proofpoint

Proofpoint Threat Report

June 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)

Spam Research (研究成果)

私たちは常にスパマーの行動を研究しており、毎月毎月、様々な発見があります。しかし、この 6 月は特に興味深い月でした。一連の調査の結果、Proofpoint はカナダをベースに活動する、よく知られたスパマーグループに属する Web サーバーを特定したのです。

さらに調査を進めると、外部に公開されているいくつものディレクトリを発見しました。これらのディレクトリの中には、スパムのターゲットと思われる E メールアドレスのリスト(全部で 7,584,246 件もありました!)、過去のスパムに使われた IP アドレスのアーカイブデータ、そしてこれから使われると思われる 5,500 枚もの画像が含まれていました。私たちは、これらのコンテンツを管理していると見られる複数の人物も特定し、現在、さらに行動を監視しています。この発見により、このグループからの攻撃には確実に対抗しやすくなったと言えるでしょう。

Operation High Roller (グローバルなサイバー金融詐欺)

McAfee と Guardian Analytics は、6 月末に *Dissecting Operation High Roller* というレポートをリリースしました。(日本語版はこちら) このマルウェアは Zeus や SpyEye と同じファミリーに属するものですが、動作が高度に自動化されており、入力画面をシミュレートすることによって入力内容を捕捉し、二要素認証を突破します。攻撃はスピアフィッシングの手法を用いて拡散します。コンテンツは E メールの受

信者に合わせて作成されており、攻撃のボリュームは非常に少ないものです。この種の攻撃は、まさに Proofpoint が先頃発表した Targeted Attack Protection が想定しているものです。

Phishing Conviction

米連邦地検は、有線通信不正行為の共謀の疑いで Osarhieme Uyi Obaygbona が有罪判決を受けたと発表しました。 Obaygbona とその一味は、個人や金融機関に数百万ドルもの損失をもたらした複雑なたくらみに関わっていました。不正な Web ページで個人情報を収集し、偽の運転免許証と偽造したサインでその個人になりすましていたのです。その上で米 ADP 社（給与計算等のアウトソーサー）のアカウントにアクセスし、架空の従業員に給与を支払っていました。

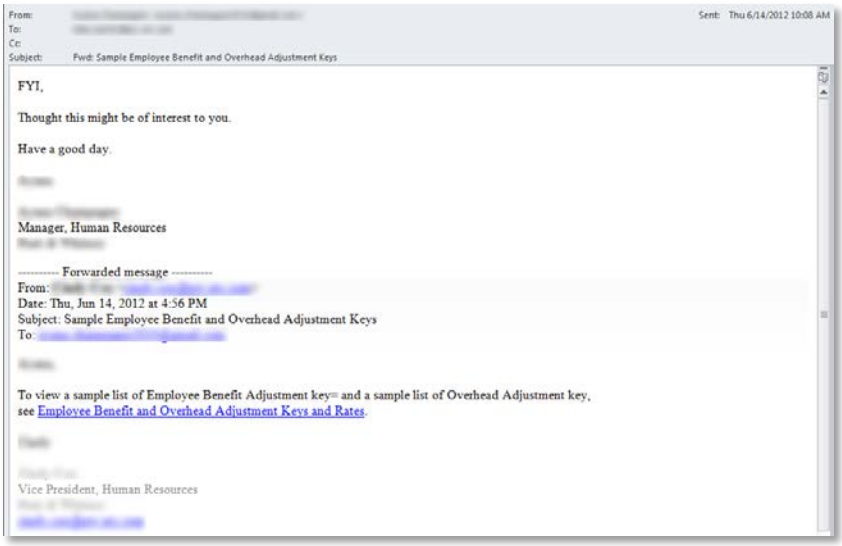
Flame

先月のこのレポートで紹介した Flame マルウェアについて、Microsoft が詳細な解析をリリースし、このマルウェアがどのようにして Microsoft certificate を偽造したかを解析しています。マルウェア制作者は MD5 ハッシュコリジョンを生成してコードサインに有効な証明書を作成していたということです。

Threat Models（手法）

Spear Phish (スピアフィッシング)

巨大な多国籍企業が、特定の個人を狙ったスピアフィッシングに晒されています。コンテンツが「普通に見える」ようにするためには、多大なリサーチを行う必要があります。



このスクリーンショットには、多くの個人名が含まれています。（ぼかしてありますが）これらは実際に子会社に所属している社員の名前です。この攻撃者は子会社についてだけでは無く、実際に進行中のプロジェクトについての概要も知っています。ここで使われている名前は、実際のプロジェクトのメンバーです。

「フォワードされた」メッセージは子会社から送られてきたもののように見えます。このメッセージは「人事担当マネージャ」の名前にひも付いた Gmail のアドレス宛に送られ、上のメールはその Gmail のアドレスから発信されています。

