proofpoint™

Proofpoint Threat Report

March 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)

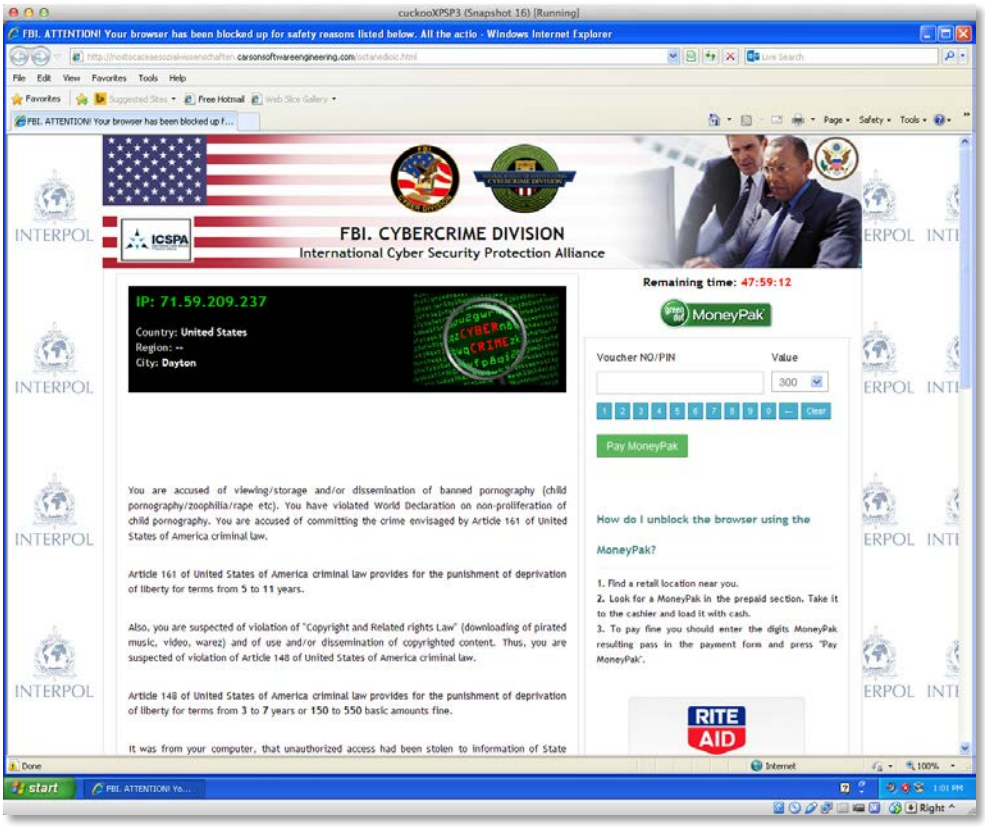
FakeLocker

先頃、私たちは興味深い「はえ縄型攻撃」を観測しました。この攻撃は、最初はよく見かける Facebook のメールテンプレートを使っていましたが、その中に他とは違う「パスワードリセットについて」のテンプレートを使っているものがありました。このテンプレートの方がクリックさせる効果が高いと考えられます。

予想通り、「let us know immediately (パスワードリセットの要求をしていない場合、すぐにご連絡下さい)」のリンクは Facebook ではなく、悪意のあるペイロードを指しています。このメールはよく見かける「友達リク

エスト」を装ったものよりも高いクリック率を得られるでしょう。私たちのソリューションはこのメールを通しませんでしたので、幸いにもお客様でこのリンクをクリックした例はありませんでした。

しかし、ユーザーがもしこのリンクをクリックしたとしても、マルウェアをインストールする「ふり」をするだけで、実際にエクスプロイトキットに誘導されることはありません。飛び先の Web サイトは、ブラウザを強制的にフルスクリーンモードに切り替え、押し売りウイルスの「Reveton」ファミリによく似た画面を表示します。以下に私たちの仮想マシン上で再現した画面を掲載します。



なぜ感染の「ふり」をするだけで、実際のマルウェアをインストールしないのでしょうか? それは、ユーザーを騙してマルウェアをうまくインストールさせるのは非常に困難だからです。Javascript を使って画面を閉じることができないようにしたり、そのページから移動できないようにしたりして、あたかも「感染してしまった」ように見せかけることができれば、それで十分な場合もあります。あまりコンピュータに詳しくないユーザーであれば、これだけでお金を振り込んでしまうかもしれないのです。

巨大ボットネットから配信された Orange 請求書マルウェア攻撃

英携帯キャリア Orange を装った請求書マルウェアスパムが米太平洋標準時 3 月 10 日の午前 4 時 9 分に始まりました。メッセージは「Orange Community」「Orange Recent bills」「ORANGE UK」からのもので、<alerts@orange.co.uk>というメールアドレスとセットになっています。

全てのメッセージで以下の 2 つの件名が使われています。

1. ”Orange Accounts”
2. “Orange Billing”

