proofpoint

Proofpoint Threat Report

September 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)

Targeted Attacks (標的型攻撃)

本レポートでは、これまでの数ヶ月で 4 種類のマルウェア攻撃のうち、2 つについて解説してきました。2 つとは、マルバタイジング (Malvertising) とはえ縄型 (Longlining) です。今月号では残り 2 つのうち、標的型攻撃 (Targeted Attacks) について解説します。

英語版Wikipediaによると、標的型攻撃は「単一の企業や業界を狙ったマルウェアの種類。機密情報を盗み出す目的で作成されるために大変危険と考えられているクライムウェアのタイプ。標的型攻撃にはSMTPメール、ポート攻撃、脆弱性エクスプロイトによるゼロデイ攻撃およびフィッシングメッセージにより配信される脅威を含む。」[1] と定義されています。また、2013 年版のVerizon Data Breach Investigations Report[2] によると、標的型攻撃の 95%がフィッシングメールを介したものであると言うことで、標的型攻撃への対抗のためにはメールセキュリティが重要であることがわかります。

標的型攻撃は財務データやユーザー認証情報、知的財産権などを盗み出すよう設計されているため、大変危険でやっかいな脅威です。以下、実例を見てみましょう:

[1] http://en.wikipedia.org/wiki/Targeted_attack
[2] 2013 Verizon Data Breach Investigations Report; pg. 36

Targeted Credential Stealing (標的を絞った認証情報の窃取)

Syrian Electronic Army (シリア電子軍) を名乗るハッカー集団は、Associated Press、The Guardian および The Financial Times などのツイッターアカウントの乗っ取りで広く知られるようになりました。彼らの手口は、まず組織内の個人を狙って認証情報を盗み出すフィッシング攻撃を仕掛け、いったん組織内に入り込むとツイッターアカウントの担当者を狙って攻撃を続け、最終的にツイッターの認証情報を盗み出すというものです。

この手口は、今年 4 月に Associated Press への攻撃が広く報道された後でも、魔法のようにうまくいきました。一連の攻撃を時系列にまとめると以下の様になります:

2013 年 4 月
- Associated Press
- The Guardian

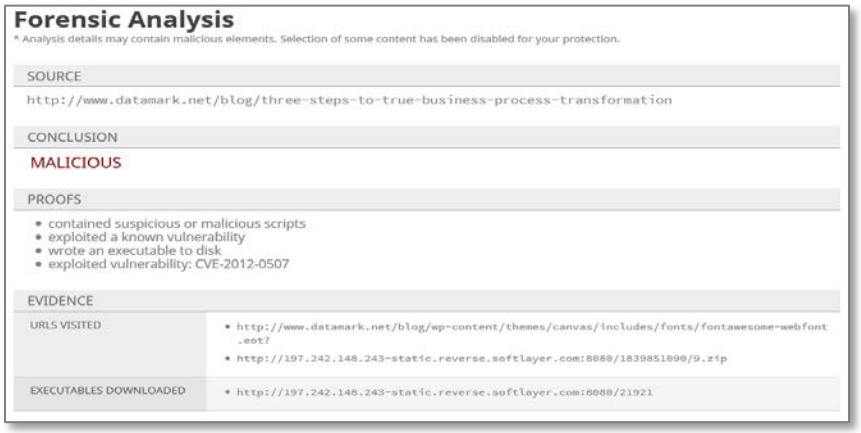
2013 年 5 月
- Financial Times

2013 年 6 月
- The Onion
- Thompson Reuters

全てのケースで、最終的な目的は価値あるツイッターアカウントの認証情報です。これら一連の攻撃が広く報道されたこともあり、ツイッターは 2 要素認証を強化しました。

Targeted Attack with a CVE (共通脆弱性識別子を伴う標的型攻撃)

標的型攻撃は有効性が高く、攻撃者が経済的利益を期待できることから、広く使われる手法となっており、Proofpoint のユーザーでもこれらと無縁ではいられません。しかし、Targeted Attack Protection をご利用頂けば、これまでの防御機構にもうひとつのレイヤーを追加でき、攻撃を受けた場合にも迅速に復旧できるようエンドツーエンドのフォレンジックを得ることができます。以下に Targeted Attack Protection が提供するフォレンジック情報の詳細を示します。



