proofpoint

# Proofpoint Threat Report

## May 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)

### IE の脆弱性を狙った APT 攻撃(CVE-2014-1776)

日本でも大きく報じられた IE の脆弱性 (CVE-2014-1776) ですが、Proofpoint のお客様の中で、このゼロデイ脆弱性を使った標的型攻撃に狙われた例を何件か確認しました。

このフィッシングメールは、国防省や航空宇宙関連企業、エネルギー関連企業、大学などを標的にしたメーリングリストに向けて送信されました。メッセージには悪意のある Web サイトに誘導するリンクが含まれており、これらのサイトはゼロデイエクスプロイトのコードをホストしています。

この攻撃は、中国の APT 攻撃グループを自称するグループの仕業と考えられています。最初の攻撃は 4 月 25 日金曜日に行われました。Microsoft は週末この攻撃に気づき、警告を発しました。https://technet.microsoft.com/ja-jp/en-s/library/security/2963983.aspx このため攻撃グループは、おそらくは追加のリソースを手配して、さらに大量のメッセージを送りました。このゼロデイ脆弱性のパッチがリリースされる前にエクスプロイトを広い範囲に配信しようとしたものと考えられます。攻撃グループは攻撃が鮮度を失わず有効に働くよう、毎日メールのテンプレートとテーマを変更し、スパム検知を逃れるよう努めました。

URL Defense Service をご利用頂いているお客様には、この URL を書き換えた上でメッセージをメールボックスに配信しましたが、解析の結果、14.6%のユーザーが URL をクリックしていました。このレートは、一般的なはえ縄型攻撃のクリック率の 2-3 倍にあたります。(LinkedIn への招待メールなど、いくつかの攻撃ではもっと高いクリック率になります)

この脆弱性自身は IE6-11 に共通とされていますが、このエクスプロイトコードは IE8-11 でしか動作しません。そうすると、観測されたクリックとの関連はどうなっているのでしょうか?

URL がクリックされたブラウザやデバイスの詳細を以下に示します。

- 64%—IE 9
- 14%—iPhone
- 7%—IE 10
- 7%—IE 8
- 7%—IE 7

観測されたクリックのうち、78%が脆弱性を持つブラウザからのものでした。この脆弱性に関するパッチがつい最近まで公開されなかったことを考えると、全世界で相当数の感染を引き起こしているものと考えられます。

## 履歴書を装ったアダルトスパム攻撃

私たちは最近、求職に関連する興味深いアダルトスパムを観測しました。サブジェクトには:

- 「アシスタント経歴書」
- 「多様な職能を持っており、アシスタントの職を探しています」

就職難の折、こういった求職の売り込みはよくあることです。しかし、メッセージ本文は少し変わっています。

- 「私の経歴書を添付します」
- 「役員秘書/オフィスマネージャーの職を探しています。デートも可能です。履歴書を添付します。」

この本文に含まれる、以下の異様な部分に注目して下さい:

- 「デートも可能です」

添付されているファイル名の例は以下の通りです。

- BrianaCreepingtree.pdf
- DebbieDozzio.pdf
- AdreannaGobongon.pdf
- SloaneCsarina.pdf
- RamonaErgoeisenheim.pdf
- EsmayLookintowardsthefuture.pdf
- TrudyChukwudum.pdf
- ShawnetteChotbenjakul.pdf
- MacieMehrdar.pdf
- ElsaMundharinti.pdf
- ChenilleFarisl.pdf
- GwynethSupavita.pdf

案の定、これらのメッセージに含まれているプロフィールのリンクは Twitter の URL 短縮機能を介して SuperHookup というアダルトサイトに繋がっています。この攻撃は、私たちがこれま

で見た中でも、最も巧妙なアダルトサイトへの誘導であり、現代のスパム業者がセキュリティソリューションをすり抜けるために如何に努力しているかを示すものです。

## Threat News (ニュース)

### eBay がサイバー攻撃を受け、1 億 4 千 5 百万ユーザーにパスワードの変更を依頼

3 ヶ月前のサイバー攻撃により顧客データが流出したとして、eBay はオンラインコマースプラットフォームのユーザー1 億 4 千 5 百万人に対し、パスワードを変更するよう呼びかけました。セキュリティの専門家は eBay の顧客に対し、詐欺への警戒を呼びかけています。特に、他のアカウントと同じパスワードを使っている場合には一層の注意が必要です。

2 月末から 3 月初めにかけて、未知の攻撃者がメールアドレス、暗号化されたパスワード、生年月日、住所その他の情報を盗んだとされています。盗まれた情報には金融情報は含まれていません。eBay の担当者は、大量のアカウントが流出した可能性があると語っています。支払いを担当する子会社の PayPal によると、金融情報やクレジットカード情報に不正なアクセスがあった証拠は確認されていません。PayPal 自身のデータは別に暗号化され、保存されています。データ流出は 5 月初めに発覚しました。捜査は捜査当局とセキュリティ専門家により進行中です。

詳細はこちらからどうぞ: http://www.reuters.com/article/2014/05/21/us-ebay-password-idUSBREA4K0B420140521.

