脅威アクタープロフィール；INC 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】

INC ランサムウェアは、医療分野を含む複数の業界を標的とし、金銭を目的とした攻撃を行うサイバー犯罪グループです。特別に高度な技術に依存するというよりも、一定の手順に沿った再現性の高い攻撃を特徴としています。

本グループは、まず認証情報の漏えいやアクセス制御の不備、フィッシング攻撃などを利用して侵入し、環境内での調査や権限拡大、内部移動を段階的に進めます。その後、データを暗号化する前に外部へ持ち出し、情報公開を示唆することで圧力をかける「二重恐喝」を行います。

攻撃手法としては、特殊・専用的なツールではなく、一般的に利用されている管理機能や既存ツールを組み合わせて実行されるため、通常の業務活動と区別がつきにくい点が特徴です。標準機能や普通の仕組みを悪用して静かに拡散する動きを取るため、監視体制が十分でない環境では侵入後の活動に気付きにくくなります。

【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。

【脅威アクターの性質】

国家支援のないサイバー犯罪者で、ハイブリッド型ランサムウェア・アズ・ア・サービス（RaaS）です。

【医療分野への影響】

特にセキュリティ成熟度が低い小規模な病院やクリニックを対象に、100 近くの医療機関が被害を受けています。

脅威アクタープロフィール；INC Ransomware

【概要】

INC ランサムウェアは、2023 年頃に確認された比較的新しいランサムウェアグループであり、医療分野を含む複数の業界に対して機会主義的な攻撃を展開しながら勢力を拡大してきました。初期の活動では、特定の高度な脆弱性に依存するのではなく、認証情報の漏えいや公開されたリモートサービスといった一般的な侵入手法を活用することで、着実に攻撃範囲を広げてきた点が特徴です。

2024 年に入ると、本グループは攻撃手法をさらに発展させ、データを暗号化する前に外部へ持ち出す「二重恐喝」の手法を本格的に取り入れました。この動きは、リモート接続が公開されている環境や認証管理が不十分な組織を中心に被害が拡大していることを示しており、複雑な技術を用いなくても侵入が成立する状況が背景にあります。

2025 年から 2026 年にかけて、INC はアフィリエイト型の運営モデルを取り入れ、複数の攻撃主体が並行して活動する構造へと移行しました。この体制により、医療、専門サービス、製造、公共部門など、多様な分野に対して同時に攻撃を展開することが可能となっています。

攻撃の流れとしては、フィッシングや漏えいした認証情報、VPN や RDP などの公開サービスを利用して侵入し、その後、内部の調査や権限の昇格、標準的な管理ツールを用いた横方向の移動を行うという、体系化された手順に沿って進行します。また、データの持ち出しは本グループの中核的な戦術であり、情報公開のリスクを利用して被害組織に強い圧力をかけます

このように INC は、特別に高度な技術ではなく、再現性の高い手法と組織的な運営を組み合わせることで、継続的に影響力を拡大しているランサムウェアグループであるといえます

【活動地域】

INC は、特定の地域に限定されず活動していますが、被害の多くは米国を中心に確認されており、ヨーロッパ各国でも報告されています。この分布は、地域を絞った攻撃ではなく、条件に該当する組織を広く狙うという攻撃特徴を示しています。

また、標的となる業種は、医療、専門サービス、製造業など多岐にわたり、特に中規模の組織が狙われる傾向があります。中でも医療分野は、業務停止の影響が大きく、かつ機密性の高い情報を扱うことから、継続的に主要な標的となっています。

【攻撃の特徴】

INC のランサムウェアは、高度で複雑な技術よりも、スピードと確実性を重視して設計されています。特別に作り込まれたマルウェアに依存するのではなく、既存の仕組みや一般的なツールを組み合わせることで、安定して攻撃を成功させる点が特徴です。

本グループは、PowerShell やコマンドライン、リモート管理ツールなど、通常の運用でも使われる機能を利用し、偵察や権限の拡大、内部での移動を行います。これにより、悪意のある

動きが通常のシステム操作に紛れ込みやすく、検知が遅れやすくなります。

また、攻撃に使用されるプログラム自体は比較的シンプルであり、侵入と内部展開が完了した段階で効率よく実行されるよう設計されています。そのため、準備が整った後は、短時間で環境全体に暗号化を広げることが可能です。さらに、認証情報を利用した正規アクセスを起点とすることで、従来の防御策を回避しながら活動を進める点も特徴です

