［インターネットの現状］／セキュリティ

2017 年第 4 四半期エグゼクティブサマリー

Akamai

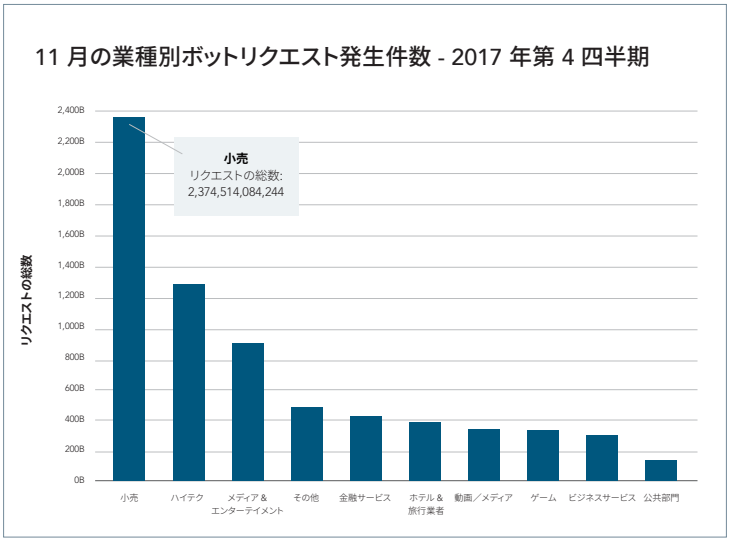
エグゼクティブサマリー／Akamai は世界最大の最も信頼されるクラウド配信プラットフォームです。世界各地に分散している Akamai Intelligent Platform™ を使用して、毎日数兆ものインターネット取引を処理しています。この処理を通じて、ブロードバンド接続、クラウドセキュリティ、メディア配信に関連した指標について莫大な量のデータを収集しています。これらのデータや知見を活用して、企業や政府機関による的確な戦略的意思決定のお手伝いができないかということで、「インターネットの現状」レポートが作成されました。Akamai が四半期ごとに発表する「インターネットの現状レポート」は、このデータに基づいて、ブロードバンド接続とクラウドセキュリティに主眼が置かれています。

ビジネスへの影響／最も被害額が大きく破壊的ないくつかの攻撃があったことで、2017 年の重要なインシデントは、サイバーセキュリティのビジネスへの影響度の大きさに対する意識を高めました。ハードウェアに内在した欠陥 Spectre、Meltdown は、悪意のあるプログラムがコンピュータのメモリー内にあるデータを特別な権限なしに読み取ることを許してしまいます。これらの広範かつ隠れていた脆弱性の存在と、それが引き起こした大きな混乱には、これまでは状況を楽観視していた企業でさえも注目せざるを得なくなっています。

現在発生している攻撃の多くで、よく知られている脆弱性が依然として利用されていますが、そのような欠陥は文書化されパッチがリリースされているので、防御が可能です。「言うは易し、行うは難し」ですが、セキュアコーディングの実践、タイムリーなパッチの適用、適切なデバイスの設定や慎重なパスワード管理などの基本に忠実な包括的な取り組みが、防御を固めるうえで大きな効果につながります。

サイバー犯罪者が狙う新たな攻撃対象が増える中、セキュリティの状況は絶えず変化しています。モバイルデバイス、モノのインターネット（IoT）、API をターゲットにした攻撃は、2018 年に予想される攻撃の重要なテーマです。攻撃の戦略の進化も続いています。我々はエンタープライズシステムを標的にした、新たな攻撃の傾向を目の当たりにしています。この攻撃はシステムデータを盗むだけでなく、コンピューティングリソースまでも奪います。おそらく、暗号通貨（仮想通貨）の隆盛に伴うマイニングリソースの潜在的価値の高まりが一因であると考えられます。さらに、この四半期のインターネットの現状／セキュリティレポートでは、ネットワーク接続、ボットネットトラフィック、認証情報の悪用（なりすまし）に関する Akamai 独自のデータから、ウェブサイトへのログインの多く（43%）が不正アクセスであることを明らかにしています。今日、デジタル接続されたエンタープライズ組織にとって、その健全性を維持していくためには、このような傾向を理解しておくことが不可欠です。

