脅威アクタープロフィール；Interlock Ransomware

[TLP：White]

※本資料は Health ISAC が 2026 年 8 月に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】

Interlock Ransomware は、2024 年後半に出現した、金銭目的の機会主義的な脅威アクターです。Ransomware-as-a-Service（RaaS）モデルではなく、閉鎖的なグループとして活動する Interlock は、機密データを抜き取りシステムを暗号化した後、身代金が支払われなければ盗んだデータを Tor ベースの Worldwide Secrets Blog にリークすると標的/被害者に脅迫するという二重の恐喝戦略を採用しています。

＜Interlock のロゴ＞

【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】

日和見主義的／人間が操作するランサムウェアグルー。

【医療分野への影響】

2025 年から 2026 年（現在まで）にかけて、さまざまな分野で Interlock ランサムウェアは攻撃を行っています。教育分野が攻撃件数で上位を占めていますが、医療分野もランサムウェア攻撃の標的となる上位 4 分野に入っています。

脅威アクタープロフィール；Interlock Ransomware

【概要】

Interlock Ransomware は、2024 年 9 月に金銭目的の攻撃者として出現して以降、短期間で攻撃手法と運用能力を高度化させ、成熟した二重恐喝型ランサムウェアグループへと発展しました。

当初は「Chaya_002」と呼ばれ、TDS（トラフィック配信システム）を利用してニュースサイトや中小企業、コミュニティサイトなどから悪意ある JavaScript を配信。Chrome や Teams の偽アップデート、偽エラー画面を表示させ、PowerShell バックドアを通じて認証情報を窃取するなど、比較的限定的・機会主義的な活動が中心でした。

2024 年 10 月には「Interlock」の名称が確認され、組織的なランサムウェア攻撃の実態が明確化され、さらに 2025 年 2 月には FortiClient VPN や Cisco AnyConnect などのリモート接続ソフトウェアを装う手法が拡大的に利用されるようになっています。出現からわずか 1 年ほどで、単純な情報窃取型 RAT を用いる攻撃者から、継続的にツールや標的を改善する重大なランサムウェア脅威へと変貌しています_

【活動地域】

Interlock は機会主義的な脅威アクターであり、特定のセクターに焦点を当てるのではなく、脆弱性やアクセス状況に基づいて組織を標的にします。主に北米やヨーロッパを中心に、地方自治体から大手医療機関、重要インフラ企業まで、幅広い組織に攻撃を行っています。

【攻撃の特徴】

Interlock の攻撃は、ソーシャルエンジニアリングによって端末への初期侵入を実現した後、OS 標準機能や正規のリモート管理ツールを悪用して検知を回避しながら、内部探索、認証情報窃取、横展開、データ窃取、暗号化へと進む点に特徴があります。独自開発したマルウェアだけに依存せず、一般的な管理ツールを組み合わせることで、通常の管理操作に紛れて攻撃を継続しています。

初期侵入では、侵害したニュースサイトや小売サイトなどの正規 Web サイトを利用し、Google Chrome、Microsoft Edge、FortiClient、Cisco AnyConnect などのソフトウェアアップデートを装った偽ファイルを配布します。また、ClickFix と呼ばれるソーシャルエンジニアリングも多用しています。これは CAPTCHA やシステム警告を偽装し、利用者自身に Windows の「ファイル名を指定して実行」を開かせ、Base64 などで難読化された PowerShell スクリプトを実行させる手法です。マルウェアそのものを直接実行させるのではなく、正規の Windows 機能を利用者に操作させることで、従来型のセキュリティ対策をすり抜けることを狙っています。

侵入後は、Interlock RAT、NodeSnake、PowerShell バックドアなどを展開して遠隔操作環境を構築します。さらに、ショートカットファイル（.lnk）や実行ファイルを Windows のスタートアップフォルダへ配置したり、「Chrome Updater」など正規ソフトを装った名称でレジストリの Run キ

