proofpoint

Proofpoint Threat Report

October 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。

Proofpoint が Threatinsight を立ち上げ

Proofpoint は先頃、マルウェアやユーザー行動などの情報セキュリティに対する脅威について取り上げるサイトとして Threatinsight を立ち上げました。悪意のある攻撃やフォレンジックに特化した他のサイトとは違い、Proofpoint Threatinsight は、エンドユーザーの行動という視点から新しい発見や観察結果を情報セキュリティコミュニティに対して提供するリソースとしてご活用いただける場を目指しています。

是非、www.proofpoint.com/threatinsight でのコミュニケーションにご参加下さい。

Threat Models (手法)

ウォータリングホール型攻撃 (Watering Hole Attacks)

本レポートでは、これまでの数ヶ月で 4 種類の主要なマルウェア攻撃のうち、3 つについて解説してきました。今月はそのシリーズの最後として、ウォータリングホール攻撃について解説します。

ウォータリングホール型攻撃は水飲み場型攻撃とも呼ばれ、野生動物が獲物を水飲み場で待ち伏せする姿のアナロジーとして定義されています。デジタル世界においては、攻撃者が特定の興味を持つグループ

(業界、地域、組織など) を標的とし、それらのグループに属するユーザーが興味を持っている/持ちそうなコンテンツを供給している有名な、あるいは信頼されているサイトを攻撃して支配下に収め、そのサイトにアクセスするユーザーに iframe などを使って悪意のあるコートを感染させるものです。あたかも、水飲み場に来る獲物を待ち伏せするように・・・

「特定のグループが信頼するWebサイトを使うことにより、スピアフィッシングやその他の形態のフィッシングには騙されにくいユーザーにも有効な戦略となっている。[*1]」

PHP.net を狙った最近の攻撃には、完全にこの定義が当てはまります。PHP は Web 開発で広く使われているサーバーサイドスクリプティング言語で、PHP.net はそのコミュニティサイト (または「水飲み場」) です。Alexa によると、このサイトは世界でも 228 番目に人気のあるサイトだと言うことです。サービスを提供している数多くの Web サーバーのうち、2 つが悪意のある JavaScript に侵害されたとのことで、このスクリプトはアクセスしてきた無防備のユーザーをサードパーティのサイトに誘導し、そのユーザーのブラウザに Adobe Flash のような脆弱性を持つプラグインがインストールされているかどうかをスキャンし、見つかったプラグイン用のエクスプロイトをインストールします。Web サイトの開発者が標的ですから、その組織の Web サーバーのアクセス権を持っていることが期待できるというわけです。

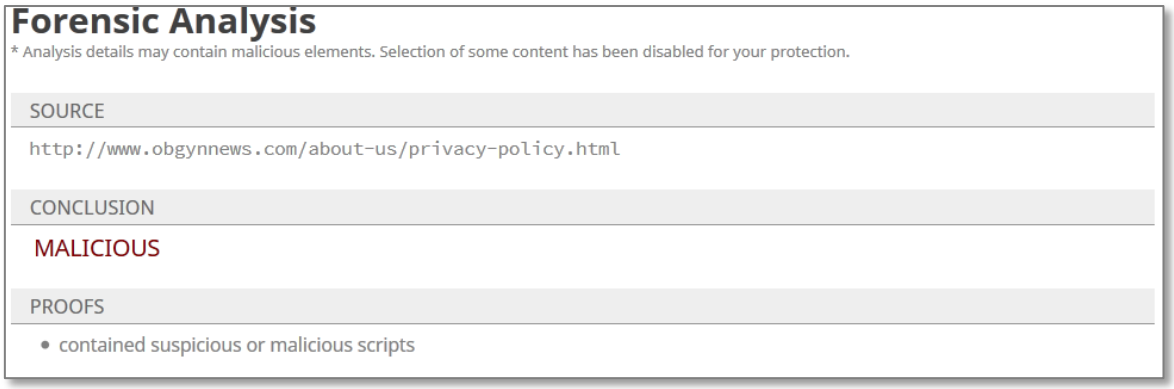
家畜産業のサイトである cattlefax.com が、この夏攻撃を受けました。Cattlefax は「… 牛肉産業の研究・解析・情報についてのグローバルリーダー[*2]」とされており、Cattlefax.comは業界の情報限としてよく知られています。攻撃は、アクセスしてきたユーザーを他のサイトにリダイレクトする悪意のあるスクリプトを使っていました。被害者のマシンにドライブバイダウンロードが仕掛けられ、これはCVE-2013-1493 (miter.orgで詳しい情報を見ることができます) のJavaエクスプロイトを利用しています。