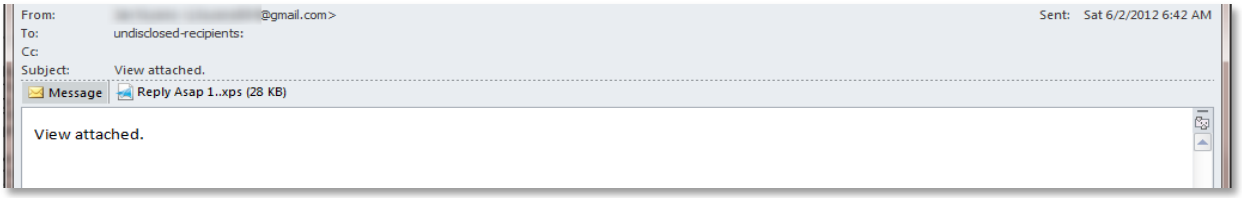
メール中の URL は汚染された Web サイト上の zip ファイルを直接指し示しています。この zip ファイルは CHM ファイルと PDF ファイルを含んでおり、開封された場合にはユーザーのシステムに感染します。CHM ファイルは古いバージョンの Adobe Acrobat をインストールしようとし、PDF ファイルにはセキュリティ設定を無効化する攻撃が含まれています。一番あり得るのは、その後に弱体化したセキュリティ部分を狙った攻撃が行われることです。

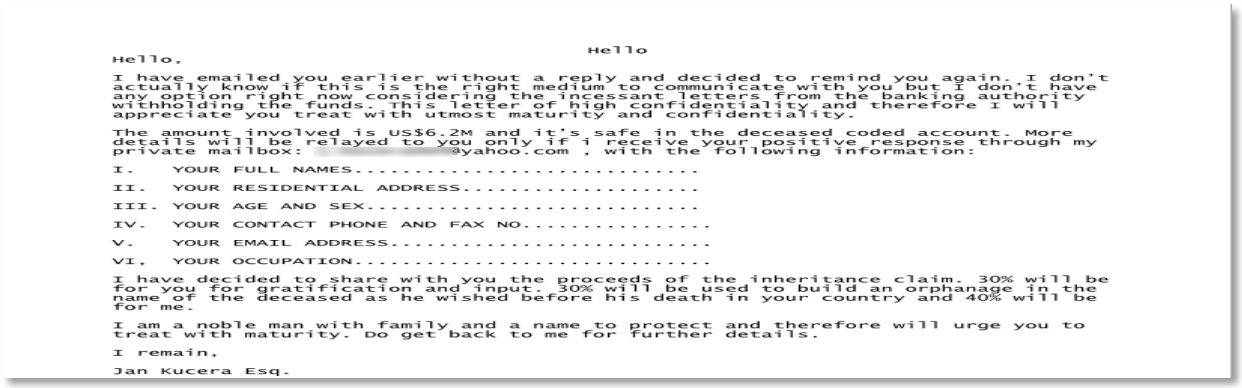
Safelisting (セーフリスト)

大量配信のソーシャルエンジニアリングメールに、有名ブランドを利用するのは、昔からよく知られた手法です。なりすまされた UPS と ADP による攻撃は何年も前から普通に行われています。しかし、この 6 月には通常よりも大規模な攻撃がいくつか見られました。いくつかのお客様からのレポートに、大量のメッセージの受信が報告されていたのです。何故でしょうか？これらのお客様は皆、送信者の ADP あるいは UPS をセーフリストに登録し、それらのメールは全て受信するよう設定しています。これはビジネス上重要なメールの取りこぼしを無くすためにセーフリストを活用するスパムソリューションでは一般的な運用です。しかし一方で、Proofpoint はセーフリストにメールアドレスを使うことを推奨していません。メールアドレスは「なりすまし」しやすいのです。その代わりに、Proofpoint ではホストネームまたは IP アドレスによるセーフリスト作成を推奨しています。Proofpoint ではまた、すべてのセーフリストまたはブロックリストがその時点でのビジネス目的に合致しているかどうかを定期的にレビューすることをお薦めしています。

419 Spam (ナイジェリアの手紙)

上記の UPS スパムと同様、419 スパム（ナイジェリアの手紙）もまた古い手法です。しかし、419 スパムの新しいアタッチメントタイプを発見しました。この最初のスクリーンショットはメール本文です。非常にシンプルな「添付を呼んで下さい」というメールです。添付ファイルは XPS ファイルで、一般的な XML ファイルです。ほとんどの OS で内容を表示できます。





Hello

Hello.

I have emailed you earlier without a reply and decided to remind you again. I don't actually know if this is the right medium to communicate with you but I don't have any option right now considering the incessant letters from the banking authority withholding the funds. this letter of high confidentiality and therefore I will appreciate you treat with utmost maturity and confidentiality.