ーを変更したりすることで、端末の再起動やユーザーログイン後も攻撃基盤を維持しています。

内部探索では、systeminfo、Get-PSDrive、tasklist /svc、Get-Service などの Windows 標準コマンドを使用し、端末情報、論理ドライブ、稼働中のサービスなどを調査します。これによりネットワーク環境だけでなく、EDR やアンチウイルスなどのセキュリティ製品の存在も把握しています。その後、Lumma や Berserk などの情報窃取マルウェア、キーロガー、独自の NTLM 認証情報収集 DLL などを投入し、Web ブラウザに保存された ID・パスワードやユーザー入力などを窃取していきます。加えて Kerberoasting によって Kerberos サービスチケットを取得・解析し、より高い権限を持つアカウントへのアクセスも試みる場合もあります。

水平展開では、窃取した認証情報を利用した RDP 接続に加え、AnyDesk、PuTTY、ConnectWise ScreenConnect など、本来はシステム管理に使用される正規ツールを悪用します。C2 通信には Cobalt Strike や SystemBC、Cloudflare Tunnel のほか、Interlock RAT や NodeSnake といった独自ツールを組み合わせる傾向が強いです。こうした正規サービス・ツールの利用は、攻撃通信を通常の管理通信に紛れ込ませ、検知を困難にする効果を持っています。

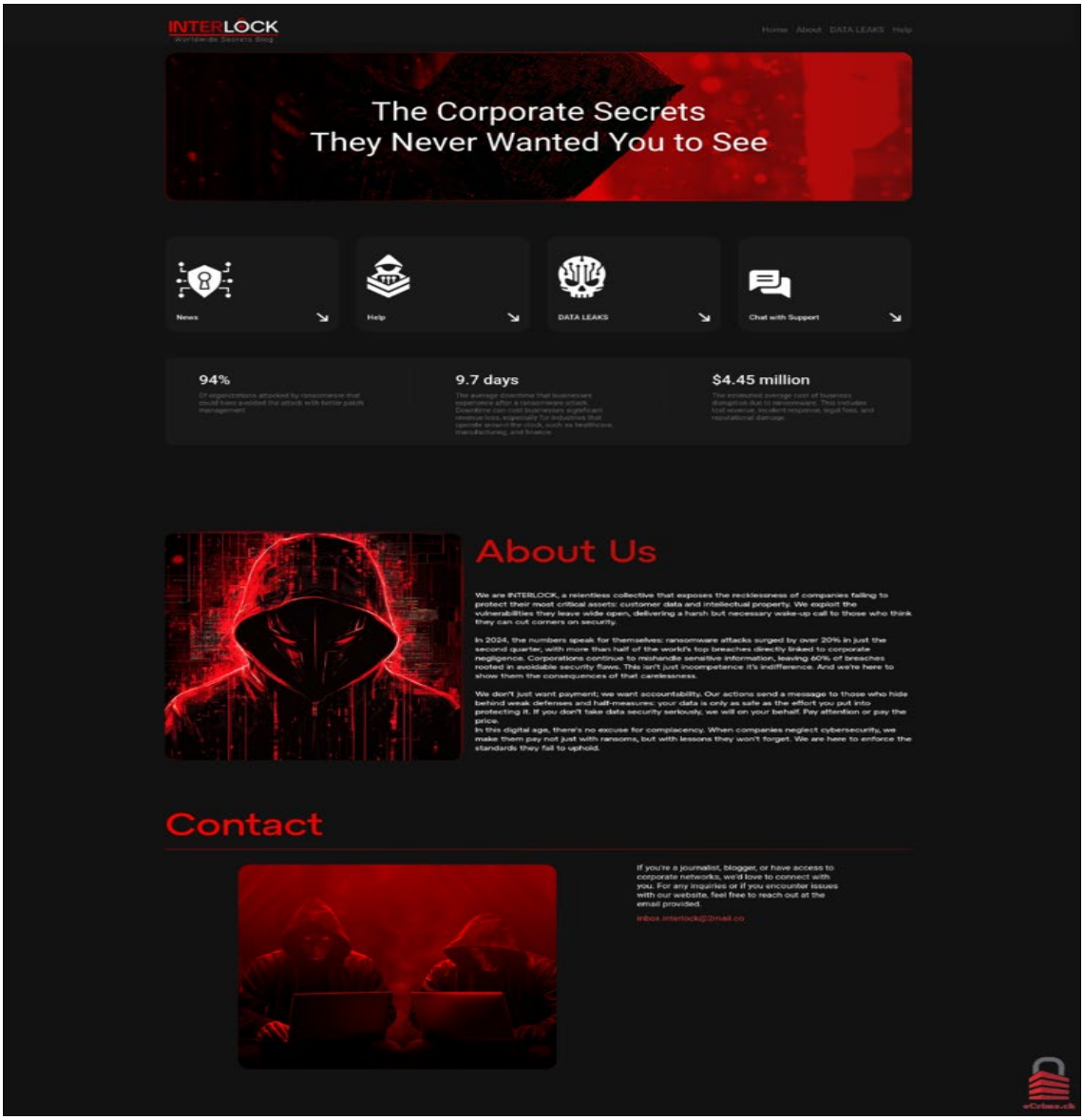
最終段階では、機密情報を暗号化前に外部へ持ち出し、データ公開を材料とした恐喝を行ったうえで、Windows および Linux 環境向けのランサムウェアを展開します。特に仮想化基盤上の VM を重点的に暗号化することで、多数の業務システムを一度に停止させ、事業継続へ大きな影響を与えています。

