proofpoint

Proofpoint Threat Report

September 2012

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 News (ニュース)

Internet Explorer へのゼロデイ攻撃

先月レポートした Java へのゼロデイ攻撃を行ったのと同じグループが、Internet Explorer の別の脆弱性を狙ったゼロデイ攻撃に関与しています。9 月 18 日付の PC World 誌の記事 によれば、Internet Explorer 7、8 および 9 にはリモートでコードを実行できる脆弱性があり、現在でも攻撃に利用されている、ということです。このうちの一つは同じシステムに Java がインストールされている時に脅威となり、他のものは Adobe Flash がある場合に脅威となります。

Microsoft はこれをセキュリティ情報に載せると共に、この脆弱性に対応するために MS12-063 パッチをリリースしました。この脆弱性は Windows XP、Windows 7 および Windows Server を含む全ての Winddows システムに存在します。詳しくはマイクロソフトの Security Advisory 2757760 および CVE-2012-4969 を参照して下さい。

Apple の端末 ID が流出

ハッカー集団のアノニマスは、今年だけでも何回かニュースになっていますが、9 月にもメディアに取り上げられました。FBI から Apple の端末 ID (UUID) 1,200 万件を盗んだという声明を発表したのです。UUID (Universal(ly) Unique Identifiers: UDID とも呼ばれます) は、iPhone、iPad、iPod Touch を含む全ての Apple 社製デバイスに付与されている固有のシリアル番号です。1,200 万件のうち 100 万件分が、

他の個人情報が消去された形でインターネット上に公開されました。現時点では、この他の個人情報が盗まれたかどうかはわかっていません。FBI では、この種の情報を取り扱っていないと言っており、侵害された事実も無いと言っています。これについては後に NBC ニュースによって、実際のデータはフロリダ州の出版社である Blue Toad のものであったことが確認されました。Blue Toad が自社のデータと公開されたデータを解析した結果、98%の相関があったとのことです。

UUID が何に使われているのかということについて沢山のレポートが出ていますが、iOS アプリケーションの開発者がアプリケーションの利用状況を追跡したり、ゲーム用のネットワークを設定したり、その他単純な設定情報を保存するためだという見方が一般的です。いくつかのレポートでは、もっと無害なものだと指摘しているものもあるようです。Apple は実際、今年初めには UUID を利用する iOS アプリケーションの申請をリジェクトし始めたとされています。もっと詳しい情報については、このレポートをご覧ください。

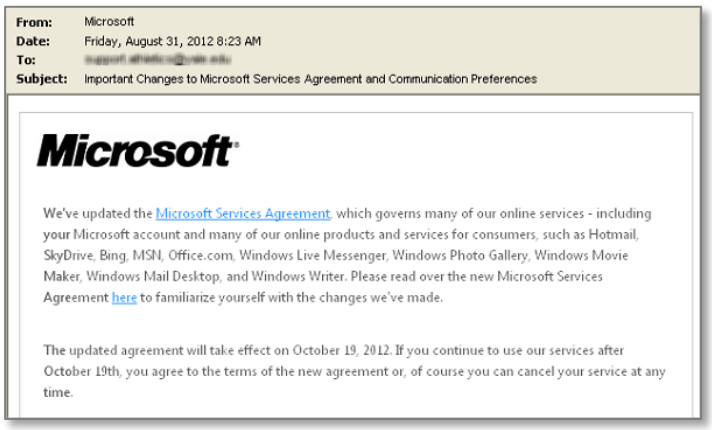
Microsoft のボットネット解体活動

Microsoft は 今月、新たなボットネットの解体に取り組みました。こうした活動に同社が関わるのは、過去 3 年間で 5 回目になります。「オペレーション b70」と名付けられたこの活動は、販売前または利用前に侵害された製品の証拠を見つけ出すことを主眼に置いていました。Nitol と呼ばれるこのマルウェアは、中国で流通している新品のマシンに感染しており、2011 年に Microsoft が中国で調査したサプライチェーンで発見されました。 Microsoft のレポートによると、Nitol マルウェアは Windows Explorer の設定を書き換えます。感染したファイルを削除しても、ハードディスクの他の場所に移動するため、発見や駆除が非常に難しいということです。感染したマシンは C&C (Command and Control) サーバーにログインします。C&C サーバーはほとんどが中国にありますが、米国内にも相当数あり、特にサンディエゴ、サンノゼ、ダラス、アトランタなどが活発です。