[1] Wikipedia reference: http://en.wikipedia.org/wiki/Watering_Hole
[2] http://www.cattlefax.com/who-we-are.aspx

この種の攻撃ではよくあることですが、CattleFax のユーザーもまた、サイトに対して全く疑いを持っていませんでした。これらの攻撃に対処するためには、これまでの対策に加えてさらなる防御レイヤーが必要になります。Proofpoint の Targeted Attack Protection なら、こういったウォータリングホール攻撃からもユーザーを守ることができます。

Medical Imaging Blog もまた、9 月に攻撃されました。医療機器メーカーであるMcKessonが 2009 年に立ち上げたこのブログは、「医療画像処理に関する情報やイベント、業界の発表を探しているユーザーのための情報源[*3]」になっています。医療関係者にとっての信頼できる情報限であり、コミュニティサイトなのです。ProofpointのTargeted Attack Protectionが、このサイトが悪意のあるスクリプトに感染していることを突き止めました。

Obgynnews.comは産科医と婦人科医向けのコミュニティサイトです。サイトでは「Ob. Gyn. Newsは、現役の産科医/婦人科医に治療法の開発に関連する情報や解説、専門医のヘルスケアポリシーや医療技術への影響などに関する情報を提供する独立系の新聞です。[*4]"」と紹介されています。このサイトのプライバシーポリシーのページであるwww.obgynnews.com/about-us/privacy-policy.htmlが悪意のあるスクリプトに侵害されました。



この攻撃はマルバタイジング (malvertising) と組み合わされています。悪意のあるスクリプトは第三者の広告主から出稿されているバナー広告を通じて配信されていたのです。

これらの例をからわかるように、ウォータリングホール攻撃は、信頼されたサイトを通じて知識を共有するコミュニティを狙う攻撃ということができます。悪意のあるコードは、いくつもの経路で流されており、さらにこれらの攻撃は外からは見えないように行われ、攻撃に気づいたユーザーは希でした。

攻撃者は過去の様々な攻撃の手法を組み合わせ始めました。今回の攻撃は、ウォータリングホールとマルバタイジングの組合せで、広告コンテンツから産業サイトへの配信だったのです。

[3] http://www.medicalimagingtalk.com/about-medical-imaging-talk/
[4] http://www.obgynnews.com/about-us.html

Threat News (ニュース)

ソーシャルエンジニアリングの実例

米政府機関の情報セキュリティ最高責任者のコンピュータが、標的型フィッシングメールによって侵害されました。ソーシャルエンジニアリングが新たなレベルに入ったのは間違いないようです。この事件では従業員から誕生祝いのメッセージが贈られたのですが、問題はその従業員が実在しなかったことです。

侵入テストを行う企業である World Wide Technologies の侵入テストチームが、テストの一部として「Emily Williams」を考え出し、この攻撃を仕掛けたのです。Williams 嬢は、ソーシャルメディアの偽プロファイル上は「魅力的で頭の良い MIT 出身の女性」とされており、セキュリティに関するバックグラウンドやログインアカウントも設定されています。彼女の LinkedIn コネクションは全部で 55 人で、標的となった組織の実在の従業員も含まれていました。これらのコネクションは、営業部門や会計部門などの担当者レベルへの攻撃によって追加されており、その後セキュリティチームに標的を移し、責任者も含むようになりました。最後にはついにセキュリティ部門の責任者を捉えたのです。

この顛末は World Wide Technology の Aamir Lakhani によって RSA Europe カンファレンスで発表されました。そのソーシャルエンジニアリングに関する詳細は Sophos のブログにあります: http://nakedsecurity.sophos.com/2013/11/03/fake-femme-fatale-dupes-it-guys-at-us-government-agency/

イギリス法務省が深刻なデータ流出で罰金を課される

イギリス Cardiff 刑務所に収監されている受刑者 1,182 人の個人情報が 3 組の受刑者の家族に誤ってメール送信されました。これらは別々の状況下で起こったと言うことです。メールに添付されたのは「名前、民族、住所、刑期、出所日、コード化された全ての罪状」でした。イギリス法務省はこの件でデータプライバシーの監視機関である Information Commissioner's Office (ICO) から 14 万ポンドの罰金を科されました。委員会はこの件を「非常に深刻なデータ流出事件」と説明しています。10 月 25 日号の *SC Magazine* が詳細を報じています: http://www.scmagazineuk.com/justice-ministry-fined-140k-for-serious-data-breach/article/317945/