【暴露サイト、感染ファイル等】

- **関連サイト**
  - 主要データ漏洩サイト（別名：ワールドワイドシークレットブログ） –
    hxxp://ebhmkoohccl45qesdbvrjqtyro2hmhkmh6vkyfyjjzfllm3ix72aqaid[.]onion
  - サポート／交渉ポータル–
    hxxp://ebhmkoohccl45qesdbvrjqtyro2hmhkmh6vkyfyjjzfllm3ix72aqaid[.]onion/support/step[.]php

脅威アクタープロフィール；Interlock Ransomware

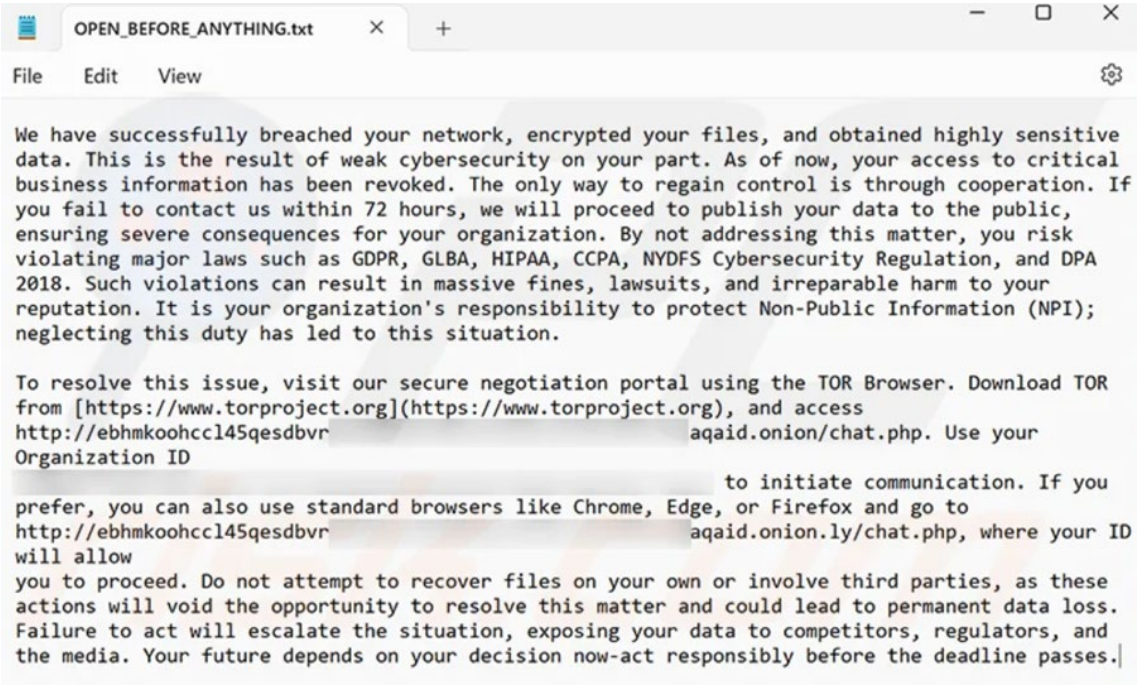
＜データ漏洩サイト － 概要、会社概要、連絡先情報＞



- **暗号化されたファイル拡張子例**
  - .interlock
  - .1nt3rlock

- **身代金要求テキスト例**
  - !_README_!.txt
  - !!!OPEN_ME!!!.txt
  - OPEN_BEFORE_ANYTHING.txt

＜身代金要求メモ例＞


OPEN_BEFORE_ANYTHING.txt

File Edit View

We have successfully breached your network, encrypted your files, and obtained highly sensitive data. This is the result of weak cybersecurity on your part. As of now, your access to critical business information has been revoked. The only way to regain control is through cooperation. If you fail to contact us within 72 hours, we will proceed to publish your data to the public, ensuring severe consequences for your organization. By not addressing this matter, you risk violating major laws such as GDPR, GLBA, HIPAA, CCPA, NYDFS Cybersecurity Regulation, and DPA 2018. Such violations can result in massive fines, lawsuits, and irreparable harm to your reputation. It is your organization's responsibility to protect Non-Public Information (NPI); neglecting this duty has led to this situation.

