proofpoint

Proofpoint Threat Report

July 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)

Malvertising (悪意を持った広告)

Online Trust Alliance (OTA) は Malvertising を「悪意のあるコード、またはマルウェアを仕込んだ広告を正規の広告ネットワークに流す攻撃手法」と定義しています。Malvertising は非常に気づきにくい攻撃方法です。よく知られたサイトや信頼されているサイトに掲載されているのは「安全な」広告だと一般には思われています。しかし、実際には一部の広告にはマルウェアが仕込まれており、ユーザーはそれと気づきません。サイトにアクセスするだけで、ドライブバイダウンロードによって感染してしまったり、知らないうちに悪意のあるサイトにリダイレクトされてしまったりするのです。

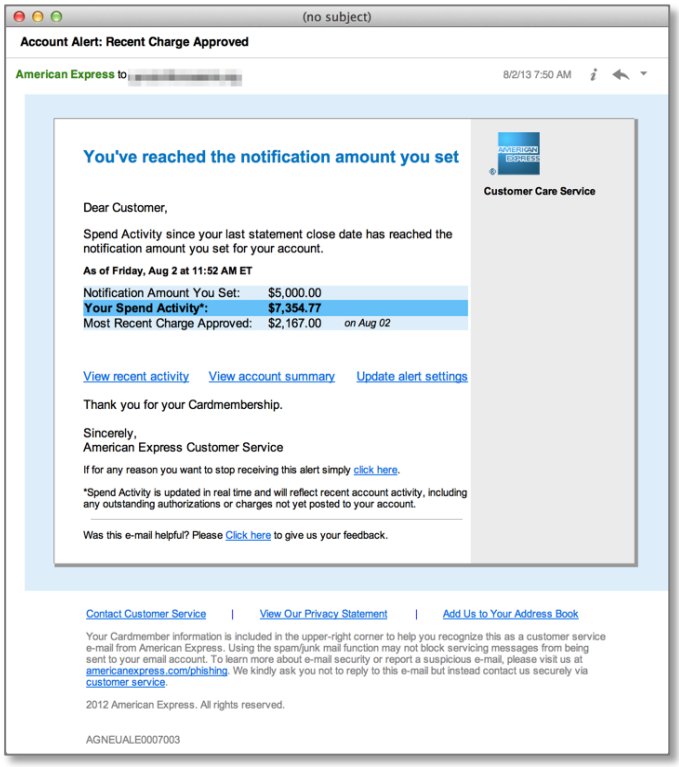
Malvertising を検知するのは非常に困難です。通常、広告はサイト内や複数のページ間で交互に表示される場合が多く、エンドユーザーもほとんど注意を払わないため、フォレンジック上の痕跡がほとんど、あるいは全く残りません。

一方で Malvertising は至る所に入り込んでおり、OTA は 2012 年だけでも 100 億 (10Billion) 件もの広告インプレッションが侵害されていたと見積っています。つい最近も、Proofpoint の研究者は New York Times によって配信されている Malvertising 攻撃を確認しました。

しかし、前述したような数値を見れば、New York Times のような信頼性の高いサイトでもこのようなことが起こることはある程度予見できることです。広告の配信元を見るとさらに驚きは増します。この広告は Google の広告ネットワークで配信されていたのです。これらを考え合わせると、攻撃者が得た広告の露出とインプレッションは膨大なものとなるでしょう。Proofpoint Targeted Attack Protection はこのような攻撃にも効果があります。

