脅威アクタープロフィール；BianLian

[TLP：White]

※本資料は Health ISAC が 2026 年 7 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】

BianLian は、このグループは 2022 年頃に出現し、複数の分野にわたる重要インフラや組織に影響を与える攻撃に関与してきた。2026 年現在も、BianLian はランサムウェア攻撃やデータ恐喝活動を行う活発なサイバー犯罪グループとして活動を続けています。

【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】

金銭的利益を追求するサイバー犯罪者で、ランサムウェアとデータ恐喝を中心とした活動を行います。

【医療分野への影響】

BianLian ランサムウェアの活動は、87 か国にわたる約 1,473 件の医療関連事件と関連付けられており、そのうち 375 件は過去 12 か月間に記録されたもので、医療関連組織に対する世界的な圧力が継続していることを示しています。

脅威アクタープロフィール；BianLian

【概要】

BianLian は、侵入後の情報収集、権限昇格、横展開、データ窃取を重視する脅威アクターであり、近年は暗号化よりも窃取データを利用した恐喝を主軸とする傾向が強いです。

初期侵入では、スピアフィッシング、盗まれた認証情報、公開 RDP、インターネット接続システムの脆弱性悪用などが用いられます。
侵入後は、正規の管理ツール、コマンドライン、スクリプト、リモート管理機能を悪用し、通常業務に紛れながらドメインコントローラー、バックアップ、ファイル共有、機密データ保管場所へ到達します。

特に医療分野では、患者情報や業務継続への影響を材料に、リークサイトでの公開示唆や被害組織への直接連絡を通じて、法的・財務的・評判上の圧力をかける点が特徴です。

【活動地域】

BianLian の活動は主に北米、特に米国の組織に影響を与えており、ヨーロッパ、インド、オーストラリア、その他の地域でも被害が確認されています。このグループは、米国の複数の重要インフラ部門の組織や、オーストラリアの民間企業に影響を与えています。

【攻撃の特徴】

BianLian は、ステルス性、認証情報アクセス、横方向移動、データ窃取、恐喝を重視する人間操作型の脅威アクターです。初期には、窃取データと暗号化を組み合わせた二重恐喝を行い、暗号化されたファイルに「.bianlian」拡張子を付与する暗号化ツールも使用していました。しかし近年は、暗号化よりもデータ流出を利用した恐喝を主軸とする傾向が強まっています。

初期アクセスでは、有効な RDP 認証情報、フィッシングで窃取したアカウント、公開リモートサービス、インターネット接続された Windows や ESXi 環境、公開アプリケーションの脆弱性を悪用します。ProxyShell チェーンに含まれる CVE-2021-34473、CVE-2021-34523、CVE-2021-31207 の悪用にも関連付けられており、外部公開システムは高リスクな侵入口となります。

侵入後は、PowerShell、Windows コマンドシェル、Advanced Port Scanner、SoftPerfect Network Scanner、SharpShares、PingCastle などを用いて、ドメインコントローラー、Active Directory の関係、ドメイン信頼関係、ユーザーアカウント、ネットワーク共有、バックアップ基盤、機密ファイルの所在を探索します。

さらに、Go 言語ベースのカスタムバックドアを展開し、コマンド実行、ペイロード配信、継続的アクセスを可能にします。また、TeamViewer、Atera Agent、SplashTop、AnyDesk などの正規リモートアクセスツール、Ngrok や Rsocks などのプロキシツール、Exchange サーバーへの

Web Shell 設置、ローカル管理者・ドメイン管理者・クラウドアカウントの作成や有効化、スケジュールされたタスクの作成により、環境内での制御を維持します。

権限昇格と認証情報アクセスでは、LSASS メモリのダンプ、NTDS.dit へのアクセス試行、保護されていない認証情報の探索、SessionGopher によるリモートアクセスツールの保存セッション情報抽出などを行います。CVE-2022-37969 を悪用した権限昇格も確認されています。
横方向移動では、有効アカウント、RDP、PsExec、SMB、Windows 管理共有、ネイティブの管理ツールを利用し、ドメインコントローラー、ファイルサーバー、クラウド接続システム、機密リポジトリへアクセスを拡大します。

防御回避では、PowerShell やコマンドシェルを悪用して Windows Defender、AMSI、Sophos 関連の保護機能を無効化・変更し、レジストリ設定や Windows ファイアウォールルールを操作して RDP アクセスを許可します。また、バイナリやスケジュールタスク名を正規の Windows サービスやセキュリティツールに似せるほか、UPX 圧縮された実行ファイルを使い、解析やシグネチャベース検知を困難にします。

