proofpoint

Proofpoint Threat Report

June 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)

株式売買を勧める大量のスパム攻撃

Proofpoint のスパム対策チームがまた大きな勝利を収めました。チームは 6 月後半、株式売買を勧誘する複数の大量スパム攻撃への対応に追われました。新規のフォーマットと戦法に対応するために、スパム定義のアップデートが必要で、新しい事前検知ルールを開発する必要がありましたが、これによってお客様サイドでのアップデート無しに今後も亜種を阻止することができます。以下に攻撃のサンプルを示します。

Campaign #1

最初の大規模なボットネット攻撃は、米太平洋時間 2014 年 6 月 21 日午前 10 時 44 分に Proofpoint のスパムトラップに捕捉されました。数千通に及ぶメッセージは全て「Scottrade」からのものでしたが、実際の送信元はランダムなメールアドレスで、以下の様なものでした。

1. From: “Scottrade” <281e57881a@wanadoo[.]fr>
2. From: “Scottrade” <jaydavis1f7@rr[.]com>
3. From: “Scottrade” <bweavernn8511c@bezeqint[.]net>
4. From: “Scottrade” <awestruck443a0@pronet[.]bg>
5. From: “Scottrade” <gislen0b@cox[.]net>

また、全てのメッセージの件名は以下のようなものでした。

Subject: Inv///est today. Ca///sh Out next m///onth

(スラッシュ「/」が追加されているのは、このレポートがスパムとして検知されないためです)

以下は URL ペイロードの例です。

- hxxp://www.accentuating599D4[.]com
- hxxp://www.accentuating754B158[.]com
- hxxp://www.advisoryd5030ED[.]com
- hxxp://www.advisoryd59062[.]com
- hxxp://www.agayathri6FE0C3[.]com
- hxxp://www.agayathri7C30A67[.]com
- hxxp://www.ahf31C5F98[.]com
- hxxp://www.ahf7F4262[.]com

攻撃開始から 13 分後の 10 時 57 分にスパム定義がアップデートされ、この攻撃をブロックしました。最初のブロック後も、万全を期すために定義のアップデートがいくつか出されています。本レポート執筆時点で新しい亜種は確認されておらず、攻撃は完全に封じ込められています。

サンプルメッセージ

> xxxx 様
>
> 昨晩のボイスメールを聞いてびっくりしました。
>
> 先月、せっかく　　についてお教えしたのに、興味が無か=たのですね。確か、あの時点ではまた 10 セントか 15 セントだったはずです。私が教えなかったとは言わせませんよ。
>
> まあ、それはもう良いです。しかしまだ　　を買い損ねたことでご立腹でしたら、まだ遅くないということを申し上げておきます。しかし、今度はできるだけ多=の　　「株」を月曜日の朝までに買って下さい。さもないと、すぐに値段は上が=てしまいます。それができなければ貴方の責任です。それについて私に電話=たり、ボイスメールを残さないで下さい。
>
> この件に関して私はアナリストと話をし、彼はこの株が 30 日以内に 1 ドルを超えるだろうと言っています。今度はチャンスを逃さないで下さいね！
>
> では
>
> キャロル

Campaign #2

次の攻撃は 2014 年 6 月 22 日日曜日の深夜に発見されました。メッセージ数は数千通です。送信者は全て「TD Ameritrade」ですが、例によってメールアドレスはランダムなものです。

1. From: “TD Ameritrade” <pluggerdd05e4@stowfordhouse.plus[.]com>
2. From: “TD Ameritrade” <meech8d6@dsldevice[.]lan>
3. From: “TD Ameritrade” <gpfd087@92-247-195-78.spectrumnet[.]bg>
4. From: “TD Ameritrade” <margaret.sanderd3e@yalihuyuk[.]com>
5. From: “TD Ameritrade” <3dalgor37f@missioncontrolsf[.]org>

全てのメッセージの件名は以下のようなものでした。

Subject: Ano///ther Big Re///port this M///onday at the ope///n!

