proofpoint

Proofpoint Threat Report

January 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)

在米ペルー大使館のサイトが侵害される

どのような組織も、先進的な攻撃に対して完全に安全ではいられません。マイクロソフトへの攻撃やホワイトハウスへのフィッシング攻撃、法律事務所や中規模企業からの給与明細の流出なども大きなニュースになりました。今月は在米ペルー大使館の Web サイトが侵害された事件を取り上げます。在米ペルー大使館はワシントン D.C.にあります。左はその画面ショットです。

攻撃自体はよくある標的型攻撃で、大使館の特定の職員が標的とされました。(詳細は後述) またこの攻撃はウォータリングホール型攻撃の特徴も併せ持っていました。サイトの信頼性が高く、同じ興味をもった人々がアクセスしてくるという点から、大使館サイトはウォータリングホール (水飲み場) と定義できると考えられるからです。

いくつかの重要な特徴から、この攻撃には Sweet Orange というエクスプロイトキットが使われたことがわかります。最初の特徴としては、URL に<英単語>.php?<英単語>=<数字>というパターンが使われていること、2 つ目の特徴は Web トラフィックに 7761 番か 60012 番のポートを使っていること、3 つ目は、画面外の見えない場所 (-10,000 ピクセルの位置) に iframe が置かれていることです。図 2 にこれらの特徴を示します。

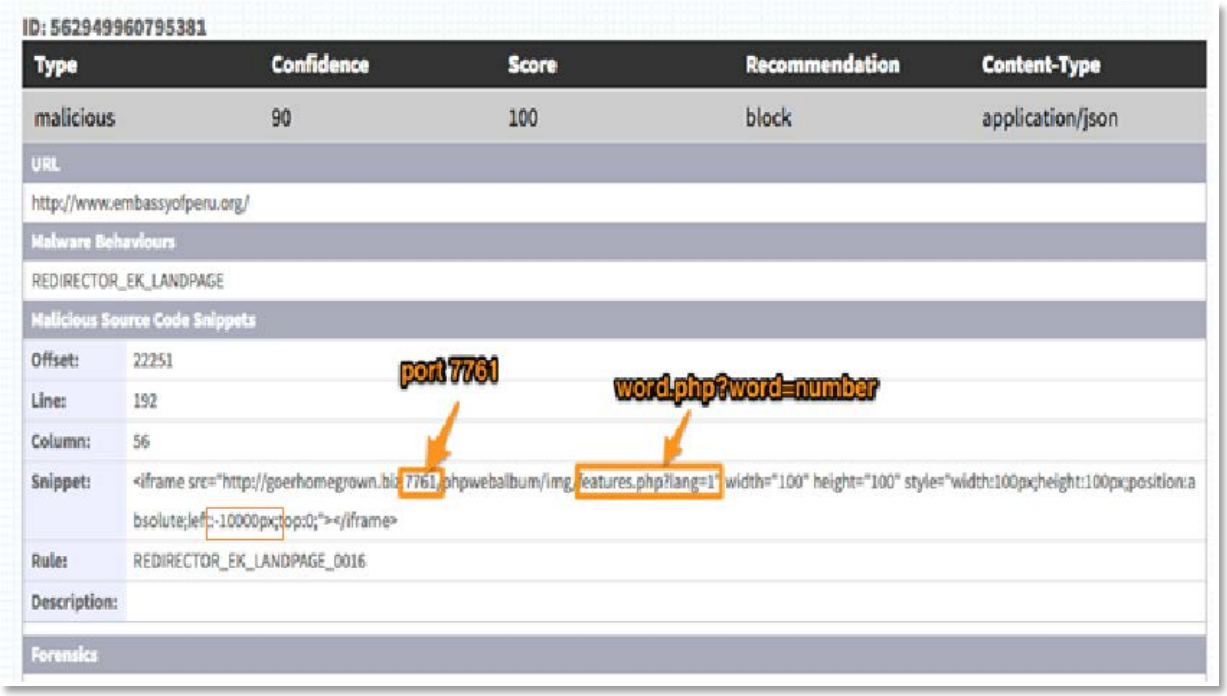


図 2: Sweet Orange の特徴

詳細なフォレンジック解析によって Java が感染経路であったことが確認されました。ドロッパーはホスト上に置かれており、これが起動され、複数のプロセッサに感染し、他のマルウェアをダウンロードします。これらは最終的にはマシン内の FTP および Web メールの ID/パスワードをかき集め、コマンド＆コントロールサーバーに送信します。

