proofpoint

Proofpoint Threat Report

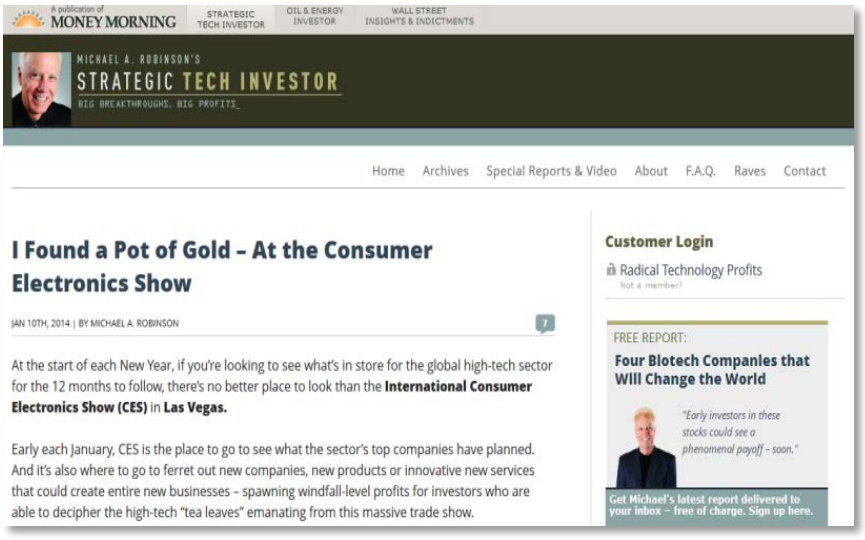
December 2013

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)

思わぬリターンを招く投資アドバイスに注意

1 年の終わりには、その年を振り返ると共に、来るべき年についての予想をするものです。特にこの時期、投資アドバイザーなどは引っ張りだこでしょう。しかし、そういったニュースレターやサイトに仕込まれた悪意のあるプログラムには十分気をつけなければなりません。



Proofpoint は、有名な Strategic Tech Investor のサイトがマルウェアに感染しているのを発見しました。よくあるウォータリングホール型の攻撃です。情報交換のコミュニティ、信頼性の高いコンテンツの利用など、サイト自身は正規のもので人気も高いのですが、ニュースレターが餌となっていました。「信頼性の高い Web サ

イトを使うやり方は、スピアフィッシングやその他のフィッシングには簡単に騙されない人々に対しても有効な戦略です。[1]」

この攻撃のでさらに興味深いのは、エクスプロイトキットの活用です。Proofpoint では、Black Hole の作者とされる人物が逮捕されて以降、攻撃手法がエクスプロイトキットを使わない手法に変化していることを観測しています。例えば、Dropbox を使う手法です。しかし今回の攻撃は Styx エクスプロイトキットを使っています。Styx を見分けるためには 3 つの特徴があります。まず第 1 に、ランダムな英数字を使った長い URL が挙げられます。第 2 に、Java のエクスプロイトが使われていること、そして最後に、エクスプロイトとしてランダムな文字列と同じトレーリングパラメータを使っていることです。3 つの特徴を図 2 にハイライトしました。