(スラッシュ「/」が追加されているのは、このレポートがスパムとして検知されないためです)

以下は URL ペイロードの例です。

- hxxps://www.pierrearD7767[.]com/9EB4CA56C191120F3EBC656A7F9CA18D9E2D50F
- hxxps://www.max.young76708CA[.]com/10388ECA8EABA98DCF0C65CB78D5A09A86C5069C814B7C3C
- hxxps://www.pef4D16C[.]com/FB3FE224C05CA9F00CE4EE62636200F2A78F2ED
- hxxps://www.jeffery_myrthu.gli-canBAF2A5[.]com/1A7A19372373ABACE1526E31AAC582BAA24E7A
- hxxps://www.t-romBCBCE[.]com/1623477F7F542DC09AF49C6A33C5D1B3E88EAE216B
- hxxps://www.aacwz17B84E9[.]com/CF4D043D8C88D8B2E092A937316CE4C

この攻撃はスパム定義のアップデートによって 20 分後に完全にブロックされました。

Campaign #3

最後の攻撃は、2014 年 6 月 23 日の午前 0 時 30 分でした。今度は Bloomberg を騙っており、送信者は「Bloomberg.com」ですが、ランダムなメールアドレスから送信されています。

1. From: “Bloomberg.com” <kmcguire5349@cableonline[.]com.mx>
2. From: “Bloomberg.com” <soggie799@ctrduraton[.]com>
3. From: “Bloomberg.com” <attentiond9882@lukasandsuzy[.]com>
4. From: “Bloomberg.com” <andowlingf5@airtelbroadband[.]in>
5. From: “Bloomberg.com” <bwateredeb6@manageathome[.]co.uk>

全てのメッセージの件名は以下のようなものでした。

Subject: Fin///ancial News: Ou///r New Stock A///lert!

(スラッシュ「/」が追加されているのは、このレポートがスパムとして検知されないためです)

以下は URL ペイロードの例です。

- hxxp://oycyubu4171bloomberg[.]com
- hxxp://keaded5287bloomberg[.]com
- hxxp://jozez7786bloomberg[.]com
- hxxp://xnmtbloomberg[.]com
- hxxp://yutoasa7828bloomberg[.]com
- hxxp://ajegyg8719bloomberg[.]com
- hxxp://kolega6861bloomberg[.]com
- hxxp://nyukut8448bloomberg[.]com

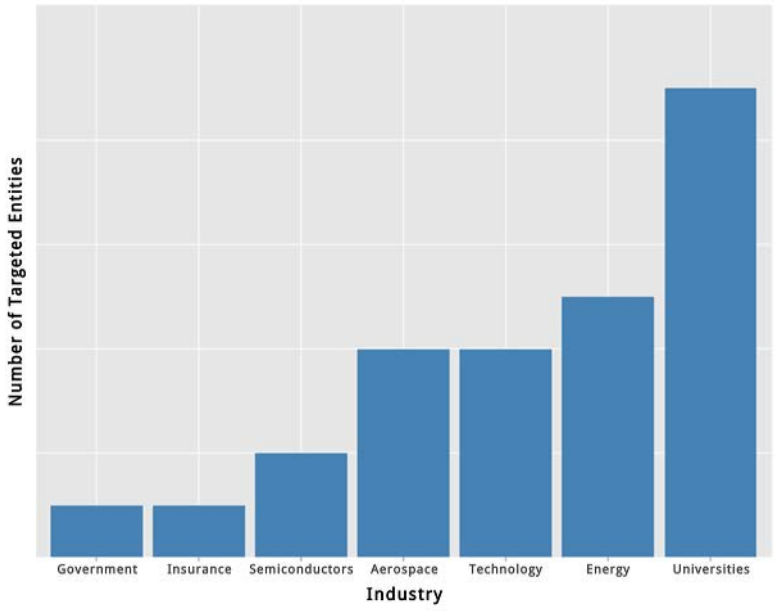
IE のゼロデイ攻撃が狙っているのは誰か?

先月号の脅威レポートでお知らせした「IE の脆弱性を狙った APT 攻撃(CVE-2014-1776)」について、誰が標的とされたのかを見てみましょう。CVE-2014-1776 については日本でも大きく報じられましたが、Proofpoint のお客様にもこのゼロデイ脆弱性を使った標的型攻撃に狙われた例が何件かあり、それらを解析しました。これらの攻撃にはいくつかの特徴があります:

フィッシングメールは米国防総省(DoD)や航空宇宙、エネルギー、大学、研究機関などを狙ったメーリングリストに対して送られました。メッセージに含まれているリンクは悪意のあるサイトに繋がっています。これらのサイトはゼロデイエクスプロイトのコードをホストしています。

この攻撃は中国の洗練された APT 攻撃グループによるものと考えられ、最初の攻撃は 4 月 25 日金曜日に確認されています。この週末、研究者はゼロデイ脆弱性を発見し、Microsoft に通知しました。Microsoft はこの攻撃について公式に発表しました。この脆弱性に対するパッチは最近までリリースされなかったため、この攻撃は相当な数の侵害を産み出したと考えられます。

この攻撃を最初に発見したのは私たちですから、いろいろなデータを得ることができました。特に、「誰が」狙われたのかについてです。以下のグラフは、検知されたフィッシングメールを元に、各産業分野における狙われた企業数を示しています。



