proofpoint

Proofpoint Threat Report

April 2015

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様々な脅威に関する情報、詳細、トレンドなどをまとめたものです。

Threat Models (手法)

The Human Factor 2015: 攻撃者はビジネスユーザーに狙いを変えた

2014 年、Proofpoint はセキュリティにおける「Human Factor (人的要因)」についてのレポートを発表しました。(https://www.proofpoint.com/us/human-factor-2014) このホワイトペーパーで、Proofpoint の研究者は幅広い調査を元に、電子メール関連の脅威におけるエンドユーザーの役割を明らかにしました。ユニークなデータ中心のアプローチにより、現状が非常に厳しいことを示しています。

この調査では、メールの中の悪意のあるリンクを誰がクリックしたのかを特定し、クリックされやすいメールテンプレートは何か、ユーザーが何時、どこでクリックしたのかを判別し、さらにはその理由までを検証しました。その結果、企業のスタッフは、業務開始前に大量に配信されるソーシャルメディアの「招待」(フィッシング) メッセージを頻繁にクリックしていることがわかりました。そして、20%のクリックが企業ネットワーク「外」で行われていたのです。

この他、新しい発見については Human Factor 2015 (https://www.proofpoint.com/us/id/WP-Human-Factor-Report-1) でご覧頂くことができます。

2014 年の動きで特筆すべきことは、エンドユーザーへの教育が効を奏し、フィッシングが脅威であることが認知され始めたことです。これにより、エンドユーザーは

1. よく使われるフィッシングテンプレートを見分けることができるようになりました
2. 未承認メールに気をつけるようになりました

一方で、エンドユーザーのサイバー犯罪への理解が浸透したため、攻撃者達はその標的を中間管理職層に移行し始めています。2014 年末までに、犯罪者達は攻撃手法を変え、違う標的を狙うようになりました。この傾向については以下のブログもご覧ください。

https://www.proofpoint.com/us/threat-insight/post/The-Human-Factor-2015

「詐欺に注意!」を呼びかける新手のフィッシング攻撃

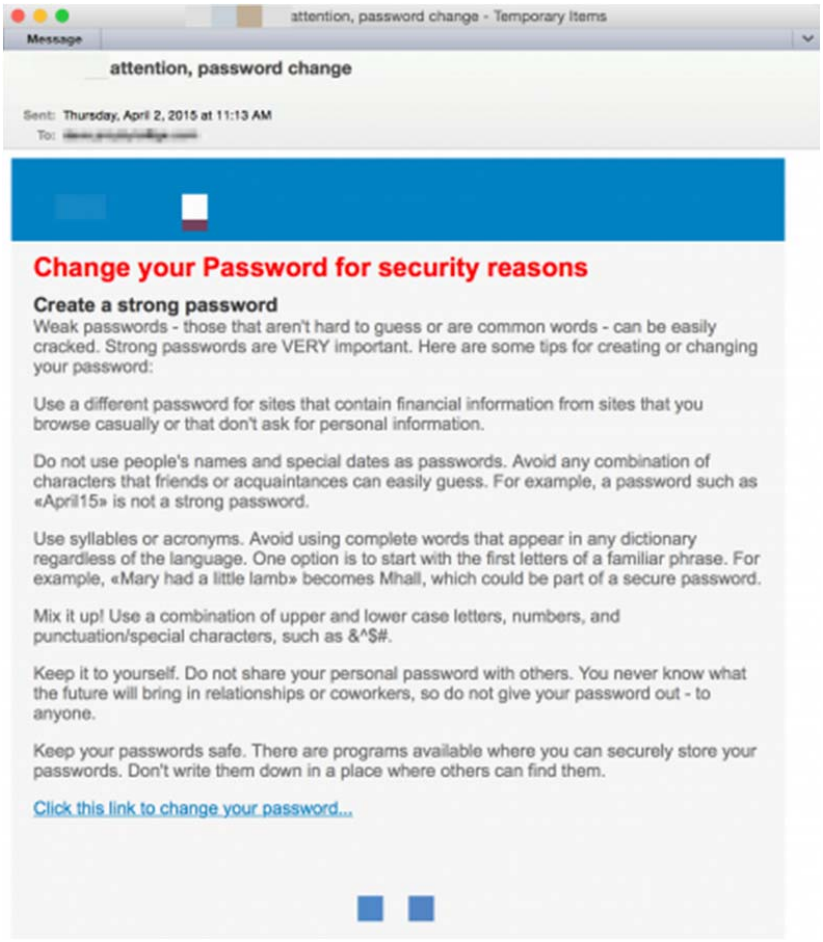
今年初め、Proofpoint では税金関連のフィッシングで使われる餌をいくつか分析しました (https://www.proofpoint.com/us/threat-insight/post/Tax-Return-Malware-Attacks) が、それによって明らかになったのは、攻撃者は被害者の不安や好奇心につけ込んで、手早い利益を得ようとしているということです。ユーザーに悪意のあるリンクや添付ファイルをクリックさせることが最終目的です。