### 過去 12 ヶ月間のデータ流出事件ワースト 10

データ流出事件のリストはインターネット上の犯罪者の手口を知る手掛かりです。広範な分野におよぶ知見をご覧ください: http://www.techradar.com/news/software/security-software/the-top-10-data-breaches-of-the-past-12-months-1248890/1#articleContent.

### 複雑な Web サイトはセキュリティの敵

セキュリティジャーナリストの Brian Krebs が 4 月末に報じたところによると、ハッカー達が Syrian Electronic Army (SEA) と連携して RSA Conference の Web サイトを侵害したということです。RSA Conference は世界最大のセキュリティカンファレンスです。

この攻撃の成功は、狙いを定めて企業の上級管理職を騙す手口が依然として有効であることを印象づけました。それに加えてこの事例は、高名な Web サイトへの侵入に際してサードパーティのコンテンツプロバイダが重要な役割を果たすことについての教科書的な事例であると言えます。rsaconference.com のハッキングは、カンファレンス開催者が 2 月に行われた RSA Conference のセッションビデオをアップロードしてから、わずか数時間後に行われました。このビデオには Ira Winkler のビデオも含まれており、彼は SEA について「インターネットのゴキブリだ」と発言しています。

Winkler 氏に対する SEA の反応は尋常ではありません: http://krebsonsecurity.com/2014/05/complexity-as-the-enemy-of-security/.

### HIPPA 関連の電子的なデータ流出によるものとしては過去最大の和解が成立

米保健社会福祉省公民権局 (Office for Civil Rights of the Department of Health and Human Services) は、New York-Presbyterian の患者データが保護されていなかったことによるデータ流出事件をうけ、ニューヨークの 2 つのヘルスケア機関 (NewYork-Presbyterian と Columbia University) との間で 480 万ドルの和解契約を締結しました。この和解は、HIPPA 対象の組織は健康情報が電子的に保護されるよう徹底的なリスク分析を行い、技術的、物理的、管理上の安全対策を施すことが求められていることを浮き彫りにしました。

この和解は、HIPPA に関連するものとしては過去最大のものです: http://www.natlawreview.com/article/electronic-data-breach-leads-to-largest-health-insurance-portability-and-accountabil.

## 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.

### 貴方へのギフトカード… マルウェア付き!

Proofpoint の研究者は洗練された攻撃を観測しました。この攻撃は、被害者に送られた個々のメールから最大の価値を引き出そうとする先進的なツールを使っています。この攻撃は、ユーザーに URL をクリックさせるために有名な米国ブランドを餌として使っており、ギフトカードのプレゼントを装っています。予想通り、URL は侵害された Web サイトに繋がっています。

詳しくはこちらからどうぞ: http://www.proofpoint.com/threatinsight/posts/a-gift-card-for-you-free-malware-included-too.php.

### TIFF の中に: フィッシングが古い脆弱性に新しい命を

Proofpoint は過去 2 日間の間に 2 回、Proofpoint のお客様を狙った PDF 攻撃を観測しました。PDF はメールに添付されており、メールは PayPal からのセキュリティに関する警告を装っています。問題を解決するため、添付の PDF を開封するよう促しており、PDF が TIFF を扱う際の脆弱性を利用しています。セキュリティに関する警告を装うメールが、往々にして攻撃の一部であることは皮肉なことですが、私たちの研究では、2 番目に効果的なのは金融アカウントに関する警告を装ったテンプレートです。

実例と分析をご覧ください: http://www.proofpoint.com/threatinsight/posts/in-a-tiff-phishing-campaign-gives-new-life-to-an-old-vulnerability.php.

### GameOver Zeus マルウェア…税還付と共に

先月の脅威レポートで、納税シーズンを狙ったフィッシングについて書きました。では、その次に来るものは何でしょうか?

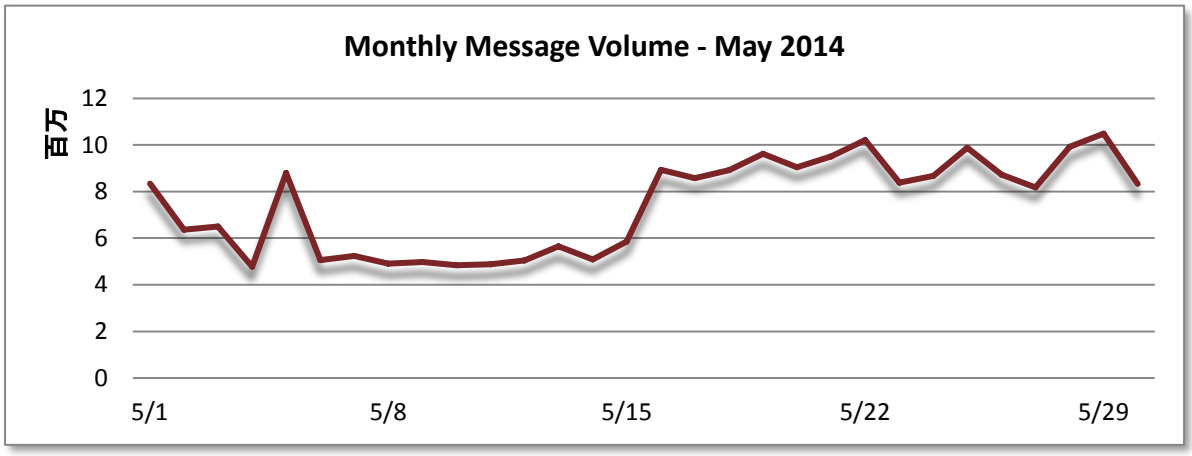
もうおわかりですね。攻撃者達は、納税シーズンに自分達が仕掛けた攻撃に続く攻撃を用意しています。税還付です。

