proofpoint

Proofpoint Threat Report

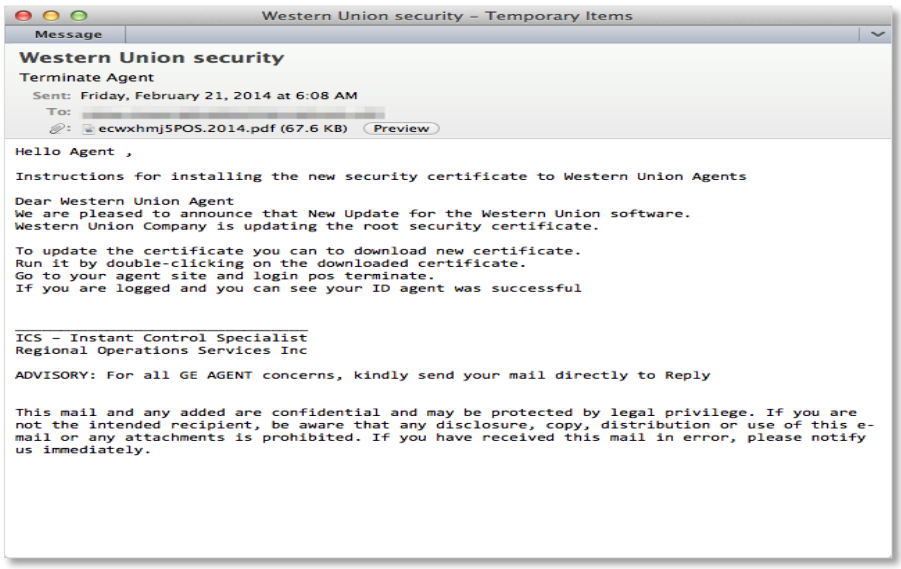
February 2014

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)

Attachment Defense が悪意のある PDF 攻撃を検知

Proofpoint TAP の新機能である Attachment Defense が、悪意のある PDF 添付ファイルを検知しました。以下は攻撃に使われたメッセージのサンプルです。


Western Union security – Temporary Items

Message

Western Union security

Terminate Agent

Sent: Friday, February 21, 2014 at 6:08 AM

To:

: ecwxhmj5POS.2014.pdf (67.6 KB) Preview

Hello Agent ,

Instructions for installing the new security certificate to Western Union Agents

Dear Western Union Agent
We are pleased to announce that New Update for the Western Union software.
Western Union Company is updating the root security certificate.

To update the certificate you can to download new certificate.
Run it by double-clicking on the downloaded certificate.
Go to your agent site and login pos terminate.
If you are logged and you can see your ID agent was successful

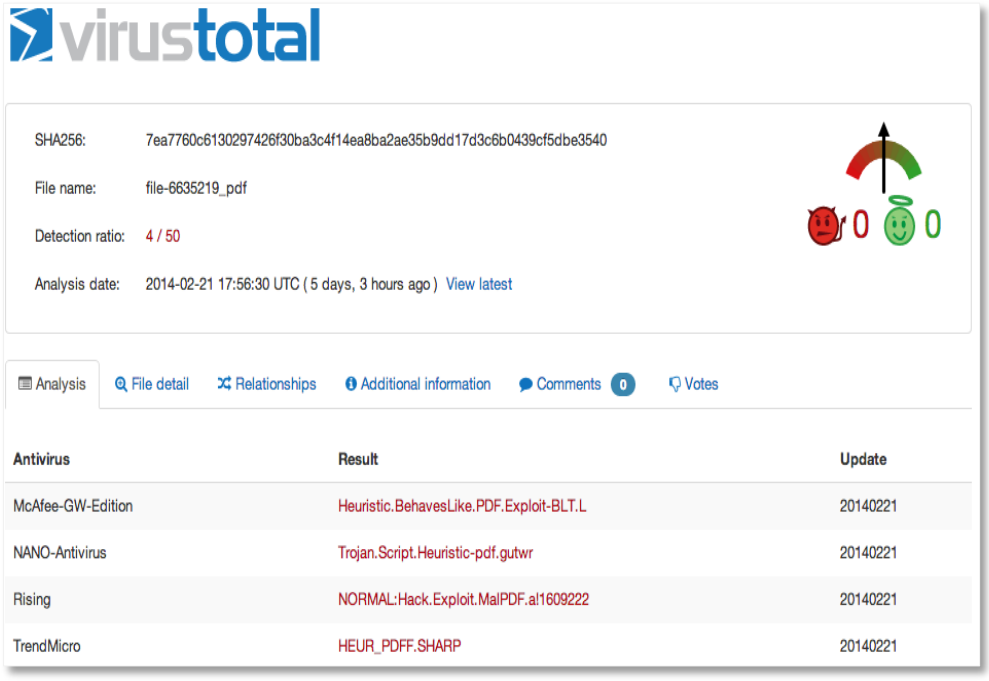
ICS – Instant Control Specialist
Regional Operations Services Inc