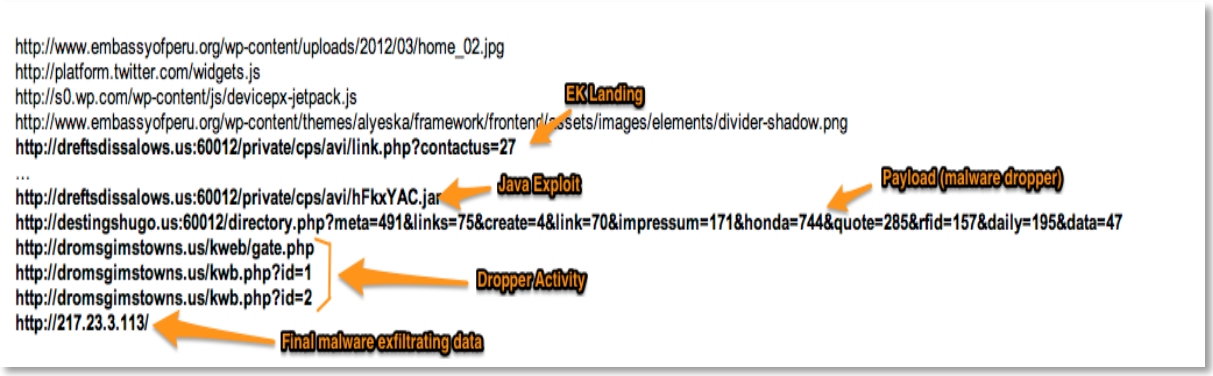


図 3: 攻撃手順の詳細

攻撃の詳細な手順とマルウェアの情報によって攻撃のメカニズムを理解することは大切です。しかし本当に重要なのは、この攻撃が大使館の組織と今後の活動に与える影響についてです。この攻撃は法務部門のスタッフと管理職のグループを狙って行われました。誰が感染したのか (そして誰

が感染しなかったのか) を突き止めることこそが重要です。それによって復旧の手順が決まり、将来の対策に活かすべき教訓が得られるからです。御社でご利用中のセキュリティソリューションはそういった情報を提供できるでしょうか？

Threat News (ニュース)

ドイツのインターネットユーザー1,600 万人に影響を与えたデータ流出

SC Magazine が 1,600 万人に影響を与えたデータ流出事件を報じています。電子メールとソーシャルメディアアカウントのユーザー名とパスワード情報に加えて、オンラインショッピングのポータルサイトへのログイン情報が盗まれたのです。事件は最初ドイツの連邦情報技術安全局 (BSI: German Federal Office for Information Security) によって発表されました。追加情報と SC の記事は以下でご覧頂けます

http://www.scmagazine.com/data-breach-affects-16m-in-germany/article/330550/

シリア電子軍が他のハッカー集団から攻撃を受ける

ハッカー集団であるシリア電子軍 (SEA) の Web サイト (sea.sy) がトルコのハッカーグループによって改ざんされるという事件がありました。サイトは「SEA の悪行を糾弾する内容がスプレーで落書きされたよう」だったということです。詳細は以下の Register のサイトでご覧頂けます。

http://www.theregister.co.uk/2014/01/15/sea_own_website_pwned/

Target のデータ流出から学ぶべき教訓

米小売り大手 Target のデータ流出事件は皆さんご存じでしょう。Forbes がこの事件から得られる教訓について興味深い分析をしています

1) 問題を共有する (迅速に)
2) 顧客からの問い合わせに備える
3) 最新のセキュリティ技術を採用する
4) 予防策に投資する
5) 信頼を再構築する

元記事では個々の項目について詳細な解説がされています。

http://www.forbes.com/sites/sungardas/2014/01/17/five-lessons-for-every-business-from-targets-data-breach/

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下さい。

http://www.proofpoint.com/threatinsight.