オバマ大統領のツイッターアカウントが Syrian Electronic Army に侵害される

ハッカー集団である Syrian Electronic Army (SEA) は、スピアフィッシングとソーシャルエンジニアリングの組合せによってツイッターのアカウントを奪取する攻撃を続けています。彼らの最新の標的はアメリカ合衆国大統領のバラク・オバマです。彼の選挙運動用のツイッターアカウントは草の根組織である Organizing for Action にリンクされており、それが SEA によるビデオにリンクされています。NextGov が攻撃の詳細を紹介しています: http://www.nextgov.com/cybersecurity/2013/10/how-hackers-compromised-links-obama-twitter-account-through-email/72785/?oref=ng-HPriver

御社は侵害されたことがありますか?

御社のネットワークやシステムは侵害されたことがありますか? どうしてそれが分かりますか? 侵害による明確な技術的な兆候は見られますか?

Dark Reading が侵害の有無を見分ける 15 個の指標を紹介しています。トップ 5 は:

1. アウトバウンドへの異常なネットワークトラフィック
2. 特権ユーザーの異常な行動
3. 地域的な不規則性
4. その他のログイン警告
5. データベース読み出し量の増加

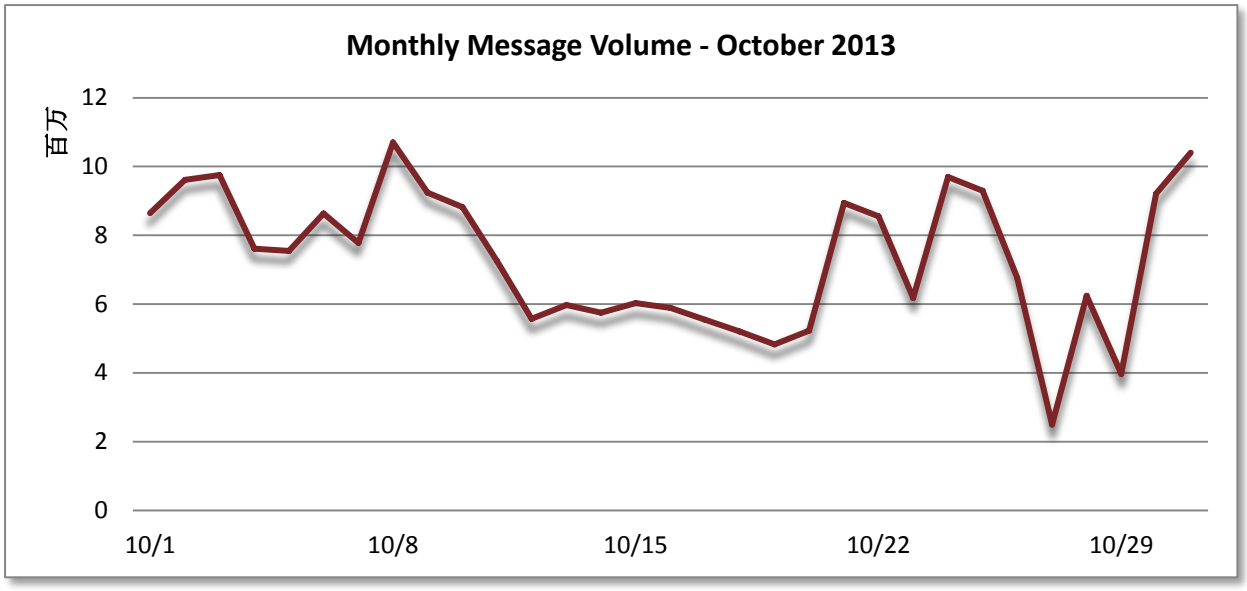
記事は技術的兆候についての詳細を解説しています。*Dark Reading* リストの全体はこちらでご覧頂けます: http://www.darkreading.com/attacks-breaches/top-15-indicators-of-compromise/240162469?pgno=2.