私たちは最近、興味深いはえ縄型攻撃を観測しました。悪意のある URL をクリックさせるために、税還付を餌として使っているのです。この攻撃はイギリスの納税者を狙っており、そのテンプレートは以下の様なものです: http://www.proofpoint.com/threatinsight/posts/gameover-zeus-malware-with-your-tax-refunds.php.

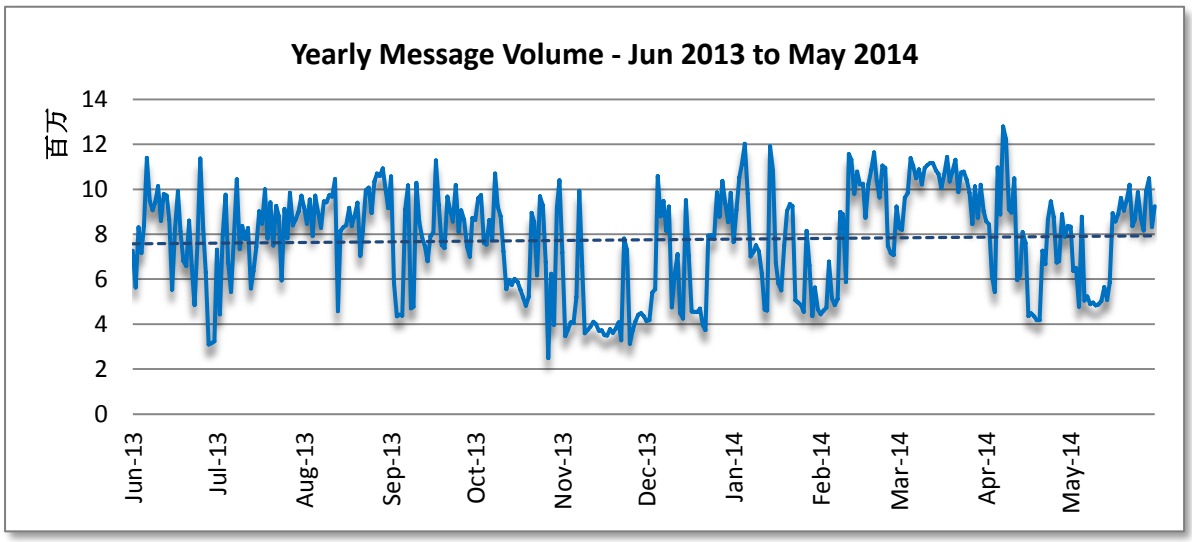
## Threat Trends (トレンド)

### 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。5 月は良い日と悪い日が混在しており、スパム量は急増したかと思えば急落し、また戻り、しばらく停滞するなどし、全体を通しては月末へ向けてじわじわと増えるという展開でした。800 万通/日で始まり、400 万通/日に落ち込み、また 800 万通を超え、そして 400 万通に落ちる、というトレンドが月中まで続き、月末に 1,000 万通/日に達しました。最終日は少し減らしています。




4 月に比べるとスパムの全体量は 2.45%と若干減少し、前年比でも 2.08%増と低い伸びに留まっています。



## Spam Sources by Country (スパム発信源)

いつものトップ 3 カ国 (EU、US、アルゼンチン) が相変わらず強く、ロシアと中国が上位を狙っています。

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。

| | | Dec '13 | Jan '14 | Feb '14 | Mar '14 | Apr '14 | May '14 |
|---|---|---|---|---|---|---|---|
| Rank | 1st | EU | EU | EU | EU | EU | EU |
| | 2nd | US | US | US | US | Argentina | US |
| | 3rd | China | Argentina | Argentina | Argentina | US | Argentina |
| | 4th | Argentina | China | Russia | India | Russia | Russia |
| | 5th | India | India | China | Mexico | China | China |

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 は全体の 40.46%で、引き続き世界のスパム量の大半を占めます。トップ 5 の残りの 4 カ国を足しても 19.46%で、EU の半分にも満たない数字です。

| April 2014 | | | May 2014 | | |
|---|---|---|---|---|---|
| **1** | EU | 39.98% | 1 | EU | 40.46% |
| **2** | Argentina | 7.64% | 2 | US | 7.96% |
| **3** | US | 6.94% | 3 | Argentina | 5.36% |
| **4** | Russia | 2.59% | 4 | Russia | 3.10% |
| **5** | China | 2.42% | 5 | China | 3.04% |


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