Proofpoint Threat Report

September 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)

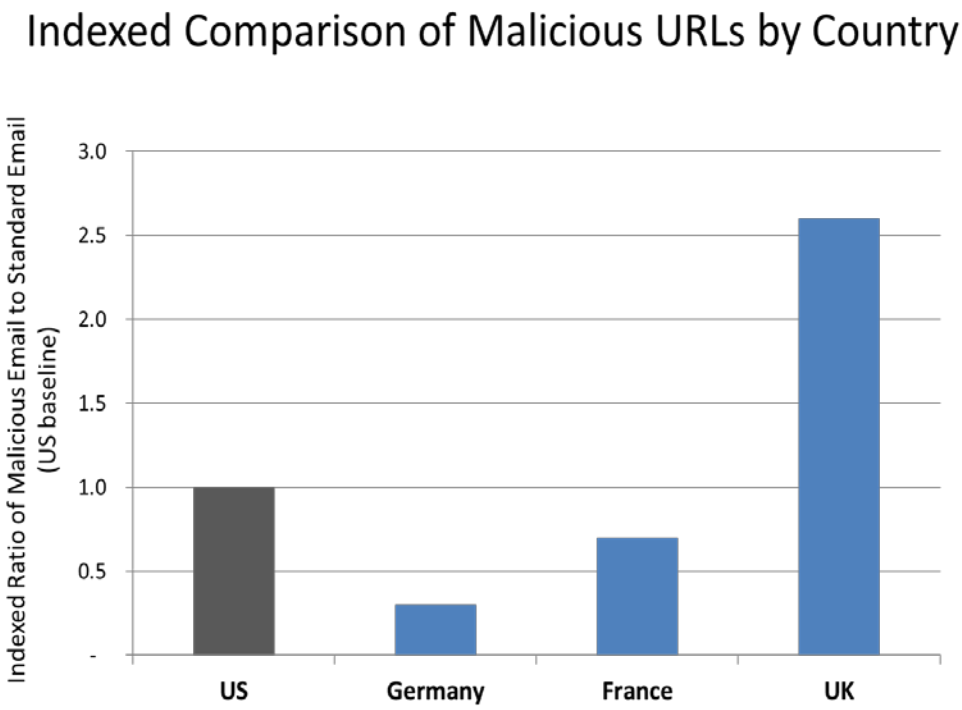
正規のサービスを利用した複雑な攻撃でも TAP なら対応可能

ヘルスケア産業向けにビジネス及び法務情報を提供している Becker's Hospital Review のサイトが侵害され、アクセスした顧客が Sweet Orange エクスプロイトキットにリダイレクトされました。このサイトから大量のメール「ニュース」が配信されましたが、このニュースには、ユーザーのクリック行動を追跡するために、メールマーケティングの Constant Contact (ra6.net) がリダイレクトレイヤーとして使われていました。

