ランサムウェアキルチェーンを断ち切る

ラテラルムーブメント（横方向の動き）を阻止する 5 つのステップ

ランサムウェアは、1 台のマシンやデバイスの侵害では終わりません。サイバー犯罪者は、このマルウェアの性質を利用して、ネットワークのできるだけ広い範囲を暗号化し、被害者に身代金を支払わせます。

2 秒ごと

2031 年までに、ランサムウェアは 2 秒に 1 回の頻度で企業、消費者、デバイスを攻撃するようになると予測されています。

Cybersecurity Ventures のランサムウェア市場レポート

既存のネットワークセキュリティに自信はありますか

レガシーファイアウォールによるセグメンテーションでは、ネットワークへのランサムウェアの拡散や、重要なアプリケーションとインフラのロックアウトを防ぐことはできません。

ランサムウェアのキルチェーン

1. **最初の足がかり**
   （スピア）フィッシングまたは脆弱性サービス
2. **ラテラルムーブメント**
   ネットワーク全体に拡散して最大のインパクトを与える
3. **流出**
   貴重なデータを検出して盗む
4. **暗号化**
   PKI での暗号化でクラッキングを防ぐ
5. **ランサムノート**
   壁紙、メール、ランサム .txt ファイルなど
6. **影響**
   データ、財務、ブランドなど

侵害は必ず発生します

横方向のデータセントラフィックで脅威を検知し、ラテラルムーブメントを阻止するセキュリティソリューションが必要です。

チェーンを断ち切る

準備する：IT 環境で実行しているすべてのアプリケーションや資産を特定します。

阻止する：一般的なランサムウェア拡散手法を阻止するルールを作成します。

検知する：セグメント化されたアプリケーションやバックアップへのアクセスを検知すると、アラートが送信されます。

修復する：攻撃を検知したとき、脅威の封じ込めと隔離対策を開始します。

回復する：可視化機能によって、段階的な回復戦略をサポートします。

2022 年には、ランサムウェア攻撃が約 13% 増加し、過去 5 年間の合計に相当する増加となりました。

Verizon 2022 Data Breach Investigations Report（データ漏えい調査レポート）

高頻度の攻撃や高額な身代金要求への対抗手段を確立していない場合は、セグメンテーションと可視化を防御戦略に組み込むチャンスです。

詳細はこちら

 | サポート | 公開日：2023 年 5 月