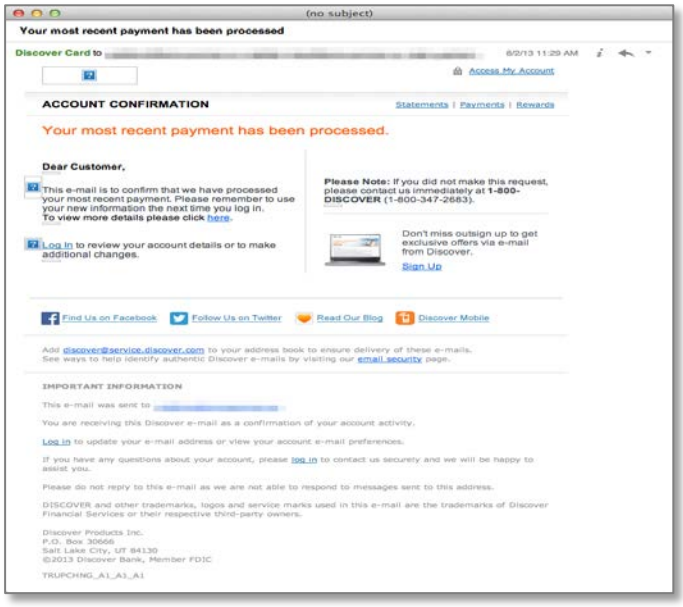
Credit Card Longlining Attacks (クレジットカードブランドを使った「はえ縄型攻撃」)

American Express と Discover Card のブランドを利用したはえ縄型攻撃が確認されました。

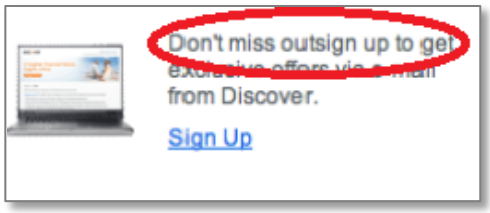


Proofpoint は 2013 年 1 月の Threat Report ではえ縄型攻撃 (Longline phishing attack) を定義しました。(詳しくはこちらのホワイトペーパーをご覧ください)。はえ縄型攻撃には以下のような 3 つの特徴があります。1) 全体としては大規模だが、個々の組織にとっては少ないボリュームの攻撃 2) 難読化と個別化技術の積極的な活用 3) 未パッチのエクスプロイトを狙ったマルウェアペイロード。

これは非常に成功した攻撃で、クリック率は 24%に上りました。この攻撃の詳細もまた興味深いものです。餌となるメールは、極めて作り込まれており、スペルミスなどもありません。American Express のケースでは、メッセージは複数の URL を含んでおり、メールの内容と目的などから、多くのユーザーが騙されてクリックしてしまいました。



この攻撃では、Discover ブランドを使った餌も使われました。一見 AMEX と同様によく作り込まれたものに見えますが、詳しく見てみるとスペルや文法のミスがあります。



この攻撃では 8,555 個の IP アドレスから 3,040 の送信者アドレスを使って 159,147 通のメールが送られました。

そして、87 個の侵害されたサイトと 916 個のユニークな URL が使われています。

Proofpoint が確認した URL パターンは以下のようなものです:

http://<compromised website>/<random dictionary word>/index.html

例えば、1 回の攻撃で 1 台の侵害されたサーバーが持つ URL は以下のものでした。

http://www.urmel-kinderladen.de/baronial/index.html
http://www.urmel-kinderladen.de/centrifuging/index.html
http://www.urmel-kinderladen.de/chug/index.html
http://www.urmel-kinderladen.de/disenchants/index.html
http://www.urmel-kinderladen.de/foldaway/index.html

各々の URL が index.html という一般的な名前で終わっていることに注目して下さい。

前に述べたように、この攻撃では 24%という高いクリックレートを達成しており、非常に成功した攻撃と言うことができます。餌となるメールは 8 月 2 日の金曜日に配信されましたが、ほとんどのクリックは 8 月 3 日の土曜日に起こっており、月曜日まで続いています。週末のクリックは全部では無いにしろほとんどが自宅やコーヒーショップなど、企業ネットワークの外側で起こっていると考えることができます。このようなパターンはよくあることで、ユーザーが企業ネットワークの内側でも外側でも、保護されるようにしなければなりません。Proofpoint Targeted Attack Protection なら、このような場合でも効果的にユーザーを保護することができます。

Threat News (ニュース)

Backdoors via Image Files (イメージファイルを使ったバックドア攻撃)

