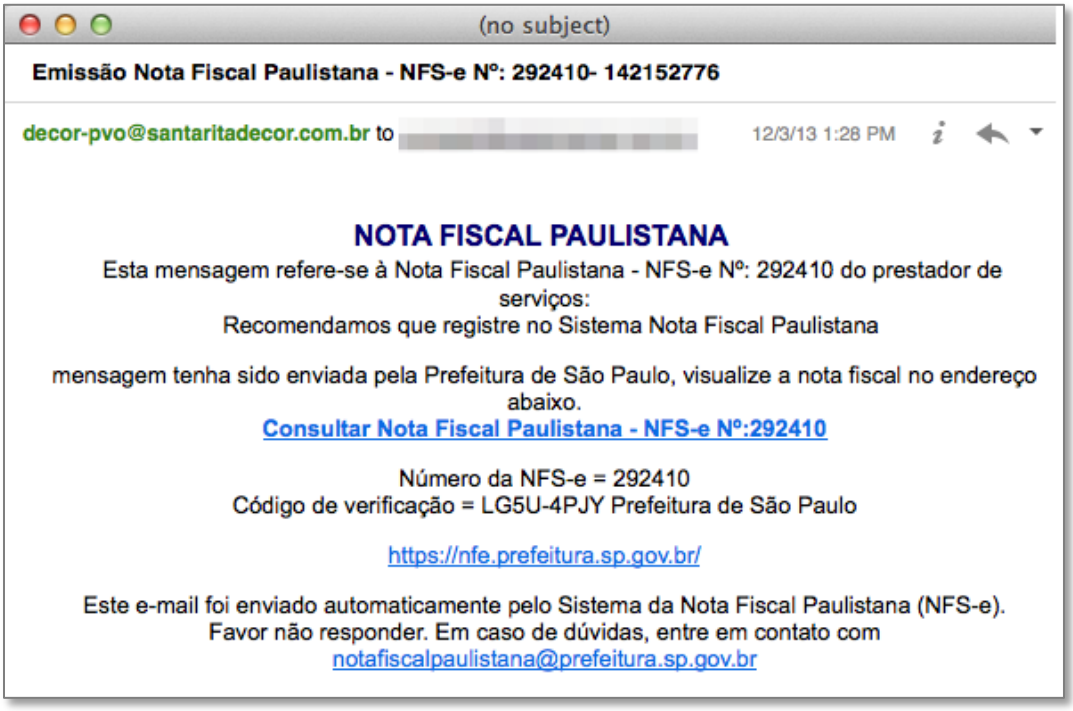
これまで 4 回にわたって、標的型攻撃、マルバタイジング、はえ縄型攻撃、そしてウォータリングホール型攻撃と、主要なマルウェア攻撃についてご説明してきました。今月からは元通り、毎月の注目すべき手法についてご説明します。

SSL 通信に隠れたマルウェア

攻撃者はユーザーにマルウェアを感染させるために、様々な手法を編み出してきました。そのうちのひとつがマルウェアへの直接リンクを送りつけるものです。ほとんどの場合、このリンクは zip ファイルに含まれており、ユーザーがそのファイルをクリックするのを待って起動し、感染します。この手法は、ドライブバイダウンロードなどに比べてクリックされる率は低いのですが、成功率の高いエクスプロイトキット攻撃に必要な複雑な仕組みを必要としません。

シンプルさを好む攻撃者が使う手法として、Dropbox 上にマルウェアを隠すものがあります。この手法なら、偽の Web サイトを立ち上げる必要は無く、苦労して正規のサイトを乗っ取る必要もありません。クラウドは様々な立場の人々を助けましたが、これらの悪人も助けてしまいました。

例として、ブラジルのユーザーを狙った攻撃が使った「餌」メールをご覧ください。



メール中の全てのリンクは偽のもので、偽のブラジル政府サイトへのリンクの他は全て Dropbox 上のマルウェアにリンクされています。このケースでの Dropbox URL は以下の様なものです:

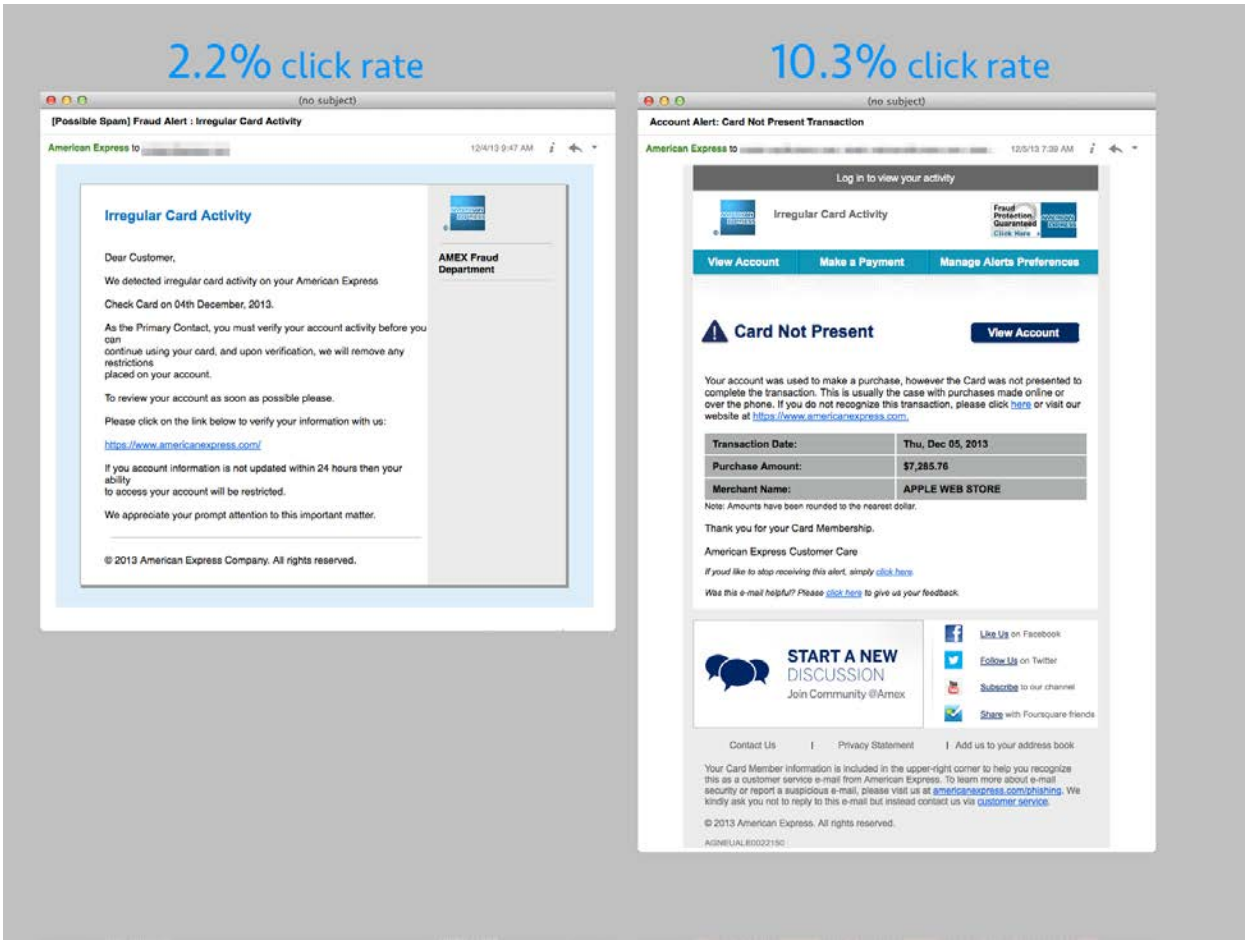
https://dl.dropboxusercontent.com/XXXX/XXXXXXXXX/nfe.fazenda.gov.br-N-007.874-12-2013.zip. (注: URL を無効化するため、一部を XXXX に変えています)

この URL で興味深いのは、暗号化通信のために https:// (SSL) を使っていることです。サンドボックスによっては SSL 通信を復号化できないため、この種のマルウェアに対しては全く無力です。そういったサンドボックスは Dropbox への SSL 通信しか見えておらず、多くの企業で同様な状況だと考えられます。さらに興味深いのは、この攻撃で使われているマルウェアは他に 3 つのマルウェアをダウンロードすることです。これらのマルウェアには独自の暗号化を施してあり、存在を隠す効果もあります。