ADVISORY: For all GE AGENT concerns, kindly send your mail directly to Reply

This mail and any added are confidential and may be protected by legal privilege. If you are not the intended recipient, be aware that any disclosure, copy, distribution or use of this e-mail or any attachments is prohibited. If you have received this mail in error, please notify us immediately.

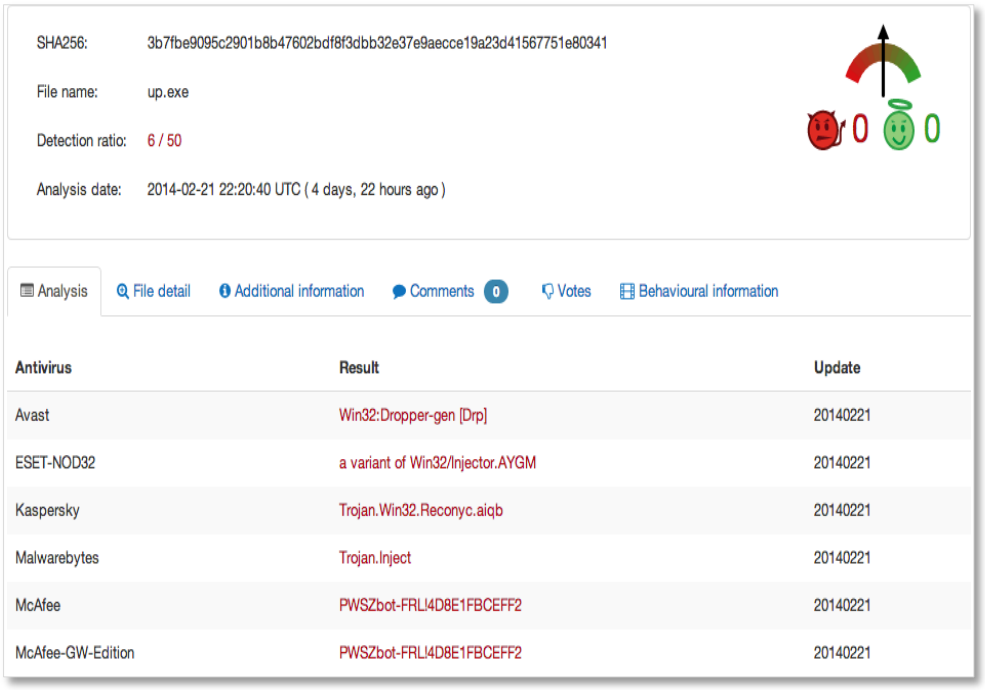
私たちは Proofpoint のお客様 49 社に送られた 326 通のメッセージと、1 社に送られた 268 通のメッセージを検討しました。攻撃に使われたメッセージ量は少なく、標的は十分に絞られていた (スパム検知にはかかりませんでした) ため、全体の 99.3%のメッセージが配信されました。