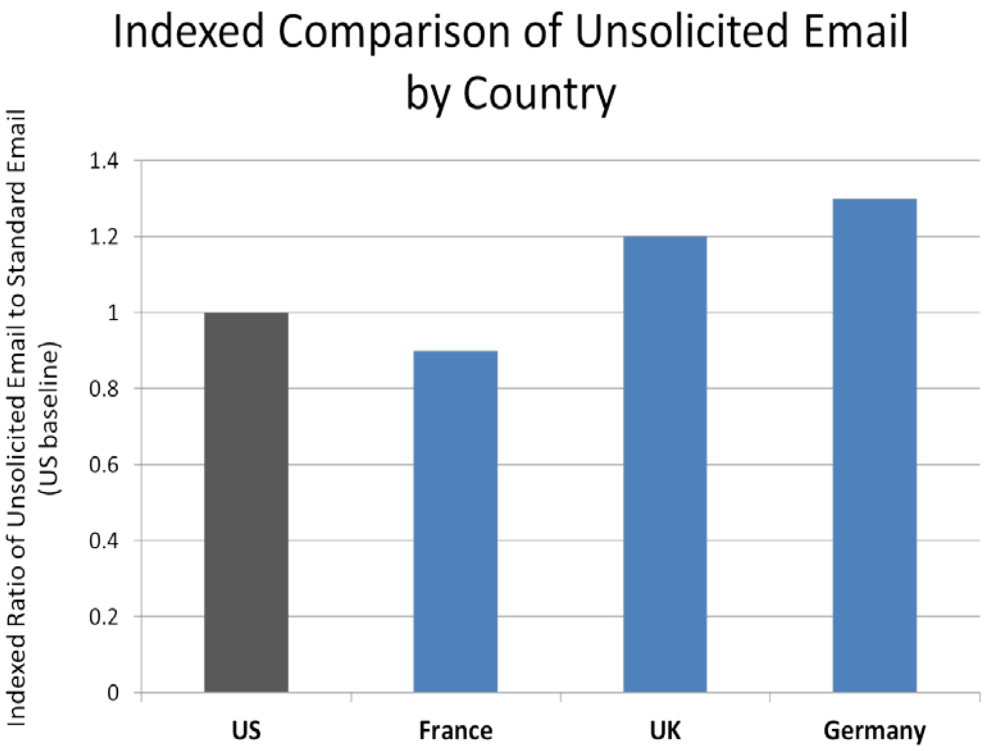
Constant Contact は多くの正規メールの配信に使われており、全てのドメインを一律にブロックするわけにはいきません。しかし、Proofpoint Targeted Attack Protection (TAP)は個別にスキャンを行い、特定の URL のみをブロックし、他はそのまま通過させることに成功しました。

ヨーロッパのフィッシング: 地域間の違いとグローバルな問題

Proofpoint では今夏、アメリカからヨーロッパにかけてのメール脅威を解析しました。その結果、興味深いことが判明しました。イギリスのユーザーに向けて配信された未承諾メールには、アメリカやフランス、あるいはドイツなどに比べて 3 倍の確率で悪意のある URL が含まれていたのです。一方で、フランスとドイツのメールに悪意のある URL が含まれている確率はアメリカに比べても低いものでした。イギリスのユーザーのメールボックスにある未承諾メールが悪意のある URL を含んでいる確率は、ドイツのおおよそ 5 倍でした。



また、Proofpoint の研究者が各国のメール総量に占める未承諾メールの割合を調べたところ、まったく違うパターンが表われました。



フィッシング (及び悪意のあるメールの継続的な増加) は全世界的な傾向ですが、それでも国毎の違いが残っていることがわかります。

Threat News (ニュース)

Tinba が米有力銀行を狙う

Tinba が戻ってきました!

"Tinba" (Tiny Banker) と "Zusy," は、ブラウザに感染してログイン情報を盗み取ろうとするトロイの木馬です。この小型 (20KB) のバンキングマルウェアは、オンラインバンキングサイトに入力フォームを追加する MITB (Man-in-the-Browser) として動作すると共に、ネットワーク上のトラフィックを盗聴することもできます。これにより、例えばクレジットカード番号や納税者番号、認証トークンなどの他の機密情報を盗み出すことも可能です。

このマルウェアは、最初のうちはそれほど注目されませんでしたが、標的となっている金融機関は、現在では 26 にまで増えています。これらの銀行は、ほとんどが米国やカナダですが、豪州や欧州の銀行も少数含まれています。

Tinba は何年もかけて銀行のセキュリティシステムを迂回すべく改良されてきました。また、そのソースコードが数ヶ月前、アンダーグラウンドフォーラムに流れたことにも注意すべきです。

最新の攻撃についてはこちらをご覧ください: http://www.net-security.org/malware_news.php?id=2868

eBay のセキュリティ上の不備が数ヶ月間放置

少なくとも 2 月から、セキュリティ上の不備により eBay の顧客が悪意のある Web サイトの脅威に晒されています。出品リストをクリックするだけで、有害なサイトにリダイレクトされてしまうのです。

eBay は、この不備は単独のインシデントであると説明していますが、複数の出品を削除しました。BBC は、複数のユーザーからの複数の出品に悪意のあるサイトへのリンクが見つかり、それらが全て同じ脆弱性を狙っていたと伝えています。

