proofpoint™

Proofpoint Threat Report

January 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)

データ流出元検知の仕組み作り

銀行は、小売店のクレジットカードシステムがハッカーに侵入された場合、それらのカード情報が闇市場に流れてすぐに、どこの小売店が侵害されたかを特定することができるそうです。しかし一般の企業が侵害され、収集した個人情報が流出した場合には、それらの情報が闇市場で売りに出された場合でも、どこから流出したのかを特定するのは非常に困難です。本記事では、こういったエンドユーザー情報の保有者が、もっと責任能力を持てるようにするためにはどうしたら良いかを考えます。

ここ数年の主なクレジットカード情報の流出事件のいくつかでは、事件が一般に知られる前に、銀行はその事実を掴んでいました。カード情報が闇市場に流れた際に、顧客の購買履歴等を分析すれば、どの小売店からカード情報が流出したかを特定できるのです。特定の期間中にすべてのカードで共通に利用されていた小売店があれば、そこが怪しいというわけです。しかし、闇市場に流れたデータから流出源まで遡るこの手法は、社会保障情報やその他の流出データを取引するデータ仲介業者 (Data Brokers) には、通常は使えません。なぜなら、それらの情報にはどこでその情報が取得されたかを分析するための有効な手掛かりが含まれていないことがほとんどだからです。

闇市場で販売されていた消費者の個人情報には、履歴が残っていたものもあり、それを解析することで流出源を探ることもできます。しかし、そういった場合でも、法の強制力の元に専門家が何年もかけないと流出源を特定できません。2011 年の 11 月に、独立系の調査ジャーナリストである Brian Krebs は ID 窃盗サービスの *Superget[dot]info* について書いた記事の中で、「購入できるデータには 2-3 文字の『情報源 ID』が含まれており、流出源を探る手掛かりになる可能性がある。」と記しています。

しかし捜査当局は、この ID 窃盗サービスの情報限について 2013 年まで把握しておらず、把握できた時には、米シークレットサービスがサイトの運営者を逮捕してから 1 年が経っていました。しかしこれにより、捜査官はこれらの ID が大手クレジットビューローExperian の子会社が販売したものであることを突き止めました。ID 窃盗サービスにデータを売った、他のデータ仲介業者同様、購入者が正規のユーザーだと思っていたのです。連邦捜査官はショップの運営者をベトナムからアメリカに誘い出すという込み入った捜査の末にそれを突き止めました。しかし、この ID 窃盗サービスが運用されていた 6 年以上の間に、Superget[dot]info には 1,300 の顧客から少なくとも 190 万ドルが支払われ、社会保障番号や誕生日、住所、引っ越し前の住所、メールアドレスその他の重要な情報が閲覧されており、様々な攻撃に使われたであろうことは覚えておくべきでしょう。

現在、サイバー犯罪の闇市場には様々なショップがあり、米国内で個人情報を盗みたいという要望に対応しています。そして、そのためのコストは驚くほど安いのです。1 件当たり$3-5 という低価格で、それらには有名で影響力を持つアメリカ人も含まれています。こういった ID 窃盗サービスの Web サイトを閉鎖させることも重要ですが、大事なのは対策が長期的に有効かどうかです。こういった「探索」に使われるサービスには、過去に解体されたサービスの第 2 世代・第 3 世代の生まれ変わりが多いのです。

データ仲介業界をもっと積極的に監督する必要があります。そのためには、これらの ID 窃盗サービス経由で再販されたデータの源を特定するための法的な強制力 (と個々の捜査官) を助けるための新しいツールが必要です。Brian Krebs は、流出検知用のレコードを作り、主要なデータ仲介業者に管理させるという方法を提案しています。ユニークなダミーID が入っていれば、どの仲介業者から流出したものかを特定するのが遙かに容易になり、それが侵害によるものなのか、アカウントのハッキングによるものなのかもわかるというわけです。

Experian のようなデータ仲介業者は、データの内容と運用体制を透明化しようとする規制当局からの呼びかけを頑なに拒んできました。米連邦取引委員会 (FTC) が、データ仲介業者をリストアップした Web サイトを作ることを提案したときに、Experian はこれに反対し、「意図しない効果により消費者を混乱させ、電子商取引への信頼を損ねる」と主張しました。この主張は、大手のデータ仲介業者のみを対象とすることは不公平であるとの考えによります。中小のデータ仲介業者はいくらでもあり、同じデータを扱っているからです。

しかし、この主張には疑問が残ります。大手のデータ仲介業者が流出検知用のレコード管理に反対するのは、それによってデータ流出が明るみに出ることを恐れているからではないかというのは、考えすぎでしょうか?