メールに添付された PDF ファイルは悪意を持ったもので、Adobe Reader を使ってこのファイルを開くと自動的に hxxp://playstation14[.][tld]/apps/up[.]exe から Gamarue trojan をダウンロードしてインストールします。このメッセージが配信されてから 5 時間後の時点で、50 種類のアンチウイルスソリューションのうち 4 つしかこのファイルを検知できませんでした。



この悪意のある添付ファイルは、4 日後にはさらに 3 つのアンチウイルスエンジンでも検知できました。

Gamarue マルウェアの検知率も同様に低く、感染から 6 時間後でも 50 個のうち 6 個のエンジンでしか検知できませんでした。



SHA256: 3b7fbe9095c2901b8b47602bdf8f3dbb32e37e9aecce19a23d41567751e80341

File name: up.exe

Detection ratio: 6 / 50

Analysis date: 2014-02-21 22:20:40 UTC (4 days, 22 hours ago)

0 0

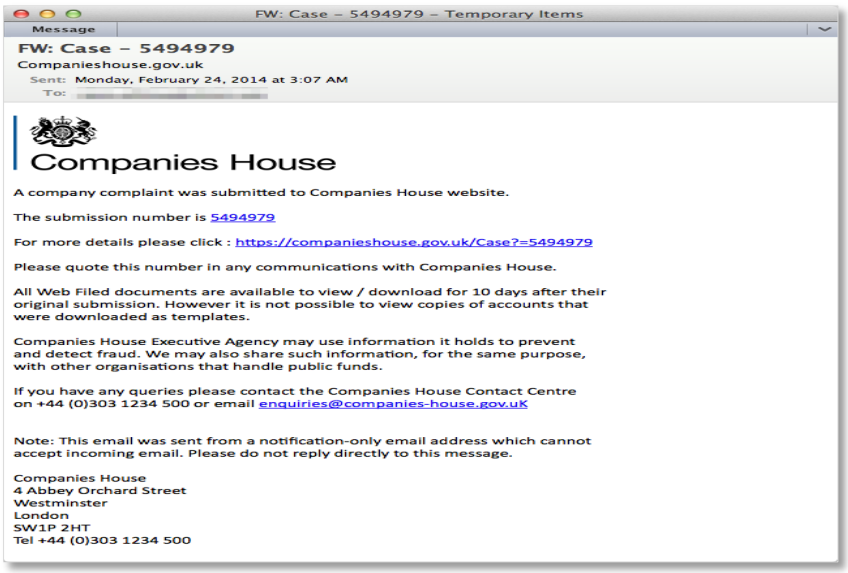
Analysis | File detail | Additional information | Comments 0 | Votes | Behavioural information

Antivirus	Result	Update
Avast	Win32:Dropper-gen [Drp]	20140221
ESET-NOD32	a variant of Win32/Injector.AYGM	20140221
Kaspersky	Trojan.Win32.Reconyc.aiqb	20140221
Malwarebytes	Trojan.Inject	20140221
McAfee	PWSZbot-FRLI4D8E1FBCEFF2	20140221
McAfee-GW-Edition	PWSZbot-FRLI4D8E1FBCEFF2	20140221

また、このマルウェアを正確に特定できたエンジンが無かったことも注目に値します。これは全ソリューションに共通の課題といえます。

女王陛下のスパム

このところ私たちの関心を集めていたのは、英国を狙った悪意のあるメールの増加です。特に、ここ 4 ヶ月ほど活動を控えていた ru8080 グループが、UK ブランドを使ったフィッシングメッセージで存在感を示しています。現時点で 2 つのテンプレートが確認されており、どちらも Redkit および Angler エクスプロイトキットを使い、GameOver Zeus マルウェアの拡散を狙っています。サンプルを 2 つご紹介します。



FW: Case – 5494979 – Temporary Items

Message

FW: Case – 5494979

Companieshouse.gov.uk

Sent: Monday, February 24, 2014 at 3:07 AM

To:

Companies House

A company complaint was submitted to Companies House website.