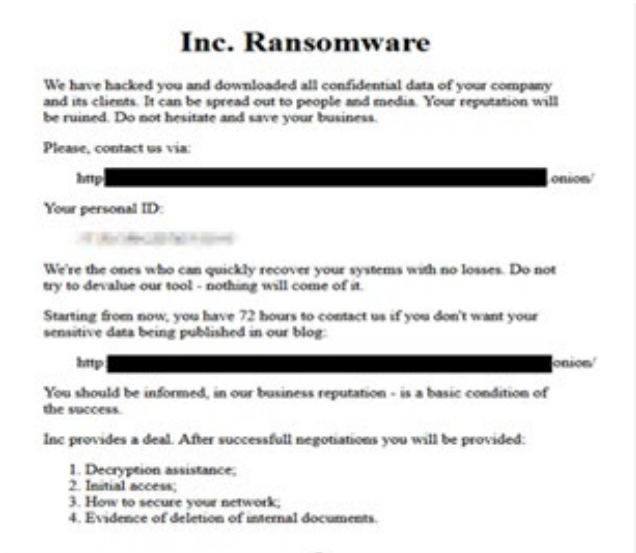
このように INC は、技術的な複雑さではなく、確立された手順を着実に実行することで、医療機関を含む幅広い環境に対して安定した攻撃を可能にしている点が大きな特徴です。

【暴露サイト、感染ファイル等】

- **データ暴露サイト**
  - hXXp[:]//incapt[.]blog
  - hXXp[:]//incapt[.]su
  - hXXp[:]//incblog7vmuq7rktic73r4ha4j757m3ptym37tyvifzp2roedyyzzxid[.]onion/blog/leaks
- **暗号化されたファイル拡張子**:
  - .INC （標準型）
  - .inc （変異型）
- **身代金要求テキスト**
  - INC-README[.]html
  - INC-README[.]txt

  等

（テキストイメージ）



Inc. Ransomware

We have hacked you and downloaded all confidential data of your company and its clients. It can be spread out to people and media. Your reputation will be ruined. Do not hesitate and save your business.

Please, contact us via:

http[redacted]onion/

Your personal ID:

[redacted]

We're the ones who can quickly recover your systems with no losses. Do not try to devalue our tool - nothing will come of it.

Starting from now, you have 72 hours to contact us if you don't want your sensitive data being published in our blog:

http[redacted]onion/

You should be informed, in our business reputation - is a basic condition of the success.

Inc provides a deal. After successfull negotiations you will be provided:

1. Decryption assistance;
2. Initial access;
3. How to secure your network;
4. Evidence of deletion of internal documents.

脅威アクタープロフィール；INC Ransomware

【攻撃特徴】

- **コアペイロードとマルウェア**
  - **暗号化**：INC ランサムウェアは、侵入後に最終段階でファイルを暗号化し、「.INC」という拡張子を付けます。処理自体は比較的単純ですが、実行速度が速く、短時間で院内の複数システムに影響を広げます。多くの場合、暗号化はデータの持ち出しが完了した後に行われるため、発動時には既に被害が発生しているケースが多いです。
  - **実行メカニズム**： 特定の専用ツールに依存するのではなく、すでに侵入時に得た権限を利用して実行されます。つまり、新たな不審プログラムを持ち込むというより、既存の環境の中で自然に動く形で展開されるため、検知されにくい状況です。
- **初期アクセスと悪用**
  - **アクセス手法**： 盗まれた ID やパスワードを使い、正規ユーザーとしてシステムにログインするケースが中心です。このため、外部からの侵入というより、内部利用に見える形で入り込まれる点が特徴となります。
  - **公開サービス**：VPN やリモート接続など、外部に公開された仕組みの設定不備や管理不足が入口になっています。特別な操作を伴わず、通常の通信として侵入されることも多いです。
- **水平展開と持続性**
  - **リモートアクセスツール**： AnyDesk などの正規の遠隔操作ツールが利用され、侵入後も継続的に内部システムを操作できる状態を維持する。
  - **管理ツール**： PowerShell や共有フォルダ機能（SMB）など、日常的に使われる Windows の標準機能を使って、院内ネットワーク内を横断的に移動します。これにより、特定の端末から全体へと影響を拡大させています。
  - **権限昇格**： 一般ユーザーの権限から管理者権限へと段階的に権限を拡大し、最終的にはシステム全体を制御できる状態を目指します。
- **防御回避**
  - **正当なツールの利用**：攻撃の多くは、既存の管理機能や標準ツールを利用して行われます。そのため、通常の運用作業と区別がつきにくく、検知が遅れやすくなります。
  - **セキュリティ機能の妨害**： 暗号化の直前に、ウイルス対策ソフトや監視機能を停止または無効化し、検知や対応を困難にします
- **認証情報へのアクセス**
  - **認証情報の窃取**： システム内部に保存されている認証情報や、メモリ上の情報を取得することで、さらに多くのアカウントへのアクセス権を獲得します。これにより、院内全体への影響範囲が拡大することになります。
- **情報流出と恐喝、バックアップ無効化**
  - **情報漏洩**： 暗号化の前に、診療情報などの重要データを外部へ持ち出します。
  - **二重恐喝**： 暗号化による業務停止に加え、「盗んだデータを公開する」と脅すことで、支払い圧力を強めます。
  - **データ転送**： 特別な手段ではなく、一般的な通信やクラウドサービスを利用して