この攻撃は CVE-2012-0507 として知られる Java Runtime の脆弱性を狙ったものです。Mitre.org は Common Vulnerability and Exposures (CVE) でこの脆弱性について「Oracle Java SE 7 Update 2 およびそれ以前、6 Update 30 およびそれ以前、5.0 Update 33 およびそれ以前のバージョンの Java Runtime Environment (JRE) に存在する未特定の脆弱性で、Concurrency サブコンポーネントに関連する未確認の攻撃により機密性、完全性および可用性に影響を与えるリモート攻撃を可能にします。」と説明しています。詳細はこちらから。

あるお客様への攻撃で狙われた肩書きは以下の通りです:

- Chief Science Officer
- Senior Vice President
- Chief Marketing Officer
- Visiting Scientist
- Vice President and Chief Scientific Officer
- Vice President of Business Applications
- Vice President of Tax
- Vice President and Associate General Counsel
- Executive Vice President
- Vice President of Business Technology
- Research Fellow

これらの狙われた肩書きからひとつ言えることは、攻撃者は標的とする企業で高い地位にいる人に関する情報を探しているということです。標的型攻撃という単語は広く使われるようになってきましたが、元々の定義は「単一の企業や業界を狙った…」であり、これまでに見てきたような特徴を持っているのです。

来月は残った最後の攻撃であるウォータリングホール型攻撃 (Watering Hole Attacks) について解説します。

Threat News (ニュース)

FOXACID – NSA 製のエクスプロイトキット

米国家安全保障局 (NSA: National Security Agency) が、狙ったシステムに侵入するために独自のエクスプロイトキットと専用のサーバーインフラを運用していたことが明らかになりました。スノーデン容疑者によって暴露された極秘資料がソースとなっています。Bruce Schneier 氏のブログによると、「コンピュータへの侵入が成功すると、秘密裏に FoxAcid サーバーにコールバックし、標的のコンピュータ上でさらなる攻撃を行って長期間にわたってそのサーバーに滞留し、盗聴した情報を NSA に送り続けます。」ということです。NSA は匿名ルーティングシステムである TOR のユーザーに強い興味を持っており、FoxAcid の主な標的となっています。オリジナルのブログはこちらでご覧頂けます: https://www.schneier.com/blog/archives/2013/10/how_the_nsa_att.html

イギリスの金融界がイングランド銀行から告知を受ける

イングランド銀行金融政策委員会 (FPC: Bank of England Financial Policy Committee) の議事録によると、イングランド銀行はイギリスの銀行およびその他の金融機関に対し、サイバー攻撃に対してどのように防御するかの戦略を 6 ヶ月以内に提出するよう命じました。6 ヶ月という短期間で各機関は戦略的計画を立て、2014 年第一四半期までに提出しなければなりません。FPC はまた、取締役会に年内に進捗状況をレポートするよう求めています。詳しくはこちらから:

http://www.computerweekly.com/news/2240206514/Bank-of-England-and-Treasury-set-banks-cyber-security-deadline

セキュリティ侵害による復旧コストが 2012 年よりも 26%上昇

Ponemon Institute が発表した *2013 Cost of Cybercrime Study* によると、セキュリティ侵害による復旧コストは 2012 年に比べて 26%上昇し、最近 4 年間で 78%も増えたということです。攻撃の洗練度が上がっていることも上昇の原因のひとつです。復旧にかかる時間も長くなっており、昨年に比べて 24 日増え、32 日となりました。Search Security の記事をご覧ください:

