proofpoint™

Proofpoint Threat Report

February 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)

組織内部からの攻撃を監視

「サイバーセキュリティ」は長らく、「外部からの侵入者に対する防御」と同義語で、「外敵から城を守る」ものと考えられてきました。アンチウイルスソリューション、ファイアウォール、メールフィルタリングを始めとする防御のためのシステムは、全て外側の脅威に対抗することを念頭に置いています。

しかし、侵入者が城の内部に居るとしたらどうなるでしょうか? 御社の社員が、顧客データベースをコピーしたり、横領を企てたり、得意先リストを盗み出そうとしているかも知れないのです。

PricewaterhouseCoopers (PWC) の Global Crime Report によると、企業の機密情報を盗み出そうとしている人の半数以上は「城の中」にいるということです。そして、この数値はここ数年変わっておらず、社員の中でも若い層が、このトレンドを主導しているようだということです。

同じ調査の中で、詐欺に関する環境変化も観測されているということに触れられています。現在、犯罪者は現金やデータを盗む際に、調達を装った詐欺を使うことが多くなっています。(例：架空の企業からの注文など)

内部の詐欺は、外部からの脅威に比べて複雑になる傾向があり、見つけにくいことが多いのです。内部の犯行者はシステムに詳しく、どのように弱点を責めれば良いかを心得ている、というのが一般的な定義です。そして、何故犯行を行うのかという動機もまた、複雑なものです。

多くの場合、企業が、金銭やその他の資産が無くなっていることに気づくには、長い時間がかかります。詐欺師の活動を長期間にわたって検知できない理由として、コンピュータネットワークの複雑さも挙げられます。コンピュータシステムは本質的に監視しにくいのです。さらに多くの企業では、巨大なネットワークに何台のデバイスが接続されているのか分からないということもよくあり、問題をさらに悪化させています。

言い換えると、企業ネットワークで行われていることはほとんどが監視されておらず、そのために現金を隠し口座に移動させようとする人間にチャンスを与えているのです。個人とデバイス、そしてアプリケーションを相互に連結し、アノマリや詐欺を見つけようとするのは、さらに大変です。

抑止力は、データの取得と監視が一体化したときに最大になります。そうでなければ詐欺の発見は遅れ、長期的には企業の利益のみならず、評判をも落とすことになります。

そして、企業にとって「評判」は、非常に重要です。

改良型 Dyre バンキングトロージャンが従来型セキュリティを脅かす

オンラインバンキングを狙うトロイの木馬である「Dyre」(Dyreza あるいは Dyranges とも) は、2014 年以降サイバー犯罪の世界では安定して高い成果を出すことで知られており、昨年はコンテンツにほとんど修正を加えずに利用されていました。昨年末までは、配信の技術は静的なものに留まっていましたが、その後、マルウェア自身もそのインフラも劇的に進化しました。

わかりやすい例として、自身の TTP (http://stixproject.github.io/data-model/1.1.1/ttp/TTPType/) を変更して、到達率とインストール成功率を上げていることが挙げられます。特に Proofpoint の研究者が注目したのは、スパムテンプレートの継続的な変更、URL ランダム化、JavaScript の難読化、解析とサンドボックスの迂回機能です。

Dyre は日々行われている高ボリュームの未承認メール攻撃を使って配信されており、悪意のある URL を含む zip 圧縮された実行ファイルが添付されています。ほとんどがシンプルなテキストベースのテンプレートを使っていますが、最近観測されたいくつかの攻撃では、洗練された HTML テンプレートが使われていました。

全体としては、サイバー犯罪者は配信するメッセージ、文書、FAX、請求書、バンキングあるいは IRS などのテーマに「餌」を付ける方法を続けています。Proofpoint の記録によると、こ

れらの餌は Dyre が 2004 年の夏に発見されて以来使われてきました。恐らく、攻撃者はテストを通じてこれらが有効であることを認識したのでしょう。メールの件名の例をいくつか挙げました。

- Important – New Outlook Settings
  - 餌: Outlook
- Your tax return was incorrectly filled out
  - 餌: IRS
- Payment Advice – Advice Ref[GB583174] / CHAPS credits
  - 餌: イギリスの銀行
- Important information about your account
  - 餌: イギリスの銀行
- Important – Please complete attached form
  - 餌: イギリスの銀行
- <bank_name> - Important Update, read carefully!
  - 餌: イギリスの銀行
- Employee Documents – Internal Use
  - 餌: 文書

Dyre を配信している犯罪者は、悪意のある URL を生成する仕組みを継続的に改良しています。一時期、悪意のあるドメイン毎に 1 つの URL が使われていました。Proofpoint の研究者は「この方法に対しては、URI パスを使えばシグネチャを作るのは比較的容易です。URL に対して 1 対 1 でシグネチャを作ることができるからです。」と言っています。

2015 年 1 月、Dyre の開発者達は新しい仕組みを導入し、今では 1 つのドメインにつき数百の URL を生成することができます。以下のリンクより、「URL ランダム化」をご覧ください。

http://www.proofpoint.com/us/threat-insight/post/Dyre-Straits-Evolution-of-the-Dyre-Banking-Trojan-Challenges-Traditional-Defenses.