外部へ送信されるため、通常の通信に紛れやすくなっています。

- **復旧手段の遮断**： ボリュームシャドウコピーなどの復旧機能を削除または無効化し、暗号化後に元に戻せない状態を作ります。これにより、業務再開を困難にし、身代金支払いを誘導します。

【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	有効なアカウント:ドメインアカウント	侵害された認証情報を使用してシステムにアクセスし、企業環境への認証を行う。
初回アクセス	外部リモートサービス	VPN、Citrix、および FortiGate を悪用して初期アクセスを行う。
実行	PowerShell	偵察およびペイロード配送のためのコマンドとスクリプトの実行。
実行	Windows コマンドシェル	cmd[.]exe を使用してコマンドを実行し、ランサムウェアのペイロードをデプロイします。
粘り強さ	仮装	正当なプロセス（例：ProgramData 内の svchost[.]exe）を装った悪意のあるペイロード。
特権の拡大	OS 認証情報のダンプ	侵害されたシステムから認証情報を抽出し、上位アクセス権限を取得する。
特権の拡大	ケルベロースティング	Kerberos チケット抽出を利用して、特権ドメイン認証情報を取得する。
認証情報アクセス	有効なアカウント	正当な認証情報を継続的に使用して、不正なアクセスや移動を行うこと。
横方向の動き	リモートデスクトッププロトコル	有効な認証情報を使用して RDP 経由でシステム間を移動する。
流出	C2 チャネルを介した漏出	暗号化前に HTTP/HTTPS 経由でデータが流出する。
インパクト	衝撃を与えるためにデータを暗号化	INC ランサムウェアのペイロードを使用して、システム間でファイルを暗号化する。
インパクト	システムの回復を阻害する	復旧を阻止するために、バックアップシステムを標的にして妨害する。

【優先的に実施すべき対策】

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示します。

1. **認証・セッション防御の強化（侵入遮断）**
   - VPN／RDP／Citrix 等のリモート接続に MFA を必須化
   - 未使用アカウントの無効化と強固なパスワード運用
   - 深夜・海外など不審ログインの常時監視
   - ベンダの保守接続にも同水準の認証強化を適用

   攻撃者は正規の ID を使って正面から入ってくるケースが多く、従来の侵入を防ぐ対策では十分でないため、認証を突破される前提で、正面入口の強度を一段階引き上げることが重要です。

2. **内部拡散の抑止と操作の可視化（被害拡大防止）**
   - 重要システムへの管理者権限によるアクセス制御（ジャスト・イン・タイム方式や踏み台サーバの強制）
   - PowerShell 等のコマンドラインツール、システム間の遠隔操作ツール等、運用ツールの利用ログを取得・監視
   - ベンダ作業を含めた操作履歴の記録と追跡性の確保

   攻撃者は侵入後、システムに搭載・導入される標準・正規ツールを使って組織ネットワークを横断的に移動します。そのため、システム標準の運用機能の制限とともに、該当機能を用いたシステム間の通信、ベンダの作業ログ等から通常とは異なる挙動をモニタリングすることが求められます。

3. **データ転送監視とバックアップ保全（被害最小化）**
   - HTTP/HTTPS での外部への大量データ転送の検知・遮断（DLP）
   - バックアップデータのオフライン保全

   攻撃はデータ外部転送→データ本体の暗号化→バックアップ削除といった流れで進みます。そのため、大量データの外部転送を早期検知し、バックアップの隔離保管を実施する体制を整備することで、攻撃の成功率を低下させる仕組が必要です。

このように INC の対策としては、正規の認証強度を高度化し（MFA やアカウント管理）、組織内部における普段とは異なるシステムアクティビティへの感度を高め（標準運用ツールの利用や運用管理作業等のログ監視）、外部への大量データ転送を早期に検知できるモニタリング体制の整備が重要となります。

以上