proofpoint

Proofpoint Threat Report

April 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)

Ransomware Variants (Ransomware の亜種)

4 月上旬、私たちのセキュリティパートナーの F-Secure が Ransomeware の亜種について報告しました。これが実行されると、ファイルシステム上の全てのファイルが暗号化され、ファイル名が書き換えられます。

暗号化されたファイルをダブルクリックしたり、他の方法で開こうとすると、復号化のパスワードを求められます。パスワードを 5 回間違えると、メッセージは消え、2 度とファイルを復号化できなくなります。以下は最初に表示される警告文です:

> Attention! All your files are encrypted! You are using unlicensed programms! To restore your files and access them, send code Ukrash or Paysafecard nominal value of EUR 50 to the email koeserg@gmail.com. You have 5 attempts to enter the code. If you exceed this of all data irretrievably spoiled. Be careful when you enter the code!
>
> (注意! あなたの全てのファイルは暗号化されました! あなたはライセンスされていないプログラムを利用しています! ファイルを復元するためには、Ukrash か Paysafecard を使って koeserg@gmail.com に 50 ユーロを支払って下さい。パスワードは 5 回まで入力できます。5 回を越えると、データは永遠に失われます。パスワードを入力する際にはご注意下さい!)

幸いなことに、この攻撃はまだそれほど広まっていません。攻撃元については現在調査中です。より詳しい情報については、ここをクリックして下さい。

その他の Ransomeware の亜種が 4 月末に発見され、それは米司法省を名乗っています。Reveton と名付けられたこの Ransomeware は、Citadel というマルウェアをインストールし、全てのファイルへのアクセスを不能にし、$100 が支払われるまでアクセスできません。しかも、他の Ransomeware と同様、支払いを行ってもファ

イルへのアクセスが可能になるだけで、マルウェア自身は削除されません。引き続きマルウェアが重要な情報へのアクセスなどを行う可能性が残ります。

Hotmail Password Hack（Hotmail のパスワードハック）

Whitec0de が報告したように、Hotmail の「パスワードを忘れた場合」機能に潜む脆弱性への攻撃が 4 月中の少なくとも 2 週間にわたって広範に行われました。どれだけのアカウントがハックされたかは不明で、Microsoft は脆弱性について公式には認めていません。ほとんどのアカウントで、4 月 20 日にはこの攻撃への対策がとられたということです。

