脅威アクタープロフィール；Akira Ransomware

[TLP：White]

※本資料は Health ISAC が発行したレポートをもとに、Health ISAC Japan で内容を再構成し、一部加筆修正を行ったものとなります。

【エグゼクティブサマリー】

Akira は、企業や医療機関のシステムを停止させ、あわせて機密情報の公開を示唆することで金銭を要求するサイバー犯罪グループです。

従来のような不特定多数を狙うメール型の攻撃から、近年は VPN やネットワーク機器の弱点を狙った、より計画的で精度の高い侵入手法へと変化しています。

医療分野では、こうした攻撃により診療業務の停止や、大量の患者情報の漏えいといった重大な影響が生じています。

【脅威アクターのステータス】

現在も継続的に活動しています。

【攻撃動機】

主な目的は金銭の獲得であり、要求額は数千万円から数億円規模に及ぶ場合があります。

【脅威アクターの性質】

組織的に活動するサイバー犯罪集団(ランサムウェア・アズ・ア・サービス)であり、金銭的利益を目的としています。

【医療分野への影響】

これまでに、世界で約 100 前後の医療関連組織が被害を受けています。
医療機関は業務の停止が患者の安全に直結するため、攻撃者にとって金銭を得やすい対象となっており、継続的に狙われています。

脅威アクタープロフィール；Akira Ransomware

【概要】

Akira は 2023 年頃に確認された比較的新しい脅威ですが、短期間で高度な攻撃を行う集団へと発展しました。
特徴的なのは、まず機密情報を取得し、その公開を示唆して圧力をかけたうえで、最終的にシステムを停止させるという手法です。これにより、被害組織は業務継続と情報保護の両面で強い対応を迫られます。

また近年では、個々の端末ではなく、院内システム全体を支える基盤（仮想化基盤など）を直接攻撃する傾向がみられます。この場合、電子カルテや検査システム、会計システムなどが同時に停止し、医療提供体制に深刻な影響を及ぼします。
さらに、ネットワークの入口となる機器の弱点を突いて侵入する手法も多く、侵入に気づきにくい点も大きな特徴です。

【活動地域】

Akira は世界的に活動していますが、特にデジタル化が進み、かつ対応コストや法的リスクの観点から身代金を支払う可能性が高い地域に攻撃が集中しています。

地域別では、

- 約 65%が南北アメリカ
- 約 25%が欧州・中東・アフリカ
- 約 8%がアジア太平洋地域
- その他が約 2%

とされています。

【攻撃パターン】

2026 年時点の Akira ランサムウェアの特徴は、侵入から被害発生までの時間が非常に短いことと、院内システム全体を支える基盤への攻撃に重点を置いている点にあります。
従来のように個々の端末を狙うのではなく、データセンターや仮想化基盤を直接攻撃することで、少ない手間で医療機関全体の機能を停止させる傾向が強まっています。主な攻撃の流れは以下のとおりです。

1. **侵入（初回アクセス）**
   - ネットワーク機器の弱点を突いて侵入する
   - 多要素認証の運用の隙を突いてログインする
   - 既に侵入済みの第三者からアクセス権を購入する
2. **潜伏と防御の回避**

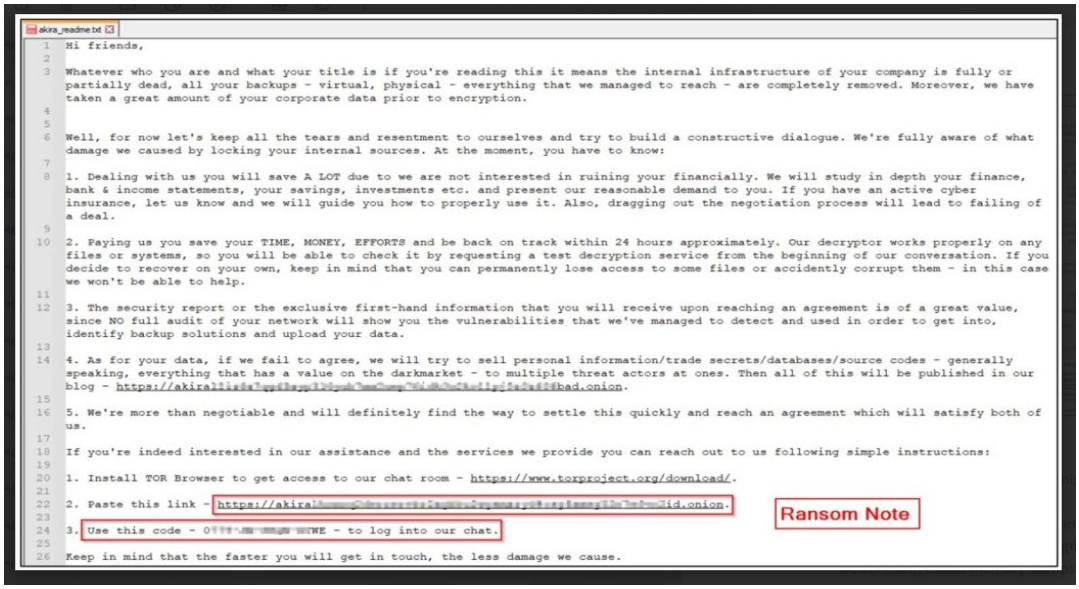
- セキュリティ対策ソフトを無効化する
- 遠隔操作ツールを使い、内部に長期間とどまる
- バックアップを削除し、復旧を困難にする
- 検知されにくい方法でデータの一部だけを暗号化する

