ランサムウェア攻撃の展開

業種：製造

攻撃者の目的

ファイルを人質にした身代金要求による利益獲得

背景

ある製造会社が、米国テキサス州ダラスの拠点で Arista NDR の価値実証試験を行いました。

このお客様が Arista NDR プラットフォームを評価している最中に、ジョージア州アトランタにある同社施設がランサムウェア攻撃を受けました。Sodinokibi ランサムウェアが実行されて 2,500 個以上のファイルが暗号化され、同社の重要なサーバー4 台が事実上シャットダウンされました。さらに、攻撃者はファイルの身代金として 75 万ドルを要求してきました。

アトランタでこの攻撃が展開されているとき、Arista NDR は正規の（ただし、侵害されたと思われる）デバイスで疑わしいアクティビティを特定しました。

Arista NDR はこの脅威を次のように検出しました。

- 認証情報の悪用、権限昇格、ネットワーク検出など、ランサムウェアの初期兆候を検出しました。
- ブラウザ以外による暗号化通信の使用などのセキュリティ対策を特定しました。
- 悪意のあるドメインがランサムウェアのダウンロードと配布に使用されていることを発見しました。

Arista NDR が選ばれる理由

Arista NDR は、ランサムウェアの脅威アクターが使用する暗号化攻撃、権限昇格、ラテラル・ムーブメントなどの TTP（戦術、技術、手順）を特定することにより、ダラスの拠点に攻撃が広がるのを防ぎました。その結果、全面的な攻撃は阻止され、被害は監視対象外のアトランタの拠点だけにとどめることができました。

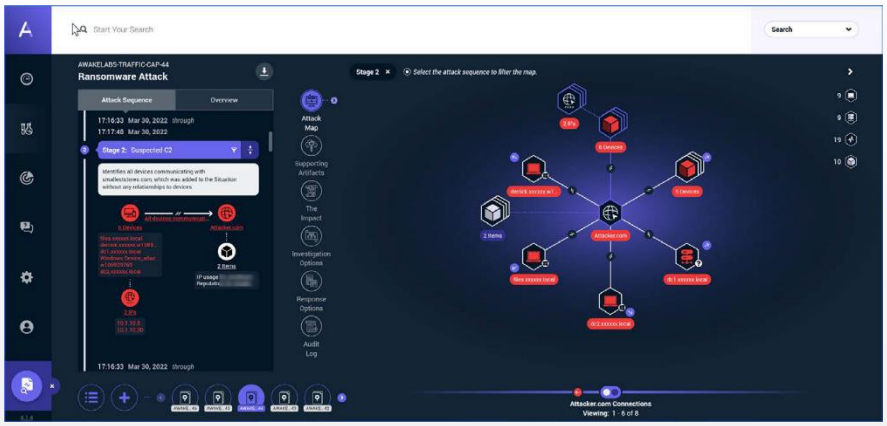

図 1：ランサムウェア拡散の試みを示す Arista NDR の「状況」ダッシュボード

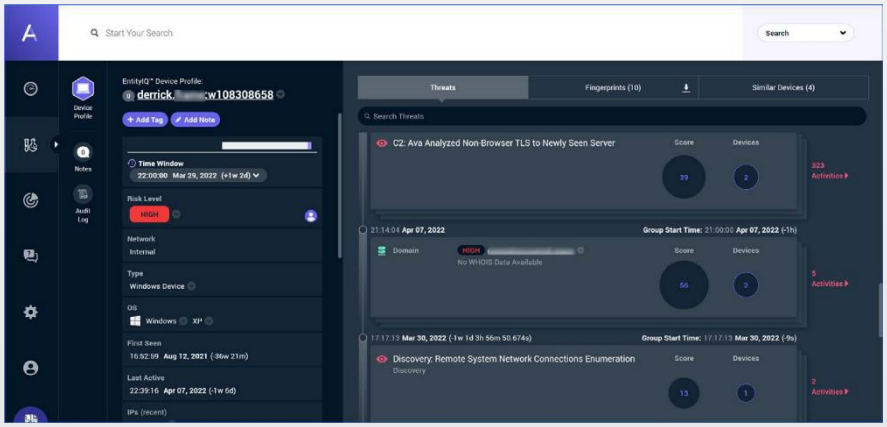

図 2：ランサムウェアがダラスの環境への拡散を試みたことを示す Arista NDR の脅威タイムライン

Arista NDR は、純粋にネットワーク・トラフィック分析のみに基づいて、攻撃者が非ブラウザベースの暗号化された通信チャネルを使用していることをセキュリティ・チームに知らせることができました。Arista NDR プラットフォームは、悪意のある Web サイトに接続しているデバイスも特定しました。これは、ランサムウェアの次のステージをダウンロードする試みだったと考えられます。最後に、Arista NDR は、アトランタにある感染したデバイスから、Arista NDR で監視中のダラスの拠点へ、ネットワーク検出トラフィックの試みがあったことを特定しました。