最終段階では、PowerShell スクリプト、WinRAR、Rclone、WinSCP、FTP、Mega などを用いて、業務、法務、財務、技術、個人情報を収集・圧縮・外部送信します。さらに、vssadmin.exe によるシャドウコピー削除やバックアップ基盤の標的化により復旧能力を低下させます。
その後、リークサイトへの掲載、被害者への直接連絡、プリンターでの身代金要求メッセージ出力、脅迫電話などを通じて、組織に強い支払い圧力をかける点が特徴です。

【暴露サイト、感染ファイル等】

- **データ暴露サイト**
  - hxxp:// bianlianlbc5an4kgnay3opdemgcry g2kpfcbgczopmm3dnbz3uaunad[.] onion/
  - hxxp:// bianlianlbc5an4kgnay3opdemgcry g2kpfcbgczopmm3dnbz3uaunad[.] onion/
  - hxxp:// bianlivemqbawcco4cx4a672k2fip3 guyxudzurfqvdszafam3ofqgqd[.] onion

- **暗号化されたファイル拡張子:**
  - .bianlian

- **身代金要求テキスト**
  - ReadMe.txt

【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	T1078	有効なアカウント（Valid Accounts）	BianLian は、被害者のネットワークにアクセスする際に、有効なアカウントを使用することが多く、特に侵入前に取得した侵害された RDP 認証情報を介してアクセスする。
初期アクセス	T1133	外部リモートサービス（External Remote Services）	事業者は、公開されている RDP、VPN、およびリモートアクセスサービスを、企業環境への侵入経路として利用します。
初期アクセス	T1566	フィッシング（Phishing）	BianLian はフィッシングを利用して有効な認証情報を入手し、それによって初期アクセスとネットワーク内でのその後の横方向の移動を可能にする。
初期アクセス	T1190	公開アプリケーションの脆弱性悪用（Exploit Public-Facing Application）	攻撃者は、脆弱な外部向けアプリケーションなど、環境への直接アクセスを提供する、公開されている Windows および ESXi インフラストラクチャを標的にしている。
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）	BianLian は PowerShell を使用して、検出コマンドの実行、セキュリティ保護の無効化、ツールの準備、およびデータ漏洩前のデータ準備を行います。
実行	T1059.003	コマンド／スクリプトインタープリタ：Windows コマンドシェル（Command and Scripting Interpreter: Windows Command Shell）	オペレーターは、Windows コマンドシェルを使用して、ツールを実行したり、設定を変更したり、検出コマンドを実行したり、横方向の移動をサポートしたりします。
実行	T1053.005	スケジュールされたタスク／ジョブ：スケジュールされたタスク（Scheduled Task/Job: Scheduled Task）	BianLian は、DLL ペイロードを実行したり、SYSTEM レベルの実行権限を含む、昇格された権限で悪意のあるコマンドを実行したりするためのスケジュールされたタスクを作成します。
永続化	T1098	アカウント操作（Account	オペレーターは、侵害された環境でアカウントを作成または有効化した後、アクセスを維持する

脅威アクタープロフィール；BianLian

戦術	ID	技術	手順 / 観測可能値
		Manipulation)	ためにパスワードやアカウント設定を変更する。
永続化	T1136.001	アカウント作成：ローカルアカウント(Create Account: Local Account)	BianLian は、ローカル管理者アカウントを作成または有効化し、継続的なアクセスを可能にするためにユーザーをリモートデスクトップグループに追加します。
永続化	T1136.002	アカウント作成：ドメインアカウント(Create Account: Domain Account)	オペレーターは、永続性、特権アクセス、およびドメインコントローラーへの移行をサポートするために、ドメイン管理者アカウントを作成します。
永続化	T1136.003	アカウント作成：クラウドアカウント(Create Account: Cloud Account)	BianLian は、被害を受けたシステムやクラウド接続環境へのアクセスを維持するために、Azure AD アカウントを作成しました。
永続化	T1505.003	サーバーソフトウェアコンポーネント：Web シェル(Server Software Component: Web Shell)	オペレーターは、アクセスを維持し、後続の活動を支援するために、侵害された Exchange サーバー上に Web シェルを展開します。
権限昇格	T1068	権限昇格のための脆弱性悪用(Exploitation for Privilege Escalation)	BianLian は、CVE-2022-37969 を含む Windows のローカル脆弱性を悪用し、侵害したシステム上でより高い権限を取得しました。
防御回避	T1562.001	防御機能の妨害：ツールの無効化または変更(Impair Defenses: Disable or Modify Tools)	オペレーターは、検出および対応能力を低下させるために、Windows Defender、AMSI、および Sophos の保護機能を無効化または変更します。
防御回避	T1562.004	防御機能の妨害：システムファイアウォールの無効化または変更(Impair Defenses: Disable or Modify System Firewall)	BianLian は Windows ファイアウォールのルールを変更して受信 RDP トラフィックを許可し、それによって侵害されたシステムへのリモートアクセスを可能にする。
防御回避	T1112	レジストリの変更(Modify	オペレーターはレジストリ設定を変更して、RDP の保護機能を弱めたり、リモートアシスタンスを