To resolve this issue, visit our secure negotiation portal using the TOR Browser. Download TOR from https://www.torproject.org, and access http://ebhmkoohccl45qesdbvr aqaid.onion/chat.php. Use your Organization ID to initiate communication. If you prefer, you can also use standard browsers like Chrome, Edge, or Firefox and go to http://ebhmkoohccl45qesdbvr aqaid.onion.ly/chat.php, where your ID will allow you to proceed. Do not attempt to recover files on your own or involve third parties, as these actions will void the opportunity to resolve this matter and could lead to permanent data loss. Failure to act will escalate the situation, exposing your data to competitors, regulators, and the media. Your future depends on your decision now-act responsibly before the deadline passes.

【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	ID	技術	手順 / 観測可能値
初期アクセス	T1189	ドライブバイ侵害（Drive-by Compromise）	ClickFix を利用し、偽 CAPTCHA や警告画面を表示して、被害者自身に悪意あるコマンドをコピーさせ、Windows の「ファイル名を指定して実行」などへ貼り付けて実行させる。
初期アクセス	T1204.004	ユーザーによる実行：悪意のあるコピー＆ペースト（User Execution: Malicious Copy and Paste）	侵害した正規 Web サイトなどを経由して、Chrome、FortiClient、Cisco AnyConnect、Sophos 等のアップデートを装った悪意あるペイロードを配布し、端末への初期侵入を図る。
実行	T1059.001	コマンド／スクリプトインタープリタ：PowerShell（Command and Scripting Interpreter: PowerShell）	PowerShell を利用して Interlock RAT 等のバックドアや後続ペイロードをダウンロード・実行するほか、システム探索や永続化に必要な処理を実行する。
実行	T1218.011	システムバイナリプロキシ実行：Rundll32（System Binary Proxy Execution: Rundll32）	Windows 標準の rundll32.exe を利用して klg.dll や autoservice.dll などの悪意ある DLL を実行し、正規バイナリ経由でコードを実行することで検知回避を図る。
永続化	T1547.001	ブート／ログオン自動起動実行：レジストリ Run キー／スタートアップフォル	悪意ある.lnk ファイルを Windows のスタートアップフォルダへ配置したり、Chrome Updater 等を装ったレジストリ Run キーを作

