proofpoint

Proofpoint Threat Report

August 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)

「壊れた」スパム攻撃は止められるのか?

最近、Proofpoint のスパム対策チームは大規模な「壊れた」スパム攻撃を観測しました。Proofpoint では、この攻撃に対抗するためにいくつかのスパム定義のアップデートを迅速にリリースしましたが、この攻撃は非常に風変わりで興味深いものでした。

メッセージには URL や添付ファイルが含まれておらず、何のアクションもとらないのです。何もしないのにも関わらず、この攻撃を検知することは簡単でした。この攻撃は 4 万ものユニークで未使用の IP アドレスを持つ大規模なボットネットから送られており、私たちのスパムトラップが米太平洋時間 2014 年 8 月 26 日火曜日の午前 2 時 50 分に検知したのです。このメッセージは件名がランダムで、本文に 2-3 行のテキストを含んでいます。全ての件名は Google 検索で得られる wiki や百科事典のエントリと完全に一致しており、ピリオドで終っています。

メッセージサンプル

Dear little snowflake, soft and white. The 2000 Census reported a total population of 2,128 for all of Mapleton Township. Barbana Hospital was opened. Her next tournament was Moscow, where she was seeded second.

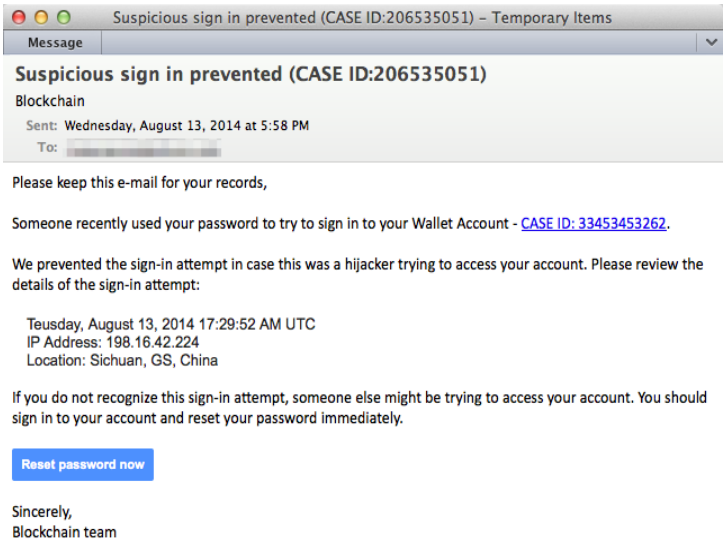
ビットコインを餌に興味本位のクリックを誘う攻撃

ビットコインはインターネット上の仮想通貨で、国家や中央銀行によって管理されている通常の通貨とは全く違うものです。通貨当局の規制を受けず、匿名性も確保されており、今では 68 億ドル相当が流通し、サイバー犯罪者の収益源ともなっています。最も有名なビットコインの Web サイトである blockchain.info によると、2013 年 9 月以降、利用者は飛躍的に伸びており、現在では 200 万人を越え、一日の取引回数は 3 倍近い 3 万件/日以上になっているということです。これだけ利用者が増えれば、ビットコインユーザーを狙ったフィッシング攻撃が増えるのも当然です。攻撃者は攻撃の成功率を上げるために、アクティブなビットコインユーザーのリストを使ったり、ビットコインに関連した「よくある誤解」を利用したりします。ほとんどの攻撃はアカウント情報を盗み出すために行われます

ビットコインを知っている人は多いですが、実際に利用している人はそれほど多くないでしょう。ですから、Proofpoint の研究者がビットコインを餌に使ったフィッシング攻撃を発見したときには非常に驚きました。なんと、2.7%ものクリック率を記録していたのです。これは、一般のユーザーに占めるビットコインユーザーの割合よりもかなり大きいと思われます。Proofpoint ではこの攻撃で 12,000 通のメッセージを検知しました。教育、金融サービス、テクノロジー、メディアそして製造業など、様々な業界の 400 以上の組織に対して、2 回にわたって送りつけられました。これまで発見されたビットコインに関連した攻撃は、ビットコインユーザーを狙っていましたが、今回の攻撃は幅広いターゲットを狙っていたのです。

以下にメッセージのサンプルをご紹介しますが、テンプレートはよく使われる「アカウントに関する警告」です。他の攻撃と違うのは、銀行やオンライン支払いサイトでは無く、ビットコインのサイト(blockchain.info)に誘導されていることです。このメッセージは、中国から不正ログインの試みがあったことを伝えており、中国からのハッキングに対する懸念を利用して危機感を煽る内容です。CASE ID などの表示も、本物のメッセージを装うのに貢献しています。

メッセージサンプル


Suspicious sign in prevented (CASE ID:206535051) – Temporary Items

Message

Suspicious sign in prevented (CASE ID:206535051)

Blockchain

Sent: Wednesday, August 13, 2014 at 5:58 PM

To: [redacted]

Please keep this e-mail for your records,

Someone recently used your password to try to sign in to your Wallet Account - CASE ID: 33453453262.