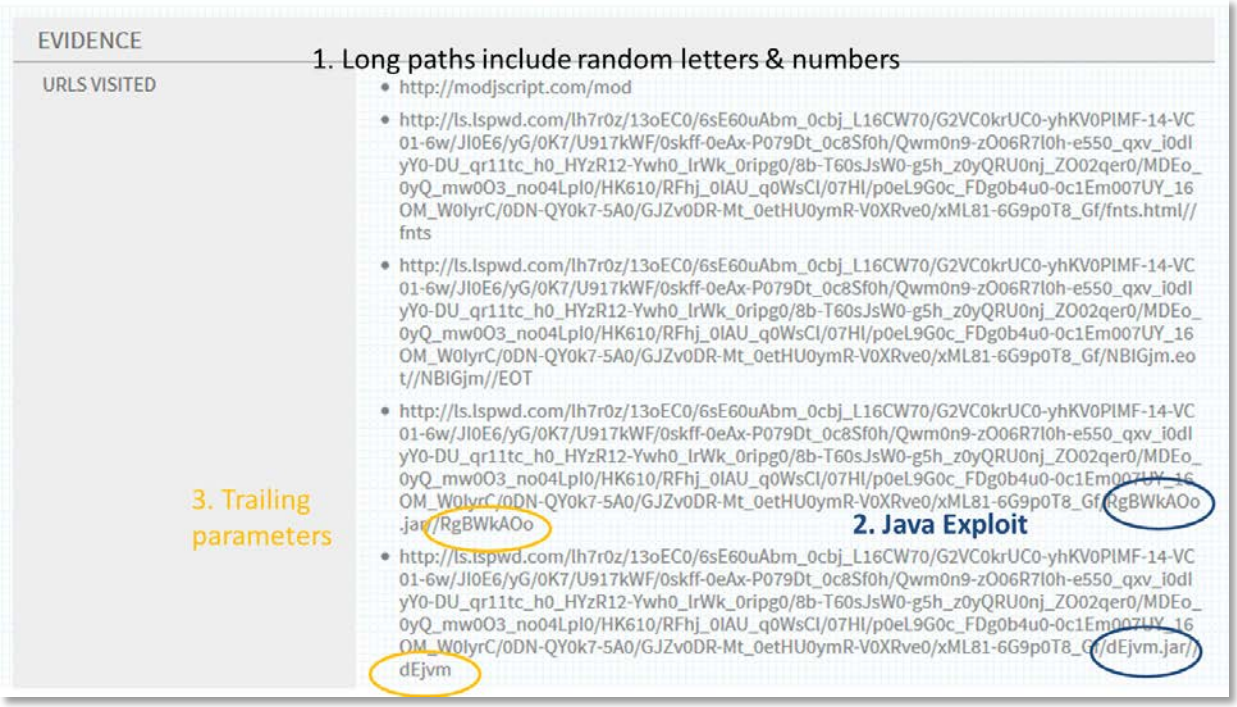
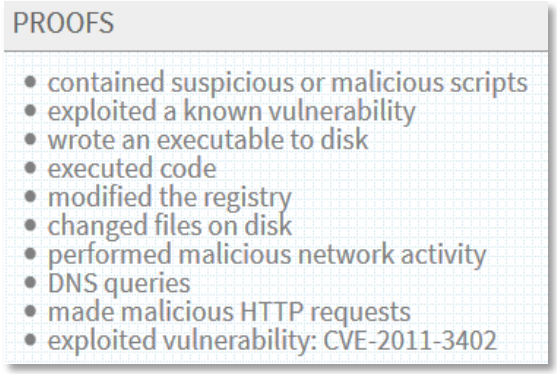


図 2: Styx エクスプロイトキットの特徴

Proofpoint の Dynamic Malware Analysis Service によるフォレンジック情報を見てみると、Styx は既知の脆弱性である CVE-2011-3402 を狙っていることが分かります。この CVE は Mitre.org のサイトに詳細があり [2]、IPA のサイトには「この脆弱性は、TrueType フォントファイルの処理に存在します。攻撃者は、この脆弱性を悪用した攻撃コードを埋め込んだウェブサイトを作成し利用者を誘導、または攻撃コードを埋め込んだ文書ファイルを作成し利用者に開かせます。利用者がそのウェブサイトを閲覧、または



[1] Wikipedia を参照: http://en.wikipedia.org/wiki/Watering_Hole
[2] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3402