戦術	ID	技術	手順 / 観測可能値
		ダ（Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder）	成したりして、ログオン時の自動実行を確保する。
権限昇格	T1558.003	Kerberos チケットの窃取または偽造：Kerberoasting（Steal or Forge Kerberos Tickets: Kerberoasting）	Kerberos サービスチケット（TGS）を取得し、その暗号化部分に対してオフラインでパスワード解析を行うことで、サービスアカウントの認証情報取得を狙う。
防御回避	T1036.005	偽装：正規の名前または場所との一致（Masquerading: Match Legitimate Resource Name or Location）	悪意あるファイルに conhost.exe、conhost.dll など正規 Windows コンポーネントに類似した名称を付与し、正規ファイルに見せかけて発見・分析を困難にする。
防御回避	T1070.004	痕跡の削除：ファイル削除（Indicator Removal: File Deletion）	remove()関数や OS 標準コマンドなどを利用して、攻撃に使用したランサムウェア等のファイルを削除し、フォレンジック上の痕跡を減少させる。
認証情報アクセス	T1555.003	パスワードストアからの認証情報：Web ブラウザからの認証情報（Credentials from Password Stores: Credentials from Web Browsers）	Lumma Stealer や Berserk Stealer、カスタムツール等を利用し、ブラウザに保存された認証情報やセッショントークンなどを窃取する。
認証情報アクセス	T1056.001	入力キャプチャ：キーロギング（Input Capture: Keylogging）	klg.dll などのキーロガーを展開してキーストロークを記録し、ユーザーが入力した認証情報等の機密情報を取得する。
探索	T1082	システム情報の探索（System Information Discovery）	systeminfo などを使用して OS、ホスト等のシステム情報を収集し、侵害環境を把握する。
探索	T1007	システムサービスの探索（System Service Discovery）	tasklist /svc や Get-Service 等によって稼働中のサービスを列挙し、EDR、アンチウイルス、監視製品などを特定する。
探索	T1016	システムネットワーク構成の探索（System Network Configuration Discovery）	arp -a 等を使用して ARP キャッシュやネットワーク情報を取得し、内部ネットワークの構成や接続先を把握して後続の横展開に利用する。
横展開	T1021.001	リモートサービス：リモートデスクトッププロトコル（RDP）（Remote Services: Remote Desktop Protocol）	窃取した有効な認証情報を使用して内部ホストへ RDP 接続し、侵害範囲を他のシステムへ拡大する。
横展開	T1219	リモートアクセスソフトウェア（Remote Access Software）	AnyDesk、ConnectWise ScreenConnect などの正規リモートアクセスソフトウェアを悪用し、侵害端末への遠隔操作経路を確保・維持する。

戦術	ID	技術	手順 / 観測可能値
C2（コマンド＆コントロール）	T1105	侵入ツール転送（Ingress Tool Transfer）	PowerShell 等を利用して Cobalt Strike、SystemBC、Interlock RAT、NodeSnake など、後続の攻撃ツールやペイロードを侵害環境へダウンロードする。
C2（コマンド＆コントロール）	T1090	プロキシ（Proxy）	SystemBC による SOCKS5 プロキシや Cloudflare Tunnel などを利用し、攻撃者と侵害環境間の C2 通信を中継・隠蔽する。
情報窃取	T1530	クラウドストレージからのデータ（Data from Cloud Storage）	Azure Storage Explorer 等を使用してアクセス可能なクラウドストレージを探索・閲覧し、そこに保存された機密データを収集する。
情報窃取	T1048	代替プロトコルを介したデータ窃取（Exfiltration Over Alternative Protocol）	WinSCP 等のファイル転送ツールを利用し、C2 とは異なる通信経路・プロトコルを介して、収集したデータを攻撃者管理下のインフラへ転送する。
インパクト	T1486	データ暗号化による影響（Data Encrypted for Impact）	Windows、Linux、FreeBSD 等を対象とする暗号化ツールを展開し、AES と RSA 等を組み合わせてファイルを暗号化する。.interlock や.1nt3rlock 等の拡張子を付加し、身代金要求メモを配置してシステム・データを利用不能にする。