メールに含まれるリンクをクリックすると、ユーザーは最初の悪意のあるサイトに誘導され、さらに 2 つの悪意のあるドメインから JavaScript コンテンツをダウンロードします。以下のリンクより、「スクリプトの難読化とサンドボックスの迂回」をご覧ください。

http://www.proofpoint.com/us/threat-insight/post/Dyre-Straits-Evolution-of-the-Dyre-Banking-Trojan-Challenges-Traditional-Defenses

また、「バイナリランダム化」についての Proofpoint の専門家のプレゼンテーションもご覧ください。

http://www.proofpoint.com/us/threat-insight/post/Dyre-Straits-Evolution-of-the-Dyre-Banking-Trojan-Challenges-Traditional-Defenses.

Dyre が突然進化を早めて回避策を取込み始めたことで、より洗練された標的型の脅威が、今日のセキュリティ環境の中心的な課題として注目を浴びています。Proofpoint の専門家は「先進的な脅威は、シグネチャやレピュテーションを使ったセキュリティソリューションを迂回することで効果を増しており、その技術がマルウェアと攻撃を多様化させています。」と述べています。

Threat News (ニュース)

オランダ政府の Web サイトがサイバー攻撃によって停止

2 月 11 日水曜日、オランダ政府関係者はその週の火曜日の 9 時(GMT) に Web サイトへの攻撃があったことを認めました。一連の Web サイトが 7 時間にわたってアクセス不能になったのは、サイバー攻撃が原因だったということです。攻撃の規模のせいでバックアッププランが機能せず、インフラの脆弱性が浮き彫りになりました。

奇しくもオランダへの攻撃と同じ日に、アメリカのサイバーセキュリティ関連法が強化され、サイバー攻撃の解析を行うために情報収集を行う組織の創設が決まりました。また、オランダへの攻撃に続いてフランス政府のサイトも狙われているとの警告が行われました。

サイトの停止は政府の主要な Web サイトに影響を与え、公共やメディアへの情報提供にも影響がありましたが、電話やその他の緊急連絡手段には影響を与えませんでした。オランダ政府はそれが DDoS 攻撃 (特定のサイトに大量のアクセスを行い、他のユーザーがサイトを使えなくしてしまう攻撃) によるものだったことを認めました。捜査当局は現在、容疑者について何も情報を公開していません。

この攻撃の複雑さについては、以下をご覧ください。

http://www.bbc.com/news/technology-31440973.

小規模企業がサイバーセキュリティに取り組む

「欲張り」という言葉は、普通は金銭に貪欲だったり、得たものを手放したくないと考えている人に与えられる呼称です。サイバー泥棒達はこの「欲張り」に侵されており、他人のお金を盗んだり、それによって生活することを望んでいます。さらに、技術的能力と巨大な富を手に入れる力を持っています。

過去数ヶ月の間、これらのスキルはうまく効果を上げています。Home Depot、eBay あるいは Target などのデータ流出事件です。そして、小規模な企業にとって、この問題は遙かに深刻になっています。

小規模な企業は、これらの攻撃に対して大企業と同じ脆弱性を抱えており、その反面、セキュリティ知識や社内リソースは限られています。悲しいことに、これらの小規模な企業は現在犯罪者集団の標的となっており、激しい攻撃に遭っています。サイバー攻撃によって 1 日当たり

30,000 の Web サイトが侵害されているとも言われています。そして、10 万ドルから 17 万 5 千ドルと言われる被害額も悩みの種です。

以下で詳細をご確認下さい。

http://www.bbc.com/news/technology-31039137.

