proofpoint

Proofpoint Threat Report

August 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)

複数のはえ縄型攻撃を確認

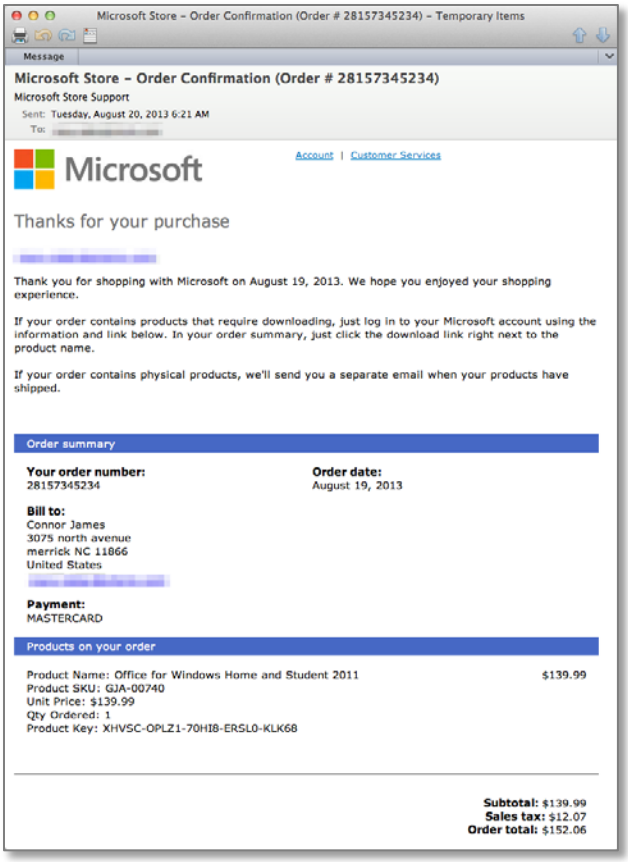
Proofpoint の研究チームは 8 月中、複数のはえ縄型攻撃を観測しました。新たな攻撃である「はえ縄型攻撃」については Proofpoint が今年始めに定義し、2 月の Threat Report でお知らせしました。はえ縄型攻撃の特徴は以下のとおりです。(はえ縄型攻撃についての詳細はホワイトペーパーをご確認下さい)

1. **狙われた組織毎には比較的少量だが、全体としては大量の攻撃:**
   個々の企業が受け取る攻撃メールの量はその企業の受信メール数全体の 0.1%未満と、高度な標的型攻撃ほどには絞り込まれていませんが、一般的な攻撃に比べると非常に少ないと言えます。このため従来型のセキュリティソリューションでは検知しにくいのです。しかし、はえ縄型は複数の企業を同時に狙うため、攻撃全体で見ると数百万通のメールが数時間のうちに送信されるほどの大きな規模になります。
2. **難読化・カスタマイズ技術を駆使:**
   - 送信元の IP アドレスや偽の送信アドレスを頻繁に変更しながら送信
   - 数十もの侵害されたサイトがマルウェアを配信
   - ハッシュ値を変えるために一部の単語を変えたり、標的となる企業や送信時間に合わせて件名や本文を変えるなど、**メール毎に内容を変更**

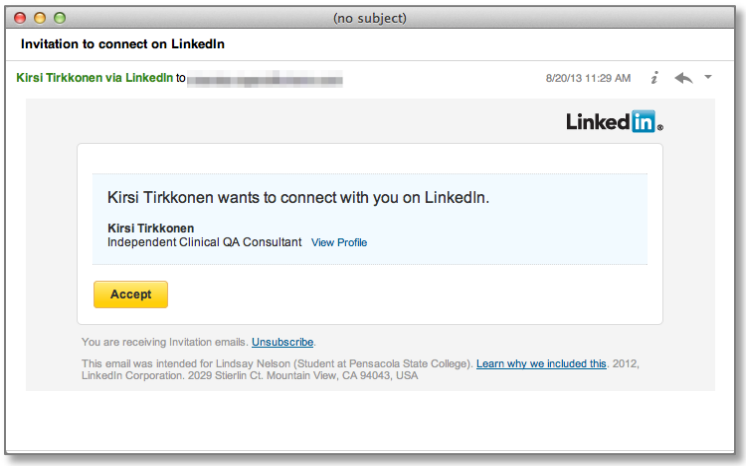
- **URLの頻繁な変更とリンク先の偽装** (HTMLにリンクを埋め込んで偽装したり短縮URLを使うなど)

