脅威アクタープロフィール；Sinobi 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】

Sinobi は、2025 年半ば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、東欧を拠点とする可能性が指摘されています。既存のグループ（Lynx）の流れを引き継ぐ形で出現し、組織的に運営されています。

本グループは、まず機密データを取得し、あわせてバックアップを削除したうえで暗号化を実行するという手法を採用しています。これにより、復旧を困難にすると同時に、情報公開を示唆して圧力をかける「二重の恐喝」を行います。

侵入経路としては、ネットワーク機器（SonicWall や Fortinet など）の弱点や、認証情報の不正利用が中心と考えられます。そのため、これらの機器の適切な管理と、不正ログインに強い多要素認証の導入が重要となります。

これまでに少なくとも 35 の医療機関が標的とされており、医療分野にとって無視できない脅威となっています。

【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。

【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】

これまでに少なくとも 35 の医療関連組織が標的とされています。

脅威アクタープロフィール；Sinobi Ransomware

【概要】

Sinobi Ransomware は、2025 年 6 月下旬に初めて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、急速に活動を拡大しています。名称は日本語の「忍」に由来するとみられますが、実際の拠点はロシアまたは東欧と考えられています。
本グループは、目立たない侵入と、データの公開を示唆する強い脅迫を組み合わせた攻撃手法を特徴としています。

Sinobi は 2025 年 6 月に出現し、既存の Lynx ランサムウェアの流れを引き継いでいると考えられています。解析の結果、機能面で高い共通性が確認されており、Lynx の再編または発展形である可能性が指摘されています。
運営形態としては、限られたメンバーで構成される閉鎖的なモデルを採用しています。一般的なランサムウェアのように広く協力者を募るのではなく、経験のある少数のメンバーによって運営されている点が特徴です。

【活動地域】

Sinobi は、一定の支払い能力を持ちながらも、セキュリティ対策に隙がある組織を主な対象としています。主なターゲットは中堅企業（年間売上高 1,000 万～5,000 万ドル規模）で、被害の約 90%以上が米国、カナダ、オーストラリア、英国が次に多いといわれます。