Proofpoint Targeted Attack Protection (TAP) は、ネットワークトラフィックのレベルでは無く、アプリケーションのレベルでメッセージを検査しますから、これらを見逃すことはありません。TAP はこのタイプの攻撃から企業ユーザーと資産を守ります。

Match the Hatch

「Match the Hatch」はフライフィッシングの用語で、湖沼や川で水生昆虫の羽化 (Hatch) が始まって魚が追う時期に、その昆虫に似せたフライ (擬餌針) で魚を釣ることです。先頃見られた American Express を利用したマルウェア攻撃で、Proofpoint の研究者はフィッシングで使われた 2 つの餌メールを連続する 2 日間で比較しました。すると、この連続する 2 日間でクリック数が大きく異なったのです。以下がその 2 つのテンプレートで、クリックされた率も表示してあります:



右の餌メールがまさに「Match the Hatch」です。左に比べ、クリック率が 79%も高くなっています。2 つの餌メールを比べてみると; 高額な表示が太文字で記されており、ブランドロゴがより多く使われています。「虫の居るところ」を正しく突く攻撃が成功率を著しく上げるという例です。

Threat News (ニュース)

Google Docs を餌に使ったフィッシングメール

SANS Institutes の ISC (Internet Storm Center) が、Google Docs をフィッシングの餌に使った詐欺について警告を発しています。この餌メールは偽の Web メール業者へのリンクを含んでおり、ログイン情報を盗み出すフィッシングサイトにリンクされています。詳しくはこちらのサイトでご確認下さい: http://www.spamfighter.com/News-18688-ISC-Warns-Phishing-Emails-Abusing-Google-Docs-Circulating-on-Internet.htm

他社の情報流出事故から何を学ぶべきか？

攻撃者の創作能力には果てがありませんし、全てのパッチが当たっているシステムなどほとんど存在しません。情報を守るためには、重要なデータベースへのアクセスを最小限にすることが重要です。特

に、Web を通じた公衆インターネットからのアクセスには注意が必要です。メインのデータベースからエンドポイントにデータをコピーしている場合には、それを考え直す必要があります。

Dark Reading が 2013 年に起きた 4 つのデータ流出事件をピックアップして記事にしており、大変役に立ちます: http://www.darkreading.com/database/lessons-learned-from-4-major-data-breach/240164264.

Commtouch が 11 月だけで 34 万個もの悪意のある Web サイトを新しく発見

Proofpoint のパートナーである Commtouch の Security Lab が 11 月に 343,972 個の新しい悪意のある Web サイトを発見しました。彼らの発見の詳細は以下のブログ記事に列挙されています: https://blog.commtouch.com/cafe/miscellaneous/343927-new-malicious-sites-commtouch-security-number-of-the-month-for-november

ThreatInsight Blog (ブログ)

今月から新しいセクションが始まります。Proofpoint の新しいセキュリティ情報サイトである ThreatInsight のブログ記事から、興味深い記事をピックアップします。皆さんも是非、ThreatInsight に登録してディスカッションに参加して下さい: http://www.proofpoint.com/threatinsight

「Whatsapp」マルウェア攻撃が Nuclear エクスプロイトを利用

モバイルメッセージングアプリの WhatsApp ブランドを餌に使ったマルウェア攻撃がこの数週間続いています。この攻撃が注目されるのは、Nuclear エクスプロイトキットを使っており、GeoIP データベースを使ったカスタマイズを行い、さらに攻撃方法にいくつかのバリエーションを持っていることです。

全文をこちらでご確認下さい: http://www.proofpoint.com/threatinsight/posts/malware-campaign-that-says-whatsapp-goes-nuclear.php

ホリデーシーズンのため、攻撃が増加 - しかし、ユーザーはクリックするでしょうか？

マルウェア攻撃のうちで最も効果的なもののひとつとして、有名小売業者のオンラインショップからの「注文確認」や「お買い物の内容」などを装ったものが挙げられます。ホリデーシーズンとクリスマス向けのショッピングシーズンに際して、私たちは 2013 年に観測された攻撃の中から、今後 6 週間程度、北米、欧州、アジアなど全ての国において増加しそうなものを見直してみることにしました。

詳細はこちらでご確認下さい: http://www.proofpoint.com/threatinsight/posts/holiday-shopping-season-equal-more-threat-campaigns-but-will-users-click.php

