2018 年 5 月 16 日
Press Release
アカマイ・テクノロジーズ合同会社

アカマイ「インターネットの現状／セキュリティ：キャリア・インサイト・レポート」を発表
サイバー脅威対策における情報共有の重要性に注目

DDoS、マルウェア、ボットネット攻撃への防御対策強化に役立つ
14 兆超の DNS クエリーを含めたビッグデータのレイヤー分析

世界最大、かつ最も信頼性の高いクラウド・デリバリー・プラットフォームを有する Akamai Technologies, Inc.（NASDAQ：AKAM、以下「アカマイ」）は、「インターネットの現状／セキュリティ：キャリア・インサイト・レポート 2018 年春版」を発表しました。このレポートでは、情報共有がサイバー脅威に対する対策において、重要なカギであることが明らかになりました。なお本レポートは、2017 年 9 月から 2018 年 2 月までの期間にアカマイが世界中の通信サービスプロバイダー（CSP）ネットワークから収集した 14 兆を超える DNS クエリーデータを分析し、まとめたものです。

2017 年にアカマイが買収した Nominum は、19 年以上にわたり、DDoS 攻撃、ランサムウェア、トロイの木馬、ボットネットなどの巧妙なサイバー攻撃に対する包括的な防御策の改善のため、詳しい DNS データを活用してきました。アカマイのキャリア・インサイト・レポートは、Nominum の専門知識を基盤に、他の複数のセキュリティレイヤーからのデータを加えて強化された DNS ベースのセキュリティの効果について重点的に論じています。このようなセキュリティのレイヤーアプローチには、組織のデータを集合的に保護するための、多様なセキュリティソリューションの収集が含まれます。

アカマイの Threat Intelligence、Data Science 担当ディレクターである Yuriy Yuzifovich は次のように述べています。「個々のシステムに対する攻撃を単発で理解するだけでは全体が見えず、複雑化した現在の脅威状況に対応できません。さまざまなチーム、システムおよびデータセットにまたがる知識を取得するには、多様なプラットフォームとの通信が不可欠です。当社のサービスが提供する DNS クエリーは、セキュリティチームに脅威状況の全体像を把握させる適切なデータを提供するために、戦略的な要素として機能すると考えています」

Mirai ボットネット対策：チームのコラボレーション

Mirai をより包括的に検出できるようにする取り組みのための、Mirai のコマンド & コントロール（C&C）ドメインの発見において、アカマイ内部のコラボレーションが重要な役割を果たしました。アカマイ Security Intelligence and Response Team（SIRT）は、Mirai が初めて登場してから、Mirai の通信の検出およびその C&C サーバーの特定のために、ハニーポットを使用して Mirai を追跡してきました。

2018 年 1 月下旬に、アカマイの SIRT チームと Nominum のチームは、疑わしいとされる 500 以上の Mirai C&C ドメインのリストを共有しました。共有の目的は、DNS データと人工知能を活用することで、この C&C リストを拡張し、今後 Mirai をより包括的に検出可能なのかを明らかにすることでした。いくつかのレイヤー分析により、社内合同チームは、Mirai ボットネットと Petya ランサムウェア拡散者間の接続を検出するために、Mirai C&C データセットを拡張することができるようになりました。

このコラボレーションによる分析から、IoT ボットネットの進化の示唆が得られました。IoT ボットネットは、DDoS 攻撃の開始のみを主な目的とするものから、ランサムウェアの拡散や暗号通貨マイニングなど、より巧妙な活動へと進化しつつあると考えられます。IoT ボットネットは、感染の兆候がほとんどないため、ユーザー自身で検出するのは困難ですが、複数のチームが協力して調査することで、ボットネットの活動を制御するために、新しい C&C ドメインを検出・ブロックできる可能性がでてきました。