文書ファイルを開いた場合、コンピュータを攻撃者により制御される恐れがあります。」とあります。図 4 に TrueType フォントの脆弱性を使った例を示します。

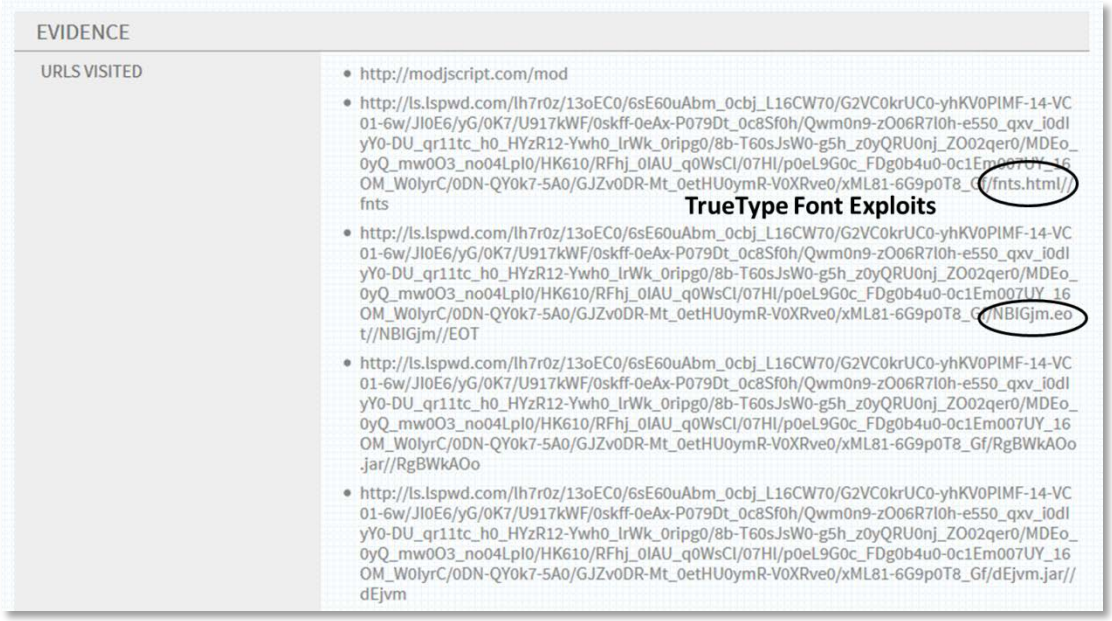


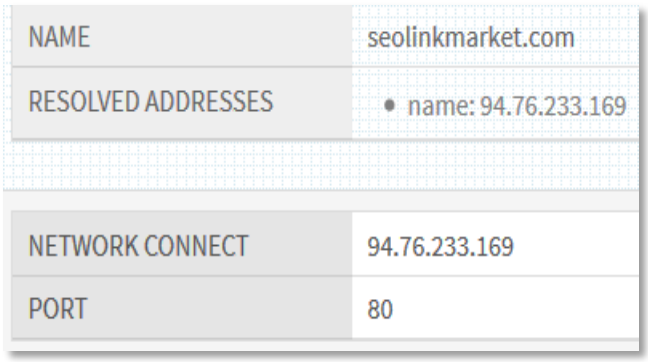
図 4: TrueType フォントエクスプロイト

図 4 の中の最初のリファレンスが fnts.html を指しており、名称から分かるように、これはフォントファイルです。2 つ目のリファレンスに含まれている .eot という拡張子は、Embedded Open Type (EOT) のことです。これらは「Microsoft が開発した Open Type のコンパクト版で、Web ページに埋め込むためのもの [3]」です。ターゲットマシンを侵害した後にダウンロードが始まり、ペイロードを実行します。実行ファイルは URL と同様のランダムな名前が付けられています。図 5 にダウンロードされた実行ファイルを示します。

図 5: 実行ファイル

[3] http://en.wikipedia.org/wiki/Embedded_OpenType

マシンが感染すると、マルウェアはコマンド&コントロール(C&C)サーバーにコールバックしようとします。図 6 の DNS クエリとネットワークアクティビティが詳細を明らかにします。



seolinkmarket.com とその IP アドレスは、Fareit/Tepfer マルウェアにリンクされています。Microsoft はこれを PWS:Win32/Fareit.gen!I と呼んでおり「パスワードを盗み出すトロイの木馬で、ログインやパスワードなどの秘密情報を集め、リモートの攻撃者に送ります。他のマルウェアをダウンロードすることも可能で、それには PWS:Win32/Zbot も含まれており、攻撃者があなたのコンピューターを操作できるようになります。[4]」と説明しています。PWS:Win32/Zbot は Zeus としても知られている、広範囲に存在するトロイの木馬で、オンラインバンキングへのログイン情報を盗み出します。いったん感染すると他の感染を引き起こし、亜種や他の目的を持ったマルウェアを呼び寄せます。

