2022 年 6 月 21 日

Press Release

アカマイ・テクノロジーズ合同会社

Akamai、インターネットセキュリティの脅威に関する調査レポートを 3 本公開

ランサムウェア、Web アプリケーションと API、DNS トラフィックに関する知見をまとめたレポート

※本リリースは 2022 年 6 月 7 日（現地時間）マサチューセッツ州ケンブリッジで発表されたプレスリリースの抄訳版です。

オンラインライフの力となり、守るクラウド企業、Akamai Technologies, Inc.（NASDAQ：AKAM）は本日、RSA Conference 2022 で新たに 3 本の調査レポートを公開しました。これらの詳細なレポートは、Web セキュリティで最も重要な 3 つの分野であるランサムウェア、Web アプリケーションおよび API、DNS トラフィックに焦点を絞ったものです。

Akamai のリサーチチームは、複数のプラットフォームにまたがる数兆件のデータポイントを分析し、多用されている攻撃トラフィックとテクニックから攻撃者のふるまいに関する新たな知見を導き出しました。この 3 本のレポートは、最も顕著なセキュリティトレンドとリンクし、最新の攻撃環境マップを正確に描いています。最新のランサムウェア攻撃のトレンド分析では、リスクを強調して緩和を提案しています。一方、Web アプリケーション攻撃と API 攻撃のトレンド分析では、ランサムウェアオペレーターやその他の攻撃者が使用する感染ベクトルに対する新たな視点を挙げています。DNS の分析では、インターネットの最も基本的なテクノロジーの 1 つで分析した攻撃の全体像により、レポートを補完しています。

Akamai のサイバーセキュリティ・エキスパート・チームは、攻撃トレンドやテクニックとともに、現在最も差し迫ったサイバーセキュリティ問題を解決するソリューションを主軸として分析を展開しています。各レポートのハイライトは以下の通りです。

- Akamai ランサムウェア脅威レポート： Conti ランサムウェア集団による攻撃など、サービスとしてのランサムウェア（Ransomware as a Service: RaaS）攻撃が増加する中、Akamai は、ランサムウェア攻撃者の最新かつ最も効果的な手法、ツール、テクニックを分析し、発見しました。重要なポイントは以下の通りです。
    - 成功した Conti ランサムウェア攻撃の 60% は米国企業に対して行われ、30% は EU 圏で発生しています。
    - 攻撃を受けた業界を分析した結果、サプライチェーンの混乱、重要なインフラへの影響、サプライチェーンに対するサイバー攻撃のリスクが鮮明になっています。
    - 最も成功した Conti 攻撃は、売上高 1,000 万ドル～ 2 億 5,000 万ドルの企業をターゲットにしており、この範囲が中小規模企業の攻撃ターゲットとして「ゴルディロックス（スウィートスポット）」と言えます。

- 攻撃を仕掛ける犯罪集団の戦術、テクニック、手順（TTP）はよく知られていますが、非常に効果的です。他のハッカーが見向きもしない武器を斬新な方法で活用しています。しかし、こうした攻撃も適切な緩和策で防ぐことができます。
- Conti のドキュメントでは、暗号化よりもハッキングやハンズオンの伝播に重点が置かれています。そのため、ネットワーク防御者も同様に、暗号化ではなく、キルチェーンにおけるハッキングやハンズオンの伝播に重点をおいて防御する必要があります。

- Akamai Web アプリケーションおよび API 脅威レポート： 2022 年前半、Akamai は世界中で Web アプリケーション攻撃と API 攻撃の大幅な増加を確認しました。現在までに 90 億件以上の攻撃の試みを観測しています。各社の主な調査結果の詳細は以下の通りです。
  - 弊社のお客様に対する Web アプリケーション攻撃の試みは、前期だけで前年同期比 300% 増となり、Akamai がこれまでに観測した最大の増加幅となっています。
  - LFI 攻撃は今や SQLi 攻撃を上回り、最大の WAAP 攻撃ベクトルとなっており、前年比 400% 増に迫る勢いです。
  - コマース分野は最も影響を受ける業種であり、最近の攻撃アクティビティの 38% を占めています。一方、テクノロジー分野は 2022 年にこれまでで最大の成長を見せています。

- Akamai DNS トラフィック知見脅威レポート：1 日に 7 兆件以上の DNS クエリーを分析し、マルウェア、ランサムウェア、フィッシング、ボットネットなどの脅威を未然に特定してブロックしている Akamai リサーチャーは、以下のように分析結果をまとめています。
  - 監視対象のデバイス 10 台のうち 1 台以上が、マルウェア、ランサムウェア、フィッシング、コマンド & コントロール（C2）に関連するドメインと少なくとも 1 回以上通信しています。
  - フィッシングトラフィックの分析によると、ほとんどの被害者はテクノロジー業ブランド（被害者の 31%）と金融業ブランド（同 32%）を悪用・模倣した詐欺被害に遭っています。
  - 1 万個以上の悪性 JavaScript サンプルを分析した研究によると、マルウェアドロッパー、フィッシングページ、詐欺行為および暗号通貨マイニングのマルウェアなどの代表的な脅威では、分析したサンプルの 25% 以上が JavaScript 難読化手法を使用して検知を回避しています。

Akamai Security Research 担当 Senior Director の Ofri Ziv は「これらの新しいレポートは、組織が現在直面している最も差し迫ったセキュリティ問題のいくつかに詳細な見解をもたらしています。また、Akamai のグローバルな脅威環境に対する比類のない可視性により、Akamai リサーチャーは他のグループではほとんど発見できないイベントを分析して関連付けることができます。Akamai は、コミュニティが攻撃者の主な標的を理解し、脅威が進化し続ける中で、こうした新しい脅威から自らを守るための効果的な防御策を把握できるようにサポートしたいと考えています」と、述べています。

詳細な情報については、新しい Akamai セキュリティハブ にアクセスし、Twitter で @Akamai_Research をフォローしてください。Akamai の脅威リサーチャーと交流し、貴重な知見を得ることができます。

Akamai について：

Akamai はオンラインライフの力となり、守っています。世界中のトップ企業が Akamai を選び、安全なデジタル体験を構築して提供することで、毎日、いつでもどこでも、世界中の人々の人生をより豊かにしています。クラウドからエッジまで、世界で最も分散されたコンピューティングプラットフォームにより、Akamai は、アプリケーションの開発や実行を容易にし、同時に、体験をユーザーに近づけ、脅威を遠ざけます。Akamai のセキュリティ、コンピューティング、デリバリーの各ソリューションの詳細については、akamai.com および akamai.com/blog をご覧いただくか、Twitter と LinkedIn で Akamai Technologies をフォローしてください。