3. **システム全体への攻撃**
   - 仮想化基盤を優先的に狙い、複数のシステムを同時に停止させる
4. **内部調査と横展開**
   - 院内ネットワークを調査し、重要なサーバーを特定する
   - 管理者権限の情報を盗み、さらに広範囲に侵入する
5. **データの窃取と暗号化**
   - 侵入から数時間以内にデータの持ち出しを開始する
   - 高速な手法でデータを暗号化し、業務を停止させる
   - 復旧を困難にするため、認証情報やバックアップ関連のデータを優先的に狙う

【暴露サイト、感染ファイル等】

- **データ暴露サイト**
  - hxxp://akiralkzxzq2dsrzsrvbr2xgbbu2wgsmxryd4csgfameg52n7efvr2id[.]onion (プライマリ)
  - hxxp://akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad[.]onion (レガシー)
  - hxxps://akira[redacted_victim_id][.]onion (交渉/チャットポータル)
- **暗号化されたファイル拡張子**:
  - 標準型 – .akira
  - Akira v2 (Megazord) – .powerranges
  - Akira v2 (Megazord) – .akiranew
  - キャッシュファイル /大容量データ – [.]arika
- **身代金要求のテキスト**:
  - akira_readme[.]txt
  - fn[.]txt

(身代金要求テキストイメージ)



【戦術、技術、手順（TTP）】

攻撃は以下の流れで一般的に行われます。

戦術	技術	手順 / 観測可能値
初回アクセス	公開アプリケーションを悪用する	CVE-2024-40766（SonicWall）および CVE-2023-20269（Cisco ASA）の悪用が積極的に行われています。
初回アクセス	有効なアカウント	初期アクセスブローカー（IAB）の認証情報を使用したり、MFA 攻撃を行ったりする。
維持	外部リモートサービス	AnyDesk、RustDesk、または Cloudflare トンネル経由のアクセスを維持する。
維持	アカウント操作	再侵入を確実にするため、ローカル/ドメイン管理者アカウント（例：backup_admin）を作成します。
特権の拡大	OS 認証情報のダンプ	Mimikatz または comsvcs[.]dll を使用して LSASS メモリをダンプし、平文パスワードを収集します。
特権の拡大	特権拡大のための搾取	CVE-2024-40711 を悪用して、Veeam バックアップサーバー上で管理者権限を取得する。
防御回避	防御を弱体化させる：ツールを無効にする	task[.]bat スクリプトを使用して、Windows Defender および EDR のリアルタイム監視を無効にします。
防御回避	ソフトウェアパッケージ	従来のシグネチャベースのアンチウイルスを

	ング	回避するために、メガゾード（ラスト）のバリアントを展開する。
発見	リモートシステム検出	Advanced IP Scanner と netscan[.]exe を使用して、臨床サブネット（PACS/EMR）をマッピングします。
発見	システム情報検出	PCHunter64 を使用して、カーネルレベルのセキュリティフックとドライバを特定します。
横方向の動き	リモートデスクトッププロトコル（RDP）	盗んだ管理者認証情報を使用して、内部 RDP セッション経由でネットワーク内を移動する。
横方向の動き	SSH	2026 年の重点テーマ：SSH を使用して VMware ESXi および Nutanix AHV ホストにアクセスし、暗号化する方法。
収集	ユーティリティ経由でアーカイブ	7-Zip または WinRAR を使用して、機密性の高い医療ファイル（PHI）を準備および圧縮します。
漏洩	クラウドストレージへのデータ流出	RClone を使用して、データを Mega[.]nz、Backblaze、または Wasabi ストレージに同期します。
インパクト	衝撃を与えるために暗号化されたデータ	.akira または .powerranges バリアントを断続的暗号化を使用して展開する。
インパクト	システム回復を阻害する	ボリュームシャドウコピーの削除と、Veeam 構成データベースのターゲット設定。

【優先的に実施すべき対策】

Akira の攻撃特徴や TTP を考慮した観点より、優先的に行うべき三つの対策例とその理由をまとめます。

1. **ネットワーク境界と認証の強化（侵入遮断）**
   - VPN やファイアウォール（SonicWall／Cisco 等）の脆弱性を迅速に修正
   - リモートアクセスに強固な MFA（可能であれば耐フィッシング型）を適用
   - 不要な外部公開サービスを停止し、アクセス元を制限

   攻撃者は「入口の機器の脆弱性」と「認証の隙」をピンポイントで突いてくるため、そこを塞ぐことで、侵入リスクを大きく低減します。

2. **仮想化基盤・重要サーバーの防御（全停止の回避）**
   - VMware ESXi や Nutanix AHV 等、仮想化基盤へのアクセス制御を強化

- SSH や管理経路の制限、管理アカウントの厳格管理
- 電子カルテ、PACS、ActiveDirectory 等、中核システムのネットワーク分離

攻撃者は「端末ではなく基盤を潰す」ことで一撃で全システムを停止させる傾向があるため、基盤の強化が不十分なまま、エンドポイント端末の対策を実施しても効果が低いといえます。

3. **バックアップの隔離と復旧能力の確保（最終防衛線）**
   - オフラインまたは改ざん不能なバックアップの確保
   - バックアップ環境と本番環境の分離
   - Active Directory を含めた全体復元手順の検証

Akira はバックアップや認証基盤（Active Directory）を優先的に破壊するため、ゼロから復旧する準備の水準が業務継続の成否をわけます。

以上