Threat Models (手法)

Microsoft サービス契約

8 月末、Microsoft は顧客に電子メールを送り、サービス契約が変更され、10 月 17 日から発効する旨を通知しました。その後ハッカーは、このメールを悪意のある Web サイトに誘導するためのテンプレートとして利用しており、そのことを Computer world はじめ、いくつかの媒体が報じています。

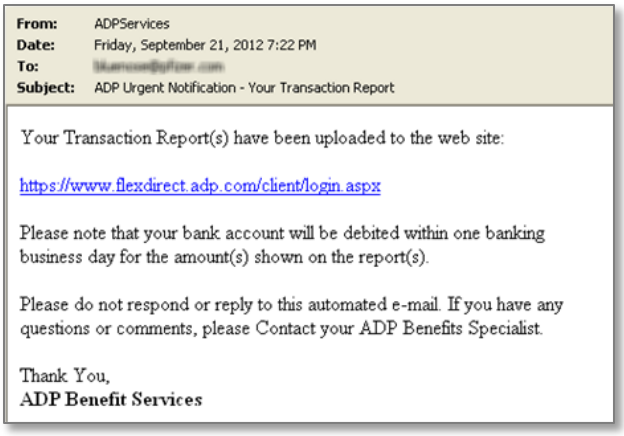

From: Microsoft
Date: Friday, August 31, 2012 8:23 AM
To:
Subject: Important Changes to Microsoft Services Agreement and Communication Preferences

Microsoft

We've updated the Microsoft Services Agreement, which governs many of our online services - including your Microsoft account and many of our online products and services for consumers, such as Hotmail, SkyDrive, Bing, MSN, Office.com, Windows Live Messenger, Windows Photo Gallery, Windows Movie Maker, Windows Mail Desktop, and Windows Writer. Please read over the new Microsoft Services Agreement here to familiarize yourself with the changes we've made.

The updated agreement will take effect on October 19, 2012. If you continue to use our services after October 19th, you agree to the terms of the new agreement or, of course you can cancel your service at any time.

直近でこのメールが使われたのは先月の Java の件で、恐らく今回の Internet Explorer のゼロデイ攻撃にも使われていると考えられます。Proofpoint では、これらの攻撃が複数の顧客に対して行われていることを確認しており、それらはフィッシングあるいはスパムとして検知されています。サンプルのメールでは、オリジナルの Microsoft のメール中、一つのリンクだけが変えられており、ユーザーを感染したサイトに誘導します。

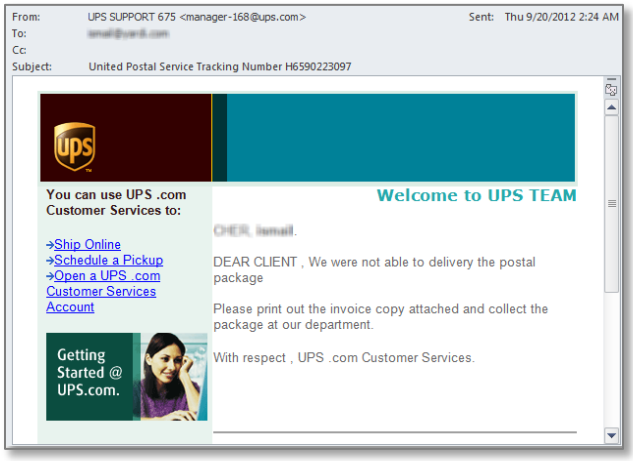


ADP トランザクションレポート

ADP（米国の大手給与計算代行会社）のトランザクション通知メールは過去に何度もフィッシング用のテンプレートとして利用されてきました。先月、攻撃者はこのテンプレートと Java の脆弱性 CVE-2012-1723 を使って人事・給与部門を狙いました。Proofpoint では 9 月になっても何件かこの攻撃を確認しています。リンクを解析すると、これらの URL は、今では最新の IE の脆弱性への攻撃が参照しているようです。

