本レポートの主な知見

このアジア太平洋・日本（APJ）地域版スナップショットは、ランサムウェアに関する包括的な SOTI レポート「猛威を振るうランサムウェア：進化する悪用手法と執拗なゼロデイの利用」（英語版のみ）に付随するレポートです。ランサムウェアグループの攻撃の傾向、手法、技法に関する詳細な分析、攻撃の段階に関する説明、組織を保護するための各段階に応じたソリューションと推奨事項、および調査手法については、SOTI レポート本体をご参照ください。

概要

ランサムウェアは、組織に大きな損害を与え続けており、被害企業は増える一方です。攻撃者は絶えず進化し、攻撃手法を変化させ、新たな手口を導入し、拡大するアタックサーフェスを悪用し、セキュリティ予算の制約を逆手に取っている状況です。こうした危険な傾向の影響は、ランサムウェアグループが注目を集め、大きな成功を収めていることからも読み取れます。それを裏付けるように、APJ 地域では、被害を受けた企業の数が 2021 年第 4 四半期から 2022 年第 4 四半期の間に 50% 増加しています。また、2022 年第 1 四半期と 2023 年第 1 四半期を比較した場合、被害企業数は前年比 204% と大幅に増加しています。

この APJ スナップショットでは、拡大するこの懸念に対する効果的な防御方法とリスク管理のために、以下のようにさらなる知見を共有します。

- 2021 年 10 月から 2023 年 5 月の期間は、LockBit がランサムウェアシーンを席巻し、CL0P が台頭して脆弱性を積極的に悪用しました。フィッシングからゼロデイ脆弱性やワンデイ脆弱性の悪用へと攻撃手法が変化した結果、被害企業数は大幅に増加しました。
- 全世界で一致している傾向として、被害を受けた組織が最も多い業種は製造業であり、ビジネスサービス業がそれに続いています。
- ランサムウェア被害者の大半は、収益が 5,000 万米ドル以下の小規模な組織でした。ただし、最大規模の組織も攻撃を受けています。