戦術	ID	技術	手順 / 観測可能値
		Registry）	有効にしたり、セキュリティ製品の改ざん防止機能を無効にしたりする。
防御回避	T1036.004	偽装：タスクまたはサービスの偽装（Masquerading: Masquerade Task or Service）	BianLian はバイナリファイルやスケジュールされたタスクの名前を正規の Windows サービスやセキュリティツールに一致するように変更し、通常の活動に溶け込む。
防御回避	T1027.002	難読化されたファイルまたは情報：ソフトウェアパッキング（Obfuscated Files or Information: Software Packing）	オペレーターは、静的検出やマルウェア分析をより困難にするために、実行ファイルを UPX で圧縮する場合があります。
認証情報アクセス	T1552.001	保護されていない認証情報：ファイル内の認証情報（Unsecured Credentials: Credentials In Files）	BianLian は、ローカルシステムおよびネットワーク共有を検索し、保存または公開された認証情報を含むファイルを探します。
認証情報アクセス	T1003.001	OS 認証情報ダンピング：LSASS メモリ（OS Credential Dumping: LSASS Memory）	オペレーターは LSASS メモリにアクセスし、権限昇格や横方向の移動に再利用できる認証情報を収集する。
認証情報アクセス	T1003.003	OS 認証情報ダンピング：NTDS（OS Credential Dumping: NTDS）	BianLian は、Active Directory の認証情報データとドメイン情報を収集するために、NTDS.dit にアクセスしたりコピーしたりしようとします。
認証情報アクセス	T1552.004	保護されていない認証情報：秘密鍵（Unsecured Credentials: Private Keys）	オペレーターは SessionGopher を使用して、リモートアクセスツールから保存されているセッション情報を抽出し、認証情報の再利用をサポートします。
探索	T1046	ネットワークサービスの探索（Network Service Discovery）	BianLian は、Advanced Port Scanner と SoftPerfect Network Scanner を使用して、開いているポート、到達可能なシステム、および実行中のサービスを特定します。

脅威アクタープロフィール；BianLian

戦術	ID	技術	手順 / 観測可能値
探索	T1135	ネットワーク共有の探索（Network Share Discovery）	オペレーターは、SoftPerfect Network Scanner と SharpShares を使用して、共有フォルダとアクセス可能なネットワーク共有を特定します。
探索	T1482	ドメイン信頼関係の探索（Domain Trust Discovery）	BianLian は PingCastle とネイティブコマンドを使用して Active Directory の信頼関係をマッピングし、横方向の移動の機会を特定します。
探索	T1087.002	アカウントの探索：ドメインアカウント（Account Discovery: Domain Account）	オペレーターはドメインコントローラーに問い合わせを行い、ドメインユーザー、ドメインコンピューター、および重要度の高い管理者アカウントを特定します。
探索	T1069.002	権限グループの探索：ドメイングループ（Permission Groups Discovery: Domain Groups）	BianLian はドメイングループを列挙し、機密システムへのアクセス権を持つ特権グループとアカウントを特定します。
探索	T1018	リモートシステムの探索（Remote System Discovery）	オペレーターは、ドメインコントローラー、到達可能なデバイス、および横方向の移動をサポートできる内部ホストのリストを収集します。
探索	T1033	システム所有者／ユーザーの探索（System Owner/User Discovery）	BianLian は現在ログインしているユーザーをチェックし、アクティブなセッションを把握して、ターゲットにする価値のあるアカウントを特定します。
探索	T1057	プロセスの探索（Process Discovery）	オペレーターは PowerShell スクリプトを実行して、アクティブなプロセスを一覧表示し、セキュリティツールやビジネスアプリケーションを特定します。
探索	T1518	ソフトウェアの探索（Software Discovery）	BianLian はインストールされているソフトウェアの一覧を表示することで、環境を把握し、セキュリティ製品や有用なアプリケーションを特定するのに役立ちます。
探索	T1082	システム情報の探索（System Information Discovery）	オペレーターは、侵害された環境を把握するために、ローカルドライブ、ホスト、およびシステム情報を収集します。
探索	T1012	レジストリの照会（Query Registry）	BianLian マルウェア（system.exe など）は、レジストリ値を列挙して構成や環境の詳細情報を取得します。
探索	T1083	ファイル／ディレクトリの探索	オペレーターは、収集および持ち出しの前に、機密ファイル、バックアップフォルダ、データベ