UPS 通知と iPhone 5

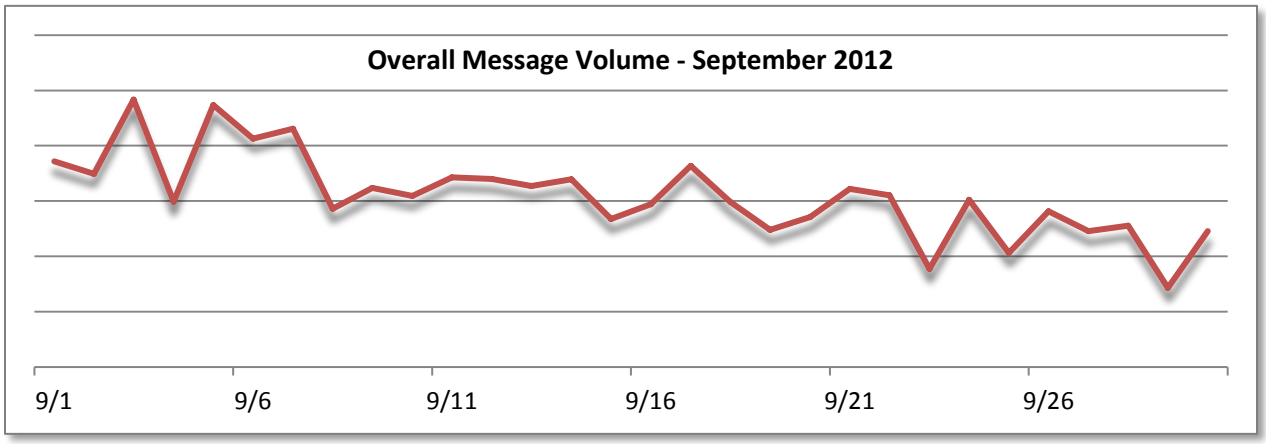
iPhone 5 は最初の週末で 500 万台の売上を記録すると見られていました。しかし、中には出荷が 3-4 週間遅れることを通知されてがっかりしたユーザーもいます。ハッカー達はこの情報もフィッシング攻撃に利用しました。9 月末にかけて、UPS (United Parcel Service) からの不正な通知が増えています。複数のマルウェアデリバリーモデルが使われており、ユーザーにリンクをクリックするか、PDF または HTML ファイルを開くよう促します。