3. **ゼロデイエクスプロイトを狙うマルウェアペイロード**
   はえ縄型攻撃で使われるフィッシングメッセージは、まだパッチがリリースされていないセキュリティホールを狙うマルウェアや、発見されたばかりでパッチがまだ当てられていないと考えられるセキュリティホールを狙うマルウェアを使います。

最初の攻撃例では Microsoft の名前を騙り、Microsoft Store の偽の領収書を使っています:

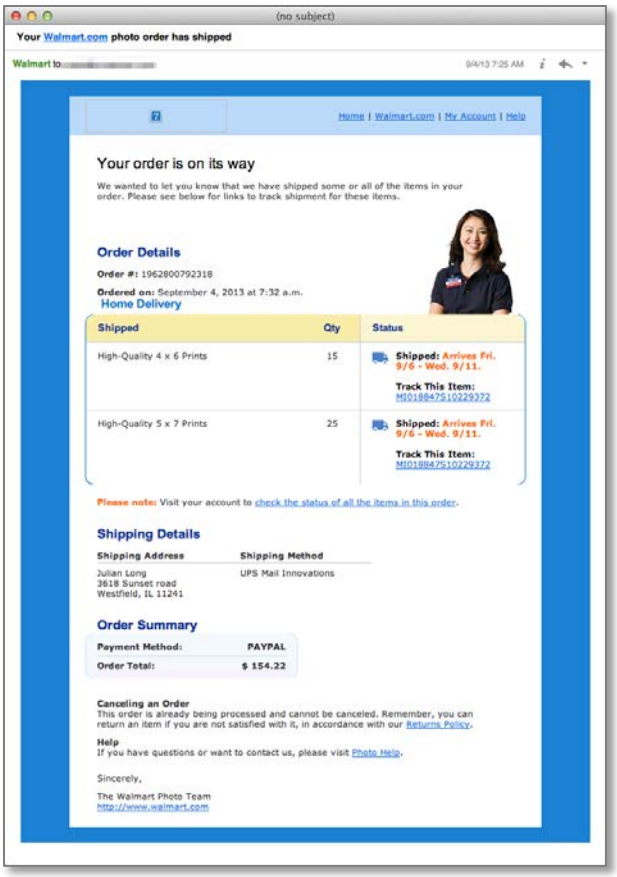


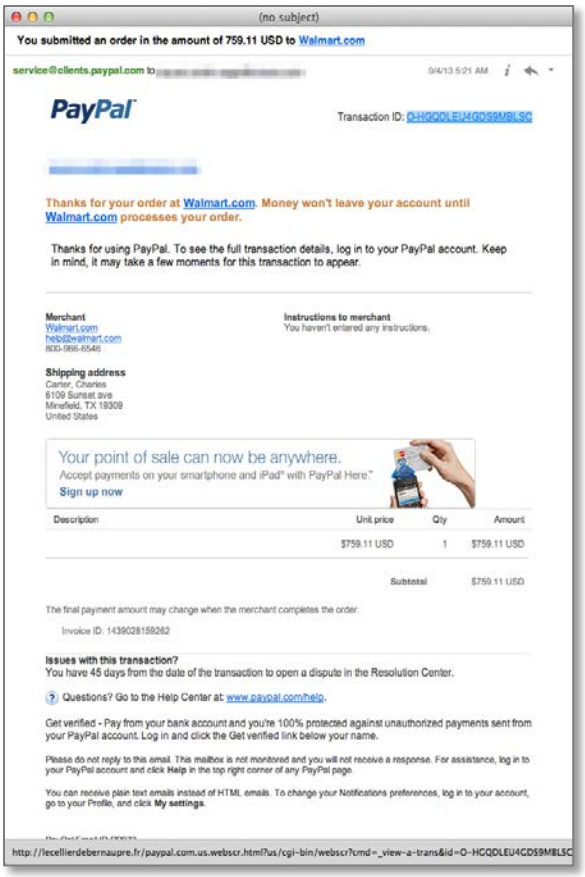
この攻撃で使われたマルウェアは Blackhole エクスプロイトキットのインスタンスから配信されています。