戦術	ID	技術	手順 / 観測可能値
		(File and Directory Discovery)	ース、および共有ディレクトリを特定します。
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)	BianLian は、有効なアカウントを使用して RDP 経由でシステム間を移動し、高価値資産にアクセスします。
横展開	T1021.002	リモートサービス:SMB／Windows 管理共有(Remote Services: SMB/Windows Admin Shares)	オペレーターは、SMB 接続と Windows 管理共有を使用してネットワークログインセッションを確立し、横方向に移動します。
横展開	T1570	横展開時のツール転送(Lateral Tool Transfer)	BianLian は、侵害されたシステム間でツールやペイロードを転送し、発見、認証情報へのアクセス、およびデータ流出を支援します。
収集	T1115	クリップボードデータ(Clipboard Data)	BianLian マルウェアは、ユーザーのクリップボードデータを収集し、コピーされた認証情報、ファイルパス、または機密テキストを漏洩させる可能性があります。
収集	T1560	収集データのアーカイブ (Archive Collected Data)	オペレーターは、収集したデータを外部に持ち出す前に、PowerShell スクリプトを使用して圧縮または暗号化します。
収集	T1005	ローカルシステムからのデータ (Data from Local System)	BianLian は、財務、顧客、ビジネス、技術、個人データなどの機密性の高いローカルファイルを収集します。
収集	T1039	ネットワーク共有ドライブからのデータ(Data from Network Shared Drive)	オペレーターは、ファイルリポジトリと共有フォルダを特定した後、アクセス可能なネットワーク共有からデータを収集します。
C2(コマンド&コントロール)	T1105	侵入ツール転送 (Ingress Tool Transfer)	BianLian は、外部インフラストラクチャからツール、バックドア、および関連ファイルを被害者の環境に転送します。
C2(コマンド&コントロール)	T1219	リモートアクセスソフトウェア (Remote Access Software)	オペレーターは、TeamViewer、Atera Agent、SplashTop、AnyDesk などの正規のリモートアクセスツールを使用して、対話型制御を行います。
C2(コマンド	T1090	プロキシ	BianLian は、Ngrok や Rsocks などのプロキシ

戦術	ID	技術	手順 / 観測可能値
&コントロール）		（Proxy）	ツールを使用して、攻撃者が制御する経路を経由してアクセスし、トラフィックをルーティングします。
C2（コマンド&コントロール）	T1090.002	プロキシ：外部プロキシ（Proxy: External Proxy）	通信事業者は、Rsocks を介した SOCKS5 トンネルを利用して、コマンドおよび制御トラフィックの最終宛先を隠蔽します。
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）	BianLian は FTP 経由で盗んだファイルを外部に持ち出し、被害者の環境外にデータを移動させます
情報窃取	T1537	クラウドアカウントへのデータ転送（Transfer Data to Cloud Account）	攻撃者は Rclone を使用して、盗んだデータを攻撃者が管理するクラウドストレージアカウントに移動させる。
情報窃取	T1567.002	Web サービスを介したデータ窃取：クラウドストレージへの窃取（Exfiltration Over Web Service: Exfiltration to Cloud Storage）	BianLian は、盗んだ被害者のデータをアップロードして保存するために、Mega のクラウドストレージを利用しています。
インパクト	T1486	データ暗号化による影響（Data Encrypted for Impact）	以前、BianLian はデータ窃盗後にファイルを暗号化し、拡張子を.bianlian に付加していたが、その後、暗号化を行わずに恐喝を主目的とするようになりました。
インパクト	T1657	金銭的窃取（Financial Theft）	BianLian は、情報漏洩現場の暴露、身代金要求の手紙、直接の電話、従業員、パートナー、顧客、規制当局への連絡を脅迫するなどして、被害者に圧力をかけている

【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、攻撃特徴や TTP を考慮した観点より、国内医療機関における BianLian 対策として特に優先すべき三つの対策例とその理由を示します。

1. **「正規ログイン」による RDP・保守 VPN 侵入を防止する（認証情報悪用対策）**
   - 診療系ネットワークへ接続する保守 VPN、RDP、リモート管理ポータルにフィッシング耐性を有する MFA を適用