医療制度改革が新たなウォータリングホール型攻撃を誘発

年末が近づき、オバマケアが効果を発揮し始めています。Proofpoint はヘルスケア関連のサイトが次々に侵害され、マルウェアの配信をしているケースを観測しています。

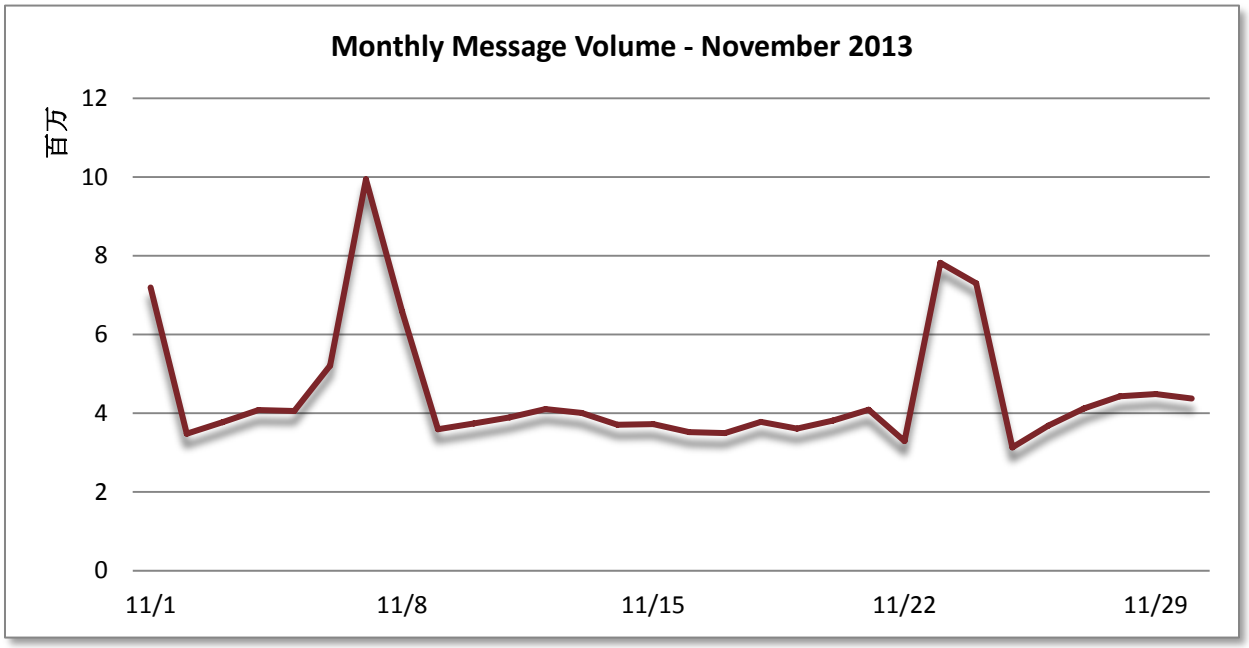
私たちの研究チームは過去 90 日間、私たちのサンドボックスで悪意があると判定された数百万の URL 全てを調査し、ヘルスケアに関連するものを抽出しました。その後それらの URL の中からスパム攻撃の一貫として侵害されたドメインや、あからさまな SEO サイトを除き、ウォータリングホール型の攻撃のためにマルウェアのホスティングを行っているサイトを特定しました。過去 90 日間の間マルウェアを配信していた 43 ドメインが残りました。「accesshealthsystems.co」や「advancemedicals.com」などのドメインを含みます。

詳細はこちらでご確認下さい: http://www.proofpoint.com/threatinsight/posts/healthcare-reform-also-driving-up-watering-hole-attacks.php