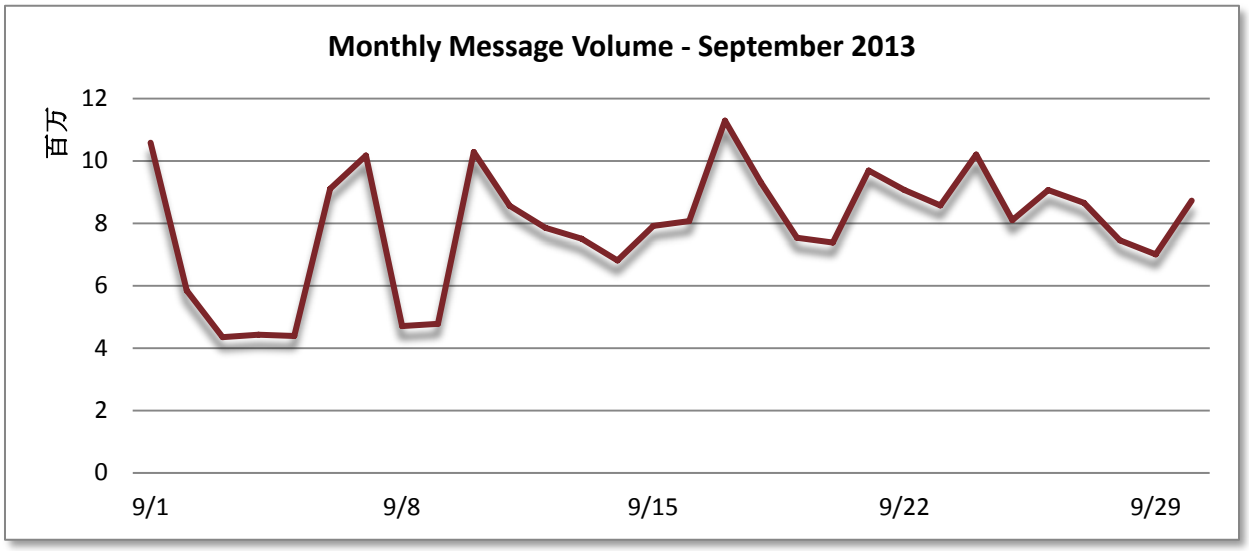
http://searchsecurity.techtarget.com/news/2240206878/Average-cost-of-cybercrime-grows-again-due-to-sophisticated-attacks

Threat Trends (トレンド)

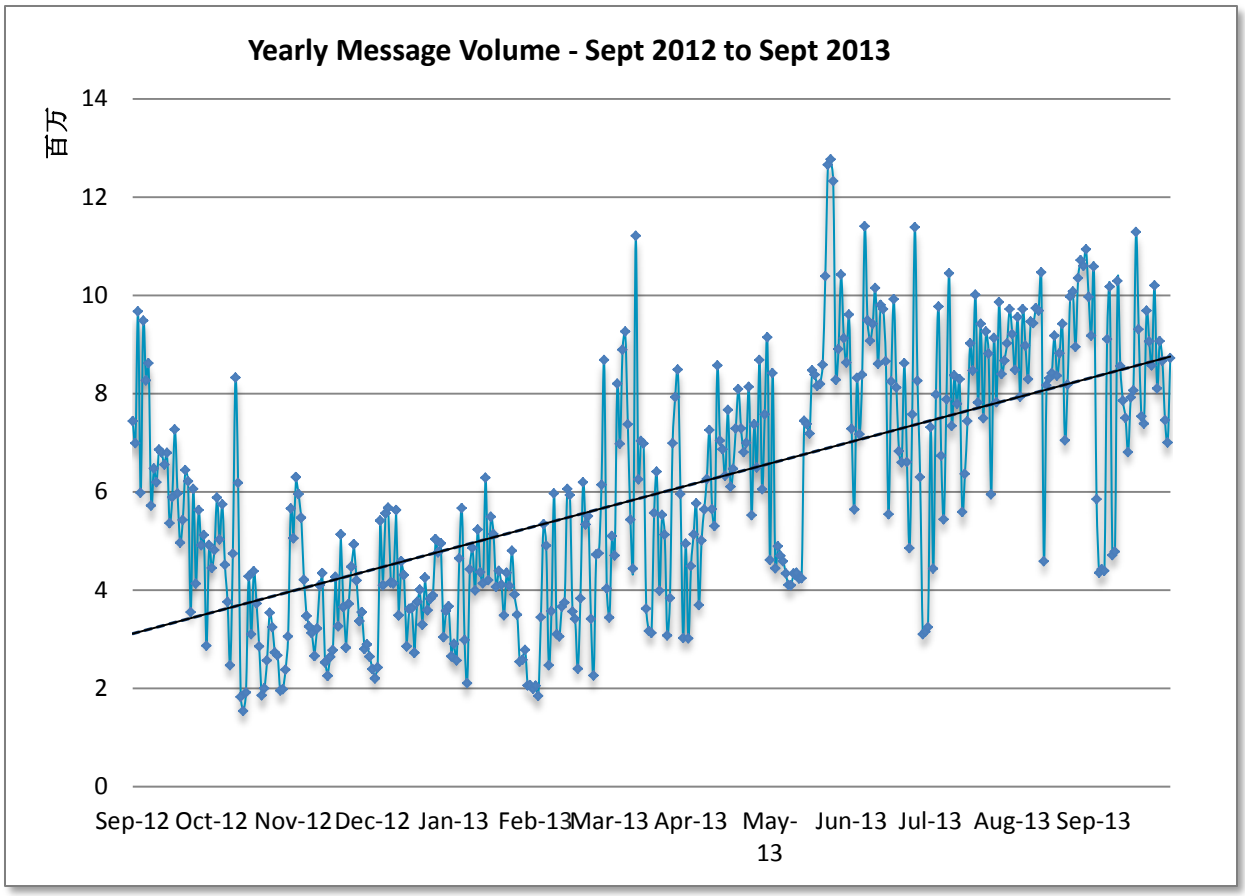
Spam Volume Trends (スパム量のトレンド)