次の攻撃は、餌として人気がある LinkedIn が使われたものです。メッセージの一例を示します。
この攻撃では ZeroAccess または Kryptik Trojanmpどちらかが使われます。

3 番目の攻撃では Walmart が使われました。全ユーザーに対し、二つの異なる餌が使われました。





どちらの餌も、同じエクスプロイトキットから作成されたマルウェアを配信します。そのため、これらは同じ攻撃に属するものと判断されました。

Threat News (ニュース)

ロシアで大規模な Viagra スパムのボットネットを発見

ロシア当局者及び最近のモスクワの裁判所の判決から世界最大のスパムボットネットの詳細が明かになりました。Topol-Mailer として知られるこのボットネットは、全世界のスパム量の 1/3 を配信する能力がありました。

Festi と呼ばれる Igor A. Artimovich は中心的なプログラマの一人とされており、彼と他の 3 人は、2010 年の Aeroflot (ロシアの国営航空会社) に対する DDoS 攻撃に関与したとして有罪判決を受けました。これにより、増加傾向にあった世界のスパム量に変化が現れるかもしれません。

New York Times の記事の全文はこちらでご覧頂けます。

http://www.nytimes.com/2013/09/03/business/global/online-attack-leads-to-peek-into-spam-den.html?pagewanted=all&_r=1&

暗号化はデータを守ることができるのか？

スノーデン容疑者による機密文書公開によって新たな事実が明らかになりました。New York Times、The Guardian と ProPublica は、NSA (米国家安全保障局) がインターネット上の暗号化通信を解読可能であると報じました。それによると、NSA は暗号化の強度を弱めるよう規格に干渉し、商用ソフトにバックドアを用意させ、暗号解読を行うなどの 3 つの活動を行っていたということです。
The Guardian の記事では、NSA がどのようにして暗号をクラッキングしていたかを詳細に説明しています。http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

また、ジョンズホプキンス大学の教授であり、セキュリティ研究者の Matthew Green 氏が、この件が及ぼす影響について技術的な観点から検討しています。
http://blog.cryptographyengineering.com/2013/09/on-nsa.html

Botnet が作り出した数百万の Tor クライアント

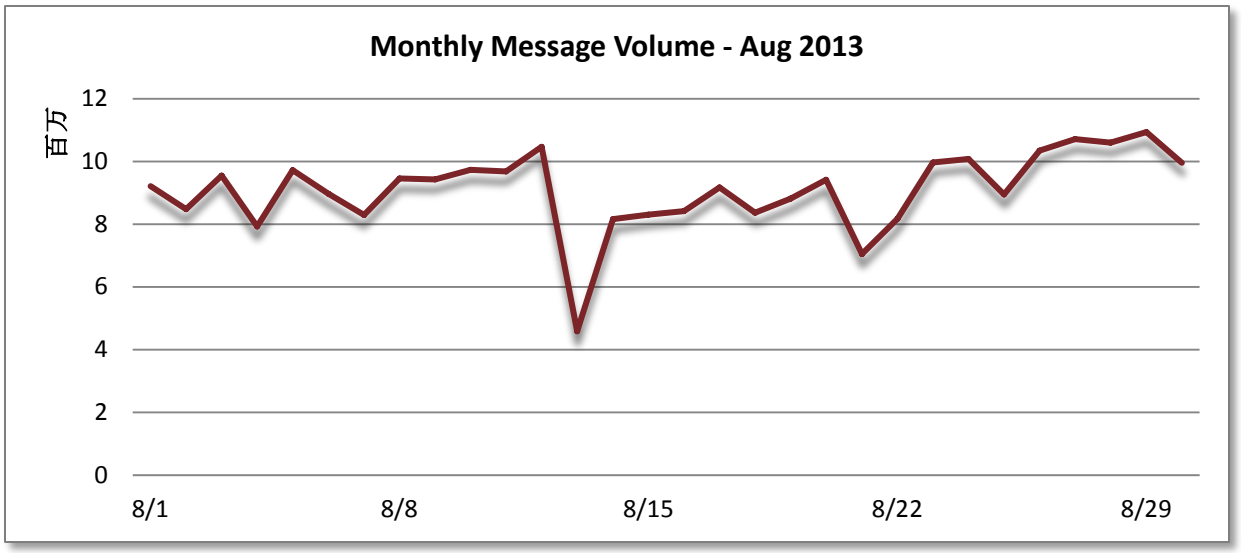
接続経路匿名化システムである Tor のセキュリティ研究者達は、最近急増した Tor クライアントが Botnet によるものであることを突き止めました。第三者機関である Fox-IT の研究者もこれを認めています。
8 月 20 日以降、数百万の Tor クライアントがネットに接続されました。Tor は通信経路を匿名化するシステムであり、世界中のユーザーがインターネットへ接続のプライバシーを守るために利用しています。Tor のプロジェクトリーダーであり初期からの開発者の一人である Roger Dingledine は次のように述べています。「Tor クライアントのこのような急激な増加は、人間によるものとは思えない。」