この中で、ある餌はフィッシングメール、悪意のあるリンク、そして電話ベースのソーシャルエンジニアリングを組み合わせていましたが、興味深いことに、最近発見された Dyre 攻撃でも同様な手法が見られました。(https://threatpost.com/dyre-banking-malware-a-million-dollar-threat/112009)

今年の税申告時期にも税還付申告を餌にした詐欺が多く見られましたが、Proofpoint では攻撃者の使う餌が IRS を装うものから、税申告ツール向けに詐欺防止を呼びかけるものに変化していることを発見しました。一つの例としては、定番の税申告ソフトウェアパッケージ向けにパ

スワードリセットの案内を装ったものがあります。これは Angler エクスプロイトキットにリンクされていました。この攻撃は標的型攻撃の特徴も持っており、通常、数十万通が送られる一般的な攻撃に比べ、メール数が非常に少ないのも特徴です。

餌はよく考えられており、税申告におけるよくある心配を煽る内容になっています。



リンクをクリックすると、Angler エクスプロイトキットのサーバーに接続します。特筆すべきは、各メッセージに含まれている URL には個々に違ったホストネームが使われており、この攻撃全体の検知率を大幅に引き下げていることです。

最終的にエクスプロイトキットが侵入に成功すると、Bedep トロージャン (http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Win32/Bedep#tab=2) がインストールされます。これは、主に他のマルウェアのダウンロードやデータ窃盗、詐欺広告ツールなどとして機能します。

ベンジャミンフランクリンはかつて、「この世で確かなものは、税金と死だけだ」と言いました。

しかし、サイバー犯罪者が標的を狙い、潜り込み、操作し、そして制御しようとしていることは、それと同じくらい確かなことです。このケースでは、詐欺に気をつけるよう呼びかけるメールが餌になっている、ということです。よく考えられています。

Threat News (ニュース)

コールセンターでのデータ流出に対し、FCC が AT&T に 2500 万ドルの罰金を課す

米連邦通信委員会 (FCC) は、2013 年と 2014 年に起こったコロンビア、メキシコ及びフィリピンのコールセンターでのデータ流出事件について、AT&T と前例の無い合意に達しました。米国の顧客情報約 28 万人分が流出したのです。その中には、名前、社会保障番号 (全部もしくは一部) に加え、「保護された」顧客関連情報 (への不正アクセス) が含まれています。

この事件に、2500 万ドルの罰金が課されました。

FCC の法執行局によると、これは情報セキュリティまたはプライバシーに関する罰金としては史上最高額で、総額では米国の過去最高額になるかも知れないと言うことです。

FCC はその意図を明確に示しています。データプライバシーに関することについては、厳しく対処すると言うことです。

International Association of Privacy Professionals (IAPP) の社長であり CEO である J. Trevor Hughes によると、「FCC は明確な目標を持ち、積極的に行動している」ということです。

詳しくはこちらをご覧ください: http://www.scmagazine.com/att-fined-by-fcc-for-breaches-in-three-call-centers/article/408114/.