図 6: DNS とネットワークアクティビティ

クラウドベースのサンドボックス解析のような動的なマルウェア解析ツールは、攻撃の複数のレイヤーと複雑性についてのフォレンジック情報を提供できます。これらのツールは、刻々と変化するセキュリティ環境を管理者が把握できるようにサポートもします。例えば、マルウェアのインスタンスやフォレンジック情報が減少している場合、特定のマルウェアあるはファミリーが消滅したことを示していると考えることができます。さらに、巨大なマルウェアの亜種やプレイヤーが消滅したような場合にも、Proofpoint の Dynamic Malware Analysis Service のようなクラウドベースのサンドボックスは、これまで見つかっていなかった脅威についての重要なインサイトを提供でき、情報のギャップを埋めることができます。

Threat News (ニュース)

Experian の調査: 2014 年、ヘルスケア業界ではデータ流出が増える

InformationWeek は Experian の最近のレポートを引用して、2014 年はヘルスケア業界にとって厳しい年になるだろうと述べています。「*2014 Data Breach Industry Forecast*」の中で「2014 年、ヘルスケア業界は最もデータ流出の影響を受ける業界となるでしょう。」ビジネス規模の大きさと、新しい Healthcare Insurance Exchanges が、新しい脅威を生み出すということです。2014 年には HIPPA/HITECH 規制が完全適用となります。これらの強力な規制は、記録的な罰金を生み出すかも知れません。

[4] http://www.microsoft.com/security/portal/threat/encyclopedia/Entry.aspx?Name=PWS%3AWin32%2FFareit.gen!I

全文はこちらからご確認下さい: http://www.informationweek.com/healthcare/policy-and-regulation/healthcare-data-breaches-to-surge-in-2014/d/d-id/1113259

Adobe の流出データを悪用するハッカー達

Adobe 社がブログにて警告したところによると、Adobe のライセンスキーの配布を装ったフィッシング攻撃が行われていると言うことです。ブログでは、怪しいメッセージを削除し、添付ファイルやリンクをクリックしないよう呼びかけています。

Adobe 社のブログはこちら; http://blogs.adobe.com/psirt/?p=1035

Threatpost.com がメッセージの例を使ってもっと詳しい解説を行っています; http://threatpost.com/adobe-warns-of-new-license-key-scam-phishing-campaign/103278

英国の大企業の 93%が 2013 年に侵害を経験

イギリスの政府機関であるビジネス・イノベーション・職業技能省 (Department for Business, Innovation and Skills: BIS) の依頼により行われた調査によると、2013 年に大企業の 93%がセキュリティ侵害を経験したということです。より小さい企業の侵害率は 87%でしたが、2012 年の 76%からは上昇しています。攻撃と侵害は全ての産業のイギリス企業にコストを強いています。「大企業におけるセキュリティ侵害の最悪のケースでは、45 万ポンドから 85 万ポンドものコストがかかっており、小さな企業でも 3 万 5000 ポンドから 6 万 5000 ポンドの損害です。」詳細はこちらから; http://www.itproportal.com/2013/12/16/93-of-organisations-suffered-a-data-breach-in-2013/

Threat Insight Blog (ブログ)

この項では Proofpoint の新しいセキュリティブログである Threat Insight から、興味深いポストをご紹介します。Threat Insight の購読や会話への参加については以下をご覧下さい。

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

5 つ以上の攻撃者グループ: “docx.image” エクスプロイトキットを解剖

先頃報告されたゼロデイドキュメントエクスプロイト (CVE-2013-3906) は、複数の新しいテクニックを使っており、現時点で少なくとも 5 つの異なる攻撃者グループが攻撃に利用しています。これだけ短期間に複数の攻撃者に利用されていることから、このフレームワークは今後も MS Office ドキュメントへの攻撃に使われる可能性があると考えられます。

いくつかのベンダーが個々のインシデントについて別々のポストを書いていますが、このエクスプロイトフレームワークそのものについての総体的な検証はこれまで行われていません。以下のポストに全ての情報を集めました。

http://www.proofpoint.com/threatinsight/posts/dissecting-docx-image-exploit-kit-cve-exploitation.php

「詐欺の予防」を偽装する攻撃者の詐欺に注意!