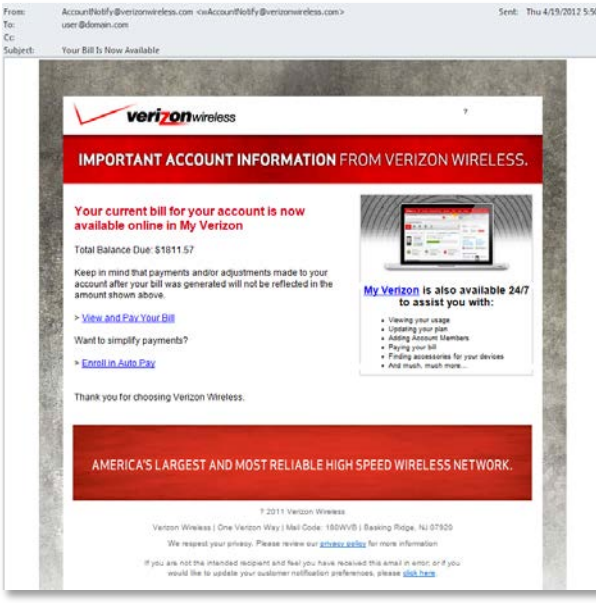
The Unknowns

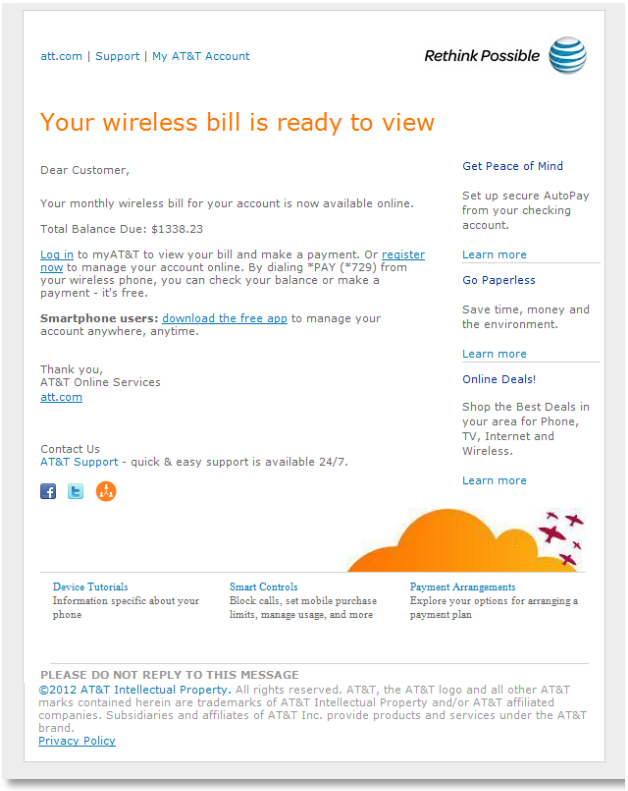
LulzSec と Anomymous が抜けた穴を埋めるのにあまり時間はかかりませんでした。新しい grayhat 集団である「Unknowns」が NASA、バーレーン王国国防省、Renault など 10 サイトをハッキングしたと発表しました。SQL インジェクションを使い、名前、住所、メールアドレスおよびドキュメントを取得し、pasteblin と MediaFire に投稿しました: 声明文はこちらで読むことができます

Threat Models（手法）

Wireless Bills（通信料金の請求書）

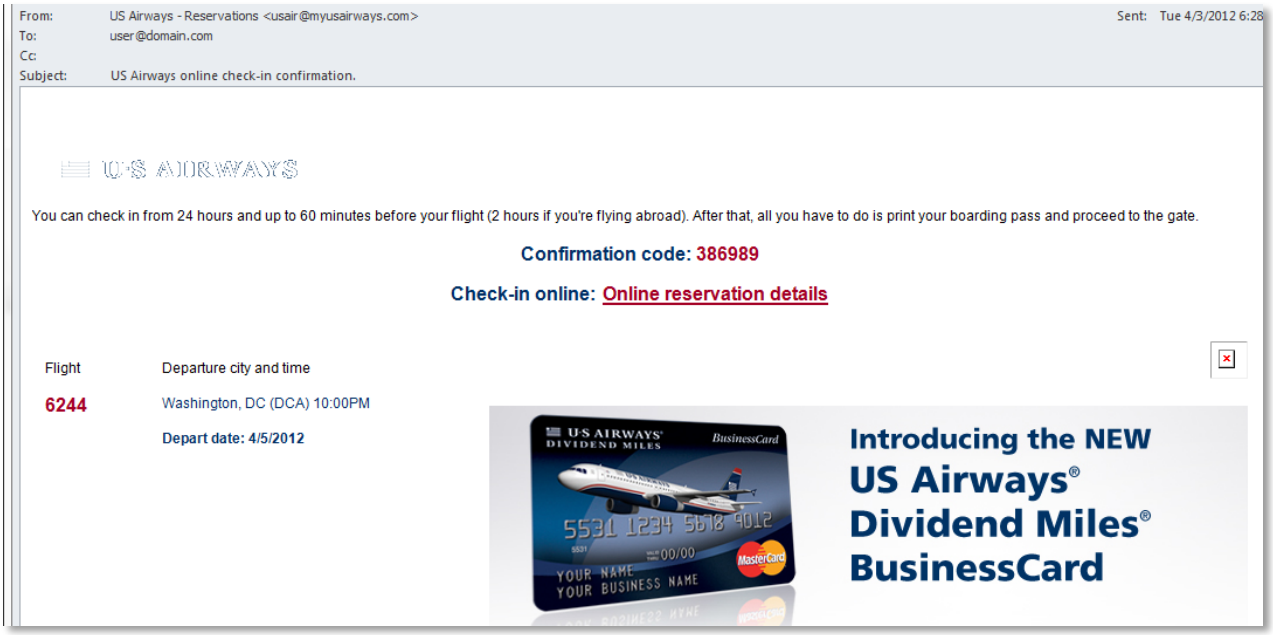
米国の大手ワイヤレスキャリヤが、ソーシャルエンジニアリングを使った二つの手法により狙われました。多額の請求金額が記載された通信料金の請求書は非常に精巧に似せられており、受信者は金額にびっくりして思わずクリックしてしまいます。クリックすると汚染されたサイトに誘導され、多くの場合、既知の脆弱性を含む PDF にリンクされています。