We prevented the sign-in attempt in case this was a hijacker trying to access your account. Please review the details of the sign-in attempt:

Teusday, August 13, 2014 17:29:52 AM UTC
IP Address: 198.16.42.224
Location: Sichuan, GS, China

If you do not recognize this sign-in attempt, someone else might be trying to access your account. You should sign in to your account and reset your password immediately.

Reset password now

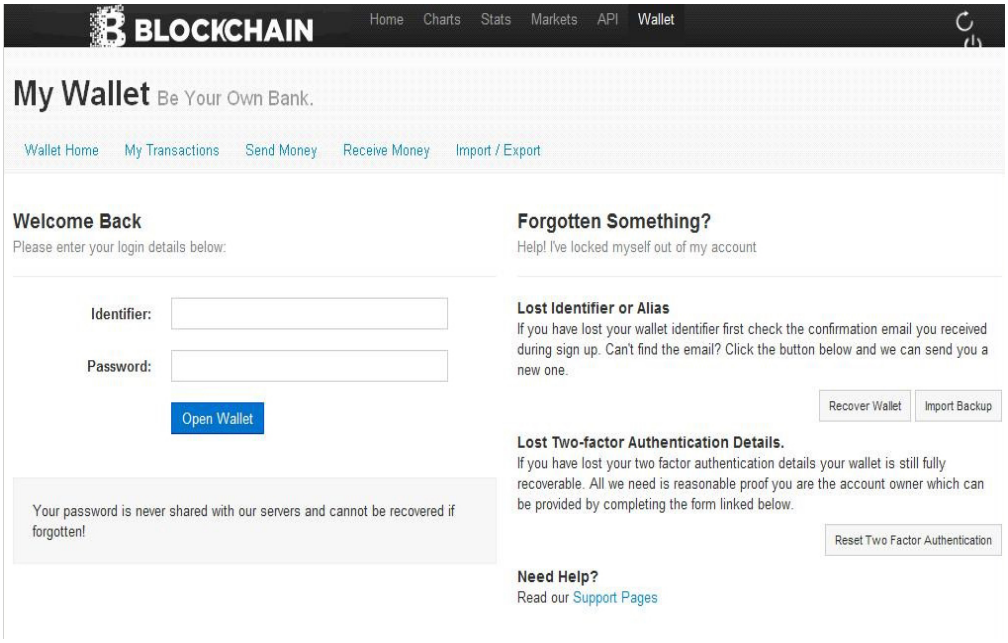
Sincerely,
Blockchain team

この攻撃は 2 日間にわたって行われ、一般的なフィッシング攻撃同様に繰り返されました。メッセージと内容は同じで、URL だけが変更されています。

- 初日は個々のメール毎にランダム化された URL に含まれるホスト名は 1 種類(blockchain.info)でした。
- 二日目の攻撃では、ランダム化された URL に複数のユニークな.com ドメイン(例えば http://blockchain [dot] info [dot] caseid832482834 [dot] com など)が使われています。これらは事前に生成され、登録されたものと考えられます。複数の新規ドメインを循環させる方法は、レピュテーションベースの検知を逃れ、攻撃の成功率を引き上げます。

初日と二日目の戦略の違いは、初日の攻撃に対して Proofpoint がとった対抗策に起因するものかもしれません。

2.7%ものクリック率は、ビットコインユーザーだけで無く、それ以外のユーザーもクリックしたことを示しています。本文中の「パスワードをリセット」ボタンを押すと、Blockchain のログインページによく似たサイトに誘導されます。



このサイトで入力した情報はすぐさま攻撃者に送られると共に、ユーザーにはログインに失敗した旨のメッセージが表示されます。いったんログイン情報を入手してしまえば、攻撃者は自由に実際のアカウントにログインして、ビットコインを好きな相手に送金できます。ビットコインの取引は取り消せない仕組みになっており、追跡も難しいため、被害に遭うとほとんど回収は不可能です。さらに、通常のオンラインバンキングに適用される消費者保護の規制はビットコインには適用されず、銀行の助けも当てにできません。

このシンプルで効果的な攻撃から導き出される教訓は、自社のセキュリティに関係の無いメールなど無いということです。実際には自分に関係の無いメールでも、ユーザーはクリックしてしまうのですから、セキュリティ関係者は決して油断してはなりません。

Threat News (ニュース)