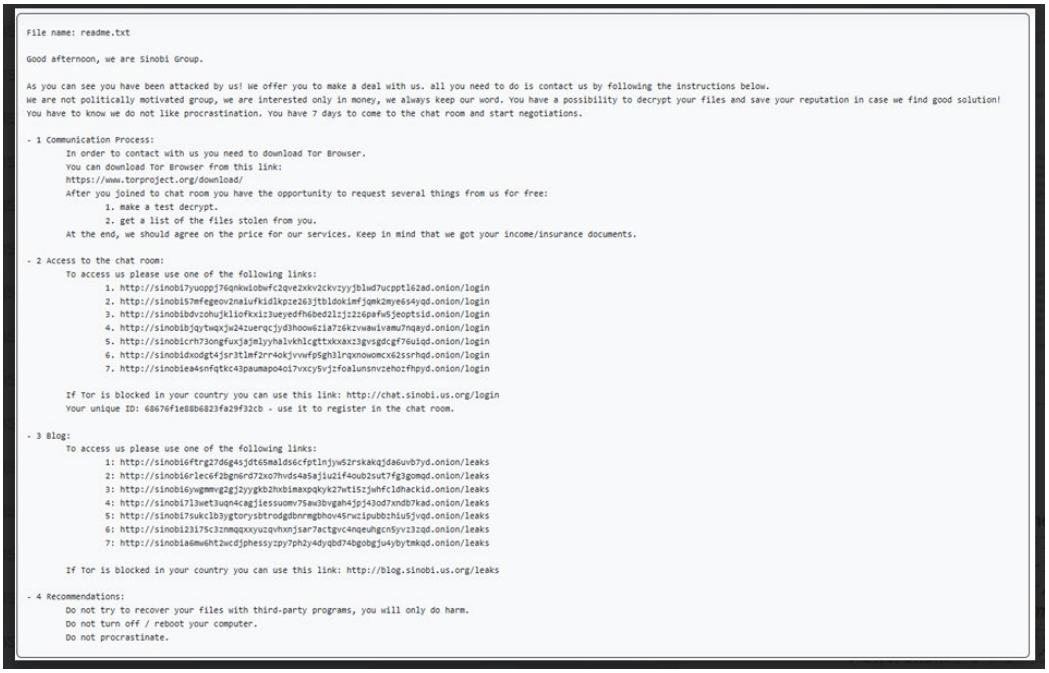
【攻撃の特徴】

Sinobi のランサムウェアは、処理の速さと確実性を重視して設計されており、一度暗号化されると、手動で元に戻すことは極めて困難です。
本グループは、鍵のやり取りに「Curve-25519」、実際のデータの暗号化に「AES-128-CTR」を組み合わせた方式を採用しています。これにより、高度な暗号化と高速な処理を両立しています。
また、プログラム内部では、Windows の標準機能（I/O 完了ポート）や複数の処理を同時に行う仕組み（マルチスレッド）を活用しています。その結果、従来のランサムウェアと比べて、短時間で大規模なサーバーやシステム全体を暗号化することが可能となっています。
このように Sinobi は、「短時間で広範囲を一気に暗号化する」能力を持つ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[://]sinobia6mw6ht2wcdjphessyzpy7ph2y4dyqbd74bgobgju4ybytmkqd[.]onion/leaks
- **暗号化されたファイル拡張子**:
  - ..SINOBI
- **身代金要求テキスト**
  - ReadMe.txt

（Readme.txt イメージ）



```
File name: readme.txt

Good afternoon, we are Sinobi Group.

As you can see you have been attacked by us! We offer you to make a deal with us. all you need to do is contact us by following the instructions below.
We are not politically motivated group, we are interested only in money, we always keep our word. You have a possibility to decrypt your files and save your reputation in case we find good solution!
You have to know we do not like procrastination. You have 7 days to come to the chat room and start negotiations.

- 1 Communication Process:
        In order to contact with us you need to download Tor Browser.
        You can download Tor Browser from this link:
        https://www.torproject.org/download/
        After you joined to chat room you have the opportunity to request several things from us for free:
                1. make a test decrypt.
                2. get a list of the files stolen from you.
        At the end, we should agree on the price for our services. Keep in mind that we got your income/insurance documents.

- 2 Access to the chat room:
        To access us please use one of the following links:
                1. http://sinobi7yuoppj76qnkwiobwfc2qve2xkv2ckvzyyjblwd7ucpptl62ad.onion/login
                2. http://sinobi57mfegeov2naiufkidlkpze263jtbldokimfjqmk2mye6s4yqd.onion/login
                3. http://sinobibdvzohujkliofkxii3ueyedfh6bed2lzjz2z6pafw5jeoptsid.onion/login
                4. http://sinobibjqytwqxjw24zuerqcjyd3hoow6zia7z6kzvwawivamu7nqayd.onion/login
                5. http://sinobicrh73ongfuxjajmlyyhalvkhlcgttxkxaxz3gvsgdcgf76uiqd.onion/login
                6. http://sinobidxodgt4jsr3tlmf2rr4okjvvwfp5gh3lrqxnowomcx62ssrhqd.onion/login
                7. http://sinobiea4snfqtkc43paumapo4oi7vxcy5vjzfoalunsnvzehozfhpyd.onion/login

        If Tor is blocked in your country you can use this link: http://chat.sinobi.us.org/login
        Your unique ID: 68676f1e88b6823fa29f32cb - use it to register in the chat room.

- 3 Blog:
        To access us please use one of the following links:
                1: http://sinobi6ftrg27d6g4sjdt65maldsécfptlnjyw52rskakqjda6uvb7yd.onion/leaks
                2: http://sinobi6rlec6f2bgn6rd72xo7hvds4a5ajiu2if4oub2sut7fg3gomqd.onion/leaks
                3: http://sinobi6ywgmmvg2gj2yygkb2hxbimaxpqkyk27wti5zjwhfcldhackid.onion/leaks
                4: http://sinobi7l3wet3uqn4cagjiessuomv75aw3bvgah6jpj43od7xndb7kad.onion/leaks
                5: http://sinobi7sukc1b3ygtorysbtrodgdbnrmgbhov45rwz1pubbzhiu5jvqd.onion/leaks
                6: http://sinobi23i75c3inmqqxxyuzqvhxnjsar7actgvc4nqeuhgcn5yvz3zqd.onion/leaks
                7: http://sinobia6mw6ht2wcdjphessyzpy7ph2y4dyqbd74bgobgju4ybytmkqd.onion/leaks

        If Tor is blocked in your country you can use this link: http://blog.sinobi.us.org/leaks

- 4 Recommendations:
        Do not try to recover your files with third-party programs, you will only do harm.
        Do not turn off / reboot your computer.
        Do not procrastinate.
```