サイバー脅威インテリジェンスの重要性の認識と活用の間の断絶

サイバー脅威に関するインテリジェンスの無い企業は、サイバー攻撃によって被害を受けるリスクが高いという調査結果が出ました。最新の、正確ですぐに行動に結びつけることができるデータをタイムリーに入手することは、効果的な対策を行うために不可欠です。

新たに発表された「*Importance of Cyber Threat Intelligence to a Strong Security Posture*」レポートでは、重要なインフラを守る為のサイバーセキュリティを実用的なソリューションとするためには、サイバー脅威インテリジェンスの活用が重要であることを解説しています。

Webroot が Ponemon Institute に依頼して行ったこの調査では、ほとんどの企業が、完全なサイバーセキュリティ防御のためにはサイバー脅威インテリジェンスが必須であると考えており、そう考える十分な根拠があるとも述べています。

以下に本調査でわかった主なポイントを挙げます

- 調査対象企業の 40%が過去 24 ヶ月に重大なセキュリティ侵害を受けている。
  - そのうち 80%は、サイバー脅威インテリジェンスがインフラの一部として組込まれていたら、攻撃を防げたか、被害を最小限に抑えられただろうと考えている。

- 回答者のうち、たった 36%しか、自社のサイバーセキュリティが強力だと考えていない。
  - つまり、現在のサイバーディフェンスへの取り組みは無力だと考えてられている。
- 回答者の半数近くが、攻撃に対抗し、被害を最小限に抑えるために、サイバー脅威インテリジェンス情報の蓄積を増やしている。

この調査は、全米 693 人の IT 及び IT セキュリティのプロフェッショナルを対象にしています。回答者の 61%は、フォーチュン 1,000、グローバル 2,000、フォーブスの「Largest Private Companies」に所属しています。

この続きはこちらで: http://www.darkreading.com/vulnerabilities---threats/survey-reveals-disconnect-between-perception-and-use-of-cyber-threat-/d/d-id/1319796.

Dropbox がハッカーグループに反撃

無料のファイルホスティングサービスである DropBox は、同社のクラウドストレージサービスを不正利用して Bartalex マクロマルウェアを保存し拡散したハッカーグループに対して反撃を行いました。

Trend Micro のアナリストである Christopher Talampas は、米国内で金融取引を電子的に行う Automated Clearing House (ACH) を狙った攻撃を調べているときに、偶然この攻撃を発見しました。

最終的に、Dropbox はリンクを共有していたアカウントの機能を停止しました。

Trend Micro では、攻撃の最盛期には 1,000 を超える悪意のある Dropbox リンクがマルウェアをホスティングしていたことを明らかにしました。

さらに詳しくはこちらで: http://www.v3.co.uk/v3-uk/news/2406081/hackers-spreading-bartalex-macro-malware-with-phishing-attacks.

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.

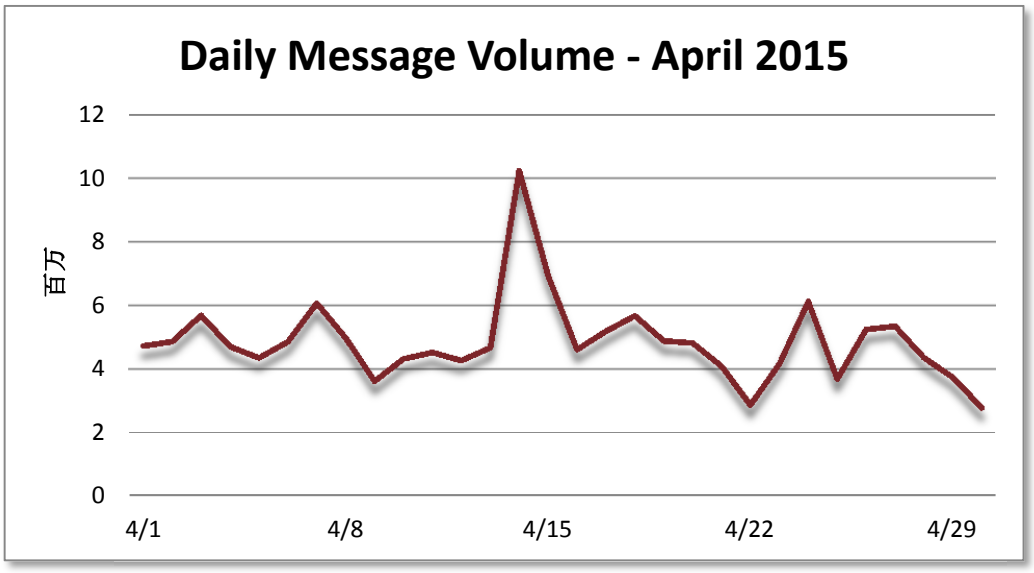
今後ブログの内容には、上の URL からアクセスしてください。本レポートのブログのセクションは、今後 Threat Model に統合されます。