そして、以下の URL が使われています。

- hxxp://i.imgur.[tld]/a8jsSqW.png?1
- hxxp://i.imgur.[tld]/hKn9R3a.png

さらに、メッセージにはポリモーフィックなファイルが添付されています。

Bill_scaned_\S+.zip

この攻撃は米太平洋標準時 3 月 10 日月曜日午前 4 時 10 分付けのスパム定義ファイル main-1403100046 で防ぐことができます。

Threat News (ニュース)

裁判所が前例のないデータ流出の和解案を承認

2 月 28 日、フロリダ州の米連邦裁判所がデータ流出の被害者を救うための 300 万ドルの和解案を承認しました。これは被害者が証拠を示さなくとも救済が受けられるという前例の無いものです。この事件はフロリダを拠点とする健康保険会社の AvMed が起こした不祥事で、ノート PC が盗まれて顧客データが数万件流出しました。この和解案に関する詳細は以下をご覧ください。

http://www.computerworld.com/s/article/9247017/Court_approves_first_of_its_kind_data_breach_settlement

世界最大級のデータ流出事故を集めたグラフィックス

世界最大級のデータ流出事故のインフォグラフィックスが公開されています。3 万件以上のデータ流出事故を集めています。http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

政治的ハッカーのフィッシング攻撃で Microsoft の醜聞が公に

Microsoft の企業ネットワークが成功裏に侵害されたとする注目すべき推定証拠が存在するということです。容疑者は悪名高いシリア電子軍(SEA: Syrian Electronic Army)です。SEA はスピアフィッシングによってソーシャルメディアのアカウントやプライベートネットワークを侵害したり、報道メディアを狙うハッカー集団です。今回のケースでは、Microsoft の Global Criminal Compliance チームと FBI の Digital Intercept Technology Unit の間の秘密通信が傍受されました。記事はこちらからご覧頂けます。

http://arstechnica.com/security/2014/03/taken-in-phishing-attack-microsofts-dirty-laundry-aired-by-hacktivists/

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

実現するまで騙し続ける

Proofpoint の研究者は偽の Facebook メールを使った興味深い「はえ縄型攻撃」を発見しました。偽の Facebook 攻撃は以前にもあり、今回のものも最初は以前の攻撃と変わりませんでしたが、すぐに興味深い展開を見せました。

この攻撃では、Facebook の「パスワードのリセット」を騙るメールから始まります。ユーザーが「let us know immediately」のリンクをクリックすると、Facebook ではなく他のページに飛び、悪意のあるペイロードをダウンロードします。続きはこちらからどうぞ。

http://www.proofpoint.com/threatinsight/posts/fake-it-till-you-make-it.php.

電子メールは 2014 年も依然として最大の脅威? (これまで以上に)

米大手スーパーTarget のカード情報流出に続き、今年に入ってからもメリーランド大学のデータ流出、Sally Beauty、Neiman Marcus、Michaels、シアーズなどでのカード情報の流出、フォーブスの Web サイト侵害など、大規模な侵害が続いており、最近では Uroburos マルウェアなども発見されています。

セキュリティは最新の多様な脅威の前に負け続けているようにも見えます。

これらの攻撃の多くに共通する要素があります。最初の感染が電子メールを経由したものであるということです。

電子メール。

2013 年に行われた標的型および APT 攻撃の実に 95%が、この何十年も昔から使われている、主にテキストベースのコミュニケーションツールを使っていると言われています。詳しくは以下をご覧ください。

http://www.proofpoint.com/threatinsight/posts/biggest-security-threat-of-2014-email-still.php.

「m」無しに注意

Pinterest はアメリカで 12 番目に人気のある Web サイトです。そのため、偽の Pinterest サイトを使ってユーザーにクリックさせようという試みは後を絶ちません。過去数週間、私たちの研究チームは以下の URL を使った興味深い攻撃を観測しました。

hxxp://pinterest[.]co

先週、私たちのサンドボックスが上記 URL を含む大量のメッセージを観測しました。Predictive(先行的)スキャンにより、この URL は悪意のあるものであることが確認されました。私たちのチームはさらに研究を続け、誰かがこの URL にアクセスする度に異なる組合せのエクスプロイトキットとマルウェアが供給されることを突き止めました。詳しくは以下をご覧ください。

http://www.proofpoint.com/threatinsight/posts/whats-in-an-m.php.