Javascript を使用した暗号通貨マイニング：いかがわしいビジネスモデル

暗号通貨の急速な普及を反映して、さまざまなマイニングマルウェアや、それに感染したデバイスの増加が観察されています。

アカマイが把握している大規模な暗号通貨マイニングのビジネスモデルは 2 種類あります。その 1 つは、暗号通貨のトークンをマイニングするために、感染したデバイスの処理能力を利用するビジネスモデルです。もう 1 つは、そのサイトを訪問するデバイスに暗号通貨マイニングの作業をさせるコンテンツサイトに埋め込まれたコードを使用するビジネスモデルです。後者のビジネスモデルについてアカマイが分析を実施したところ、ユーザーとウェブサイトオーナーの両者に新たなセキュリティの課題が浮かび上がりました。アカマイは暗号通貨マイニングドメインの分析の後、コンピューターの処理能力とマイニングからの利益の両要素からこの活動のコストを試算しました。この調査結果で興味深いのは、暗号通貨マイニングが広告収入に代わってウェブサイトの資金源になる可能性があるという点です。

変化する脅威：マルウェアや攻撃の目的変更

サイバーセキュリティに安定はありません。研究者たちにより、ハッカーは現在のデジタル環境に合わせて古い手法を再利用していることがわかっています。アカマイはこのデータを半年以上収集してきましたが、いくつかの顕著なマルウェアキャンペーンや攻撃において、以下のような行動手順の変化が見られました。

- 2017 年 11 月 24 日から 12 月 14 日の期間に、Windows システムを中間者攻撃にさらす目的で Web Proxy Auto-Discovery（WPAD）プロトコルを利用するケースが発見されました。本来 WPAD は、保護されたネットワーク（LAN など）内での利用を想定したものであり、インターネットに露出されていると、コンピューターを重大な攻撃に対して常にオープンな状態にします。
- マルウェアの作成者は金融関連の情報に加えて、ソーシャルメディアのログイン情報の収集にも手を出し始めています。Zeus ボットネットの亜種である Terdot は、ローカルプロキシを作成

し、攻撃者が被害者のブラウザーでサイバースパイ攻撃を実施したり、フェイクニュースを拡大したりできるようにします。

- Lopai ボットネットは、ボットネットの作成者が、より柔軟なツールを作成していることを示す例です。このモバイルマルウェアは主に Android デバイスを標的としたものですが、オーナーが新機能を追加してアップデートを作成できるモジュール構成を使用しています。

「インターネットの現状／セキュリティ：キャリア・インサイト・レポート 2018 年春版（英文）」は こちら から ダウンロードできます。
https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/spring-2018-state-of-the-internet-security-report.pdf

手法

アカマイのセキュリティ調査チームは、サイバー犯罪者の次の行動を予測するために、1 日、1 週間、四半期単位でデータセットを分析しています。大量の DNS データの中から攻撃の前兆を検出し、既知の攻撃タイプを確認すると同時に、未知の悪意ある新しい攻撃を検出することが目的です。この調査チームは、民間と公共のデータソースを利用するとともに、アカマイ のお客様から得られる毎日 1000 億のクエリーを分析しています。アカマイは、40 カ国以上で、130 以上のサービスプロバイダーと協力し、毎日 1.7 兆のクエリーを解決しています。これらのサンプルは、世界中のユーザーと企業が生成する DNS トラフィック全体の約 3% に相当します。

アカマイ について：

世界最大、かつ最も信頼性の高いクラウド・デリバリー・プラットフォームを有するアカマイは、デバイスや場所に関係なく、最高、かつ最もセキュアなデジタル体験をお客様に提供します。アカマイのプラットフォームは 130 カ国に 20 万台以上という比類のないスケールで展開されており、お客様に優れたパフォーマンスとセキュリティを提供しています。ウェブ/モバイルパフォーマンス、クラウドセキュリティ、エンタープライズアクセス、ビデオ・デリバリー・ソリューションによって構成されるアカマイのソリューションは、優れたカスタマーサービスと 365 日/24 時間体制の監視によって支えられています。グローバルトップの金融機関、e コマース事業者、メディア・エンターテインメント企業、政府機関等が、アカマイを信頼する理由について、<www.akamai.com/jp/ja/> または <blogs.akamai.com/jp/> および Twitter の @Akamai_jp でご紹介しています。

※アカマイとアカマイ・ロゴは、アカマイ・テクノロジーズ・インクの商標または登録商標です
※その他、記載されている会社名ならびに製品名は、各社の商標または登録商標です
※本プレスリリースの内容は、個別の事例に基づくものであり、個々の状況により変動しうるものです