- 外部公開への RDP を原則廃止し、必要な RDP は VPN や認証済み管理端末からのみ利用可能とする
- 保守ベンダーの共用 ID を廃止し、担当者単位でアカウントを付与するとともに、接続元・時間帯・接続先を限定
- アカウントロックアウトを設定し、認証失敗の連続、営業時間外、国外・異常地域、通常と異なる端末からのログインを監視
- ローカル管理者、ドメイン管理者、Azure AD 等の特権アカウントを定期的に棚卸しし、新規作成・権限追加・パスワード変更を監視

BianLian は、侵入前に入手した**有効な RDP 認証情報を使用して正規利用者としてログインすること**を主要な侵入手段としています。 また、侵入後にも新たなローカル管理者、ドメイン管理者、クラウドアカウントを作成・有効化し、アクセスを維持します。そのため、脆弱性対策だけでなく、**「パスワードが正しいから通す」という認証モデルそのものを見直し、盗まれた正規アカウントを使わせないこと**が最優先となります。

2. **正規管理ツール・Windows 標準機能に紛れる攻撃を検知する（ステルス・横展開対策）**
   - TeamViewer、Atera Agent、SplashTop、AnyDesk 等のリモート管理ツールを許可制とし、未承認インストールや新規セッションを検知
   - PowerShell、Windows コマンドシェル、PsExec、SMB、Windows 管理共有等について、利用端末・管理者・用途を限定
   - Advanced Port Scanner、SoftPerfect Network Scanner、SharpShares、PingCastle 等による内部探索を監視
   - LSASS、NTDS.dit へのアクセスや SessionGopher 等による保存済み認証情報の取得を重点監視
   - Defender、AMSI、Sophos、Windows ファイアウォール、レジストリ等のセキュリティ設定変更をリアルタイム検知
   - VPN、AD、EDR、RDP、ファイアウォール等のログを中央環境へ集約し、十分な期間保持

BianLian は、専用マルウェアだけに依存せず、**PowerShell、RDP、SMB、PsExec、TeamViewer、AnyDesk 等の正規ツールや標準管理機能に活動を紛れ込ませる**点に特徴があります。 また、Windows Defender や AMSI を無効化し、ファイアウォールやレジストリを変更して RDP 接続を許可するなど、侵害後に管理環境そのものを攻撃者に都合のよい状態へ変更します。保守ベンダーが同じような正規管理ツールを日常的に利用する状況のもと、単純なツール禁止では現実的ではありません。そのため、**「何を使ったか」ではなく、「誰が・どこから・何に対して・どのような管理操作をしたか」を継続監視し、通常保守との差異を検知すること**が重要です

3. **暗号化を伴わない患者情報窃取を前提とした流出検知・証跡保全を強化する（データ恐喝対策）**
   - 電子カルテ、ファイルサーバー、共有フォルダ等における患者情報・診療情報への

大量アクセス、一括コピーを監視

- PowerShell、WinRAR 等による大量圧縮や、ステージング用ディレクトリへの集約を検知
- Rclone、WinSCP、FTP、Mega 等による外部転送を監視し、診療系から外部へ出るデータ転送経路を必要最小限に限定
- 通常業務量を大きく超えるファイル読み出し、圧縮、クラウドアップロードを相関分析
- 外部送信・認証・ファイルアクセスのログを改ざん困難な形で長期保存し、流出範囲を後から特定できる状態を維持
- 患者情報のリークサイト掲載、患者・取引先・規制当局への直接連絡まで想定したインシデント対応訓練を実施

BianLian は近年、従来のランサムウェアのように「暗号化して復旧不能にする」ことよりも、**機密情報を盗み、その公開を材料として支払いを迫るデータ恐喝を主軸**としています。 実際に PowerShell、WinRAR、Rclone、WinSCP、FTP、Mega 等を利用してデータを収集・圧縮・外部送信し、その後、リークサイト掲載や電話等によって被害組織へ圧力をかけます。電子カルテが暗号化されなくても、患者情報が大量に窃取された時点で重大インシデントとなります。そのため、BianLian 対策ではバックアップ以上に、**「大量データが集められていることに気付く」「外へ出る段階で止める」「何が盗まれたか後から追跡できる」こと**を独立した最優先事項として扱う必要があります。

上記の通り、国内医療機関における BianLian 対策では、**①盗まれた正規認証情報による RDP・保守 VPN 侵入を防ぐ、②正規管理ツールに紛れる探索・認証情報窃取・横展開を見抜く、③暗号化を伴わない患者情報窃取を早期に検知し証跡を残す**ことを優先すべきといえます。

以上