「あなたは癌かも知れません」という悪質なソーシャルエンジニアリング

皆様もご存じのように、ソーシャルエンジニアリングは人を心理的に操って何らかの行動を起こさせたり、機密情報を漏らすよう仕向けたりするものです。そしてこれはフィッシングや「はえ縄型攻撃」でもよく見られる手法です。

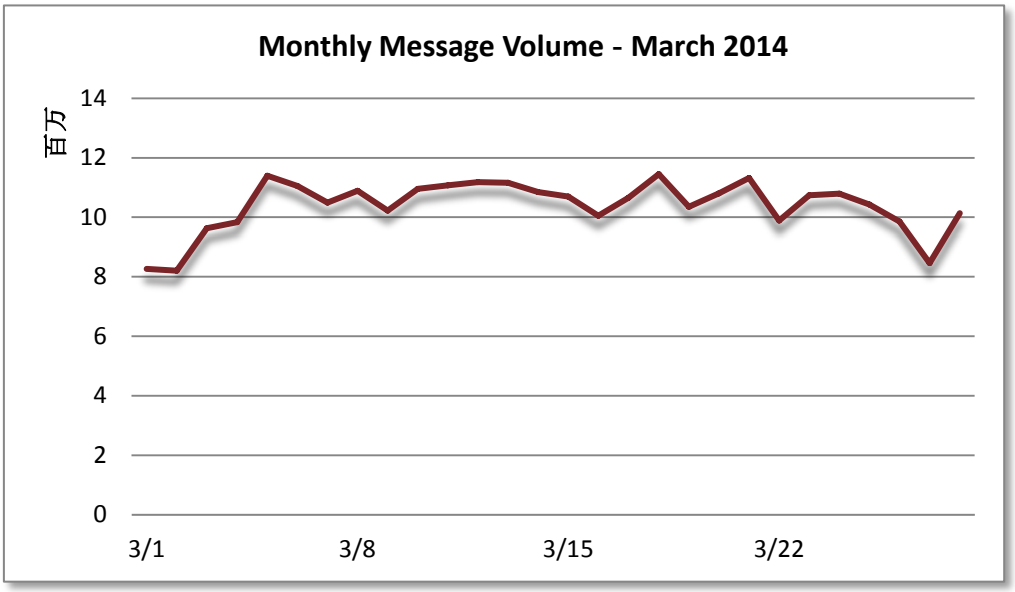
先頃 Softpedia のマルウェア研究者が 特に悪質なマルウェア攻撃の手法を明らかにしました。

http://www.proofpoint.com/threatinsight/posts/insidious-social-engineering-you-may-have-cancer.php.

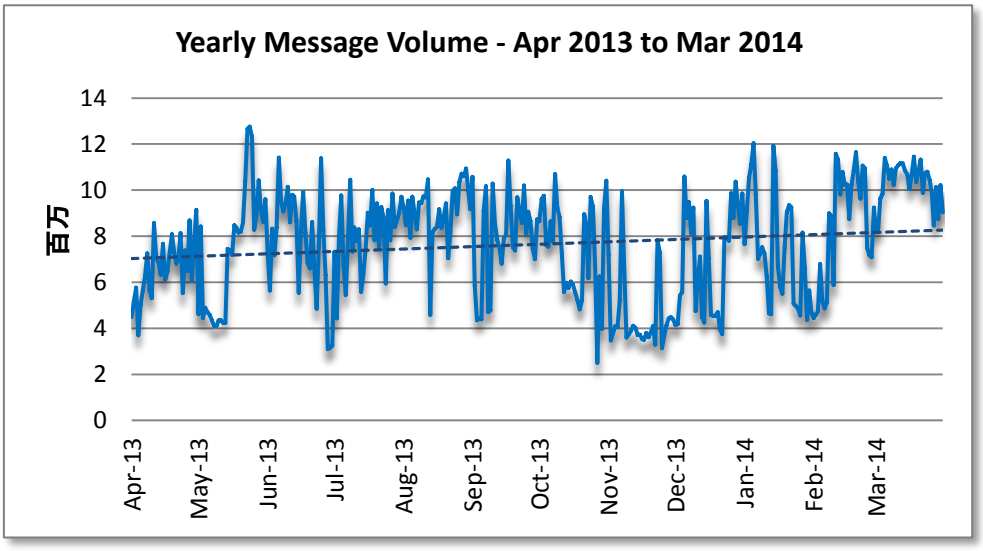
Threat Trends (トレンド)

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。3 月はその直前の数ヶ月に比べて日々のスパム量の増減は落ち着いていました。月初は 800 万通/日から始まってすぐに 1,100 万通/日のピークを迎え、その後はピーク付近を小刻みに動き、月末に最大の落ち込みを見せた後に増加傾向を見せて月を終えました。



スパム量は引き続き増加しており、2 月に比べて 21.03%も増えました。全体的な傾向も引き続き高く、前年同月比で 78.06%の増加となっています。



Spam Sources by Country (スパム発信源)

上位 3 カ国(EU、アメリカ、アルゼンチン)は変わらず、インドが上位 5 カ国に返り咲き、メキシコが初の 5 位に入りました。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。

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

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 37.78%と、引き続き世界一スパムを発信しています。他の 4 カ国合わせても約 17%と、EU の半分にも満たない数値です。

February 2014			March 2014		
1	EU	38.57%	1	EU	37.78%
2	US	6.06%	2	US	6.98%
3	Argentina	4.07%	3	Argentina	4.36%
4	Russia	2.73%	4	India	2.98%
5	China	2.69%	5	Mexico	2.70%

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