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。グラフからもわかるように、9 月を通して異常な状況が続きました。

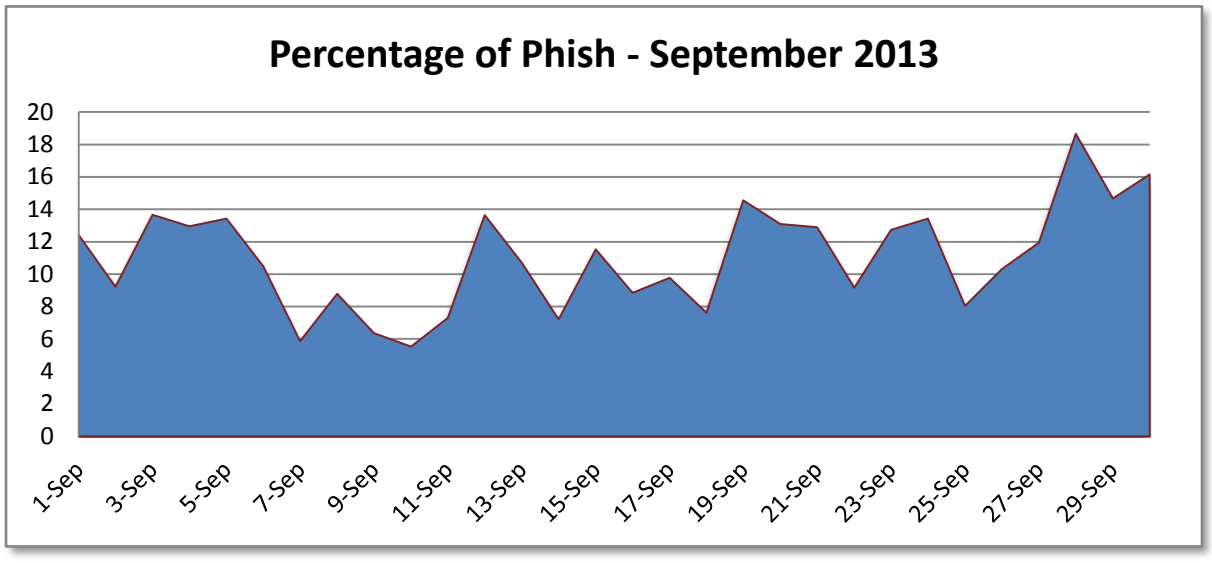
月初に 1,000 万通/日を記録した後に数日間劇的に落ち込み、また増えるという形で、1 ヶ月の間に 1,000 万通のラインを 5 回も越えています。一方で上旬に 400 万通台の日が数回ありました。月末にかけて増減の幅は縮小しました。



全体のスパム量は 1 月以来初めて減少し、7 ヶ月連続の増加に歯止めをかけました。9 月のスパム量は 8 月に比べ 13.05%減少しましたが、昨年比では 27.28%の増加となっており、年ごとの増加傾向は続いています。