攻撃者が、侵害したサーバーの制御を維持するために、既知ではあるもののほとんど使われないエクスプロイトを使っていることを Sucuri の研究者が突き止めました。イメージファイルのヘッダーにバックドアを隠すもので、ブログ用プラットフォームとして知られる WordPress やその競合の Joomla を使っているサイトが狙われます。イメージファイルのヘッダーは「POST を使って送られてきたコンテンツを実行する機能」をリモートで実行させるよう変更されています。この手法を使い、攻撃者はコマンドを実行させるか、リモートに置かれたシェルスクリプトを呼び出して実行させることができます。詳細は CSO Online のサイトでご覧いただけます。

http://www.csoonline.com/article/736622/attackers-embedding-backdoors-into-image-files

Another Type of Attack: Watering Holes (ウオータリング ホール型攻撃)

ウオータリング ホール型攻撃 (社交的集まりの場所を悪用した攻撃) は、ユーザーが業務上よく見るサイトや、ジャーナリズムなど特定の職業に従事するユーザーのためのサイト、あるいは個人的な興味の対象となるサイトを使って行われます。実世界と同様に、攻撃者は標的がいつかはそのサイトにアクセスしてくるのを知っており、そこで待っているのです。ユーザーが侵害されたサイトにアクセスすると、知らぬ間に悪意のあるホストにリダイレクトされるのです。

以下の記事では、RSA の研究者がそういったサイトにアクセスしたユーザーのうち 12%が攻撃にあったことを発見たと伝えています。

http://www.infosecurity-magazine.com/view/28450/the-voho-campaign-gh0st-rat-spread-by-waterholing

Interactive Infographic – World's Biggest Data Breaches (データ流出を可視化する対話型のインフォグラフィック)

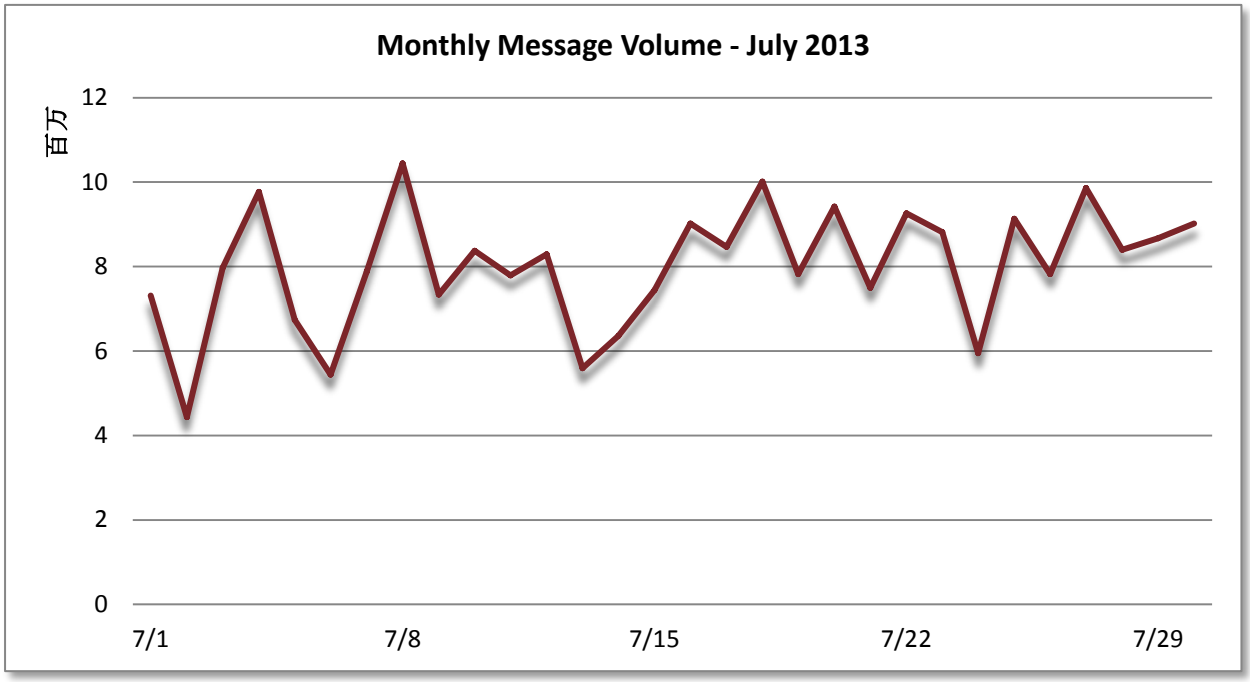
データ流出はセキュリティ侵害の別の側面です。毎日、様々な組織がエンドユーザー、顧客あるいは患者のデータを流出させたニュースが報じられます。こういったデータ流出事故の全体のボリュームを把握するのは非常に困難です。インフォグラフィックスの紹介サイトである「Information is Beautiful」のチームはデータ流出に関するインフォグラフィックスを公開しています。このサイトはインタラクティブで、様々なフィルターを備えており、バブルをクリックすると各データ流出の詳細が表示されます。