The submission number is 5494979

For more details please click : https://companieshouse.gov.uk/Case?=5494979

Please quote this number in any communications with Companies House.

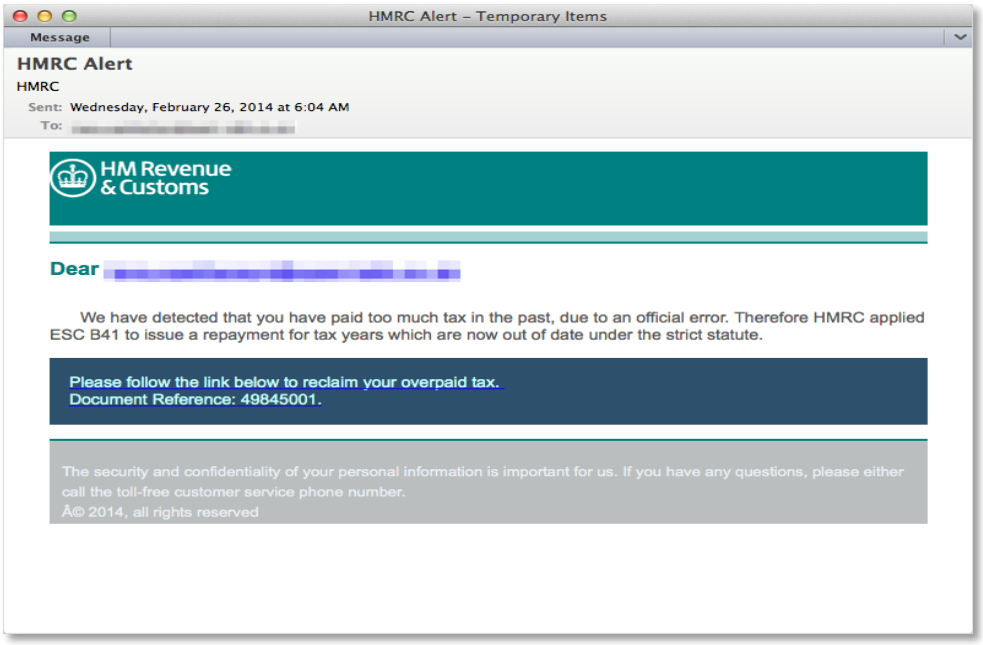
All Web Filed documents are available to view / download for 10 days after their original submission. However it is not possible to view copies of accounts that were downloaded as templates.

Companies House Executive Agency may use information it holds to prevent and detect fraud. We may also share such information, for the same purpose, with other organisations that handle public funds.

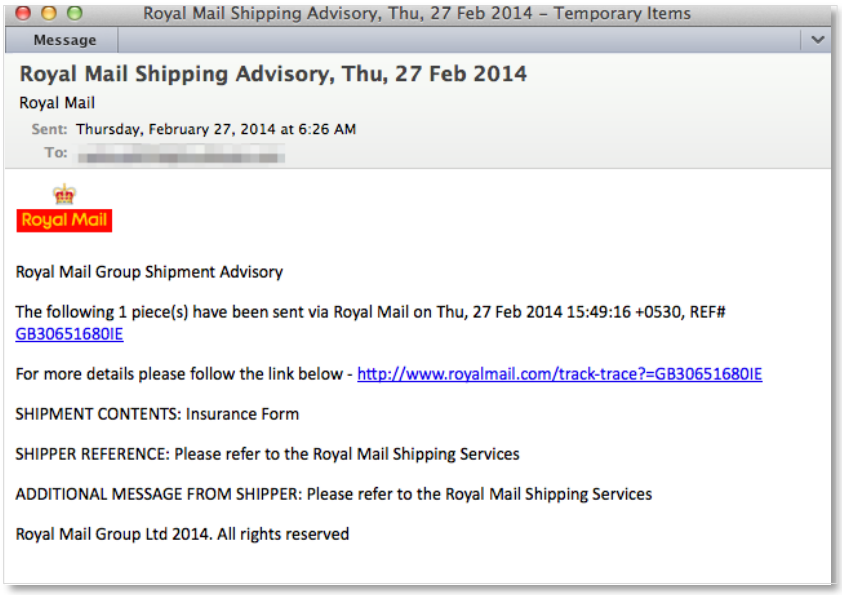
If you have any queries please contact the Companies House Contact Centre on +44 (0)303 1234 500 or email enquiries@companies-house.gov.uk

Note: This email was sent from a notification-only email address which cannot accept incoming email. Please do not reply directly to this message.