先週私たちは、あるハッカーグループの復活を観測しました。このグループはかつて American Express ブランドを餌に使った攻撃を繰り返していたグループです。このグループは常に URL ベースの攻撃を行っており、この URL が、ランダムな文字列の最後が必ず index.html で終わることから、Proofpoint ではこのグループに「index.html」という名前を付けています。このグループは Blackhole の作者とされる Paunch が逮捕されるまでは Blackhole エクスプロイトキットを使った攻撃が主でしたが、復活後はアカウントを狙ったフィッシングに戻っています。

Full details are here; http://www.proofpoint.com/threatinsight/posts/attackers-using-the-guise-of-fraud-prevention.php

より「安全」にマルウェアを配信する攻撃者達

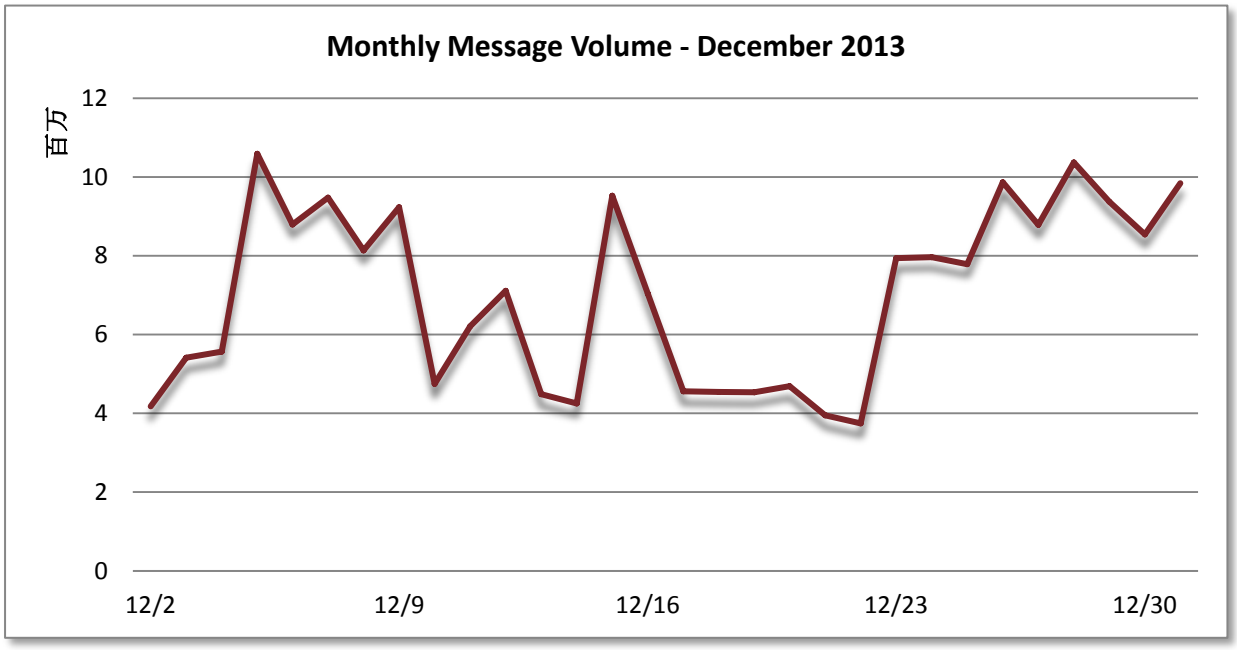
私たちは先頃、攻撃の中で SSL を使っている標的型フィッシングメールを観測しました。これは以前レポートした「Gameover」のような、トロイの木馬が悪意のあるペイロードを取得するために暗号化された SSL 接続を使うというものとは異なります。今回見つかったのは、攻撃者が SSL で保護された URL を標的型攻撃メールに組み込むもので、URL はマルウェアを含んだ zip ファイルにリンクされています。リンクをクリックしたユーザーのうち、何人かが zip ファイルを開くことを期待しているのでしょう。この手法は一般的なドライブバイダウンロードよりも成功率は低くなりますが、エクスプロイトキットを使った攻撃のような複雑なインフラが必要無いというメリットがあります。

The full post can be found at; http://www.proofpoint.com/threatinsight/posts/attackers-making-malware-delivery-more-secure.php