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

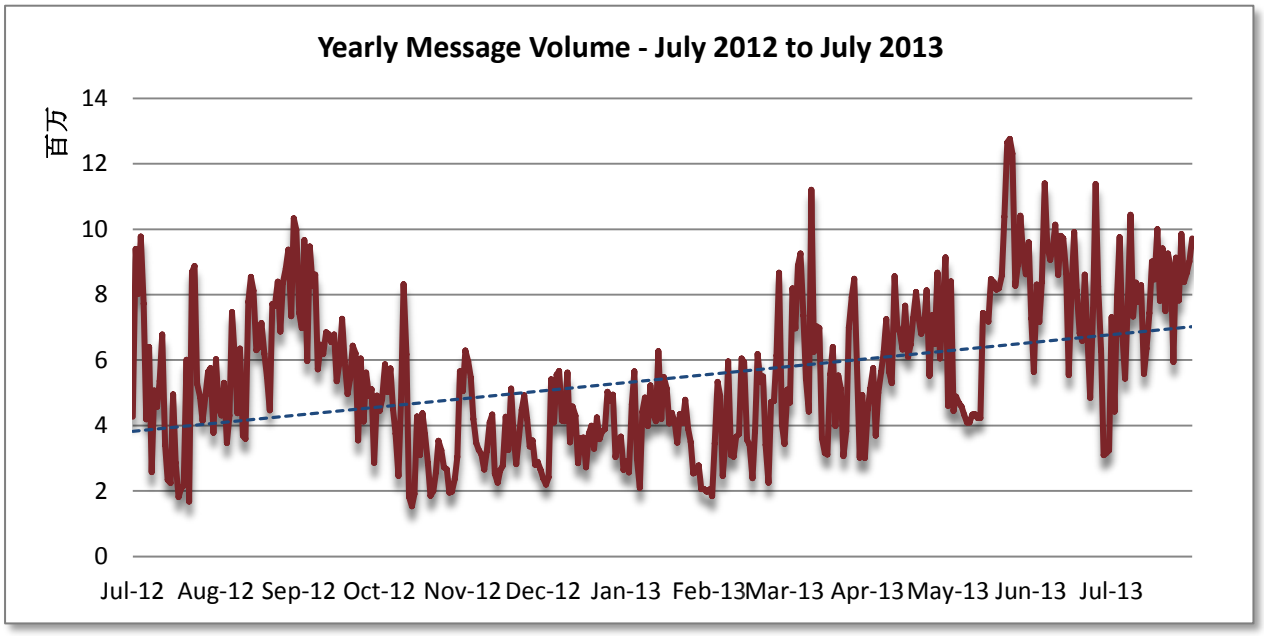
Threat Trends (トレンド)

Spam Volume Trends (スパム量のトレンド)