数百におよぶノルウェーのエネルギー企業がサイバー攻撃を受ける

政府関係者によると、ノルウェーのオイル/エネルギー企業およそ 300 社が、同国でも最大級のサイバー攻撃を受けたということです。ノルウェーは 2011 年にも大規模な攻撃を受けました。オイル/ガス/防衛関係の企業がスピアフィッシングのメールに攻撃されたのです。正体不明のハッカーが設計図面や契約書、ログイン情報などを盗み去りました。

この攻撃について、IT Governance の創始者で会長の Alan Calder は *SC Magazine UK* の中でこう述べています:

「小規模な企業のシステムが侵害され、そこから大企業へと広がっていくスピアフィッシング攻撃は、価値ある情報や知的財産権を狙う犯罪者にとって、非常に興味深い攻撃手法になっています。」

詳細はこちらからどうぞ: http://www.scmagazineuk.com/hundreds-of-norwegian-energy-companies-hit-by-cyber-attacks/article/368539/

Cryptolocker の被害者を無料で救済

FireEye や Fox-IT などのセキュリティ企業が、Cryptolocker の被害者を無料で救済するためのオンラインポータルサイトである *DecryptCryptolocker.com* を立ち上げました。これは、Cryptolocker の被害者データベースを元に作られたサイトです。

捜査当局とセキュリティ企業は最近、乗っ取られたホームコンピュータの世界的なネットワークを奪取しました。これは、Cryptolocker と Gameover ZeuS を配信していました。Cryptolocker が最初に確認されたのは 2013 年の 9 月です。非常に類型が多く、大きな被害を与えたマルウェアの系統で、ユーザーにとって重要と思われるファイル(Microsoft Office のドキュメントや写真、MP3 ファイルなど)を暗号化によってロックしてしまいます。

感染したマシン上でロックしたファイルを表示し、警告します。ファイルをアンロックするためには、少額のビットコイン(デジタル通貨)を送って復号化しなければなりません。被害者には 72 時間の猶予が与えられます。最初の要求は数ドル相当のビットコインですが、支払えばさらに高額な請求が行われます。

詳細はこちらからどうぞ: http://www.bbc.com/news/technology-28661463

カナダ NRC のような組織を侵害するためのハッカーの手法とは？

IT セキュリティにおけるハッカーとの攻防は、果てしないイタチごっこです。

カナダ学術研究会議(NRC: National Research Council of Canada)を狙ったサイバー攻撃などと同様の攻撃が増加しています。攻撃に対して有利な立場を確保するためには、攻撃者の手口を研究しなければなりません。以下の記事で、ホワイトハッカーがサイバー攻撃のプロセスを 6 つのステップに分解し、詳細を開設しています。

このプレゼンテーションはハッカーの手口を垣間見せてくれます: http://www.ctvnews.ca/sci-tech/how-do-hackers-breach-institutions-like-canada-s-nrc-1.1938113

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.

PDF と Word と ZIP、貴方ならどれを選びますか?

サイバー犯罪者は攻撃の効率を高め、最大限の価値を得るために、常に先進的な手口を考案します。

過去数ヶ月間にわたって、Proofpoint の技術者達は一風変わった攻撃を追跡していました。この攻撃では、CVE-2013-2729 脆弱性を狙う PDF ファイルが使われています。攻撃は当初、悪意のある PDF を含んだ大量の電子メールによって始まりましたが、数ヶ月後には、彼らの作戦はより多彩になりました。単一の攻撃手段だけを使うのでは無く、同じマルウェアを複数の経路で配信するのです。Proofpoint の技術者は以下の組合せを確認しています。

- 悪意のある PDF にリンクされた URL と、マルウェアにリンクされた ZIP ファイル内の URL
- 添付された PDF ファイルと、マルウェアにリンクされた ZIP ファイル内の URL
- 添付された PDF ファイルと、悪意のある Word ドキュメント(CVE-2012-0158)
- マルウェアを含んだ添付 ZIP ファイル

この攻撃に関する詳細と所見、メールのサンプルはこちらからご確認下さい:
http://www.proofpoint.com/threatinsight/posts/whats-your-vector-of-choice.php