The amount involved is US$6.2M and it's safe in the deceased coded account. More details will be relayed to you only if i receive your positive response through my private mailbox: @yahoo.com . with the following information:

I. YOUR FULL NAMES.....
II. YOUR RESIDENTIAL ADDRESS.....
III. YOUR AGE AND SEX.....
IV. YOUR CONTACT PHONE AND FAX NO.....
V. YOUR EMAIL ADDRESS.....
VI. YOUR OCCUPATION.....

I have decided to share with you the proceeds of the inheritance claim. 30% will be for you for gratification and input. 30% will be used to build an orphanage in the name of the deceased as he wished before his death in your country and 40% will be for me.

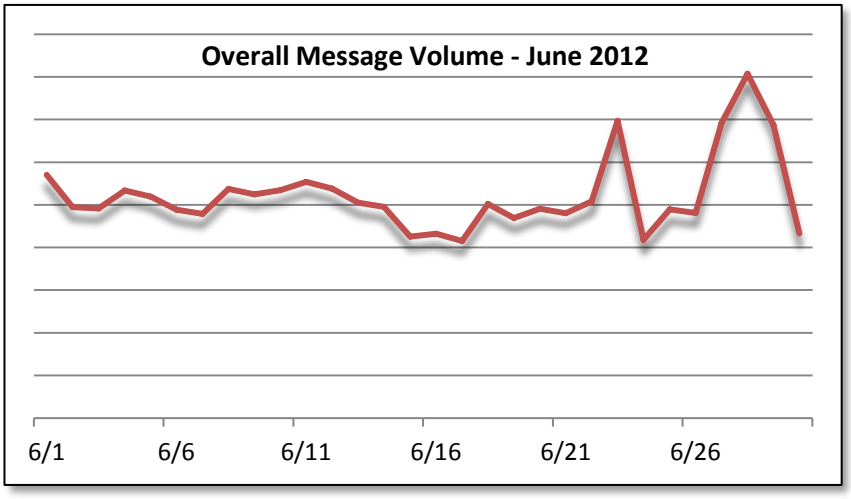
I am a noble man with family and a name to protect and therefore will urge you to treat with maturity. Do get back to me for further details.

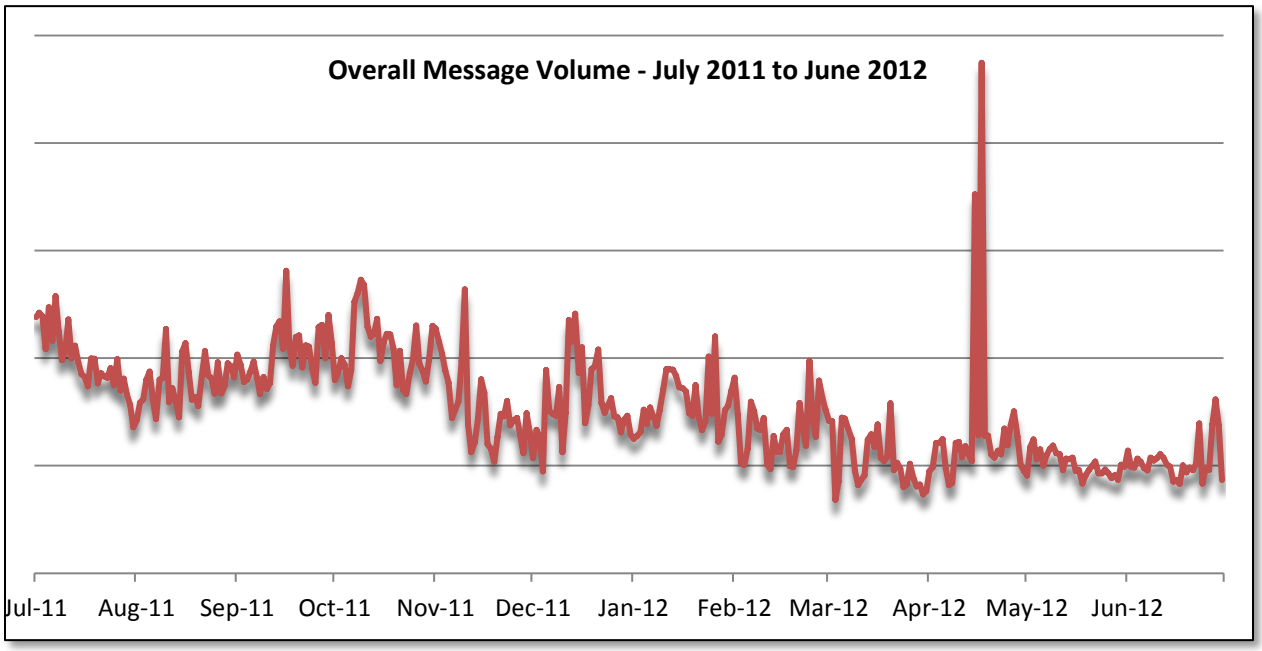
I remain,

Jan Kucera Esq.