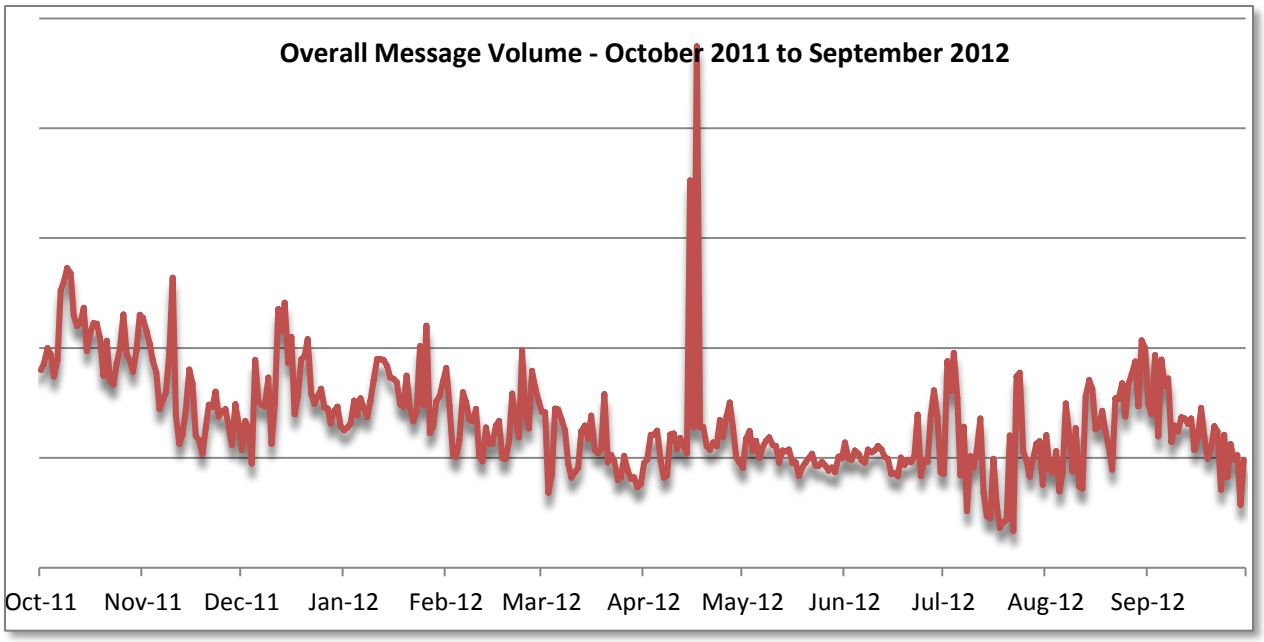
Threat Trends (傾向)

Spam Volume Trends (スパム量の変化)

今年は、ボットネットの解体は全体のスパム量に大きな影響を与えません。8 月から 9 月にかけてのスパム量に大きな変動は無く、9 月は 4 月に続いて 2 番目に多い月となりました。

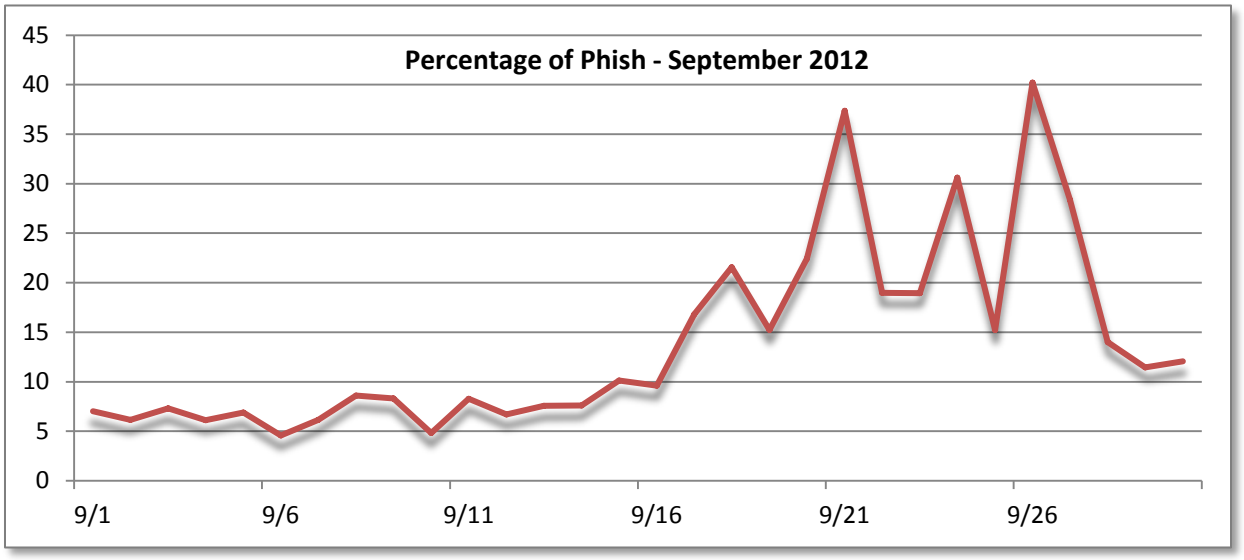


前年同月比で見ると、減少傾向は変っておらず、2011 年 9 月に比べ、39%の減少となっています。



Phish Classification Trends (フィッシング区分の変化)