エボラで一儲け: 攻撃のために人々の恐怖を煽る詐欺師の手口

Proofpoint のセキュリティ研究者は、エボラ出血熱の流行に乗じてオンラインバンキングを狙う、トロイの木馬を使った攻撃を発見しました。

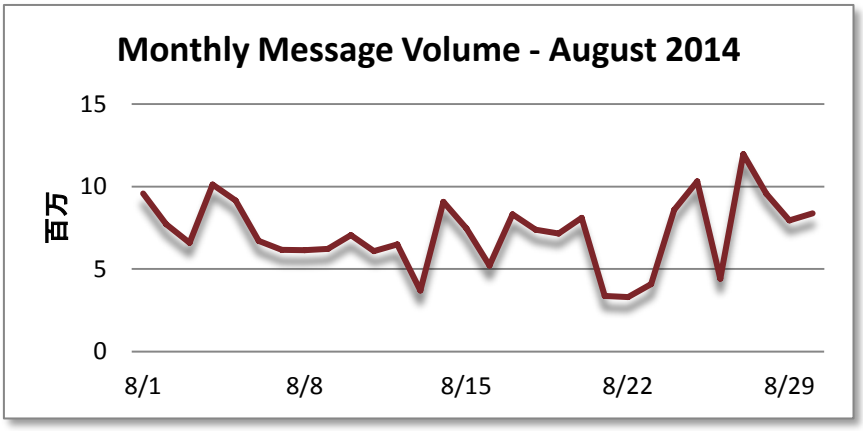
エボラ出血熱のような恐怖の伝染病が流行すれば、人々はそれについて検索し、様々なサイトを手当たり次第にクリックしてしまいます。そこに攻撃を仕掛ければ、通常よりも高い成功率を見込むことができます。この攻撃では、攻撃者は WHO のエボラ出血熱に関連するサイトを正確にコピーし、何も知らないユーザーにフィッシングメールを送りつけました。ユーザーがそのメールをクリックすると、そのサイトから Java ペイロードをダウンロードして Zeus の亜種と見られるマルウェアを実行します。

こちらでメールのテンプレートをご確認下さい:
http://www.proofpoint.com/threatinsight/posts/ebola-threat-banking-trojan.php

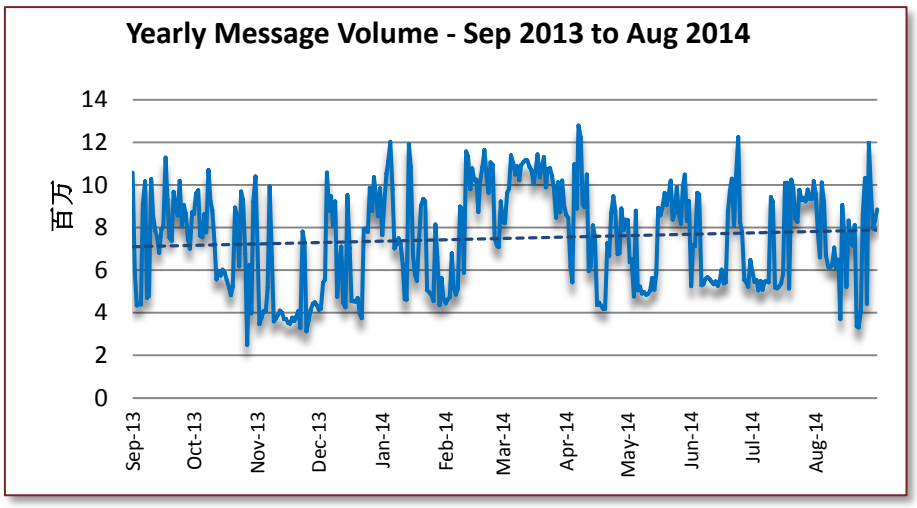
Threat Trends (トレンド)

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。8 月のスパム量は、第 1 週の初めからいきなり下降したかと思うと急増し、半ばには 1,000 万通/日に達しました。その後徐々に減少し、600 万通/日で少し安定しました。その後少し不安定になっていきなり 400 万通まで落ち込み、戻しました。最も急激な変化は第 4 週で、いったん 1,000 万通まで行ったかと思うと 400 万通まで落ち込み、今度は 1,200 万通に達しました。月末は減少傾向で、800 万通/日で終えました。



7 月と 8 月を比べると、スパム量は 3.19%の減少です。前年比ではなんと 20.09%の減少となりました。



Spam Sources by Country (スパム発信源)

EU は底力を見せ、アメリカは第 2 位につけました。アルゼンチンが 3 位に返り咲き、ロシアと中国が 4 位と 5 位を分け合いました。

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。

		Mar '14	Apr '14	May '14	Jun '14	Jul '14	Aug '14
Rank	1st	EU	EU	EU	EU	EU	EU
	2nd	US	Argentina	US	Vietnam	US	US
	3rd	Argentina	US	Argentina	US	China	Argentina
	4th	India	Russia	Russia	China	Argentina	Russia
	5th	Mexico	China	China	Russia	Russia	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 は相変わらず全スパムの 39.33%を占めており、以下の 4 カ国をあわせても 17.88%で、EU の半分にも足りません。

July 2014			August 2014		
1	EU	38.13%	**1**	EU	39.33%
2	US	6.94%	**2**	US	7.31%
3	China	5.19%	**3**	Argentina	4.82%
4	Argentina	4.58%	**4**	Russia	3.17%
5	Russia	3.61%	**5**	China	2.58%

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