Anthem を超えて広がるデータ流出事件の法的責任

法律の専門家によると、医療保険大手 Anthem が保有していた 8,000 万人分の個人情報が流出した前代未聞の事件で、ハワイからプエルトリコまでの 60 近くの健康保険制度が影響を受けるだろうということです。問われる法的責任は、途方も無いことになりそうです。流出から 1 ヶ月以内に、50 を超える集団訴訟が起こされています。

HIPAA (Federal Health Insurance Portability and Accountability Act) の元では、州法と同様、流出の責任は制度そのものが負わねばなりません。今後は個人による民事訴訟が起こされるでしょう。

その根拠は明らかです。Anthem 及びその他のブループラン(民間非営利健康保険制度)、シカゴを拠点とするブルークロスとブルーシールドアソシエーションは「ビジネスアソシエイト」契約を結んで BlueCard という全米規模の相互支払いネットワークを運用しています。そして、そのネットワークはアソシエーションによって運用されているのです。

流出は 2 月 4 日水曜日に発表されました。Anthem の 14 個の医療保険の個人情報に加え、Anthem 以外の 42 のブループランの契約者の情報がアクセスされたと言うことです。Anthem は Web サイトで、影響を受けた 42 のブループランの名称を公開しました。その中には、シカゴを拠点とするブルークロスブルーシールドアソシエーションの BlueCard ネットワークを使っているメンバーと、Anthem が保有するブループランがビジネスを行っている 14 の州が含まれています。

ブルークロスブルーシールドアソシエーションは電子メールによる発表の中で、FBI、連邦及び州の規制当局、Anthem 自身の内部チームがデータ流出をあらゆる関係から捜査していると述べています。

以下で詳細をご確認下さい。

http://www.modernhealthcare.com/article/20150223/NEWS/302239977/legal-liabilities-in-recent-data-breach-extend-far-beyond-anthem.

EU のデータ保護: 変化する世界に追いつこうとする試み

2012 年 1 月、EU はデータの収集・利用・保存に関する活動を安全かつ統合された方法で行うため、「EU データ保護規則案」を発表しました。消費者への調査では、オンラインプライバ

シー、発展するデジタル技術、グローバル化に対してその 2 年前から懸念が広がっており、これらの懸念は規制修正への原動力となりました。

この規則案では、データ保護への要求と罰則が厳しくなり、企業のデータに対する責任能力を強化するために、個人は以前よりも自分のパーソナルデータについてコントロールの幅が広がります。新しい規則は、28 の加盟国が一貫した法的拘束力と厳格な定義を持つことを求めています。そして、EU 外の組織が EU のデータを集め、保存し、処理する場合には、このルールを遵守しなければなりません。

しかし、3 年という期間は、変化の激しいデジタルの世界においては永遠にも等しいのです。しかも、規則案が採択されるまでにあと 1 年はかかりそうです。

2012 年以降、消費者の意識は大きく変わりましたが、それ以上に、新しいツールや技術によって、データをビジネスで利用する際の方法が激変しています。

規則案は、研究における個人情報の取扱いに関する強力なフレームワークを構築することを目標としており、そういったデータの匿名化に注目しています。

以下で詳細をご確認下さい

http://www.itproportal.com/2015/02/22/eu-data-protection-three-years-playing-catch-up-changing-world/.

Threat Insight Blog (ブログ)

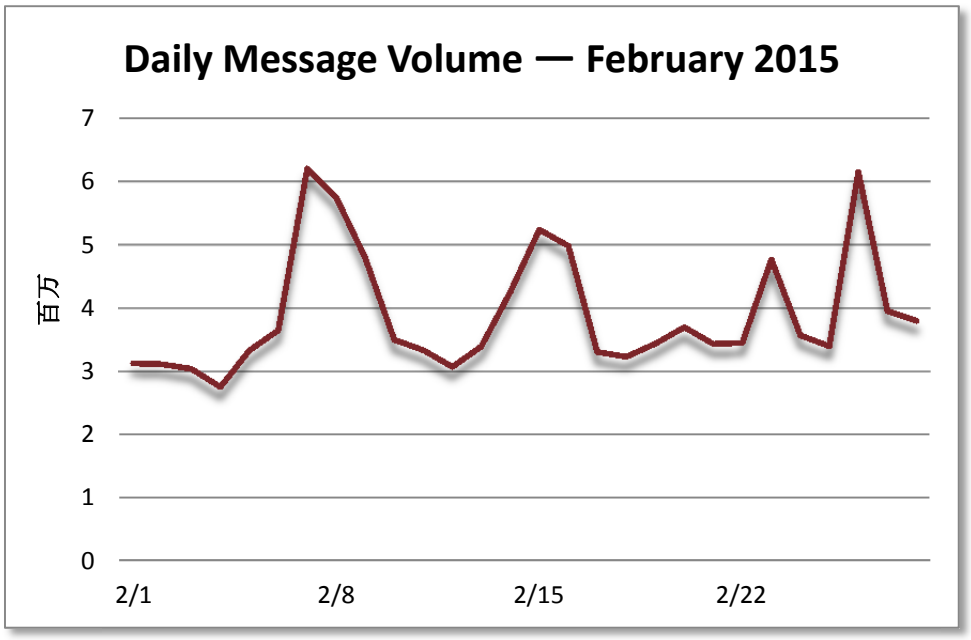
Proofpoint のセキュリティブログである Threat Insight から、興味深い記事をピックアップしました。皆様も Threat Insight のディスカッションに是非ご参加ください。
http://www.proofpoint.com/threatinsight.