詳しい情報については、こちらをご覧ください。専門家のアドバイスもあります:
http://www.bbc.com/news/technology-29279213

5 つの神話: 私たち自身がセキュリティリスクであるという自覚が必要

いまや、情報流出のニュースはほとんど毎日のように報じられています。この状況を見ると、攻撃への対策がほとんど進んでいないことが伺えます。大きな理由は、ハッカーが時間と共に洗練の度を増していることです。これにより、攻撃はより複雑化し、創造的になっています。それに加え、間違った情報の拡散があります。数々の「神話」は、読者に対してセキュリティに関する間違った印象を与えてしまいます。

以下のリンクには、これらの神話の例が記載されています:
http://www.darkreading.com/attacks-breaches/5-myths-why-we-are-all-data-security-risks/a/d-id/1315718

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

Back-to-School (新学期) フィッシングでは誰もが標的に

新学期が始まるという季節以上にフィッシングに向いた時期があるでしょうか。学生、学校、保護者が以下の様な状況に置かれます:

- 新しい環境
- 新しいコンピュータとネットワーク
- 学校運営やオフィス契約

Proofpoint の研究者は先頃、この脆弱な時期を狙った悪意のあるメール攻撃を複数観測しました。これらの攻撃からは、最近の攻撃が進化している様子も見て取ることができます。

例えば、Proofpoint ではドメインのアカウント情報を狙って Web メールを餌に使う標的型フィッシング攻撃を検知し、解析しました。これらのアカウント情報を盗み出せば、個人のメールを読んだり、VPN にアクセスしたり、大学のシステムにログインしたりすることができ、その他の違法な行動も可能になります。この攻撃は最初、私たちのシステムがある大学で見つけましたが、その後少なくとも 3 週間にわたって続けられ、その間 URL は周期的に変更され、異なる送信者アドレスと様々な件名が使われました。

新学期が始まる前に、Proofpoint からのアドバイスをご確認下さい:
http://www.proofpoint.com/threatinsight/posts/back-to-school-phishing.php

公園内の散歩は禁止: Centralpark[.]com のマルバタイジングが OpenX の感染をクローズアップ

Proofpoint の研究者は、Centralpark[.]com がマルバタイジングをホストしていることを発見しました。現在、オープンソースの広告サーバーである OpenX に対する大規模な攻撃が行われており、その結果としてマルウェアの配信を行ってしまったようです。この他にも、大量のトラフィックを抱える Clipconverter[.]cc も攻撃を受け、マルバタイジングを行っています。

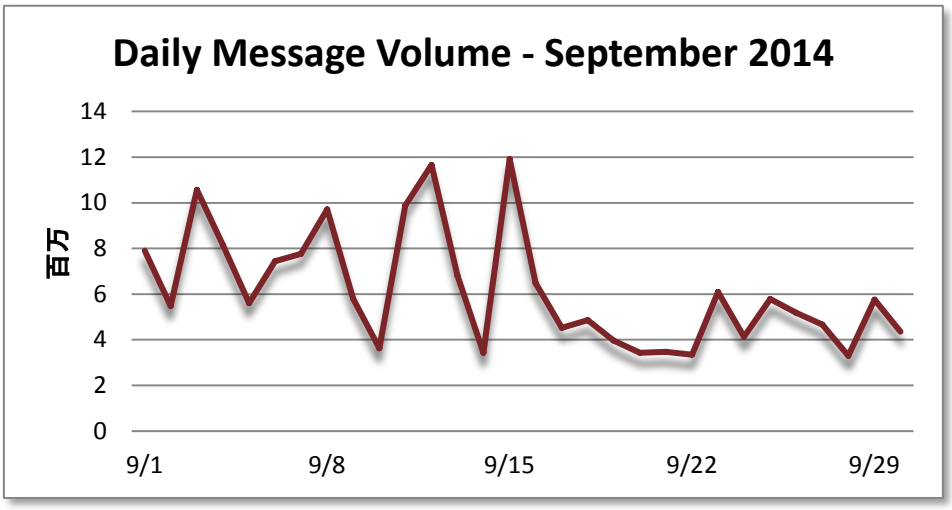
感染したサイトから配信されるエクスプロイトは、訪問者に気づかれないようにマルウェアを感染させます。単純に Web サイトを訪れただけでも感染してしまうので、注意が必要です。