CSO online で詳細をご覧頂けます。http://www.csoonline.com/article/739174/botnet-likely-caused-spike-in-number-of-tor-clients

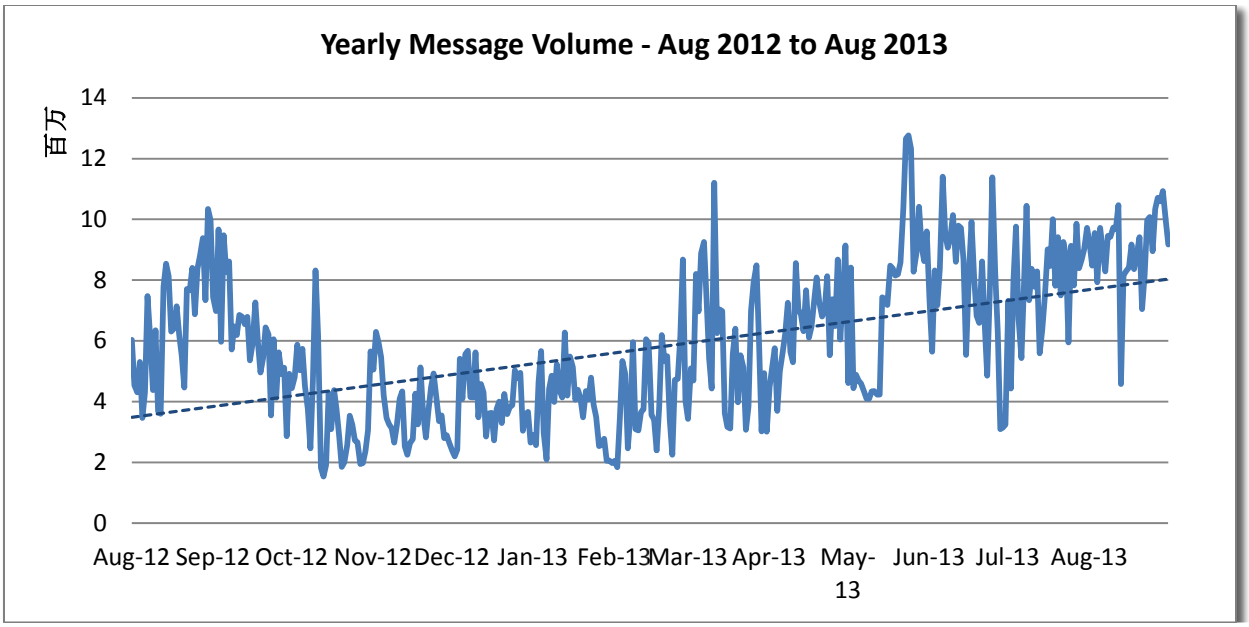
Threat Trends (トレンド)