IoT 時代の攻撃とは

12 月のホリデーシーズンに起きた大規模なセキュリティ侵害において、Proofpoint の研究者がかつて見たことの無いような高度な理論的攻撃の痕跡を発見しました。

この研究者は電子メール由来の脅威を解析していました (この解析は通常でも行われていることです) が、ある攻撃において悪意のあるメール全体 (およそ 75 万通) のうち 25% 以上が PC 以外の「モノ」から発信されていることを観測しました。様々なデバイスがインターネットに接続する「モノのインターネット (IoT)」の時代が始まっており、侵害されたモノによって構成されるボットネットを「Thingbot」ネットと呼ぶこともあります。詳しくは以下のブログポストでご覧頂けます。
http://www.proofpoint.com/threatinsight/posts/your-fridge-is-full-of-spam-proof-of-a-Iot-driven-attack.php

IoT 時代の攻撃とは: 詳細

私たちの Internet of Things (IoT) を使った悪意のあるメール攻撃に関するプレスリリース (英文) および チップセットと OS、デバイスについてのブログポストに、私たちの予想を上回る反響をいただきました。

私たちが、どのような解析手法とロジックによってこれらのデバイスが攻撃に使われたと考えたのかについて、様々な方面から沢山のお問合せをいただき、それらにお答えしました。

そこで、本件に興味をお持ちの方々と情報と理解を共有するために、これらの回答をまとめておくことにしました。私たちは、他の研究者の方々が私たちと同じ結論に達し、これら新しいセキュリティ上の脅威への対抗策を考えるために役立てていただければと考えております。

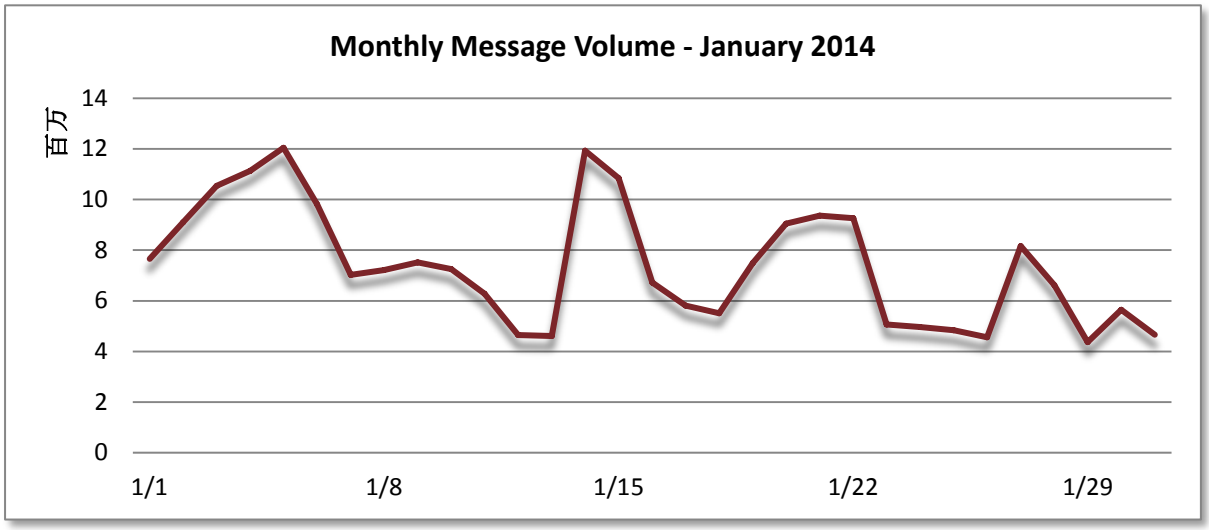
以下のブログポストに、いくつかの画面ショットと共に、解析手法についてのサマリを掲載しました。

http://www.proofpoint.com/threatinsight/posts/your-fridge-is-full-of-spam-part-ll-details.php