【国内医療機関が優先的に実施すべき対策】

国内医療機関における医療情報システム・ネットワーク環境管理の特性を踏まえ、特に優先すべき三つの対策例とその理由を示します。

1. **情報系ネットワークにおける ClickFix・偽アップデート攻撃の防止（初期侵入対策）**
   - 「CAPTCHA 解除」「エラー修復」等を理由に、Windows の「ファイル名を指定して実行」や PowerShell へのコマンド貼付けを要求された場合は実行しないよう職員教育を実施
   - Chrome、Edge、FortiClient、Cisco AnyConnect 等のアップデートは、院内 IT 部門や保守ベンダーが管理する正規経路以外から実行しない運用を徹底
   - Web／DNS フィルタリングにより、侵害サイトや不審なダウンロード先への接続を遮断
   - PowerShell の Script Block Logging 等を有効化し、難読化スクリプトや外部からのダウンロード・実行を監視
   - 情報系端末への EDR 導入と、PowerShell、Rundll32 等の制限・利用監視

Interlock は、侵害した正規 Web サイトや偽の Chrome、FortiClient 等のアップデート、ClickFix を利用し、利用者自身に Windows 標準機能から PowerShell を実行させて初期侵入します。 国内医療機関では、電子カルテや医療機器等を収容する診療系ネットワークと、メールや Web 閲覧を行う情報系ネットワークが分離されていることが一般的です。そのため、

Interlock の初期侵入はまず情報系端末で発生する可能性が高く、情報系ネットワークで侵害を止め、診療系へ波及させないことが第一の防衛線となります。

2. 情報系ネットワークと診療系ネットワークをつなぐ例外経路の統制（横展開対策）

- 診療系ネットワークへの保守用 VPN、リモートメンテナンス装置、ジャンプサーバー等の接続経路を棚卸し
- ベンダー保守用 VPN に MFA を適用し、共用アカウントを廃止して担当者単位の ID 管理を実施
- 保守接続を常時開放せず、必要時のみ接続可能とし、接続時間・接続元・接続先を限定
- 情報系ネットワークから診療系ネットワークへの RDP、SMB、管理共有等の不要な通信（ポート）を遮断
- AnyDesk、ConnectWise ScreenConnect、PuTTY 等のリモート管理ツールを許可制とし、未承認利用を検知・遮断

Interlock は、侵入後にブラウザ保存パスワードやキーロギング、Kerberoasting 等で認証情報を窃取し、RDP や AnyDesk、ScreenConnect 等の正規リモート管理ツールを悪用して横展開します。 国内医療機関では診療系ネットワークが外部インターネットから原則分離されている一方、電子カルテや医療機器を 24 時間 365 日保守するため、外部ベンダー用 VPN 等の「例外的な通用口」が設けられています。こうした外部接続点は診療継続に必要である一方、過去の国内医療機関の被害でも重要な侵入起点となっています。 そのため、ネットワーク分離そのものよりも、分離をまたぐ例外経路を厳格に管理することが重要です。

3. 診療系ネットワーク内の横展開防止と仮想化基盤の保護（診療停止対策）

- ESXi、Hyper-V 等の仮想化基盤の管理ネットワークを、一般の診療系ネットワークからさらに VLAN 等で分離
- ハイパーバイザー管理者アカウントと AD 管理者等の認証情報を分離し、MFA を適用
- 電子カルテ、検査、画像、部門システム、医療機器間の不要な RDP、SMB、管理通信（ポート）を制限
- 管理者による操作は専用管理端末からのみ実施し、一般端末からの管理アクセスを禁止
- オフラインまたはイミュータブルバックアップを保持し、電子カルテ停止を想定したリストア試験・IT-BCP 訓練を実施

Interlock は最終段階で Windows や Linux だけでなく、仮想化基盤上の VM を重点的に暗号化し、多数の業務システムを一括停止させることを特徴としています。 国内医療機関では、電子カルテ、検査、画像、部門システム等が診療系ネットワーク内の仮想化基盤へ集約されている場合があり、一度管理基盤まで侵害されると複数の診療機能が同時に停止するおそれがあります。そのため、診療系ネットワークに侵入された場合でも横展開を局所化し、仮想化基盤まで到達させないこと、さらに暗号化されても診療を復旧できることが重要です。

以上