ところで、彼らは最も重大な指標を忘れています。それは技術ではなく人間的指標です。御社の従業員こそ、攻撃に気づく最初の指標で、そこから技術的な深掘りが始まるのです。

Threat Trends (トレンド)

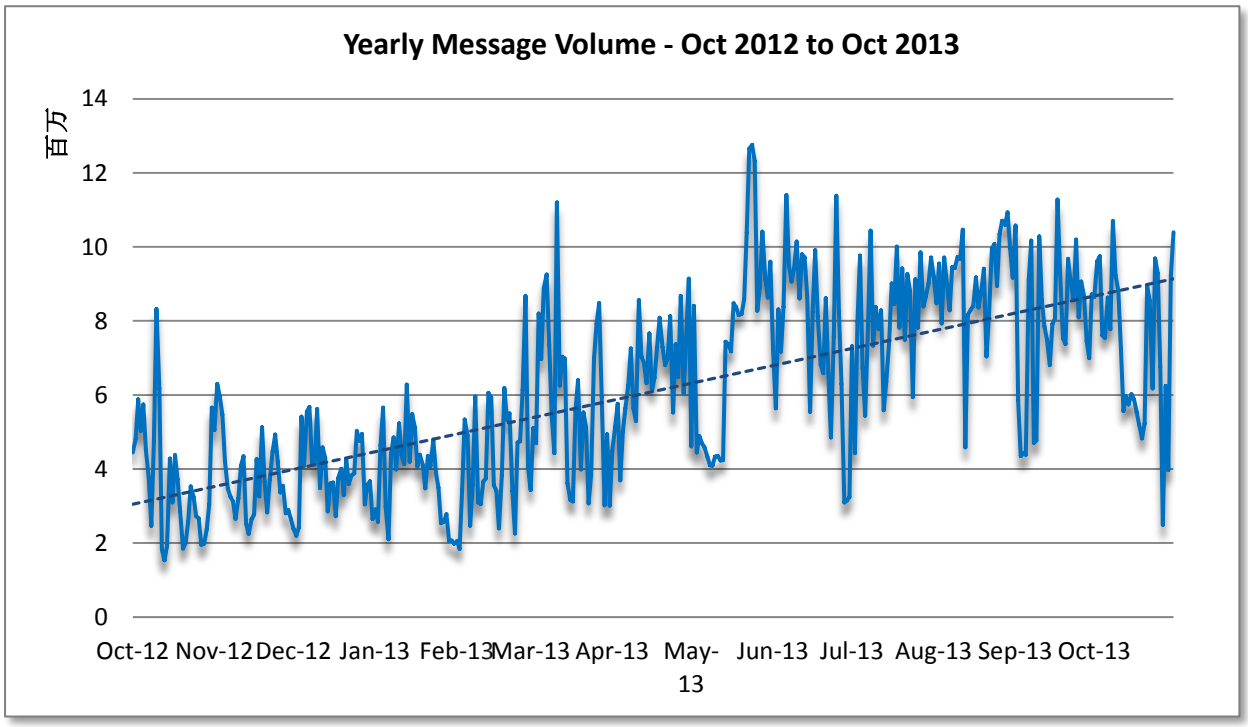
Spam Volume Trends (スパム量のトレンド)

Proofpoint ではスパム量を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。10 月のスパム量は日毎に振れ幅が大きく、最大で 1 日当たり 1,000 万通から最低で 200 万通に地が付いた日もありました。9 月末に増えたスパム量は 10 月始めも引き続き多く推移し、10 月 8 日に最大値の 1，070 万通に達しました。その後 19 日土曜日まで減少傾向が続き、その時点での月間最低値である日量 480 万通にまで落ち込みました。スパム発信者は週末、休みを取るのでしょうか。月曜には 58%増と急増し、例外的な週半ばの急減を経て週末にはまた 1,000 万通に近づきました。この週末はまた激減し、月間最低値をマークしています。最終的に 10 月は 1,040 万通/日という強力な上昇で幕を閉じました。9 月と 10 月は月初と月末にスパム量が多くなっており、今後もこの傾向が続くのかどうかが注目されます。