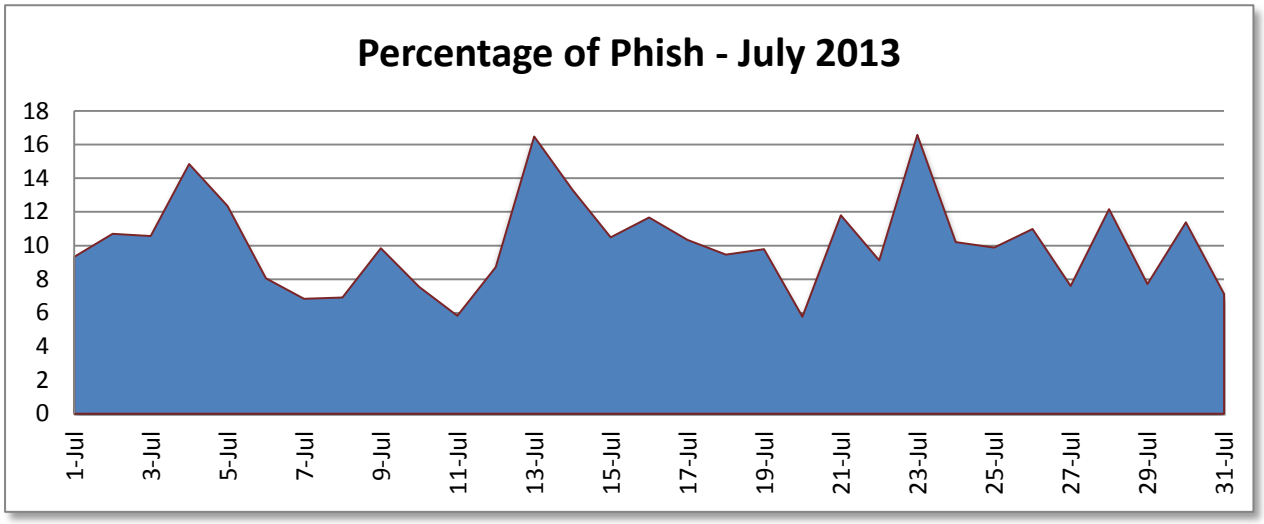
Proofpoint ではスパム量をハニーポットシステムとお客様からのデータを使って観測しています。スパム量は 7 月にまた増加しました。1 ヶ月を通じて不安定な動きを見せた 6 月とは違い、7 月は増減の幅はそれほど大きくはありませんでした。ハニーポットで観測されたスパム量が一日当たり 1,000 万通を越えるかそれに近かったピークは 4 回ありました。各々のピークは下のグラフでご確認いただけます。



7 月は 1 年を通じたスパム量の最高値を更新しました。昨年の 7 月に比べ 60.51%の増加で、ここ 2 年では最大の前年同月比増加量です。スパム量は 2013 年の初めに比べ、109%も増加しました。今後も増加傾向が続くと見られます。