編集者による概説／新たな年の開始にあたり前年のレポートで学んだことを振り返る良い機会であると考えます。



2017 年の第 4 四半期では、DDoS 攻撃とウェブアプリケーション攻撃の両方が前年同期比で引き続き増加しており、サイバー犯罪者が長年利用している実証済みの攻撃ベクトルを有効な攻撃手法として利用し続けていることを示しています。このことから、接続されたデバイスの適切な設定や、パッチの適用、入力された値の検証や、ガイドラインに沿ったセキュアコーディングなどの基本的なセキュリティのベストプラクティスに従うことの重要性に疑問の余地がないことがわかります。

第 4 四半期では、Mirai ボットネットの影響や進化が続いていることが確認されました。本四半期のインターネットの現状／セキュリティレポートでは、前年来の Mirai の活動と進化に注目し、今後の Mirai 対策に役立つ情報を掲載しています。Akamai の SIRT メンバーである Larry Cashdollar は、認識しておくべき点について、いくつかの CVE を詳しく分析しています。ここで取り上げたウェブ・サーバー・プログラムの脆弱性は最も深刻なタイプのもので、認証の必要なくシステム上で攻撃を実行されてしまいます。本四半期のレポートでは、これまでのインターネットの現状／セキュリティレポートには掲載されていなかった、ボットトラフィックの分析と Credential abuse（ボットによる大量の不正ログイン）という 2 つのデータについても分析結果を掲載しています。

DDoS 攻撃［2017 年第 4 四半期と 2017 年第 3 四半期の比較］

- DDoS 攻撃総数の減少率は 1% 未満
- インフラストラクチャレイヤー（レイヤー 3 および 4）に対する攻撃が 1% 減少
- リフレクションベースの攻撃が 3% 減少
- アプリケーションレイヤーに対する攻撃が 115% 増加

最後に、2018 年は暗号通貨がセキュリティ関連の記事で大きな話題となることが予想されます。暗号通貨は、企業のコンピュータに侵入して、その計算リソースを盗用される要因となる傾向が見えています。暗号通貨は、今後も絶えず進化する他の多くの手法とハッカーの戦略においての推進力となる可能性もあります。

DDoS の最新情報／分散型サービス妨害（DDoS）攻撃は、サイトのダウンやビジネスの混乱を引き起こすだけでなく、より悪質なデータ漏えいやシステム侵害目的の攻撃を隠して、攻撃対策リソースの注意をそらすためにも使われます。DDoS 攻撃は前の 2 回の四半期には発生件数が増加していましたが、2017 年第 4 四半期は横ばい状態になり、前四半期と比較して若干の（1% 未満）減少傾向が見られました。特に注目すべきは、アプリケーションレイヤーへの攻撃は前四半期比で 115% と大幅に増加しましたが、それでも DDoS 攻撃全体の 1% 未満を占めるにとどまっている点です。DDoS 攻撃の発生件数は、2016 年第 4 四半期から 14% 増加しており、このことは長期的に見て全体として増加傾向にあることを示しています。

第 4 四半期に最も多く標的にされたのはゲーム業界で、DDoS 攻撃全体の 79% がゲーム業界を対象としたものでした。それに次いで多かったのは金融サービス業界で、第 4 四半期に DDoS アクティビティの大幅な増加が見られ、わずか 1 週間で 45 件の攻撃が発生しました。このような頻度の高い攻撃は堅牢な DDoS 緩和ソリューションが必要であることを明確に示しています。それは、業務の中断を防止するだけでなく、より悪質な不正アクセスの隠れ蓑に DDoS を使うといった多面的な攻撃をも阻止できます。

ウェブアプリケーション攻撃の最新情報／DDoS 攻撃とは対照的に、ウェブアプリケーション攻撃は通常、アプリケーションの脆弱性を狙って、データを盗んだり、基盤となるシステムに不正アクセスしようと試みたりします。ウェブアプリケーション攻撃は DDoS 攻撃よりはるかに一般的で、攻撃者は単にインターネットをスキャンして、犠牲となる脆弱なサイトを探します。第 3 四半期に前四半期比 30% と大幅に増加したウェブアプリケーション攻撃は、第 4 四半期には若干の減少傾向が見られたものの、2017 年全体では大幅な増加が見られ、この傾向は 2018 年も続くものと予想されます。