Spam Volume Trends (スパム量の変化)

スパム量は今年 5 月と比べるとほぼ同じですが、昨年 6 月からは 53%ダウンしています。6 月の最後の数日に急増しましたが、これは標的型ではあるものの、大量配信スパムによるものでした。

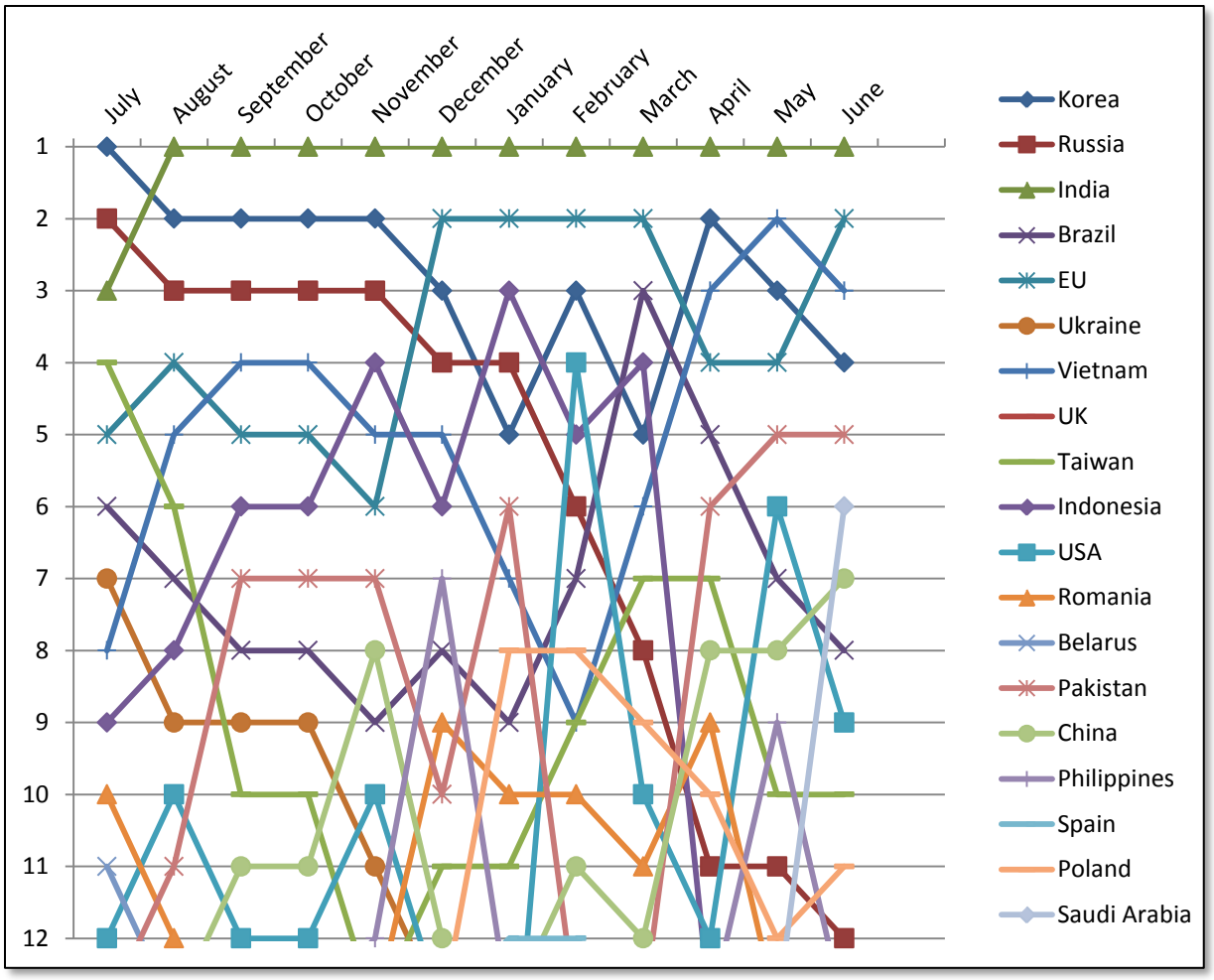




Source of Spam (スパム発信源)

インドが相変わらずスパム発信の世界一で、これは昨年 8 月から変っていません。今月最も注目されるのは、サウジアラビアがトップ 12 に初めて入ってきたことです。サウジアラビアは通常 20 位以下で安定していました。この変化については引き続き注意深く見守っていきます。

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



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。