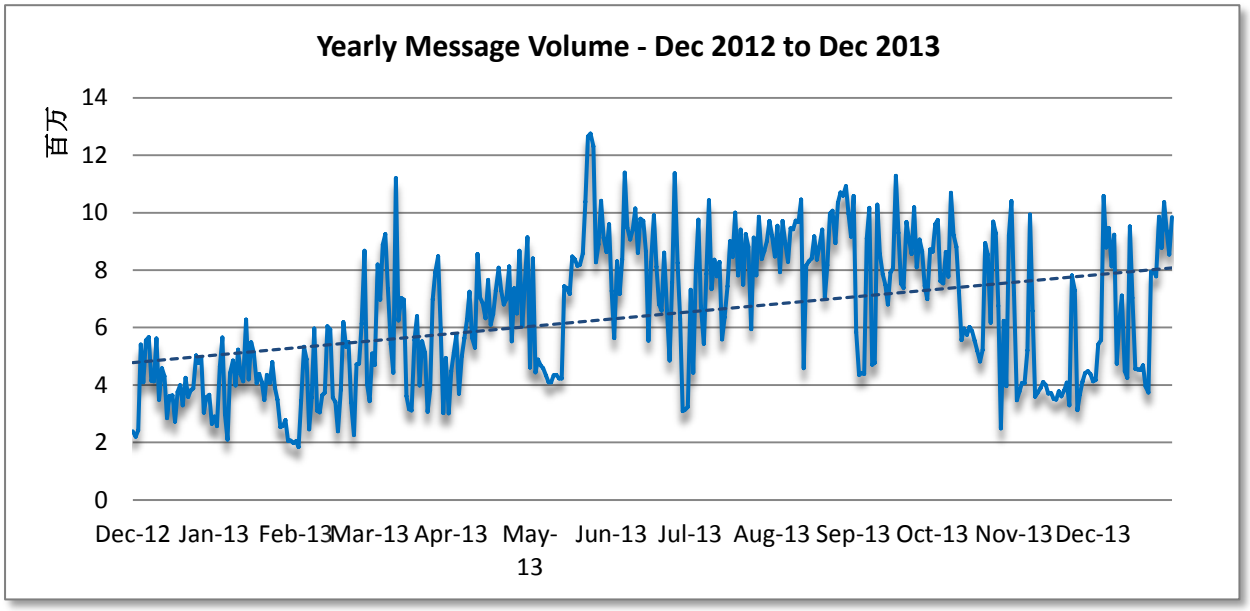
Threat Trends (トレンド)

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。11 月に減少したスパム量は 12 月に増加しました。月間を通じて不安定な動きを見せており、400 万通/日に満たない日もあれば、1,000 万通/日を超える日が何日かあり、広い範囲の中を揺れ動いています。月初めにピークがあり、10 日前後にいったん落ち込んだ後、中旬にまた急増しました。スパム配信者は休日前に早めの休みを取り、月末へ向けて大量のスパムを配信したようで、月末には 1,000 万通を伺う日が 3 日もありました。



スパム量は 12 月に入って強力なパターンに戻り、前月比の増加量は 53.25%でした。また、前年同月比は 75.88%で、これはこれまでの最高記録です。2013 年全体では 16.90%の増加でした。ハッカーへのプレッシャーとは別に、スパム配信者は元気なようです。



Spam Sources by Country (スパム発信源)

いつものメンバーが戻ってきました。EU は引き続き世界ースパムを生み出している地域として悪名を轟かせました。US はいつものナンバー2 に返り咲き、中国は 3 位に後退しました。アルゼンチンが 4 位、インドが 5 位に戻ってきました。以下のテーブルは過去 6 ヶ月間の順位です。

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

以下の表は、各国が総スパム量に占める割合を示したものです。EU はボリュームで 17.78%増加し、引き続き世界一のスパムを産み出しています。中国はパーセンテージ上は他国と同様に下がっていますが、5.27%を記録しました。

November 2013			December 2013		
1	EU	13.97%	1	EU	16.99%
2	China	12.22%	**2**	US	6.34%
3	US	7.26%	**3**	China	5.27%
4	Japan	3.37%	**4**	Argentina	4.46%
5	India	3.33%	**5**	India	3.41%

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