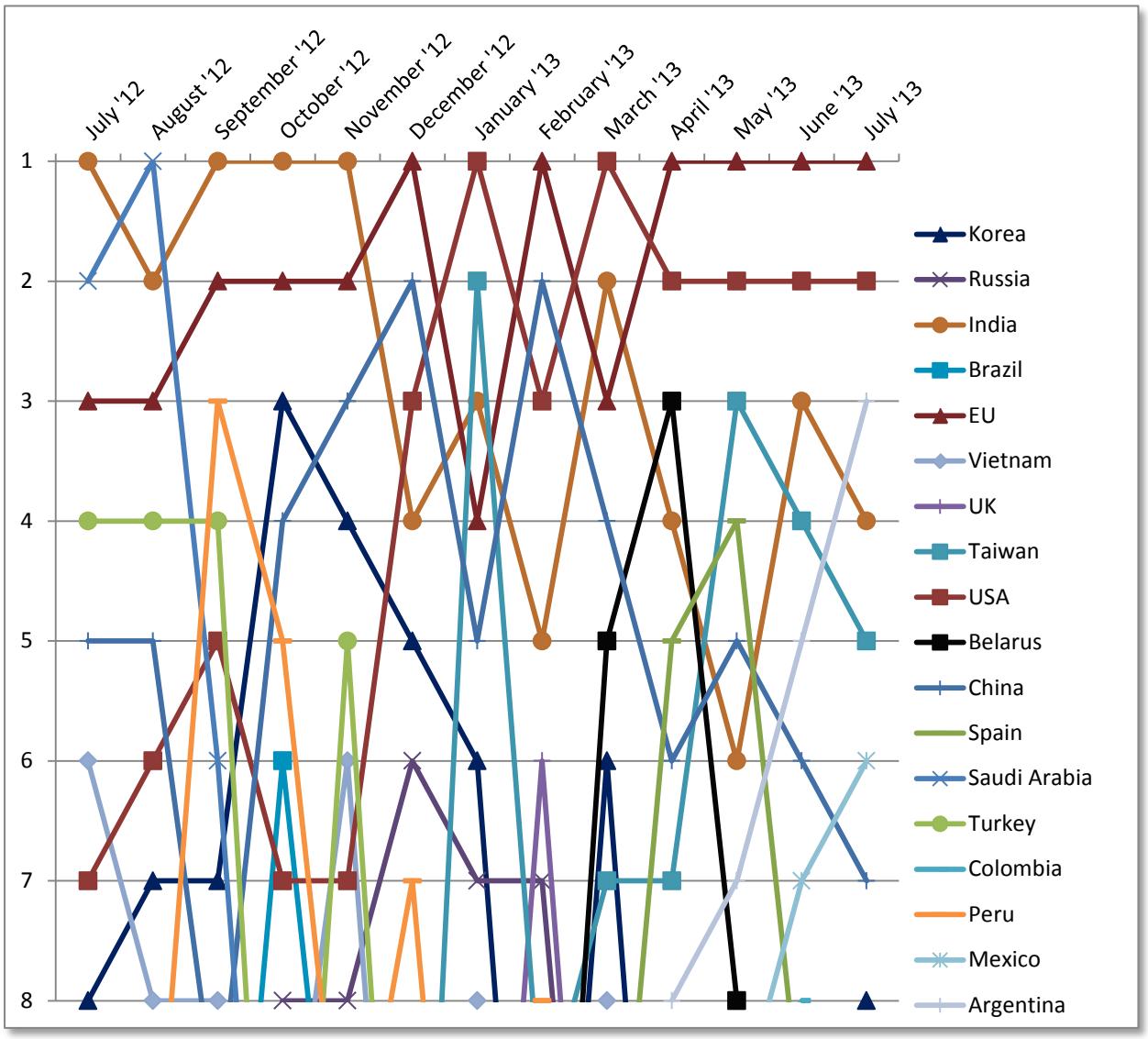
Phish Classification Trends (フィッシング分類のトレンド)



Proofpoint MLX によってフィッシングに分類されたメッセージの割合は引き続き減少傾向にあります。6 月同様、7 月には 3 つのピークがあり、最大のものは 23 日の 16.57%でした。一方で 6 月の 3 つのピークのうち 2 つは毎日のメッセージ量のうち 18%に達していました。毎日のメッセージ量のうちスパムに分類されたメッセージの割合の 7 月の平均は 10.11%で、6 月に比べ 2.5%低下しました。

Spam Sources by Country (スパム発信源)

7 月も EU がスパム発信源としてトップに位置づけられました。アメリカは 2 位です。この 4 ヶ月間、1 位と 2 位が変わっていないことになります。アルゼンチンが順位を 2 つ上げて 3 位に入りました。以下のグラフはスパム発信量上位の国の過去のトレンドを月ごとに示したものです。



下の表は 6 月と 7 月のスパム発信量（総数に対しての割合）の上位 8 カ国です。

June 2013			July 2013		
1	EU	15.88%	1	EU	17.76%
2	USA	5.71%	**2**	USA	7.05%
3	India	5.38%	**3**	Argentina	5.19%
4	Taiwan	5.01%	**4**	India	4.31%
5	Argentina	4.58%	**5**	Taiwan	3.80%
6	China	3.53%	**6**	Mexico	3.37%
7	Mexico	3.29%	**7**	China	3.14%
8	Columbia	2.75%	**8**	Korea	3.02%

proofpoint™
日本プルーフポイント株式会社
東京都千代田区麹町 3-5-2 ビュレックス麹町
www.proofpoint.co.jp