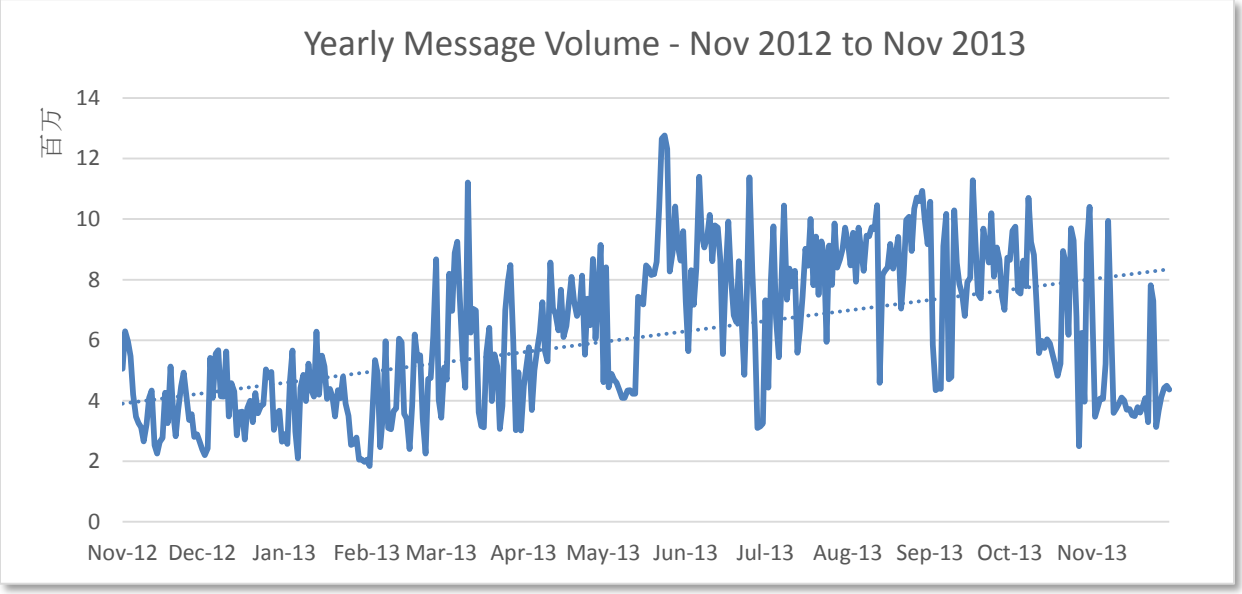
Threat Trends (トレンド)

Spam Volume Trends (スパム量のトレンド)

Proofpoint ではスパム量を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。11 月の 1 日当たりのスパム量は 10 月に比べて激減しました。10 月と同様、1 日当たりのスパム量の変動は大きく、1 日当たり 300 万通から 1,000 万通までにわたります。スパム量は月初にピークを迎えますが、その後急減し、中旬にかけて鍋底のようになります。日付毎のスパム量も減っており、10 月 30 日には 9,209,685 通だったスパムが 11 月 30 日には 4,373,549 通と 52%も減っています。



前月比のスパム量も 10 月に引き続き減少しており、11 月は 38.71%の減少でした。スパム量は 3 ヶ月連続で減っており、3 ヶ月前に比べて 58.53%減少しました。この減少により、その前に増えた分が相殺されています。1 月に比べて 10 月のスパム量が 47.37%増えていとを思い出して下さい。最新のデータではこの増加幅は 6%と、1 桁になっています。この傾向はもしかすると、通常のスパムからはえ縄型のようなより収益性の高い攻撃へのシフトの前兆なのかもしれません。



Spam Sources by Country (スパム発信源)

11 月、スパム発信源トップ 5 が少し変わりました。EU は引き続きトップですが、その他の順位は全て変わっています。中国が 5 位から 2 位に浮上しました。アメリカは 3 位に後退し、なんと日本が 4 位に入りました。日本がトップグループに入るのは初めてです。インドは 5 位に下がりました。以下のテーブルは過去 6 ヶ月間の順位です。

		June '13	July '13	August '13	September '13	October '13	November '13
Rank	1st	European Union (EU)	EU	EU	EU	EU	EU
	2nd	United States (US)	US	US	US	US	China
	3rd	Taiwan	India	Argentina	India	India	US
	4th	Spain	Taiwan	India	Argentina	Argentina	Japan
	5th	China	Argentina	Taiwan	Taiwan	China	India

以下の表は各国が総スパム量に占める割合を示したものです。EU は引き続き 1 位ですが、スパム量は前月に比べて減少しました。中国はスパム量を 300%以上増やして 12%を超えました。

October 2013			November 2013		
1	EU	18.69%	1	EU	13.97%
2	USA	6.68%	**2**	China	12.22%
3	India	4.09%	**3**	US	7.26%
4	Argentina	3.93%	**4**	Japan	3.37%
5	China	3.68%	**5**	India	3.33%

For additional insights visit us at
www.proofpoint.com/threatinsight

proofpoint

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