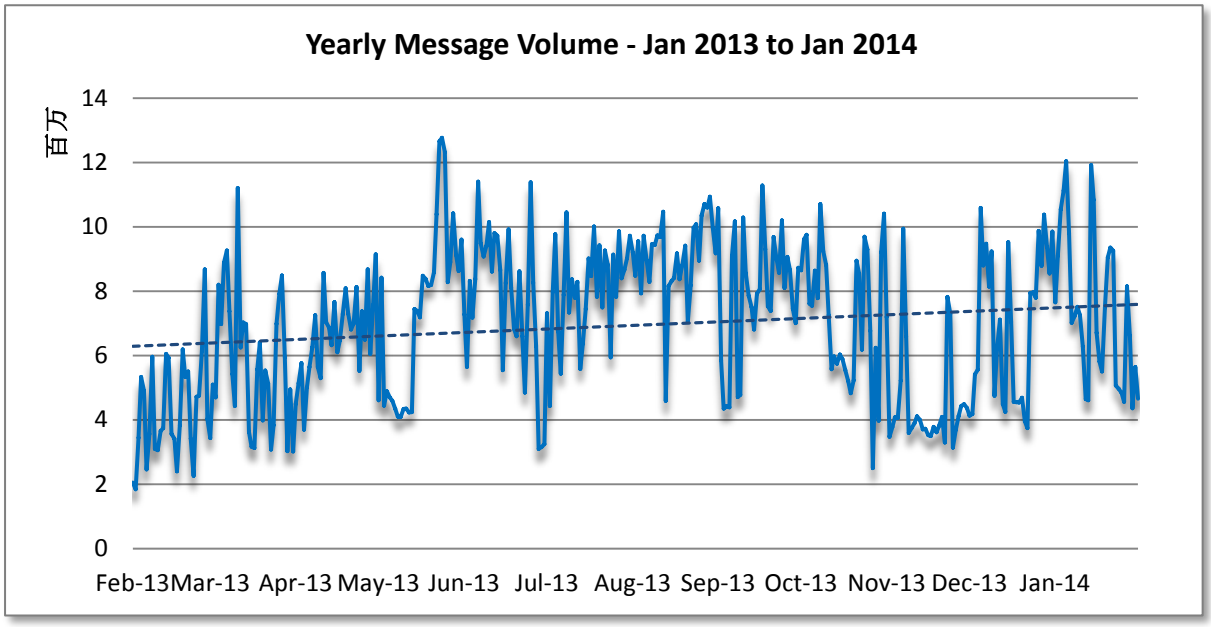
Threat Trends (トレンド)

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。1 月のスパム量は 12 月と同様に不安定な動きを示し、1 日当たり 400 万通から 1,200 万通までの間を揺れ動きました。スパム量は月初に急増し、7 日にかけて減少した後に月中には再度急増しました。そこから月末にかけては大きな減少傾向の中で揺れ動いています。



長期的に見るとスパム量は 2013 年の 10 月と 11 月に落ち込んだ後はじわじわと増えており、1 月は 12 月に比べて 6.55%の増加でした。しかし、前年比ではなんと 91.83%の増加となっており、記録的な高さを示しています。



Spam Sources by Country (スパム発信源)

かつての常連が戻ってきたようです。EU は世界一スパムを発信している地域としての悪名を維持しました。US はいつもの 2 番目の順位に居ます。中国とアルゼンチンが順位を入れ替え、アルゼンチンが 3 位となりました。インドは 5 位で変わらずでした。以下のテーブルは過去 6 ヶ月間の順位です。

	August '13	September '13	October '13	November '13	December '13	January '14
1st	European Union (EU)	EU	EU	EU	EU	EU
2nd	United States (US)	US	US	China	US	US
3rd	Argentina	India	India	US	China	Argentina
4th	India	Argentina	Argentina	Japan	Argentina	China
5th	Taiwan	Taiwan	China	India	India	India

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 の数値は今月から全加盟国を含むようになり、より正確に傾向をつかむことができます。EU は新しい計算方法では発信量が 6.4%増加し、全体に占める割合が 35.99%となりました。その他の 4 カ国を合わせても 17%未満と、EU の半分にも達しません。

December 2013			January 2014		
1	EU	16.99%	1	EU	35.99%
2	US	6.34%	**2**	US	6.20%
3	China	5.27%	**3**	Argentina	3.84%
4	Argentina	4.46%	**4**	China	3.49%
5	India	3.41%	**5**	India	3.43%

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