Threat News (ニュース)

NSA レポート: 破壊的マルウェアから身を守るために

国家安全保障情報と情報システムを守る為に、米国家安全保障局 (NSA) の情報保証理事会 (IAD) は、ビッグデータの占拠によって引き起こされる被害を軽減または防止するためのベストプラクティスを発表しました。このプランはよくできており、鍵は「Prevent (阻止)」「Detect (検知)」「Contain (包含)」です。NSA の新しいレポートによると、破壊的で被害の大きいマルウェア攻撃と闘うためには、この包括的な戦略が非常に重要であるとのことです。

サイバー攻撃に対しては、組織は受け身で無く、積極的にこれと闘う姿勢が大切です。一度攻撃者が組織のネットワークを支配すると、ネットワーク上のデータを盗み、破壊することが可能になります。基本的なルールは、組織は常に最悪の事態を想定して計画を作るべきであるということで、そのためには洗練された対策が不可欠です。そのためには、NSA の *Defensive Best Practices for Destructive Malware* レポート (https://www.nsa.gov/ia/_files/factsheets/Defending_Against_Destructive_Malware.pdf) が役に立つでしょう。

この NSA の提言は、以前公開された *Information Assurance Mitigation Strategies* report (https://www.nsa.gov/ia/mitigation_guidance/) の内容を踏襲しています。こちらからダウンロードして内容をご確認下さい: http://www.darkreading.com/attacks-breaches/nsa-report-how-to-defend-against-destructive-malware/d/d-id/1318734.

オバマ大統領のサイバー戦争プランにおいて、非営利組織が秘密兵器となるか

2015 年 1 月 12 日月曜日、オバマ大統領はサイバーセキュリティとプライバシーに関する法案と公共ポリシーを制定する計画を発表し、2015 年 1 月 20 日の一般教書演説で詳細を述べました。この提案には幅広い法案に加えて主要な企業と政府の協力についても含まれています。連邦政府はまた、民間セクターの組織とも協力し、個人のプライバシーを守るための自主規制を推進していきます。

合衆国政府がサイバー戦争に対抗するための予算措置を講じることは確実視されています。サイバー攻撃は指数関数的に増加しており、その影響も比例して増えています。アメリカにおけるサイバーセキュリティの必要性について、論争の余地は無くなるでしょう。問題は、大規模な攻撃の前にどれだけの時間が残されているか、なのです。以下の記事では、政府機関がサイバー攻撃やサイバースパイに対抗するために数十億ドルを費やしていること、アメリカ企業もまた同様であることが記されています。

この記事はまた、「隠れたヒーロー」についても触れています。多くの非営利組織が、個人や中小企業、時には大企業や政府機関に対して、必要とされるサイバーセキュリティサービスを提供しているのです。

Find out here: これらの非営利組織は、政府からほとんど資金を得ていません。そういった隠れたヒーロー達とは誰なのか? こちらをご覧ください: http://www.forbes.com/sites/frontline/2015/01/25/cybersecurity-non-profits-should-be-americas-secret-weapon-in-obamas-cyberwar-plan/.

FBI と IRS が企業や個人を狙った詐欺について警告

陳腐ながらも非常に効果的な詐欺が広がり続けています。企業や消費者の支払いを狙う手法は闇社会でますます一般化しており、犯罪者の使う手法はますます洗練されています。最近、FBI と IRS が別々にこの詐欺について警告を発しました。

FBI は、長年の取引先を装って企業を狙い、偽の請求書を送って支払わせる詐欺 (Business E-mail Compromise [BEC]) が増えていることについて警告しました。FBI によると、この詐欺は「man-in-the-middle」攻撃の改良版で、通常は最高技術責任者 (CTO)、最高財務責任者 (CFO) などの職種を狙います。これらの責任者に、ベンダーなどビジネス上付き合いのあるアカウントからのメールを送り、指定した銀行口座に振り込ませるのです。

Internet Crime Complaint Center (IC3) には、被害者から BEC に関するデータがアメリカのすべての州と海外の 45 ヵ国から送られてきています。2013 年 10 月 1 日から 2014 年 12 月 1 日までの間の統計値や示唆に富んだ解説が、以下のリンクからご覧頂けます。

一方 IRS は、犯罪者が IRS の職員を装って一般の人に架ける脅迫的で押しつけがましい電話と闘っています。この電話詐欺はここ数ヶ月で急増しており、被害者に対して即座に逮捕されると脅したり、国外退去、営業許可の撤回などをちらつかせます。

詳しくはこちらでご覧ください: http://www.csoonline.com/article/2874166/identity-theft-prevention/fbi-and-irs-warn-of-pervasive-maddening-business-consumer-scams.html.

