本レポートの主要な知見

アプリケーションと API に対する Web 攻撃は、2023 年第 1 四半期から 2024 年第 1 四半期にかけて 49% 急増しました。需要が一気に増加したアプリケーションと API は、セキュリティギャップを悪用し、標的の貴重なデータに対するアクセス権限を不正に得ようとしている攻撃者にとって利益の出やすい標的となります。

108B 攻撃

2023 年 1 月から 2024 年 6 月にかけて 1,080 億件の API 攻撃が記録されました。組織にとって目に見えないゲートウェイとして機能するこの重要なデジタルインターフェースに対して執拗に攻撃を受けると、データ窃取、ブランドの評判の低下、規制当局の罰金につながる可能性があり、高額な金銭的損失が発生しかねません。

データやサービスへのアクセスを API に頼っている企業にとって、API の悪用は大きな懸念事項になっており、それは、データ漏えい、不正アクセス、分散型サービス妨害（DDoS）攻撃など、さまざまな形で現われます。

コマース業界は Web アプリケーションおよび API 攻撃の被害を最も多く受けており、攻撃数は他のどの業界と比べて 2 倍以上多くなっています。

DDoS 攻撃は、レイヤー 3 および 4 とレイヤー 7 のあらゆるポートとプロトコルのトラフィックを妨害します。これには、ドメイン・ネーム・システム（DNS）も含まれます。Akamai の研究者によると、過去 18 か月のレイヤー 3 および 4 DDoS 攻撃イベントの 60% を DNS が占めていました。

11T 攻撃

Akamai の研究者によると、アプリケーションレイヤー DDoS 攻撃の上位 3 位の業界はハイテク、商業、ソーシャルメディアであり、わずか 18 か月の間に 11 兆件以上（攻撃の 75%）の攻撃が発生しました。