［インターネットの現状］／セキュリティ

2017 年第 2 四半期エグゼクティブサマリー

Akamai

Akamai は世界最大で最も信頼されるクラウド配信プラットフォームで、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が収集されます。「インターネットの現状」の目的は、これらのデータを活用し、企業や政府機関がインテリジェントかつ戦略的に意思決定できるように支援することです。Akamai は四半期ごとに、これらのデータを分析し、ブロードバンド接続とクラウドセキュリティに重点を置いた「インターネットの現状」レポートを発表しています。

エディター概説／「インターネットの現状／セキュリティ」レポートでは、絶えず変化を続けるインターネットの状況を紹介しています。2017 年第 2 四半期は、ボリューム型攻撃に関与する IP アドレスの数が大幅に減り、大規模攻撃が低調となるなど、トラフィックの特性に多くの大きな変化が見られました。ウェブアプリケーション攻撃の頻度は増加を続け、SQL インジェクション（SQLi）攻撃が最も多数を占めています。

Akamai で確認された DDoS 攻撃の数は、この四半期に増加しています。これまでに見られた毎秒 100 ギガビット（Gbps）を超える最大規模の攻撃が、ここ 3 年余りの期間では初めて姿を消したことが、顕著な点といえます。世界中の企業が WannaCry や Petya マルウェアの影響を受け、その経済的な対価は 40 億ドルを超える可能性があります。Mirai ボットネットは引き続き組織への攻撃に利用されていますが、同時に旧来のマルウェアが新たな目的に転用されています。これには、Akamai Security Intelligence Response Team（SIRT）が今回のレポートで検討する PBot ボットネットなどが含まれます。

Akamai の調査員は、ドメイン生成アルゴリズム（DGA）と呼ばれるマルウェアプロセスによって作成されるトラフィックを調査しました。ボットネットは DGA を用いることで、コマンド&コントロールチャネルとして利用する多数のドメインを作成し本物のチャネルを隠すため、見つけるのは至難の業です。また、ボットの接続方法について理解するために初めて、9 か月間を超える Mirai のコマンド&コントロールトラフィックを確認しました。これは、詳細な調査を進めるためのさらなる手がかりとなります。

DDoS の最新情報／分散型サービス妨害攻撃（DDoS）は、3 四半期にわたる減少の後、この第2 四半期で 28% 増加しました。対象となったお客様の DDoS 攻撃は平均 32 回にもおよび、平均で 3 日ごとに新しい攻撃を受けています。あるゲーム企業のお客様は、この四半期だけでも 558 回の攻撃を受けました。

Mirai ボットネットは多数の脆弱な IoT デバイスを利用しますが、この四半期は旧来の PBot と呼ばれるマルウェアが攻撃に転用され、侵害されたノードは（数万でなく）数十万規模にのぼります。このボットネットは、この四半期最大の攻撃に利用され、ある金融機関を標的に 75 Gbps の規模に及んでいます。

DoS 攻撃の規模は、新しいマルウェアの変種や攻撃ツールの人気や入手しやすさによって、すぐさま変動します。2016 年最大の DDoS 攻撃は 500～600 Gbps 以上で、2014 年と 2015 年の 100 Gbps から大きく拡大しました。この四半期の最大規模の攻撃は 75 Gbps と比較的控えめながら、経験的にこの状態が長く続かないことが考えられます。

インフラストラクチャレイヤーのボリューム型攻撃は、第2 四半期の DDoS 攻撃の 99% を占めますが、これは主に「貸出」型のボットネットを利用したものです。アプリケーションレイヤーを狙ったボリューム型攻撃は稀であることが大きな理由です。この種の攻撃は、総当たり攻撃に頼るよりも、Web やデータベースの脆弱性など、アプリケーションを標的とするものと考えられます。

DDoS 攻撃の大多数はリフレクション技術を使って作成されます。スプーフィングした IP アドレスで共通のインターネットプロトコルに過剰なクエリーを実行し、その応答を攻撃者のターゲットに送信します。最も一般的なリフレクターである Domain Name Services（DNS）と Network Time Protocol（NTP）は、最大 100 倍以上にもトラフィックを増幅し、世界中で利用できる態勢が整っています。

DDoS 攻撃［2017 年第 2 四半期と 2017 年第 1 四半期の比較］
- DDoS 攻撃の総数が 28% 増加
- 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 27% 増加
- リフレクションベースの攻撃が 21% 増加
- 標的あたりの平均の攻撃数が 28% 増加