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.

セキュリティのこれから: インシデント・レスポンスについて考えるべき理由

情報セキュリティは日々のニュースの中でも定番となり、組織の高い職制を狙った標的型攻撃から、USB メモリや ICS (産業制御システム) デバイス、IoT システムなどのハッキングまで、報道されない日はありません。これらの記事は興味深く、脆弱性やリスクについて考えるきっかけを与えてくれますが、一方で先進的な脅威や防御システムに注意が向けられ、インシデントへのレスポンスや復旧についてはあまり語られないことが多いのです。

SANS からインシデントレスポンスの重要性に光を当てた新たなレポートが発表され、裁判所もこの考えを支持しています。

Proofpoint の Threat Insight Blog でもこのレポートに含まれる事例やトレンドを分析しましたが、インシデントレスポンスについての見識としては秀でていると考えています。

脅威の管理を包括的に考えるためには、Proofpoint の専門家が苦労してまとめたように、人、プロセス、ツールを含めて考えなければなりません。調査、優先度づけ、包含、復旧のステップをいかに構成し、自動化するかが鍵を握ります: http://www.proofpoint.com/us/threat-insight/post/Why-We-Should-Talk-About-Incident-Response.

ロシアでフィッシングがあなたを狙っている

“spearfishing” と “spear phishing” の違いは何でしょうか? 読み方は同じ「スピアフィッシング」ですが、意味はまったく違います。

Wikipedia によると、spearfishing は「何世紀にもわたって世界中で行われてきた古来の魚釣り手法 (魚突き)」であり、現代では「spear phishing は重要な情報を狙って非正規のアクセスを行うために行われる標的型の電子メール詐欺」となります。一般的なフィッシング詐欺は、広範囲に向けてメールを発信する散弾銃のような手法ですが、スピアフィッシングは特定の組織や内部グループ、時には個人を狙ってメールを送ります。その狙いは知的財産権、財務データ、営業秘密や軍事機密、その他の機密データなどです。

最近、Proofpoint の研究者は非常に興味深いスピアフィッシングの事例を目にしました。

以前ご紹介した “Fiesta” エクスプロイトキットを使った “Tex-Mex taco salad” サイトへの攻撃 (Fiesta はスペイン語でお祭りのことで、それを使ってスペイン料理のサイトを攻撃した) を思い出させます。マルウェアに汚染された spearfishing (魚突き) のサイトに誘導する spear phishing 攻撃なのです。このケースでは、ロシアの魚突き愛好家のための Web サイトが侵害され、ログイン情報を盗むための Outlook Web Access ページをホストしていました。

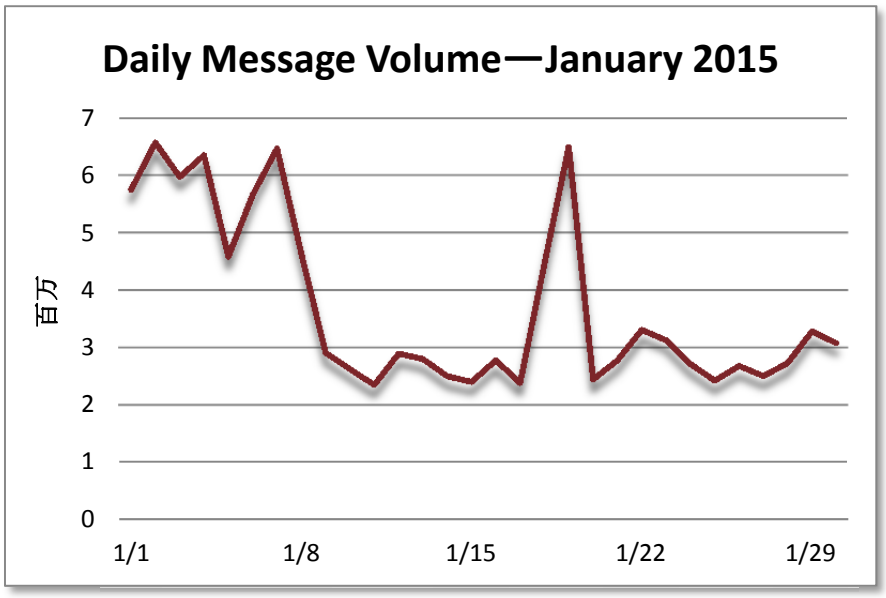
このサイトへのリンクを含んだメールが大学を狙って配信されました。攻撃の本体となるペイロードは、標的とされた大学の学生、教員、職員を騙して Outlook Web Access のログイン情報を入力させることを目的としています。この中の一人でも騙すことに成功すれば、メールアドレス、受信箱内の情報、カレンダー情報などへのアクセスが可能になり、場合によっては、より価値の高い情報 (財務データ、ヘルスケア情報、研究データなど) にアクセスできるサービスを利用できるかも知れません。