Spam Volume Trends (スパム量のトレンド)

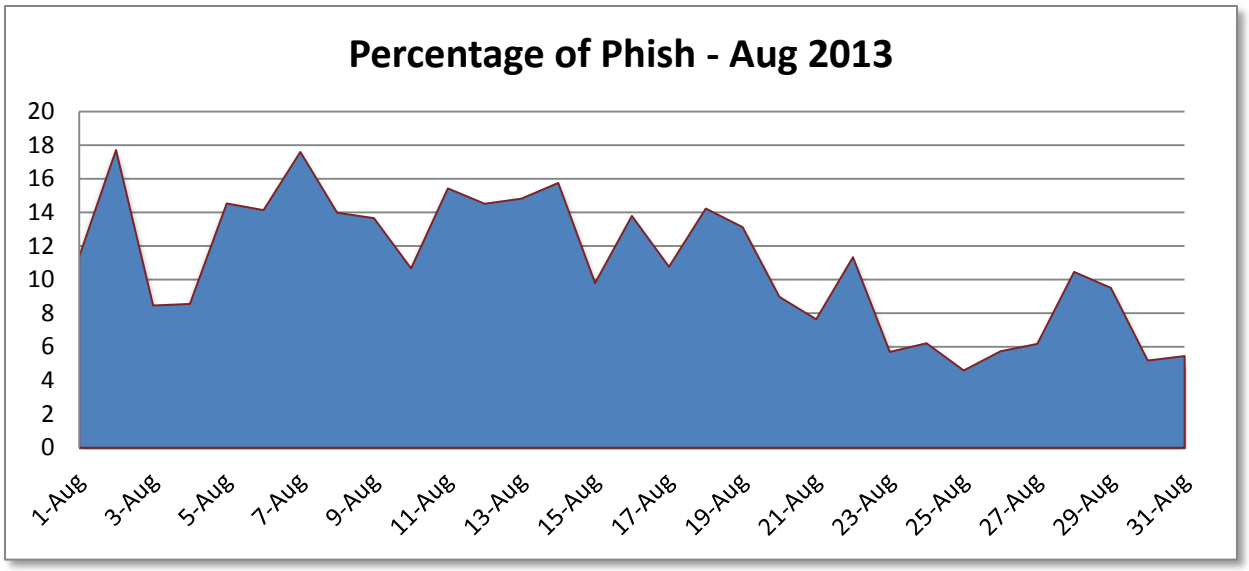
Proofpoint ではスパム量をハニーポットを使って追跡していますが、この値は Proofpoint のお客様からの報告ともほぼ一致します。スパム量 8 月に増加しました。月初の段階で既に通常の月よりも多かったスパム量ですが、12 日には一日当たり 1,000 万通を超え、翌日には突如として半減しました。その後スパム量は月末にかけて増え続け、最後の 5 日間は 1,000 万通を超える日が続きました。



スパム量は引き続き増え続けています。8 月のスパム量は 2011 年 10 月以来のレベルに達しました。7 月から 8 月にかけてスパム量は 12.83%増加し、昨年 8 月からは 37.73%増加しました。強い増加傾向は続いています。