【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-2024-53704（SonicWall SSL VPN）の悪用と、パッチ未適用の Fortinet/Citrix アプライアンスの悪用が活発に行われています。
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）から認証情報を購入し、過剰な権限を持つ MSP アカウントを利用する。
実行	PowerShell	環境検出およびセキュリティ機能無効化のためのスクリプトの実行。
実行	Windows コマンドシェル	ユーザーの作成およびサービスの終了を行うための、キーボード操作による手動コマンド。
粘り強さ	アカウント作成：ローカルアカウント	アクセスを維持するために、新しいローカル管理者アカウント（例：backup_admin）を作成します。
粘り強さ	Windows サービス	ランサムウェアのペイロードが再起動後も存続するように、システムサービスを変更または作成します。

特権の拡大	ユーザーアカウント制御をバイパスする	ロッカーバイナリのプロセス整合性を高めるために、UAC バイパス技術を使用します。
特権の拡大	ドメインアカウント	侵害された認証情報を使用して、新しく作成されたローカルアカウントをドメイン管理者グループに昇格させる。
防御回避	防御を弱体化させる：ツールを無効化または変更する	EDR エージェント（Carbon Black、SentinelOne）を積極的に終了させ、ボリュームシャドウコピーを妨害します。
防御回避	インジケーターの削除：ファイルの削除	Windows イベントログ（wevtutil）をクリアし、データ漏洩後にステージングディレクトリを削除します。
認証情報アクセス	OS 認証情報のダンプ：LSASS メモリ	ProcDump や Mimikatz などのツールを使用して、平文のパスワードや NTLM ハッシュを収集します。
発見	ファイルとディレクトリの検出	ネットワーク共有および高価値データ（財務情報、人事情報、バックアップデータなど）の自動列挙。
発見	リモートシステム検出	Active Directory ドメインコントローラーおよびバックアップサーバー（Veeam、Commvault）のスキャンを実行します。
水平移動	リモートデスクトッププロトコル	正当な管理者権限を持つ RDP を使用してネットワーク内を移動する。
水平移動	SMB/Windows 管理者共有	ランサムウェアのペイロードを管理共有（C$）を介してワークステーションに配布します。
収集	データステージング：ローカルデータステージング	盗んだファイルを.zip または.7z アーカイブに圧縮し、隠しフォルダ（例：C:¥ProgramData）に保存します。
漏洩	クラウドストレージへのデータ流出	RClone を利用して、ステージングされたデータを攻撃者が管理する Mega.nz または Amazon S3 バケットに同期します。
インパクト	暗号化されたデータ	AES-128-CTR を使用してファイルを暗号化し、拡張子を.SINOBI に追加します。
インパクト	システム回復を阻害する	maxdiffarea のサイズを 0 に変更することで、ボリュームシャドウコピーを削除します。

【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）**
   - フィッシング耐性のある MFA（FIDO2 等）を強制適用
   - MFA 疲労攻撃やセッションハイジャック対策の実装
   - 管理者権限を必要時のみ付与する設定を適用
   - レガシープロトコル（古い認証方式）の無効化

   攻撃者は盗まれた認証情報をもとにセッションを乗っ取って侵入するケースが多いため、通常の MFA では突破される前提で、防御レベルを一段引き上げる必要があります。

2. **外部公開機器と侵入口の管理（初期アクセス遮断）**
   - Fortinet、Ivanti EPMM、BeyondTrust 等、外部公開機器に優先的にパッチ適用
   - インターネット公開資産の棚卸しと不要サービスの停止
   - 外部接続経路の最小化とアクセス制限

   攻撃者は自ら侵入するだけでなく、侵入済みアクセスの情報を外部から調達するため、入口が一つでも開いていると、そこから侵入される構造になっています。

3. **バックアップ隔離とデータ流出の監視（被害最小化）**
   - オフラインまたは改ざん不能なバックアップの確保
   - バックアップと本番環境の分離
   - Mega.nz や Rclone 等への大量データ転送の監視

   「バックアップ削除→データ窃取→暗号化」の順で攻撃が進むため、復旧手段の確保とデータ流出対策を両方とも実施する必要があります。

このように SINOBI の対策においては、認証を破らせず（高度な MFA＋セッション防御）、入り口を残さない（外部機器・公開資産管理）状態とし、仮にデータを取られても戻せる・気づける（バックアップ＋流出監視）体制の整備が重要です。

以上