学生は常に入れ替わるため、大学はユーザーデータや研究データの宝庫です。ログイン情報を狙う、侵害された Web サイトを使うこの攻撃は、一見無害なメールにも危険が潜んでいることを思い出させてくれます。

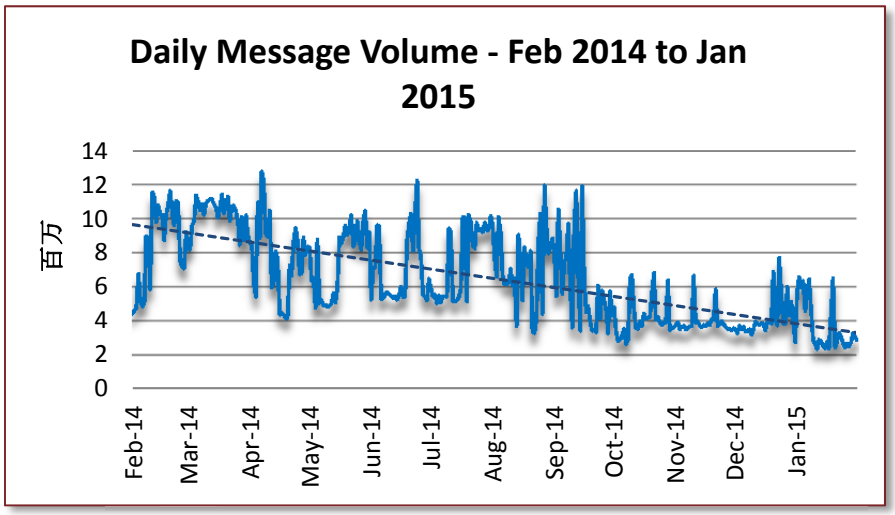
Threat Trends (トレンド)

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。1 月は 600 万通/日から始まり、第 1 週に 450 万通に急減するまでは 600～650 万通の間を推移しました。第 1 週の終わりにはまた 650 万通に戻り、第 2 週には 300 万通に急減し、その後 250 万通まで減りました。第 3 週も 250～300 万通の間で推移し、いきなり 650 万通に急増した後、また 250 万通に落ち込み、その後は 250～300 万通の間で月を終えました。



12 月と 1 月を比べると、スパム量は若干 (9.89%) 減っています。対前年比では 50%の減少となりました。



Spam Sources by Country (スパム発信源)

EU が引き続き 1 位で他を圧倒的に引き離しています。アメリカが 2 位、そのすぐ後にベトナムが続き、アルゼンチンが 4 位です。中国は衰えを見せて 5 位に下がりました。

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。

		Aug '14	Sep '14	Oct '14	Nov '14	Dec '14	Jan '15
Rank	1st	EU	EU	China	China	EU	EU
	2nd	USA	Vietnam	EU	EU	China	USA
	3rd	Argentina	China	Russia	USA	USA	Vietnam
	4th	Russia	Argentina	Vietnam	Russia	Russia	Argentina
	5th	China	Korea	USA	Argentina	Vietnam	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 1 月、全世界のスパムのうち 40.36%を生み出して圧倒的首位に立っています。残りの 4 ヵ国を足しても 16.19%に過ぎません。

December 2014			January 2015		
1	EU	24.49%	**1**	EU	40.36%
2	China	10.34%	**2**	USA	5.68%
3	USA	6.71%	**3**	Vietnam	4.53%
4	Russia	4.36%	**4**	Argentina	3.84%
5	Vietnam	3.95%	**5**	China	2.14%

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