これを見ると、攻撃者は金融業界では無く、航空宇宙やテクノロジー企業を狙っていることがわかります。過去の例から、これは機密情報を狙うための「踏み石」と考えられます。

さらに興味深いことに、この攻撃では大学が最も狙われました。2014 年に入ってから大学が関与するデータ流出が続いていますが、これは大学が研究ネットワークの中で果たす役割に関係があります。大学を経由して機密情報にアクセスする道ができているのです。私企業はセキュリティを強化し続けているため、相対的に大学の方が狙いやすいという状況なのです。

Threat News (ニュース)

サイバー攻撃のワールドカップ: ストリートファイトからオンラインの抗議行動まで

華やかなブラジルワールドカップの陰で、政治的ハッカーやサイバー犯罪者の活動も続いています。イタリアのセキュリティ企業が"The State of the Art of Digital Guerrilla During the 2014 Brazilian World Cup" (ワールドカップ中のデジタルゲリラの最先端) と題するレポートを発表しました。華やかなイベントの暗黒面を見せてくれます。Tiger Security は、ワールドカップの期間中、ブラジル当局のデジタルインフラを守る為に他の企業と共に任命されました。

より詳しいレポートはこちらからご確認下さい:
http://www.forbes.com/sites/federicoguerrini/2014/06/17/brazils-world-cup-of-cyber-attacks-from-street-fighting-to-online-protest/.

大規模フィッシング攻撃に狙われたオンラインデートサイト

オンラインセキュリティ企業の Netcraft によると、オンラインデートサイトがメンバーを騙して現金のやりとりをさせる新手の大規模なフィッシング攻撃に狙われたということです。攻撃者はメンバーアカウントの侵害を狙っています。ハッカーは偽のプロファイルを使って他のメンバーとの接触を試み、彼らの信頼を得ようとします。

現在の攻撃は侵害されたサイトをひとつ使っており、このサイトが 860 もの詐欺的な PHP スクリプトをホストしています。ほとんどはデートサイトメンバーのユーザー名とパスワードを盗みだすよう設計されています。

Proofpoint EMEA (Europe, the Middle East, and Africa) 責任者の Mark Sparshott は、他のサイバー犯罪者もオンラインデートサイトを狙う可能性があると警告しています。

http://www.infosecurity-magazine.com/view/38975/online-daters-targeted-by-massive-phishing-campaign/.

サイバー犯罪者がヘッジファンドを狙うのは何故か

サイバーセキュリティの専門家が、米ヘッジファンドが過去 2 年にわたって秘密裏に攻撃を受けていたと指摘しました。ヘッジファンドの取引戦略を盗んで、フロントランニング (株式の先回り売買) やその他の違法な取引によって利益を上げることが目的です。

このような攻撃を成功させるためにどれだけ洗練された攻撃が要求されるのか、以下のリンクからご確認ください http://www.cnbc.com/id/101778725.

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.

ワールドカップがフィッシングリスクを高める

ブラジルワールドカップが始まり、世界中の「正しい」サッカーファンはテレビやインターネット、あるいはソーシャルメディアなどで試合を追いかけていることでしょう。他のチームもまた、3 週間の期間中に大きな勝利を目指しています。ハッカーのチームです。彼らはフィッシングの餌としてのファンの興味とサッカーチームに注目しています。

フィッシングは洗練され、高度に自動化された犯罪であり、メールの受信者は友人や近親者、関係者などの信頼できそうな送信者からのメールを装っています。企業や公的機関が懸命に啓蒙に努めていますが、ユーザーは依然として悪意のあるフィッシングメールをクリックしてしまいます。これを完全に無くすことは不可能で、Proofpoint の研究によると、10 人のうち 1 人がそういったメッセージをクリックします。ソーシャルメディアを模したフィッシングテンプレートは、他のものよりも遙かに成功率が高いことにも注意が必要です。

さらに、メッセージ中の悪意のあるリンクや添付ファイルをクリックすると、システムはほぼ瞬時に感染してしまい、その過程はユーザーには見えません。結果として、マルウェアは発見されるまで何ヶ月もの間、組織内に留まることになります。攻撃者はシステムに侵入し、内部を探り、他のシステムやユーザーアカウント (特に、重要なシステムや情報へのアクセス権を持つユーザー) を乗っ取るための時間をたっぷり使うことができます。さらに、最近増えている手口として、システムを破壊して修復ソフトを押し売りするランサムウェアがあります。

攻撃者は大きなイベントを狙い、件名にイベント名を反映させます。Proofpoint では、すでにワールドカップに関連するフィッシングメールや悪意のあるサイトを確認しています。これらの詳細については以下をご覧ください。http://www.proofpoint.com/threatinsight/posts/world-cup-kicks-off-heightened-phishing-risk.php.