Threat Trends (トレンド)

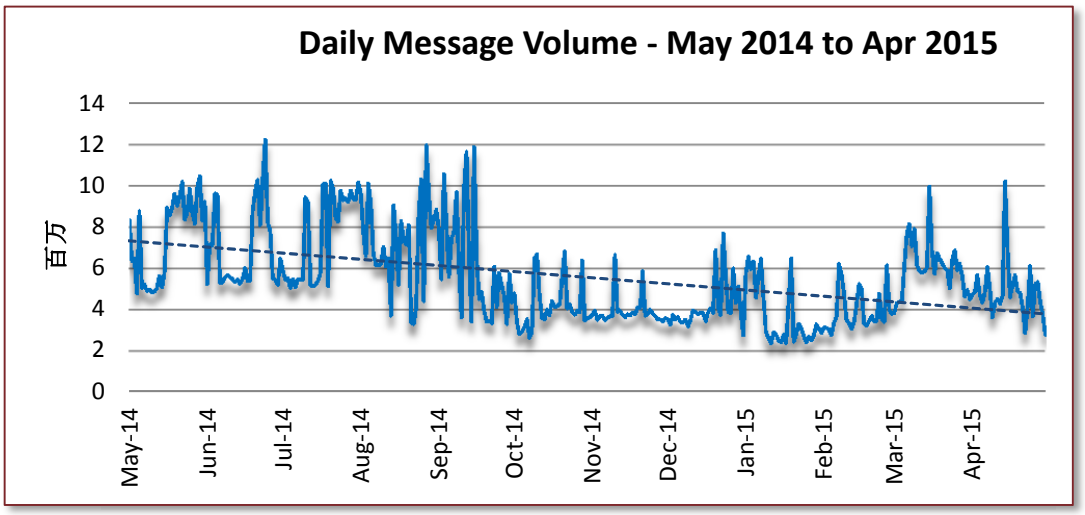
Spam Volume Trends (スパム量のトレンド)

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。

4 月のスパム量は不安定でした。400 万通/日を超えて始まり、最初の 2 週間近くは 600 万と 400 万の間を行き来し、月中にいきなり 1,000 万通に達しました。その後すぐに急落し、3 週目は 500 万通から始まり、その後は月の前半と同様の動きを見せ、最終的に 300 万通/日で終りました。



3 月と 4 月を比べると、全体のスパム量は 19.46%減少しました。対前年比では 36.60%の下落です。



Spam Sources by Region and Country (スパム発信源)

EU が 5 ヶ月連続で 1 位、アメリカは 4 ヶ月連続で 2 位です。中国は伸び悩んで 3 位、インドは 2 ヶ月連続で 4 位でした。

以下は、過去 6 ヶ月間のスパム配信量上位 5 カ国の表です。

		Nov '14	Dec '14	Jan '15	Feb '15	Mar '15	Apr '15
Rank	1st	China	EU	EU	EU	EU	EU
	2nd	EU	China	US	US	US	US
	3rd	US	US	Vietnam	Vietnam	Russia	China
	4th	Russia	Russia	Argentina	Argentina	India	India
	5th	Argentina	Vietnam	China	Russia	China	TBD

以下の表は、各国が総スパム量に占める発信量の割合を比較したものです。EU の数値はすべての加盟国を含んでおり、より正確な比較ができます。EU が世界のスパムの 14.45%を配信しており、残りの 4 ヵ国を合わせると 18.34%と、EU を少し上回ります。

March 2015			April 2015		
1	EU	30.89%	**1**	EU	14.45%
2	US	9.75%	**2**	US	10.45%
3	Russia	5.24%	**3**	China	6.73%
4	India	4.97%	**4**	India	1.16%
5	China	3.06%	**5**	TBD	TBD

以下は、EU 内の過去 6 ヶ月間のスパム配信量上位 5 カ国の表です。

March 2015			April 2015		
1	France	3.56%	**1**	Italy	1.09%
2	Italy	3.28%	**2**	Netherlands	0.84%
3	Germany	3.19%	**3**	UK	0.49%
4	Spain	2.54%	**4**	Germany	0.44%
5	UK	1.62%	**5**	Czechoslovakia	0.43%

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