Companies House
4 Abbey Orchard Street
Westminster
London
SW1P 2HT
Tel +44 (0)303 1234 500



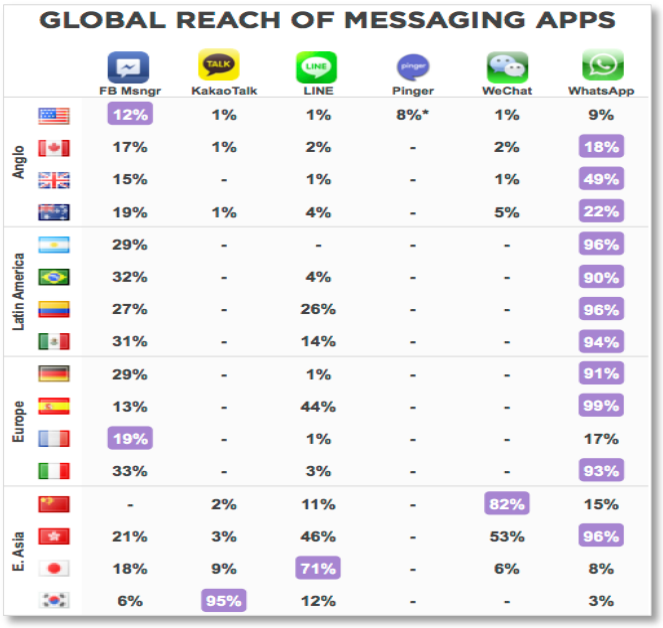
その他の例を以下に示します。



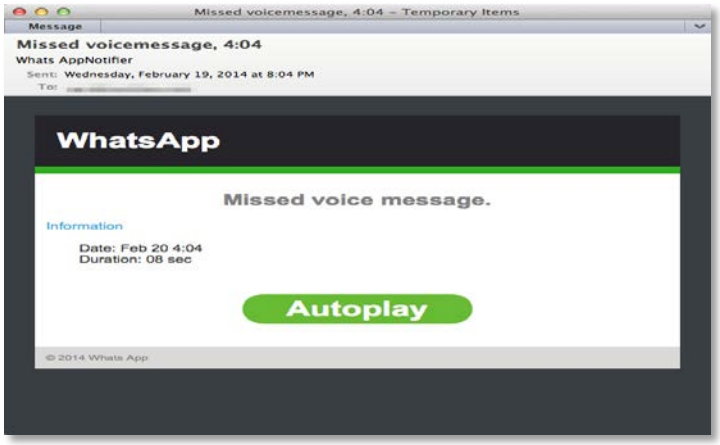
上記メッセージ中の URL は、はえなわ型攻撃を行うグループに好んで使われている Angler エクスプロイトキットに誘導されています。Angler は最新の Flash ゼロデイ脆弱性に対応した最初のキットで、こういった対応の早さはこのキットが精力的に開発されていることを示しており、それが広く活用されている理由でもあります。