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。ブログのセクションは、今後 Threat Model に統合されます。

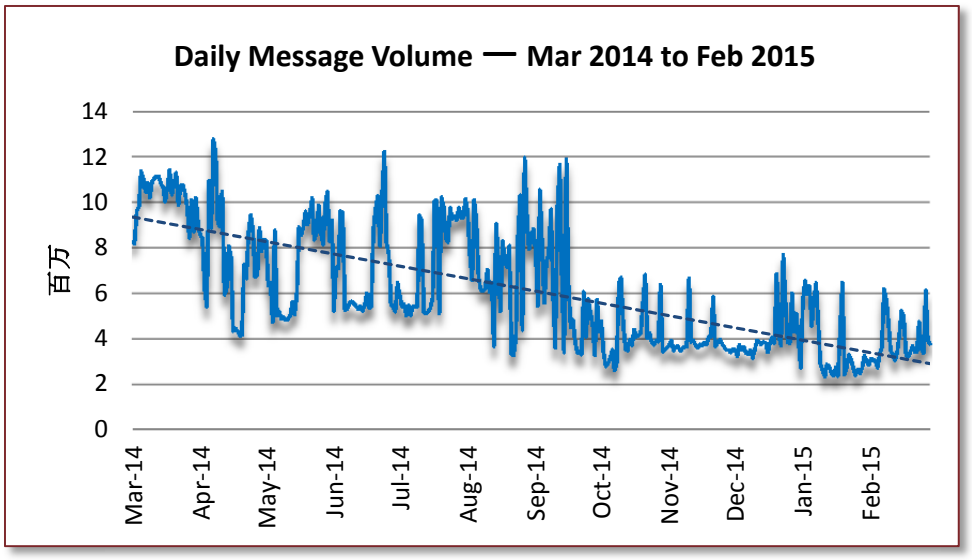
Threat Trends (トレンド)

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。2 月のスパム量は、増減の激しい展開でした。300 万通/日に始まり、第 1 週の終わりには 600 万通まで急伸しました。第 2 週はまた 300 万通まで急落し、その後 500 万通で週を終えました。翌週も 300 万通まで落ち、350 万通まで増えた後に伸び悩んで第 3 週が終りました。最終週の最初に 500 万通まで急増し、350 万通に急落の後に 600 万通まで再度急増した後、400 万通/日で 2 月を終えたのです。



1 月と 2 月の比較では、月間の総スパム量は 6.1%増加しました。前年比では 53.77%の減少となっています。



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

EU はいつも通り 1 位です。アメリカが引き続き 2 位を獲得し、ベトナム、アルゼンチンと続きます。5 位には中国に代わってロシアが入りました。

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。

		Sep '14	Oct '14	Nov '14	Dec '14	Jan '15	Feb '15
Rank	1st	EU	China	China	EU	EU	EU
	2nd	Vietnam	EU	EU	China	USA	USA
	3rd	China	Russia	USA	USA	Vietnam	Vietnam
	4th	Argentina	Vietnam	Russia	Russia	Argentina	Argentina
	5th	Korea	USA	Argentina	Vietnam	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 1 月と 2 月で比較したものです。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 は総スパム量の 35.3%を占め、第 1 位です。残りの 4 ヵ国を足しても 15.62%にしかならず、EU に遠く及びません。

January 2015			February 2015		
1	EU	40.36%	**1**	EU	35.30%
2	USA	5.68%	**2**	USA	6.67%
3	Vietnam	4.53%	**3**	Vietnam	3.64%
4	Argentina	3.84%	**4**	Argentina	2.85%
5	China	2.14%	**5**	Russia	2.46%

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。

February 2015		
1	Germany	4.45%
2	Spain	4.10%
3	Italy	3.48%
4	Romania	2.21%
5	Bulgaria	1.97%

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