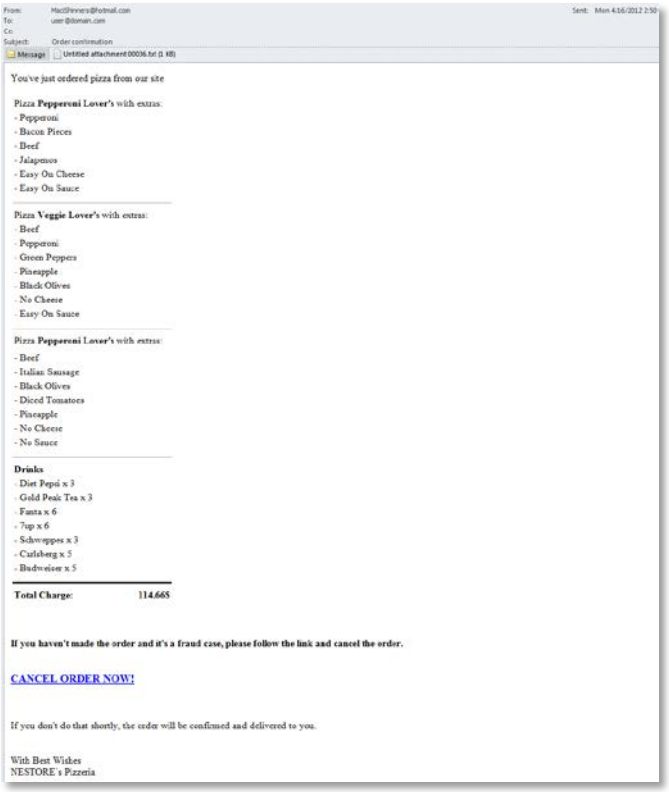
Flight Check-in（航空便へのチェックイン）

この攻撃では、ほとんどの場合、米国の航空会社がなりすましの対象となり、高頻度で変更される URL が使われます。URL をクリックすると偽の予約サイトに誘導され、その中のリンクをクリックするよう誘導されます。そのリンクは BlackHole ツールキットにより汚染されたページに繋がっており、そのページでは ZeuS ベースの情報窃盗マルウェアを配布しています。



Pizza Order（ピザの注文）

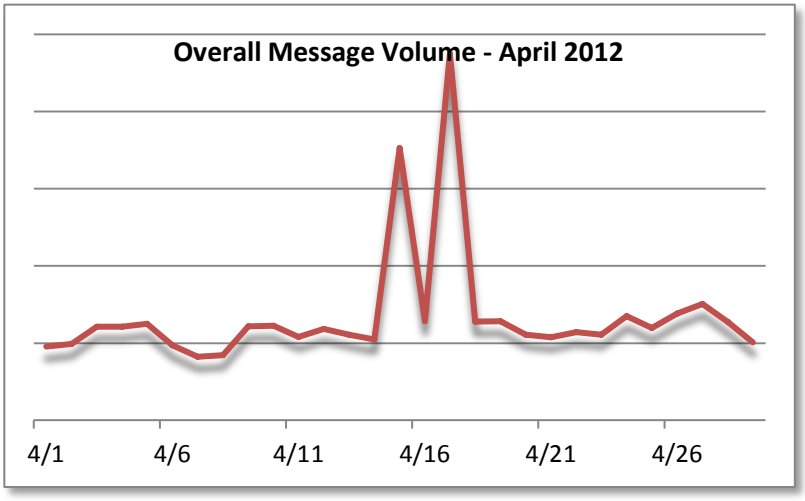
上記のワイヤレスビルと似た手法ですが、常識では考えられないような高額なピザの請求書も、ユーザーを慌てさせリンクをクリックさせるためには有効です。このメール中の唯一の URL は汚染されたサイトにつながっており、そのサイトにはユーザーを別のサイトに誘導し、マルウェアをダウンロードさせる JavaScript が仕掛けられています。