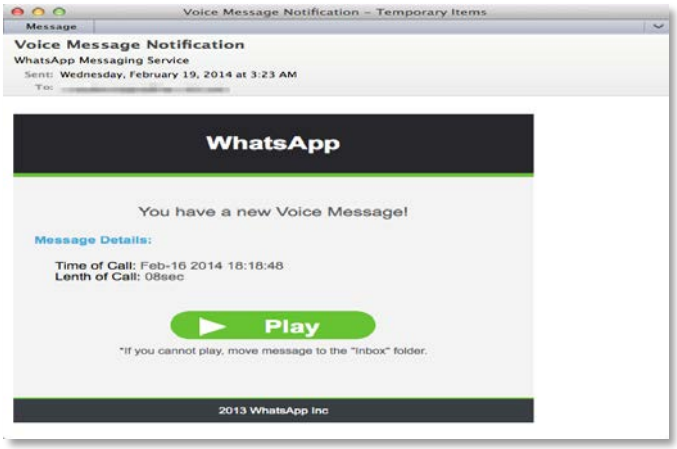
WhatsApp とは何か?

Facebook が WhatsApp を 190 億ドルで買収すると発表しました。WhatsApp は私たちがこれまで観測した中でも、最も悪用されているブランドの一つです。以下のチャートから、US ではそれほどではないものの、世界的には良く知られたブランドであることが見て取れます。



買収のニュースを祝うために、フィッシング攻撃者たちは 2 つの異なるはえなわ型攻撃を開始しました。各々の攻撃で使われたメッセージのサンプルを示します。どちらのほうが良くできていると思いますか?





Threat News (ニュース)

米国の納税シーズンにあわせたフィッシング詐欺とマルウェア攻撃

US-CERT (United States Computer Emergency Readiness Team)が、アメリカ人に向けて詐欺の被害に遭わないためのタイムリーな警告を発しました。納税シーズンのフィッシング攻撃には様々なパターンがありますが、還付金に関するものや申請方法に関するものが含まれます。だまされないためのアドバイスとして、一方的に送られてきたメール内の URL をクリックしないこと、疑わしいメッセージについて IRS に報告するためのやり方などを掲載しています。詳しい情報については以下をご覧ください。

https://www.us-cert.gov/ncas/current-activity/2014/02/26/US-Tax-Season-Phishing-Scams-and-Malware-Campaigns.

調査: データ流出は若干減少、しかし脅威レベルは引き続き高い

Ponemon Institute が毎年発表している医療患者のプライバシーとデータセキュリティに関する調査に、データ流出とヘルスケアのセキュリティトレンドについて、いくつか興味深いものがありました。最も大きな問題は、ヘルスケア機関の HIPAA “Breach Notification”ルールへの適合です。また、健康情報の交換におけるセキュリティの信頼性がいまだに低いということが興味を引きます。この問題と、その他のいくつかの発見について詳細に分析されています。詳細は Healthcare Informatics でご覧いただけます。

http://www.healthcare-informatics.com/article/survey-data-breaches-decline-slightly-threat-remains-high

Smuckers がデータ流出でオンラインストアを閉鎖

データ流出事故はすべてを変えてしまいます。今回のケースでは捜査のためにオンラインストアが閉鎖されました。こうした結果は厳しい法規制が原因のため、不可避ともいえますが、ビジネス上のリスクが大きいことを再認識させられます。閉鎖による影響は、売り上げの消失、顧客の信頼の喪失、ブランドの毀損におよびます。詳しくは以下をご覧ください。

http://blog.usfoodsafety.com/2014/03/10/smuckers-closes-online-store-for-data-breach.

ラトガース大をはじめとする米国の大学が学生の銀行口座情報を狙ったフィッシング攻撃を警告

学生、教授、職員を狙ったフィッシングメールが国中にあふれています。ラトガース大およびその他のフロリダ州からワシントン州までの大学が銀行口座情報のために狙われています。詳しい記事は以下です。

http://www.northjersey.com/news/rutgers-other-colleges-across-us-warn-of-phishing-scheme-to-steal-student-bank-information-1.735872.

