2018 年 11 月 7 日
Press Release
アカマイ・テクノロジーズ合同会社

日本を含むアジア太平洋地域におけるリスト型攻撃による損失額、1 組織あたり最大年 2,850 万ドル（約 31 億 3,500 万円）に上る

Ponemon Institute と Akamai の共同調査から、同地域における金融詐欺の金銭的コストが明らかに

※本リリースは 2018 年 9 月 25 日(現地時間)にシンガポールで発表されたプレスリリースの翻訳版です。なお、文中の円表示額は 1 ドルあたり 110 円で換算したものです。

インテリジェントなエッジプラットフォームにより安全で快適なデジタル体験を提供する Akamai Technologies (以下「アカマイ」)と Ponemon Institute は、リスト型攻撃の防御、検出、緩和にかかる潜在的コストを明らかにすべく、日本を含むアジア太平洋地域（APAC）で実施した調査の結果を公開しました。本調査の対象となった企業では、リスト型攻撃によるコストは、情報流出したアカウントの 1% に金銭的損失が生じた場合だと 284,649 ドル（約 3,100 万円）、情報流出したすべてのアカウントで金銭的損失が生じた場合だと 2,850 万ドル（約 31 億 3,500 万円）） にも上る可能性があると試算しています。

アカマイの協力で、Ponemon Institute が実施した調査「Credential Stuffing（リスト型攻撃）がもたらす損失：アジア太平洋地域」では、金融サービス、小売 & E コマース、旅行 & ホテル、メディア、エンターテインメント & ゲームなどの幅広い業界から、リスト型攻撃について詳しい知識を持つ IT セキュリティ担当者 538 人を対象としました。リスト型攻撃の結果、復旧や対応等で発生する作業コストについては、アプリケーションのダウンタイムへの対応が 120 万ドル(約 1 億 3,200 万円)、顧客喪失への対応が 150 万ドル(約 1 億 6,500 万円)、IT セキュリティチームのリソースが 110 万ドル(約 1 億 2,100 万円)に上る可能性があると回答しています。

リスト型攻撃は通常、不正行為を働く者がダークウェブで、ユーザー ID やパスワードなど、盗難された認証情報のリストを購入し、そのリストをボットネットを使用してログインページで有効化させることで発生します。その結果、盗難、かつ有効化された認証情報からアカウントが乗っ取られ、不正行為が行われることになります。この種の犯罪の主な目的は、不正購入、不正な金融取引、さらなる秘密情報の窃盗です。

主な調査結果は次のとおりです。

アプリケーションおよび組織の課題

クラウドで発生する リスト型攻撃の緩和には、幅広い戦略が効果を発揮する：

回答者の 51%が、「アプリケーションをクラウドに移行すると、リスト型攻撃を受けるリスクが増大する」に同意しています。セキュリティにはさまざまな側面があるので、組織の広範囲なクラウド戦略はセキュリティ能力に影響を与えます。異なるコンピューティングプラットフォームを使用するアプリケーション（およびさまざまなタイプの顧客に対応するエンドポイント）の数が増え続けるなか、セキュリティ担当チームがこれらのアプリケーションやエンドポイントのセキュリティを確保できるかどうかは、組織のクラウド戦略に左右されます。

リスト型攻撃の防御、検出、緩和の能力

組織はリスト型攻撃への対応に苦慮している：

回答者の 41% が「リスト型攻撃を十分に把握していない」と答えています。また、37% は、「自社のウェブサイトに対する リスト型攻撃がすぐに検出され修復されるとは思っていない」と答えています。

リスト型攻撃の定量化

攻撃は多数のユーザーアカウントに影響を及ぼす：

個々のリスト型攻撃で標的となり得るユーザーアカウント数を質問したところ、回答の平均値は 954 でした。

リスト型攻撃の影響およびコスト

組織には、問題に対処するための予算が不足している：

「自社のセキュリティ予算はリスト型攻撃の防御や封じ込めに十分である」に同意した回答者は 37% しかいませんでした。20% の回答者が「わからない」と答え、「そう思わない」または「まったくそう思わない」と答えた回答者は 43% でした。

2016 年に明らかになった米国の Yahoo の情報流出事案からも、リスト型攻撃の脅威の深刻さがわかります。Yahoo のケースでは、合計 15 億人の認証情報がインターネットに流出しました。これらの認証情報の保護にはハッシュアルゴリズムとしては弱い MD5 が使用されていました。情報の窃盗が発生したのは 2012 年と 2013 年であり、脆弱なセキュリティを破る期間が最大で 4 年間も攻撃者に与えられていました。

調査の手法

「Credential Stuffing（リスト型攻撃）がもたらす損失：アジア太平洋地域」 調査のサンプル抽出枠は、リスト型攻撃について詳しい知識を持ち、自社のウェブサイトのセキュリティ業務に責任を有している IT セキュリティ担当者 15,365 人で構成されています。調査を完了した回答者 591 人のうち

53 の回答はスクリーニングと信頼性確認により除外されています。最終的なサンプル数は 538 件です。

Akamai について

Akamai は世界中の企業に安全で快適なデジタル体験を提供しています。Akamai のインテリジェントなエッジプラットフォームは、企業のデータセンターからクラウドプロバイダーのデータセンターまで広範に網羅し、企業とそのビジネスを高速、スマート、そしてセキュアなものにします。マルチクラウドアーキテクチャの力を拡大させる、俊敏性に優れたソリューションを活用して競争優位を確立するため、世界中のトップブランドが Akamai を利用しています。Akamai は、意思決定、アプリケーション、体験を、ユーザーの最も近くで提供すると同時に、攻撃や脅威は遠ざけます。また、エッジセキュリティ、ウェブ／モバイルパフォーマンス、エンタープライズアクセス、ビデオデリバリーによって構成される Akamai のソリューションポートフォリオは、比類のないカスタマーサービスと分析、365 日/24 時間体制のモニタリングによって支えられています。世界中のトップブランドが Akamai を信頼する理由について、www.akamai.com/jp/ja/、blogs.akamai.com/jp/ および Twitter の @Akamai_jp でご紹介しています。

アカマイ・テクノロジーズ合同会社について:

アカマイ・テクノロジーズ合同会社は、1998 年に設立された、アカマイ・テクノロジーズ・インク（本社：米国マサチューセッツ州ケンブリッジ、最高経営責任者：Tom Leighton）が 100%出資する日本法人です。アカマイは、静的なコンテンツ配信だけでなく各種コンサート・スポーツ試合等の国内限定ストリーミング配信や Web アプリケーションなどの動的配信を多数実現し、日本国内では 350 社以上が当社サービスを利用しています。

アカマイ・テクノロジーズ合同会社は、2018 年に設立 15 周年を迎え、それを記念しブランディングムービーを公開しました。是非ご覧ください。
https://youtu.be/GfrXsG1AUns