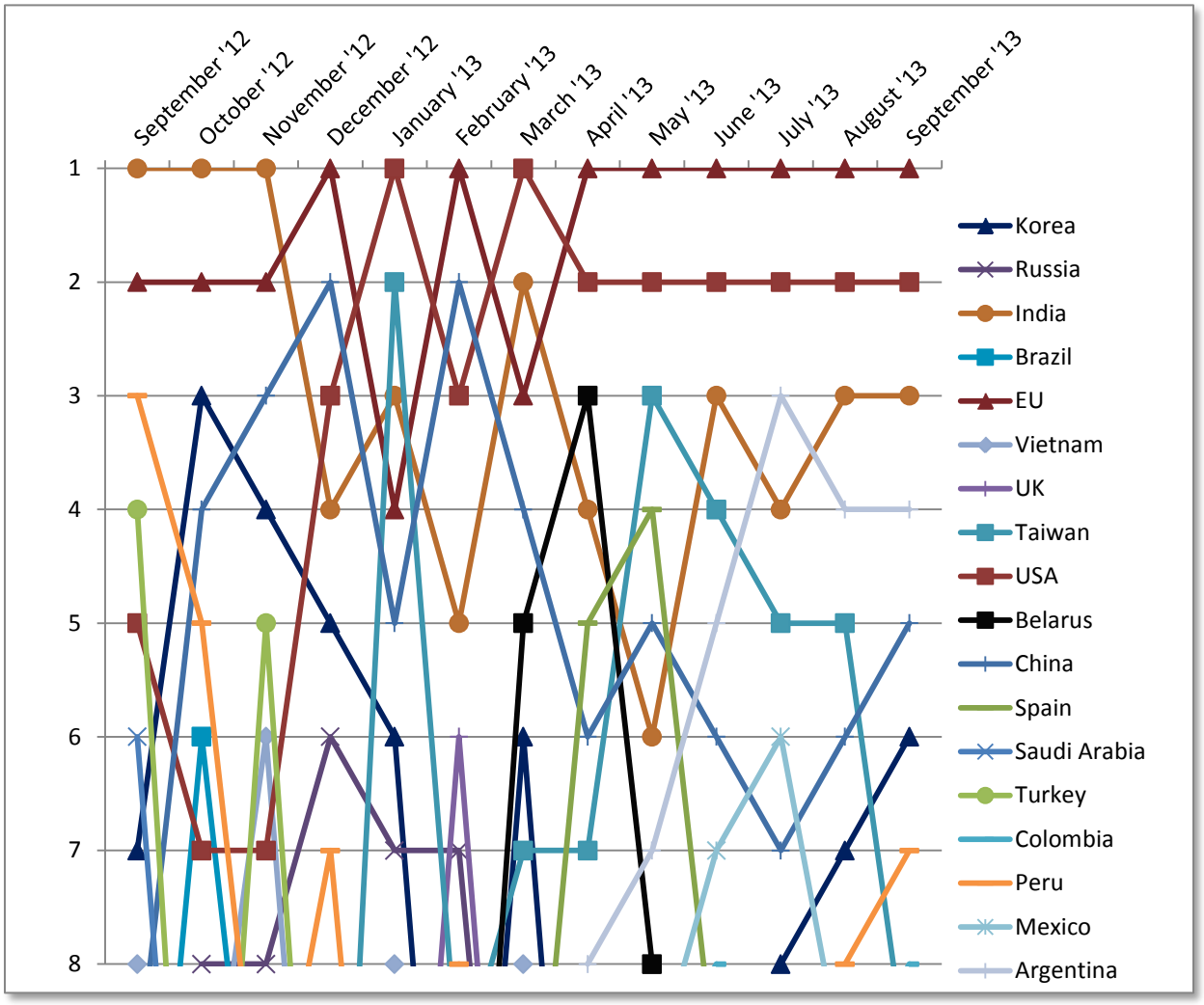
Phish Classification Trends (フィッシング分類のトレンド)



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 8 月と 9 月ではほぼ同水準で、9 月は 8 月に比べて 0.63%の増加でした。平均して毎日のメッセージ数の 11.04%がフィッシングに分類されました。

Spam Sources by Country (スパム発信源)

EU が 6 ヶ月連続でスパム発信量で第 1 位で、アメリカが第 2 位です。インドが 3 位、アルゼンチンが 4 位で安定しています。上位のランキングはこのまま固定するのでしょうか？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 8 月と 9 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。EU が 8 月に比べて 5%増加しました。

August 2013			September 2013		
1	EU	16.19%	1	EU	22.97%
2	USA	5.79%	**2**	USA	6.86%
3	India	5.70%	**3**	India	5.08%
4	Argentina	4.90%	**4**	Argentina	3.96%
5	Taiwan	3.53%	**5**	China	3.75%
6	China	2.97%	**6**	Korea	2.68%
7	Korea	2.79%	**7**	Peru	2.35%
8	Peru	2.78%	**8**	Columbia	2.78%

proofpoint

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