Threat Insight Blog (ブログ)

Proofpoint のセキュリティブログである Threat Insight から、興味深い記事をピックアップしました。皆様も Threat Insight のディスカッションに是非ご参加ください。

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

ボットの再構築

Microsoft の ZeroAccess Botnet の解体 (Microsoft が相当数の侵害されたシステムを取り除き、攻撃者のフィッシングメール送信や DDoS 攻撃、ビットコイン採掘などの能力に影響を与えた) の後、攻撃の減少が観測されています。

この減少が一時的なものか、長く続くものかを見極めるために、Proofpoint の研究者は最近の攻撃を分析しました。その結果、攻撃の減少だけでなく、ターゲッティングとペイロードの面で明白な (悪い意味で) 変化が観測されました。詳しくは以下のエントリをご覧ください。

http://www.proofpoint.com/threatinsight/posts/re-building-the-bots.php.

企業ユーザーが悪意のあるリンクをクリックするのはどのデバイスからか?

モバイルデバイスの普及に伴い、電子メールの 65%がモバイルデバイス上で最初に開封されていると推定されていることから、私たちは企業においてはどうなのかを考えてみました。

はえなわ型攻撃に関して Proofpoint が行った過去の調査結果から、私たちは企業ネットワーク外のユーザーによるクリック数の平均を調べ、5 回のうち 1 回のクリック (20%) が VPN 外のデバイスから行われたものであることを突き止めました。次の論理的な疑問は、ユーザーが悪意のある URL をクリックしたときにどのタイプのデバイスからメールにアクセスしていたか、ということです。全文は以下のエントリでご覧ください。

http://www.proofpoint.com/threatinsight/posts/what-devices-enterprise-users-clicking-malicious-links-from.php.

繰り返しクリックする人 - 企業にとっての問題児か

企業は最新の攻撃との戦いを続けています。はえなわ型、スピアフィッシング、あるいはウォータリングホール型攻撃などです。このような場合に、マシンの侵害を招きかねないユーザーの PC 使用を禁止するというのは、荒っぽいですが有効なアプローチです。ユーザーへの教育がうまくいかない場合、より厳しい措置をとることによってセキュリティリスクを最小化できるというのは昔ながらの知恵です。これら「繰り返しクリックする人たち」が企業に与える影響を調べました。詳しくは以下をご覧ください。

http://www.proofpoint.com/threatinsight/posts/repeat-clickers-the-key-problem-for-enterprises-or-are-they.php.

侵害の人的要因についてのレポート

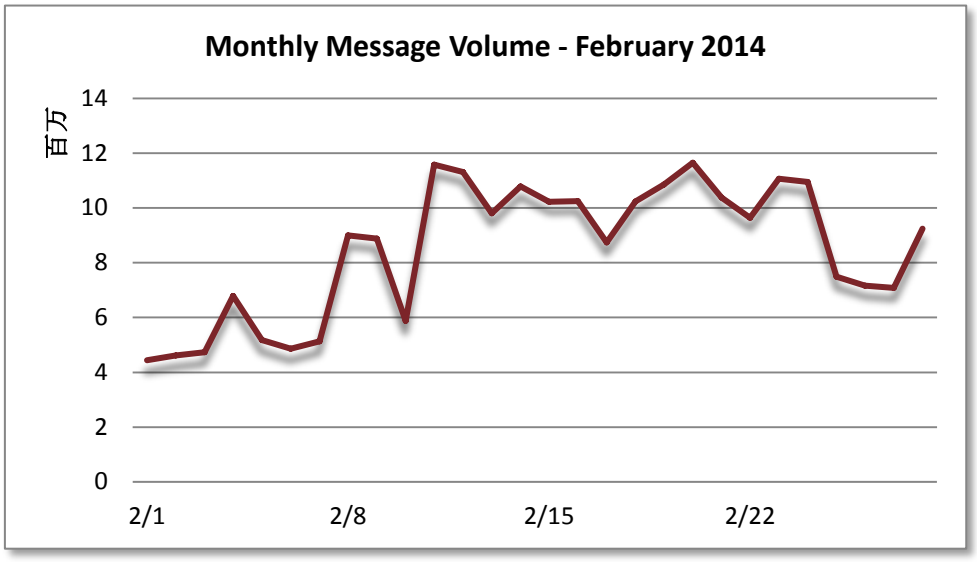
Proofpoint は、これまで ThreatInsight で発表してきた研究結果をまとめたレポートについてプレス発表しました。組織においてユーザーの行動とその傾向が悪意のある攻撃の成功にどのように関連しているかについてまとめたものです。以下からダウンロードしてご覧ください。

http://www.proofpoint.com/threatinsight/posts/the-human-factor.php.