ウェブアプリケーション攻撃［2017 年第 4 四半期と 2017 年第 3 四半期の比較］

- ウェブアプリケーション攻撃総数が 9% 減少
- 米国が攻撃元である攻撃が 29% 減少
- SQLi 攻撃が 9% 減少

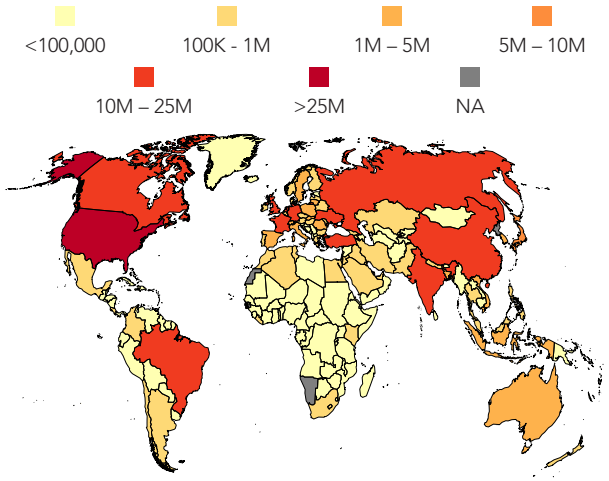
攻撃ベクトルの主流は引き続き SQL インジェクションであり、第 4 四半期に発生したウェブアプリケーション攻撃全体の 50% を占め、第 3 四半期から 47% 増加しています。このようなタイプの攻撃は自動化や拡張が簡単で、組織がユーザー入力の検証処理をコードに組み込むなどの適切な予防措置を講じない限り、有効な攻撃手段であり続けると思われます。

Akamai が確認したウェブアプリケーション攻撃トラフィックの攻撃元、攻撃対象のどちらにおいても、米国が他国を圧倒し続けています。米国で第 4 四半期に発生したウェブアプリケーション攻撃は 2 億 3,800 万件で、第 3 四半期の 3 億 2,300 万件からは減少したものの、次に多いブラジルの 10 倍以上の数の攻撃が発生しました。第 4 四半期、米国を発信元とする攻撃は 1 億 3,200 万件あり、次に多いオランダは 4,700 万件でした。

詳しい分析と調査結果は、レポートの完全版をダウンロードしてご覧いただけます。

2017 年第 4 四半期「インターネットの現状／セキュリティ」レポートでは、Akamai のグローバルインフラストラクチャから収集された攻撃データをもとに、社内の多様なチームによる調査を行っています。

ウェブアプリケーション攻撃の発信国 - 世界全体、2017 年第 4 四半期



インターネットの現状／セキュリティチーム
Jose Arteaga、Akamai SIRT Lead、Data Wrangler — 攻撃の注目点
Dave Lewis、Global Security Advocate — DDoS アクティビティ、
ウェブアプリケーション攻撃アクティビティ
Chad Seaman、Akamai SIRT — 攻撃の注目点
Wilber Mejia、Akamai SIRT — 攻撃の注目点
Alexandre Laplume、Akamai SIRT — 攻撃の注目点
Larry Cashdollar、Akamai SIRT、Sr. Engineer — 注意すべきウェブ脆弱性
Richard Willey、Sr. Data Scientist — 世界規模のネットワークを理解する方法
Elad Shuster、Security Data Analyst、Threat Research Unit
Jon Thompson、Custom Analytics

編集スタッフ
Martin McKeay、Senior Security Advocate、Senior Editor
Amanda Fakhreddine、Sr. Technical Writer、Editor

お問い合わせ先
sotisecurity@akamai.com
Twitter: *@akamai_soti* / *@Akamai_jp*
www.akamai.com/stateoftheinternet-security

レポートの完全版をダウンロード

[インターネットの現状]／セキュリティ
2017 年第 4 四半期レポート完全版