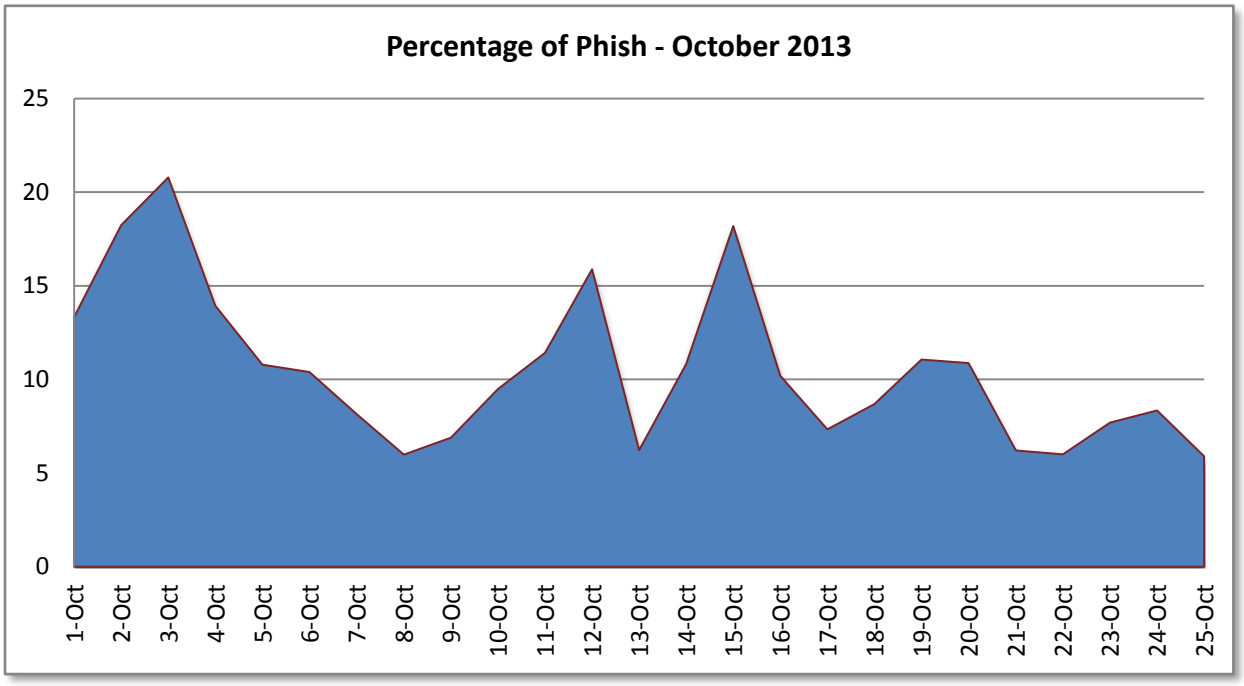


月毎の比較では、スパム量は減少を続けており、10 月も 9 月に比べて 7.31%の減少でした。興味深いことに昨年の 9 月と 10 月も同様の傾向で、しかし減少量は大きく 47.21%の減少でした。

これとは対照的に、年毎の比較では 100.98%の増加になっています。これは、2012 年の 10 月にはたったの 360 万通/月だったものが 2013 年の 10 月は 730 万通/月に増えたのが原因です。スパム量は全体としては増加を続けており、1 月に比べて 47.37%の増加となっています。



Phish Classification Trends (フィッシング分類のトレンド)



Proofpoint MLX によってフィッシングに分類されたメッセージの割合は、10 月は 10.5%でした。統計は 10 月 25 日まで取られていますが、その後のデータは本レポート作成時にはわかっていません。月毎の比較は将来も続けて行きます。

Spam Sources by Country (スパム発信源)

見やすさと解析の分かりやすさのために、スパム発信源のセクションをリニューアルしました。

トップ 5 の順位は 9 月と同じで、EU が世界一のスパム発信源を維持しました。アメリカは 2 位、インドが 3 位、アルゼンチンが 4 位で、中国は 2 ヶ月連続の 5 位です。以下の表は過去 6 ヶ月間のスパム発信国トップ 5 の推移です。

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

トップ 4 は 8 月から変わっておらず、4 ヶ月連続となります。これをトレンドと呼ぶにはまだ早いでしょうが、非常に興味深いことです。

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 は前月比18%減少しましたが、相変わらずかなりの部分を占めています。2 位から 5 位まではあまり変わっていません。

September 2013			October 2013		
1	EU	22.97%	1	EU	18.69%
2	USA	6.86%	**2**	USA	6.68%
3	India	5.08%	**3**	India	4.09%
4	Argentina	3.96%	**4**	Argentina	3.93%
5	China	3.75%	**5**	China	3.68%

もっと詳しい分析を以下でご確認ください
www.proofpoint.com/threatinsight

proofpoint

Proofpoint, Inc.
892 Ross Drive, Sunnyvale, CA 94089
Tel: +1 408 517 4710
www.proofpoint.com