配信されているマルウェアについてや、その他のポイントについては、以下をご覧ください:
http://www.proofpoint.com/threatinsight/posts/no-walk-in-the-park.php

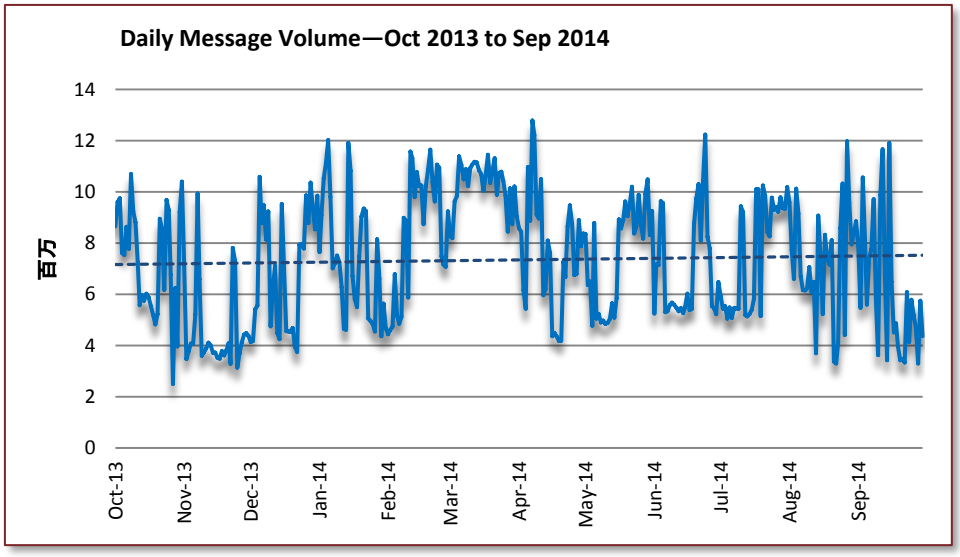
Threat Trends (トレンド)

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。9 月のスパム量は第 2 週が始まるまでは 500 万通/日と 1,000 万通/日を行き来して一定していませんでしたが、一気に 500 万まで落ち、その後 1,000 万を超え、第 3 週の初めにはまた 500 万通を割り込んだ後に最大の上げを行って 1,200 万に到達しました。そこから先は下降線で、月末には 400 万通のレベルでした。



8 月と 9 月を比べると 15.13%の下落でしたが、昨年同月と比べると、なんと 22.01%もの増加です。



Spam Sources by Country (スパム発信源)

EU が相変わらずトップで、ベトナムが 2 位に入りました。中国が盛り返して 3 位になり、アルゼンチンと韓国が続いています。

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。

		Apr '14	May '14	Jun '14	Jul '14	Aug '14	Sep '14
Rank	1st	EU	EU	EU	EU	EU	EU
	2nd	Argentina	US	Vietnam	US	US	Vietnam
	3rd	US	Argentina	US	China	Argentina	China
	4th	Russia	Russia	China	Argentina	Russia	Argentina
	5th	China	China	Russia	Russia	China	Korea

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 加盟国が 24.99%を占めており、それ以下の 4 カ国を足しても 25.21%と、EU を少し上回る程度です。

August 2014			September 2014		
1	EU	39.33%	**1**	EU	24.99%
2	US	7.31%	**2**	Vietnam	13.36%
3	Argentina	4.82%	**3**	China	4.51%
4	Russia	3.17%	**4**	Argentina	3.68%
5	China	2.58%	**5**	Korea	3.66%

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