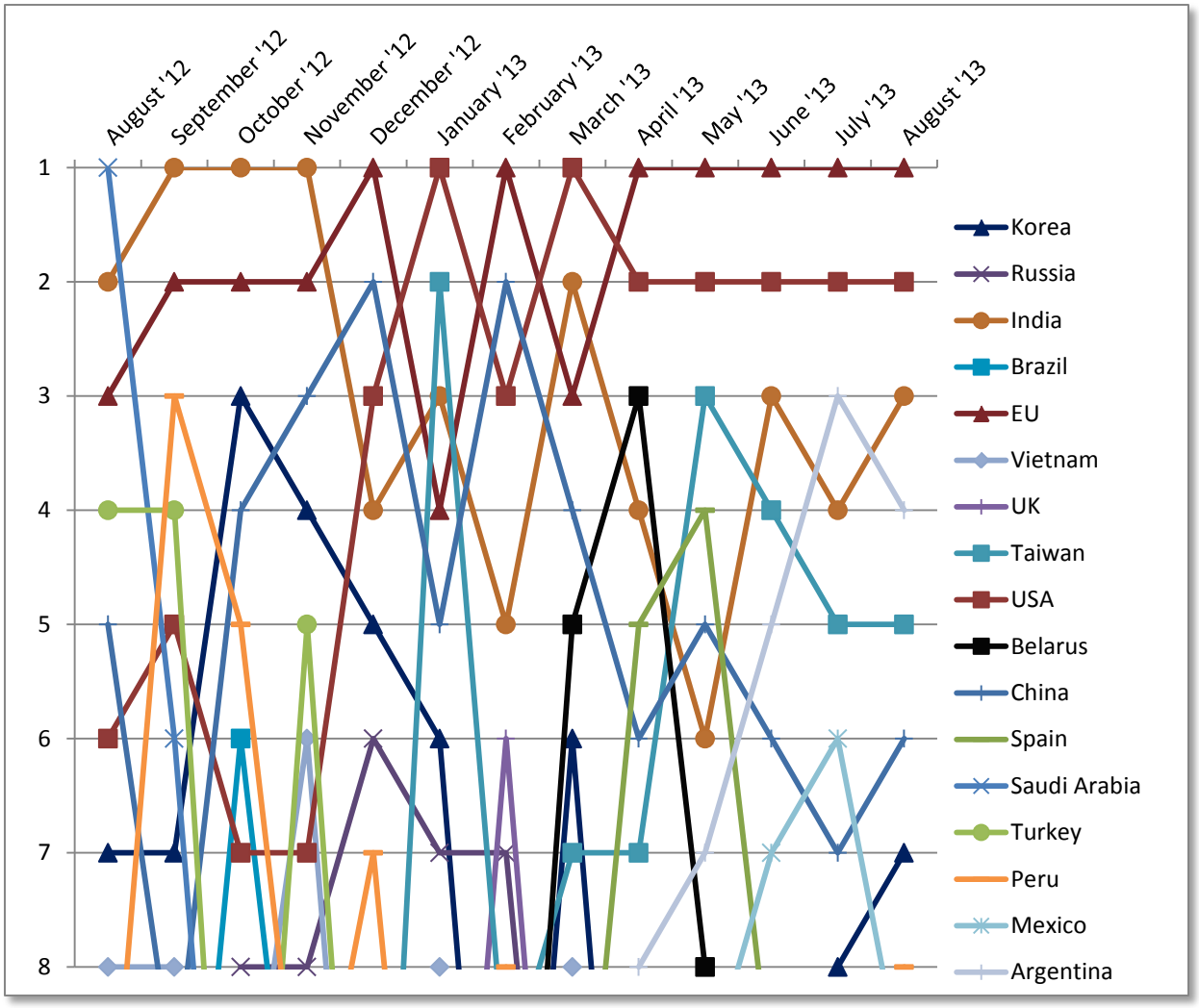
Phish Classification Trends (フィッシング分類のトレンド)



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、これまでの減少傾向に反して増加しました。フィッシングメッセージの割合は前月から 5.77%増加しています。18%近くまで上昇した日が 2 回あり、最高は 2 日の 17.72%でした。平均すると日々のメッセージ全体の 10.97%がフィッシングに分類されており、7 月に比べ増えています。

Spam Sources by Country (スパム発信源)

スパム発信源として EU が今月も首位を維持しました。アメリカも引き続き 2 位です。1 位と 2 位が動かないのはこれで 5 ヶ月連続となりました。インドが第 3 位に返り咲いています。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 7 月と 8 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。

July 2013			August 2013		
1	EU	17.76%	1	EU	16.19%
2	USA	7.05%	**2**	USA	5.79%
3	Argentina	5.19%	**3**	India	5.70%
4	India	4.31%	**4**	Argentina	4.90%
5	Taiwan	3.80%	**5**	Taiwan	3.53%
6	Mexico	3.37%	**6**	China	2.97%
7	China	3.14%	**7**	Korea	2.79%
8	Korea	3.02%	**8**	Peru	2.78%

proofpoint

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