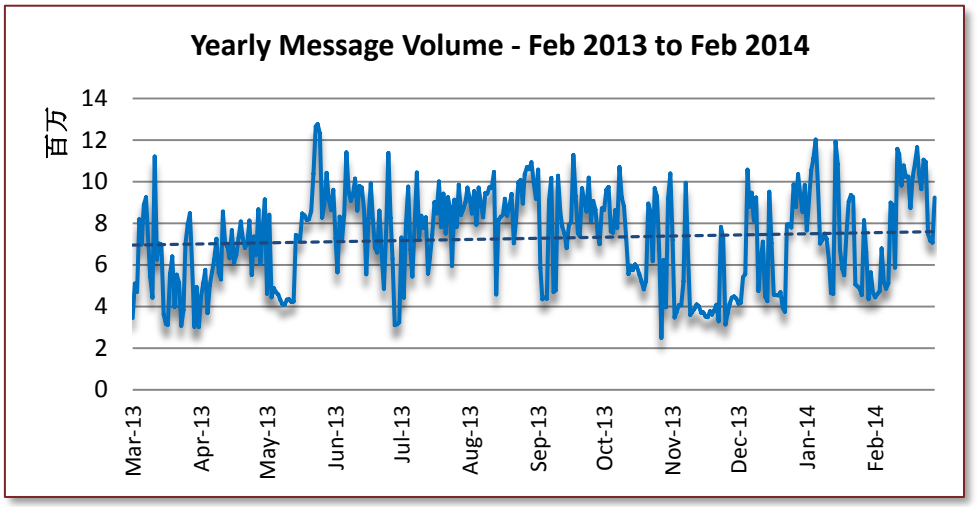
Threat Trends (トレンド)

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。2 月は先月に引き続き変わった月でした。1 日あたりのスパム量が最大 1,100 万通/日から 400 万通/日まで揺れ動きました。月初めは最小で月末近くに最大値を記録しました。7 日あたりに落ち込み、月中に急増しています。月末は増加傾向にあります。



スパム量は引き続き増加し、1 月に比べて 14.75%増えました。全体の量は過去最高で前年に比べて 99.32%の増加でした。



Spam Sources by Country (スパム発信源)

2 月にはいつもの容疑者が戻ってきました。EU は引き続き世界一のスパム発信源としての悪名をキープしました。US も同じく第 2 位です。アルゼンチンも 3 位でしたが、4 位は中国を押さえてロシアが入りました。以下は過去 6 ヶ月間のスパム発信源トップ 5 です。

		Sept '13	Oct '13	Nov '13	Dec '13	Jan '14	Feb '14
Rank	1st	EU	EU	EU	EU	EU	EU
	2nd	US	US	China	US	US	US
	3rd	India	India	US	China	Argentina	Argentina
	4th	Argentina	Argentina	Japan	Argentina	China	Russia
	5th	Taiwan	China	India	India	India	China

以下の表は、各国が総スパム量に占める発信量の割合を示したものです。EU の数値は全加盟国を含んでおり、以前よりも正確に傾向をつかむことができます。EU は引き続き世界一スパムを発信しており、今月は 38.57%でした。他の 4 カ国合わせても約 15%と、EU の半分にも満たない数値です。

January 2014			February 2014		
1	EU	35.99%	1	EU	38.57%
2	US	6.20%	**2**	US	6.06%
3	Argentina	3.84%	**3**	Argentina	4.07%
4	China	3.49%	**4**	Russia	2.73%
5	India	3.43%	**5**	China	2.69%

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