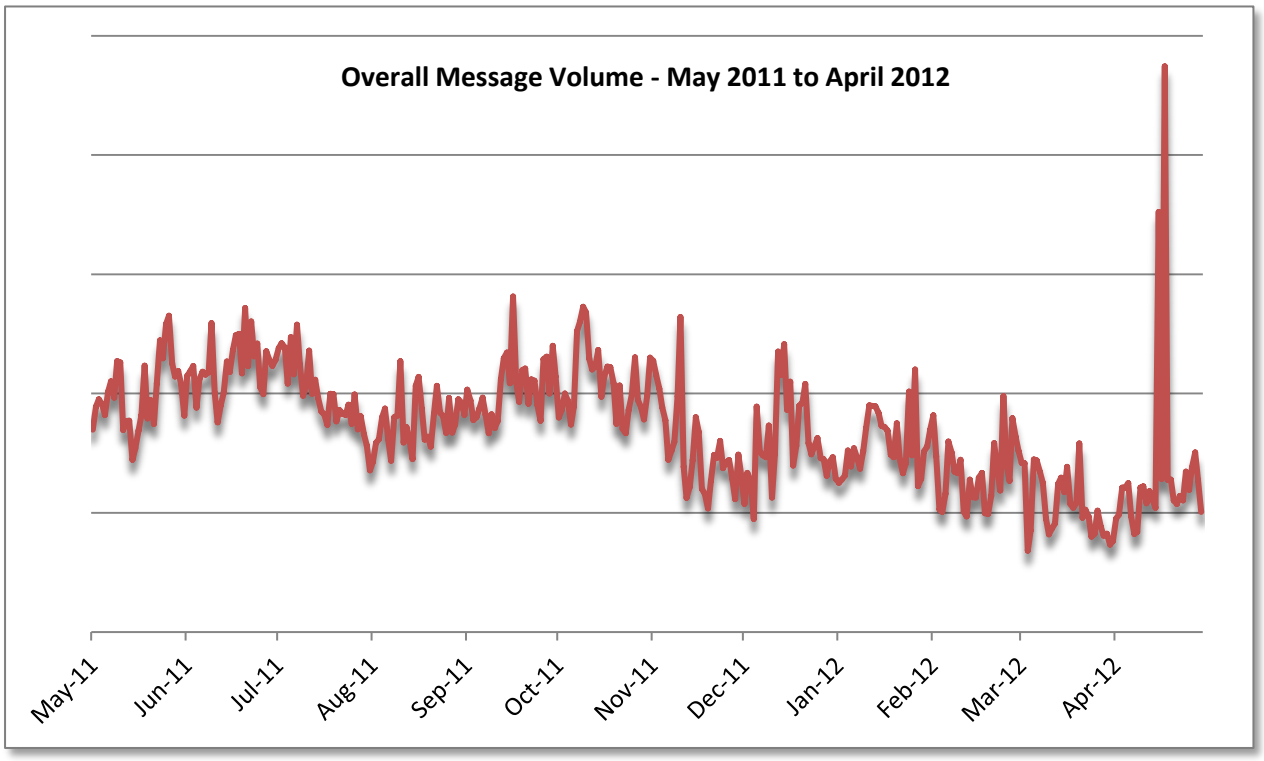


Spam Volume Trends（スパム量の変化）

4 月のスパム量グラフは中旬に2つのピークがあります。これらのピークは企業組織のトラフィックでは無く、多くが例外的なものでした。

全体として 4 月のスパム量は 3 月に比べて 26%増加しましたが、2011 年の 5 月に比べると 27%低い数値です。

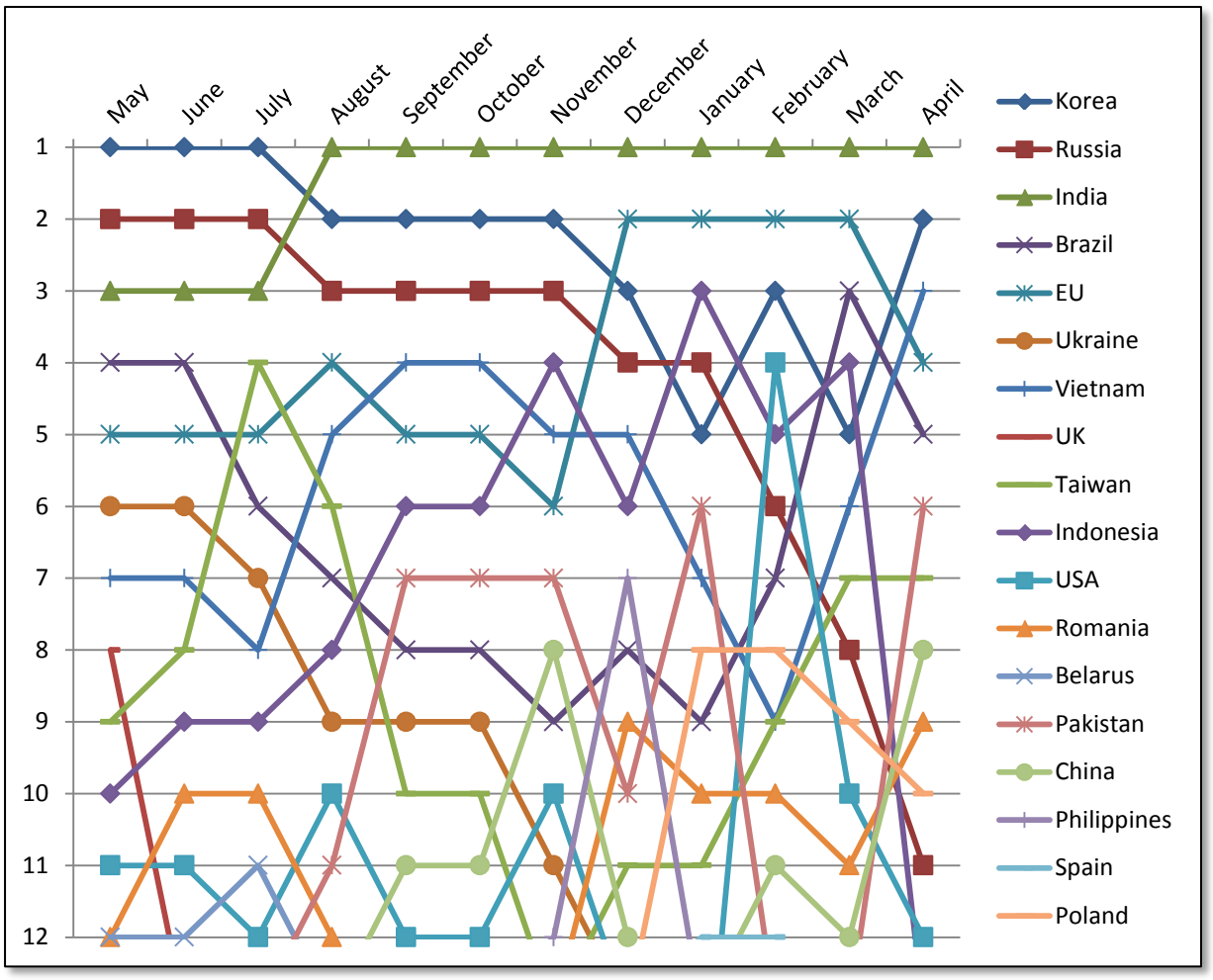




Source of Spam（スパムの発信源）

インドが2011年の8月からの連続トップです。ロシアは1月の4位から今月は11位と、順位を下げ続けています。
ベトナムが今月初めて3位になりましたが、スパム量の変化は不安定です。

Top Spam Senders by Country											
1	India	3	Vietnam	5	Brazil	7	Taiwan	9	Romania	11	Russia
2	Korea	4	EU	6	Pakistan	8	China	10	Poland	12	USA



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。