Gameover ZeuS のテイクオーバーによるフィッシングメールの急減

Proofpoint の研究者は、オンラインバンキングを狙う Gameover ZeuS ボットネットの協調テイクダウン (駆除) - より正確に言うと、テイクオーバー (奪取) - の影響を調べています。

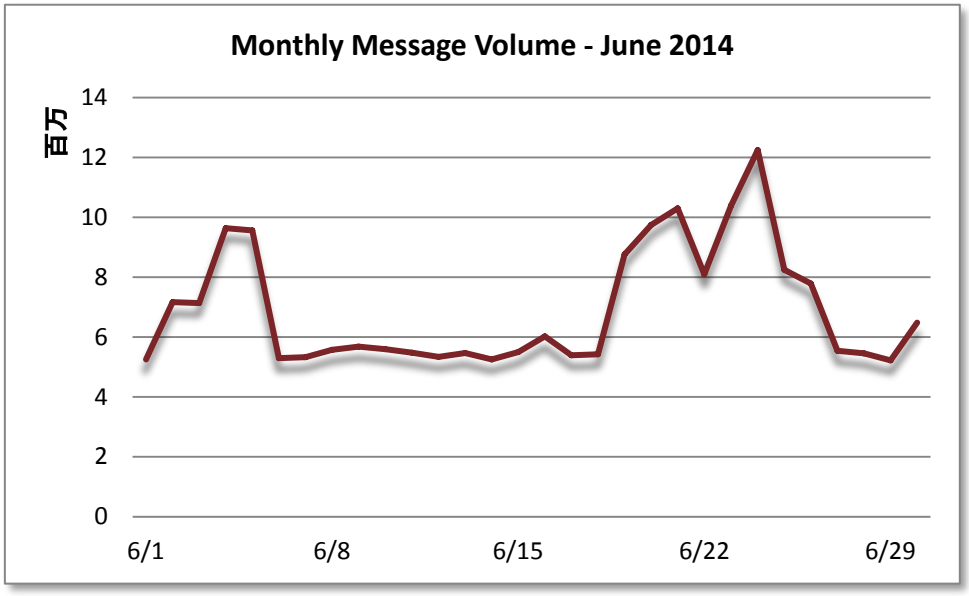
テイクオーバーの前には、大量の Gameover ZeuS が添付ファイル (特にマルウェアを含んだ ZIP ファイル) を介して拡散していましたが、私たちは Targeted Attack Protection (TAP) の情報から、テイクオーバーの後、悪意のある ZIP ファイルが急減したことを観測しました。

さらに詳しい情報はこちらを参照して下さい: http://www.proofpoint.com/threatinsight/posts/gozeus-takeover-leaves a-hole-in-phishing-email.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。6 月は比較的安定した期間がありましたが、月末へ向けて激しく変動しました。月初には 500 万通/日と低いレベルだったのが、すぐに 900 万通/日以上に増えています。第 1 週の終わりから第 3 週にかけて安定した後、月末へ向けて大きく変動しました。ピーク時には 1,200 万通/日を超えましたが、その後急減し、月末には 600 万通/日まで落ち込みました。



一方で 6 月の総スパム量は 5 月に比べて減っており、これは 3 ヶ月連続です。5 月から 6 月は 7.55%減少し、対前年比では 10.65%の減少となっています。

Spam Sources by Country (スパム発信源)

EU が 6 月も 1 位で、新顔のベトナムが 2 位に浮上しました。アメリカは 3 位に落ち、4 位・5 位はいつもの通り中国とロシアでした。

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。

		Jan '14	Feb '14	Mar '14	Apr '14	May '14	Jun '14
Rank	1st	EU	EU	EU	EU	EU	EU
	2nd	US	US	US	Argentina	US	Vietnam
	3rd	Argentina	Argentina	Argentina	US	Argentina	US
	4th	China	Russia	India	Russia	Russia	China
	5th	India	China	Mexico	China	China	Russia

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 5 月よりも大幅に減りましたが、全体のスパムの 30.89%を配信しており、第 1 位です。残りの 4 カ国を合わせると 21.39%と、EU の 2/3 以上になりました。

May 2014			June 2014		
1	EU	40.46%	1	EU	30.89%
2	US	7.96%	2	Vietnam	5.91%
3	Argentina	5.36%	3	US	5.53%
4	Russia	3.10%	4	China	5.25%
5	China	3.04%	5	Russia	4.70%

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