今月から、Proofpoint が追跡しているフィッシング区分の集計をお届けします。これは Proofpoint の顧客ベースおよびハニーポットからの情報です。以下のグラフは、Proofpoint MLX および Targeted Attack Protection が全スパム中でフィッシングと分類したメールの割合をパーセンテージで表しています。数値はレポートされる情報源のうち上位 10 件の平均値で、一日ごとに集計されています。

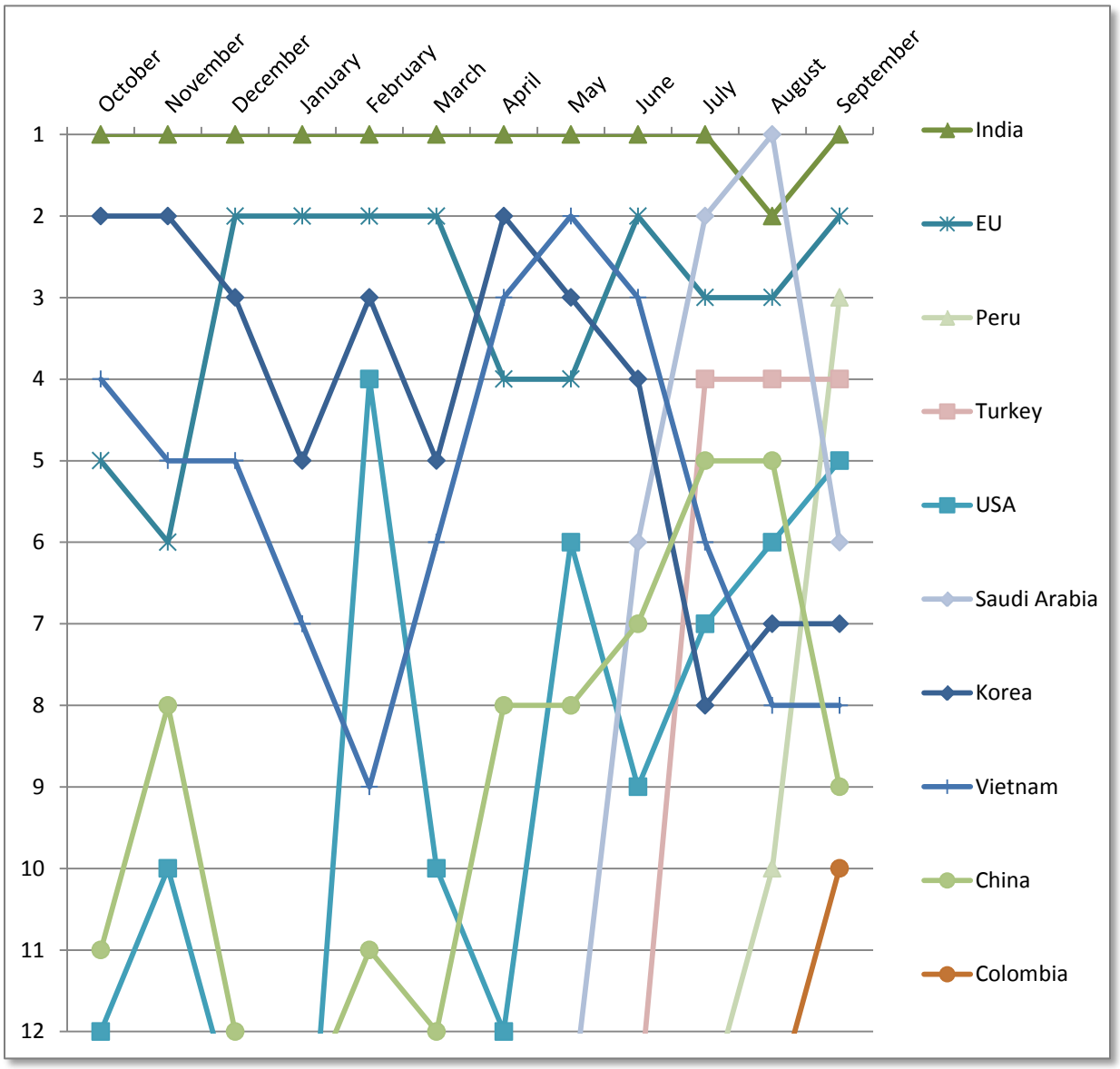


9 月中、スパムの総量は減少傾向にありますが、フィッシングの割合は高まる傾向にあります。

Source of Spam (スパム発信源)

先月 2 位に落ちていたインドが、世界最大のスパム送信国に返り咲きました。また、急速に順位を上げて 8 月には 1 位になったサウジアラビアは、今月は 6 位に後退しました。

興味深いのは、先月トップ 10 に姿を現したペルーが今月は 3 位と急速に順位を上げていることです。

