2025 年 8 月 4 日

Press Release

アカマイ・テクノロジーズ合同会社

Akamai 脅威レポート：
ランサムウェア攻撃の複雑化と脅迫の巧妙化

四重脅迫の増加、攻撃者の戦術、手口、手順と、組織への予期せぬ影響について解説

※本リリースは 2025 年 7 月 30 日 (現地時間) シンガポールで発表されたプレスリリースの抄訳版です。

オンラインビジネスの力となり、守るサイバーセキュリティおよびクラウドコンピューティング企業、Akamai Technologies, Inc.（NASDAQ：AKAM）は、攻撃者がランサムウェアキャンペーンにおいて四重脅迫という新たな戦術を使用している一方、二重脅迫が依然として最もよく見られる手口であることを確認しました。ランサムウェアは、2024 年にアジア太平洋（APAC）地域で発生したすべてのデータ漏えいの過半数を占めています。APAC の企業は、脆弱性を最小限に抑え、ビジネスレジリエンス（事業の回復力）を確保するために、サイバー防御を精査し、強化する必要があります。

Akamai の最新の「インターネットの現状（SOTI）」レポート「ランサムウェアレポート 2025：急変する脅威にさらされる中で回復力を構築」によると、新たな四重脅迫の傾向として、攻撃者は従来の二重脅迫型ランサムウェアを基盤に、さらに多様な手口を加えています。攻撃者が被害者のデータを暗号化し、身代金を支払わなければそのデータを公開すると脅す従来の二重脅迫型のランサムウェアに加え、DDoS（分散サービス妨害）攻撃や、顧客、パートナー、メディアなどのサードパーティへの嫌がらせを行うことで、被害者への圧力を一層高めるものです。

Akamai の Advisory CISO、Steve Winterfeld は「今日のランサムウェアの脅威は、もはや単なる暗号化だけではありません」「攻撃者は、盗んだデータを利用し、情報を公開し、サービスを停止させることで、被害者への圧力を高めています。こうした手口によって、サイバー攻撃はビジネスの本格的な危機へと変化しており、企業はサイバー攻撃に備え、対応する方法を見直すことを余儀なくされています」と述べています。

標的にされる APAC の医療部門と法務部門

Abyss Locker や Akira などの新参ボットが急速に増加しているものの、LockBit、BlackCat／ALPHV、CL0P などの主要なランサムウェアグループは依然として、APAC 全体で圧倒的な割合を占めています。これらのランサムウェアグループは、医療から法務サービスまで、驚くべき精度で APAC 地域の重要な部門を標的にしています。注目すべきインシデントとしては、Abyss Locker によってオーストラリアの Nursing Home Foundation から 1.5 TB の機密情報が漏えいした事件や、シンガポールを拠点とする法律事務所が Akira の攻撃を受けて脅迫され、190 万米ドルの身代金を支払った事件が挙げられます。ハイブリッドランサムウェアの活動家グループも勢いを増しています。RansomHub や Play、Anubis などのグループは、APAC 拠点の中小企業、医療機関、教育機関を標的に、Ransomware-as-a-Service（RaaS）プラットフォームを利用し

ています。オーストラリアのある体外受精クリニックと複数の医療業務は最近、こうした新たな犯罪集団による侵入被害を受けました。

コンプライアンスの複雑さで責務が増大

APAC 地域では、コンプライアンスの断片化と規制の成熟度の不均一化が、規制を利用したランサムウェアグループによる脅迫の巧妙化に拍車をかけています。たとえば、シンガポールの個人情報保護法（Personal Data Protection Act、PDPA）に違反すると、年間収益の最大 10% の罰金が科される可能性があります。インドでは刑事罰が科される可能性があります。一方日本では、現在、コンプライアンス違反に対する正式な罰金は定められていません。このような地域間での規制の差は、グローバル企業には複雑なパッチワークのようで、報告の遅延を招くおそれがあります。状況が悪化すると、悪用の機会をうかがっている攻撃者に盲点を突かれることになりかねません。

ゼロトラストとレジリエンスは依然として不可欠

Akamai は、レポートの中で、最新のランサムウェア戦術に対する基本的な防御としてゼロトラストとマイクロセグメンテーションの重要性が高まっていると強調しています。たとえば、APAC 地域のコンサルティング会社は、ソフトウェア定義のマイクロセグメンテーションを使用してゼロトラストのアクセス制御を実施することで、社内のアタックサーフェスを縮小し、被害が拡大する前にラテラルムーブメント（横方向の移動）の阻止に成功しました。

Reuben Koh（Akamai の APAC 地域担当 Director of Security Technology and Strategy）は「APAC のデジタル経済は、世界で最も急速に成長している分野の 1 つです。その主な理由は、イノベーションの急速な進化の速度にあります」「しかし、セキュリティチームは、頻繁に拡大するアタックサーフェスに対処することが求められており、ランサムウェア攻撃はこれらの盲点を標的にする傾向があります。組織は、セキュリティ対策を再評価し、取り組みを 2 倍に強化して、サイバーレジリエンスを高める必要があります。検証によって許可されたアクセスとマイクロセグメンテーションを中心としたゼロトラスト・アーキテクチャの導入は、アタックサーフェースを縮小し、ランサムウェア攻撃の影響を最小限に抑えるうえで適切な方法です。さらに定期的な復旧訓練やインシデント対応シミュレーションを併せることで、ランサムウェアなどの攻撃に対するサイバーレジリエンス（サイバー攻撃への対応力や回復力）を向上させる重要な要素となります」と述べています。

主なグローバルの知見

・生成 AI（GenAI）と大規模言語モデル（LLM）によって、技術的な専門知識の少ない個人がランサムウェアコードを作成し、ソーシャルエンジニアリング戦略を改善することが容易になっているため、ランサムウェア攻撃の頻度は高まり、その規模は拡大しています。
・ハイブリッドランサムウェアの活動家グループは、政治的な動機、思想的な動機、金銭的な動機から、自らの影響力を高めることを目的に RaaS プラットフォームを利用するケースが増えています。
・Akamai のリサーチチームが分析を行ったクリプトマイニング攻撃の約半数が非営利団体や教育機関を標的としており、これは、これらの業界におけるリソース不足が原因である可能性が高いと考えられます。
・TrickBot マルウェアファミリーは、世界中のランサムウェアグループによって使用され、2016 年以降、被害者から合計 7 億 2,400 万米ドルの暗号資産を強奪しました。

詳しくは、レポート全文をご覧ください。

Akamai について

Akamai は、オンラインビジネスの力となり、守るサイバーセキュリティおよびクラウドコンピューティング企業です。当社の市場をリードするセキュリティソリューション、優れた脅威インテリジェンス、グローバル運用チームによって、あらゆる場所でエンタープライズデータとアプリケーションを保護する多層防御を利用いただけます。Akamai のフルスタック・クラウド・コンピューティング・ソリューションは、世界で最も分散化されたプラットフォームで高いパフォーマンスとコストを実現しています。多くのグローバル企業が、ビジネスの成長に必要な業界最高レベルの信頼性、拡張性、専門知識を提供できる Akamai に信頼を寄せています。詳細については、akamai.com および akamai.com/blog をご覧いただくか、X や LinkedIn で Akamai Technologies をフォローしてください。