最大の DDoS 攻撃
- 2017 年 Q2：75 Gbps
- 2017 年 Q1：120 Gbps
- 2016 年 Q4：517 Gbps
- 2016 年 Q3：623 Gbps
- 2016 年 Q2：363 Gbps

ウェブアプリケーション攻撃／ウェブアプリケーション攻撃は、四半期ごとに増加を続けています。ボリューム型 DDoS 攻撃がサイトに与える影響は数分、数時間、場合によって数週間に及びますが、ウェブアプリケーション攻撃は組織のサイトを侵害するおそれがあり、さらに長期にわたってビジネスに大きな影響を与える可能性があります。

ウェブアプリケーション攻撃［2017 年第 2 四半期と 2017 年第 1 四半期の比較］

- ウェブアプリケーション攻撃の総数が 5% 増加
- 米国が攻撃元である攻撃が 4% 増加（攻撃元国トップ）
- SQLi 攻撃が 21% 増加

ウェブアプリケーション攻撃の上位攻撃ベクトル（2017 年第 2 四半期）

- SQL インジェクション（SQLi）：51%
- ローカル・ファイル・インクルージョン（LFI）：33%
- クロスサイトスクリプティング（XSS）：9%

ウェブアプリケーション攻撃は、大量のトラフィックでサービスに負荷をかけるものではない点でボリューム型攻撃と異なります。代わりに、サーバーの脆弱性を狙い、基盤サービスやシステムの侵害を試みます。最も一般的な SQLi、ローカル・ファイル・インクルージョン、クロスサイトスクリプティングは、ウェブサーバーのデータを入手または脆弱性を悪用しようと試みます。

多くのケースで、Akamai は行動分析手法を用いて、潜在的な悪意のある活動を検知し、ウェブアプリケーション攻撃をブロックしています。第2 四半期において、Akamai Cloud Security Intelligence（CSI）プラットフォームに記録された DNS 関連トラフィックを調べたところ、マルウェアに感染したネットワークに見られる異常な行動が確認されました。多く利用されるいくつかのボットネットは、毎日新しいドメイン名を生成してコマンド&コントロールインフラストラクチャを移動させ、発見を逃れるためのドメイン生成アルゴリズム（DGA）を使用します。関連する特性を確認し、機械学習アルゴリズムを実行することで、異常な行動を特定し、マルウェアの活動を検出およびブロックすることができます。

ビジネスへの影響／この四半期は、Akamai が保護を行っている組織をターゲットとした DDoS 攻撃とウェブアプリケーション攻撃がともに増加しました。これまでの 3 四半期と比べ、DDoS 攻撃が勢いを戻した形です。このことは、攻撃の数が将来増えることを意味しているのでしょうか？絶対とは確信できませんが、ウェブアプリケーション攻撃と DDoS 攻撃はともに周期的であり、多くの場合、それまで以上に強力化することが分かっています。この事実を変えるには、インターネットの特性に構造的なシフトが必要になるでしょう。そのため、休暇の計画を立てるように、次に高まる攻撃トラフィックへの備えが必要です。

現在攻撃者が使っている Mirai や PBot などのツールを理解することで、将来何が起こるかを推測することが可能です。ドメイン生成アルゴリズムなど、マルウェアが身を隠すために使用する方法を調べることで、マルウェアをコントロールするトラフィックを明らかにできます。悪意のあるウィザードが背後で何をしているかを詳しく知ることで、防御対象のシステムをより確実に保護することができます。

詳しい分析と調査結果は、レポート完全版をダウンロードしてご覧いただけます。

2017 年第2 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。

［インターネットの現状］／セキュリティ

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、Mirai コマンド&コントロールクラスタ
Wilber Mejia、Akamai SIRT－攻撃の注目点
Alexandre Laplume、Akamai SIRT－攻撃の注目点
Elad Shuster、Security Data Analyst、Threat Research Unit
Or Katz、Principal Lead & Security Researcher－ドメイン生成アルゴリズム
Jon Thompson、Custom Analytics
Shrijita Bhattacharya、Intern－Mirai コマンド&コントロールクラスタ

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

デザイン
Shawn Doughty、クリエイティブディレクション
Brendan O'Hara、アートディレクション／デザイン

お問い合わせ先
sotisecurity@akamai.com
Twitter：*@akamai_soti*／*@Akamai_GK*
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 2 四半期レポート完全版