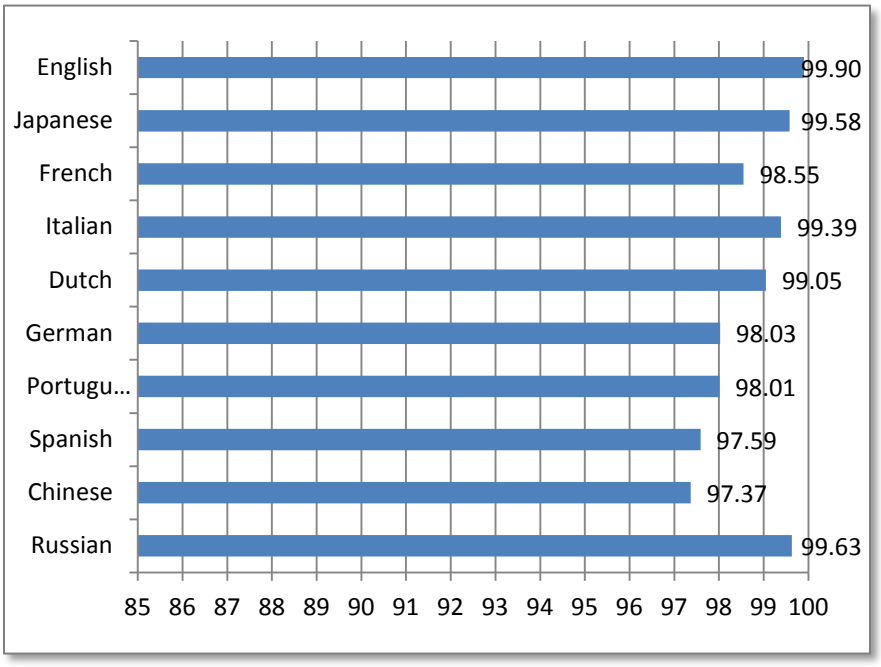


先月ペルーが始めてトップ 10 入りしたのに続き、今月も同じ南アメリカから初のトップ 10 入りした国があります。コロンビアが 10 位に入りました。次頁の表はスパム発信元のトップ 10 と全体に占めるパーセンテージです。

順位	国	パーセンテージ
1	India	17.0
2	EU	7.3
3	Peru	4.6
4	Turkey	4.2
5	USA	4.1
6	Saudi Arabia	4.0
7	Korea	3.6
8	Vietnam	3.0
9	China	2.9
10	Colombia	2.8

Language Effectiveness（言語別防御効果）

次のグラフは、Proofpoint ソリューションのスパム防御の有効性を言語毎に示したものです。



proofpoint

日本プルーフポイント株式会社
〒102-0083
東京都千代田区麹町 3-5-2
ビュレックス麹町
03-5210-3611
www.proofpoint.co.jp