脅威アクタープロフィール；Medusa

[TLP：White]

※本資料は Health ISAC が 2026 年 6 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】

Medusa Ransomware Group（メデューサ）は、医療分野を含む重要インフラを標的とした、攻撃的な二重恐喝戦術で知られる、金銭目的のランサムウェア攻撃グループです。

このグループは、フィッシング、脆弱なインターネット接続システム、認証情報の窃盗、リモートアクセスサービスの悪用などを通じて侵入します。

Medusa の工作員は偵察活動を行い、通常の管理作業のなかに攻撃を溶け込ませるため、正規の管理ツールを用いて検知を回避した後、機密データを盗み出し、システムを暗号化します。その後、情報漏洩サイトやデータ公開の脅迫によって圧力をかけます。

【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】

サイバー犯罪者で、二重脅迫型のランサムウェア・アズ・ア・サービス（RaaS）です。

【医療分野への影響】

世界中の複数の分野にわたる約 540 の組織に影響を与えており、そのうち 57 の組織が医療分野で被害を受けています。これは同グループの既知の被害者の約 11%に相当します。

脅威アクタープロフィール；Medusa

【概要】

2026 年初頭現在、Medusa は、医療、製造、教育、政府、重要インフラなど、世界中の様々な業界を標的とする、金銭目的の活発な脅威アクターです。

2021 年頃から活動している Medusa は、データ窃盗、ランサムウェアの展開、そして被害者に身代金の支払いを迫るための情報漏洩サイトの運営といった二重の恐喝攻撃で知られている。

このグループは、初期アクセス手段として、フィッシング、侵害された認証情報、公開されたリモートサービス、インターネットに接続された脆弱性の悪用などをよく利用しています。侵入後者は、偵察、権限昇格、認証情報の収集、横方向の移動、データ漏洩を行い、その後システムを暗号化しています。

また、攻撃のなかで、悪意のある活動を通常のネットワーク操作に紛れ込ませ、検出を回避するために、正規の管理ツール、LOLBins、リモート実行ユーティリティ、および一般に公開されている攻撃的なセキュリティツールを頻繁に悪用します。

【活動地域】

メデューサ・ランサムウェア・グループの活動は、主に米国とカナダの組織に影響を与えており、その他、英国、フランス、スペイン、イタリア、オーストラリア、インド、ブラジル、およびヨーロッパ、アジア、ラテンアメリカの各地で被害者が確認されています。

【攻撃の特徴】

Medusa は、単なるランサムウェアではなく、複数の役割を持つ攻撃者が分業しながら進める組織的な攻撃グループです。攻撃は一度に実行されるのではなく、侵入から恐喝までを段階的に進める特徴があります。

まず、フィッシングメール、盗まれた認証情報、公開された VPN や RDP サービス、さらには ConnectWise ScreenConnect や Fortinet 製品の脆弱性などを悪用して組織内部へ侵入します。侵入後はすぐに暗号化を行うのではなく、Advanced IP Scanner などを利用してネットワーク構成や重要システムを調査し、Active Directory、ファイルサーバー、バックアップサーバーなどの重要資産を特定します。その後、Mimikatz を利用して認証情報を収集し、管理者権限の取得や権限昇格を行います。さらに、AnyDesk、ConnectWise ScreenConnect、PsExec などの正規の管理ツールや Windows 標準機能を利用して横展開を進め、組織全体へアクセス範囲を拡大します。

Medusa の特徴は、専用マルウェアだけに頼るのではなく、管理者が日常的に利用する正規ツールや LOTL（Living Off the Land）を多用する点にあり、攻撃活動が通常の管理作業に紛

れ込みやすくなっています。

十分な権限と支配範囲を確保した後は、機密情報の窃取が行われます。財務情報、契約文書、内部資料、個人情報などを収集し、Rclone を利用して外部へ持ち出します。これは、暗号化後の身代金要求だけでなく、「支払わなければ情報を公開する」という二重恐喝を行うための準備でもあります。

暗号化の直前には、防御機能と復旧手段の無効化が実施されます。Medusa は BYOVD（Bring Your Own Vulnerable Driver）を利用して EDR やアンチウイルス製品の検知を回避し、PowerShell や WMIC、バッチスクリプトを用いてセキュリティサービスを停止します。さらに、ボリュームシャドウコピーの削除やバックアップの無効化を行い、被害組織による復旧を困難にしたうえで、AES-256 によるファイル暗号化を実行し、「.MEDUSA」の拡張子を付加します。

最後に、交渉担当がリークサイトや身代金交渉サイトを通じて被害組織と接触し、盗み出した情報の公開を示唆しながら身代金の支払いを要求します。

このように Medusa の攻撃は、「侵入」「偵察」「認証情報窃取」「権限昇格」「横展開」「情報窃取」「防御機能・バックアップの無効化」「暗号化」「恐喝」という一連の工程を段階的に実施する組織的な攻撃モデルです。

【暴露サイト、感染ファイル等】

- **データ暴露サイト**
  - hxxp[:]//xfv4jzckytb4g3ckwemcny3ihv4i5p4lqzdpi624cxisu35my5fwi5qd[.]onion/
  - hxxp[:]//7aqabivkwmpvjkyefonf3gpy5gsubopqni7kcirsrq3pflckxq5zz4id[.]onion/
  - hxxp[:]//kyfiw76eol6ph2mq7pi5e5tdvce37bicddhai62qhdc5ja6jdchz4qqd[.]onion/
  - hxxp[:]//s7lmmhlt3iwnwirxvgjidl6omcblvw2rg75txjfduy73kx5brlmiulad[.]onion/
  - hxxp[:]//cx5u7zxbvrfyoj6ughw76oa264ucuuizmmzypwum6ear7pct4yc723qd[.]onion/
  - hxxp[:]//hupxs7ps7md24kpz4lwsbra64abgxjx3pcc2wuca5ibawf2g5hlpfyqd[.]onion/
  - hxxp[:]//62foekhv5humjrfwjdyd2dgextpbf5i7obguhwvfoghmu3nxpkmxlcid[.]onion/
  - hxxps[:]//t[.]me/+lyskiDn9KiYxZjlh

- **公開連絡先:**
  - key.medusa.serviceteam[.]protonmail.com
  - medusa.support[.]onionmail.org
  - mds.svt.breach[.]protonmail.com
  - mds.svt.mir2[.]protonmail.com
  - MedusaSupport[.]cock.li

- **暗号化されたファイル拡張子:**
  - .medusa
  - .MEDUSA
  - .[victim_ID].[medusa]

- **身代金要求テキスト**
  - !!!READ_ME_MEDUSA!!!.txt
  - READ_NOTE.html
  - HOW_TO_RECOVER_DATA.txt
  - !!!RESTORE_FILES!!!.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	T1078.002	有効なアカウント:ドメインアカウント（Valid Accounts: Domain Accounts）	Medusa 攻撃者は、通常、初期アクセスブローカー（IAB）や過去の侵害から入手した、侵害されたドメイン、VPN、および RDP の認証情報を入手し、悪用して企業環境へのアクセス権を取得します。
初期アクセス	T1133	外部リモートサービス（External Remote Services）	Medusa の攻撃者は、特に多要素認証（MFA）が適用されていない環境において、公開されている RDP、VPN、Citrix、およびリモート管理サービスを侵入経路として利用します。
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）	Medusa の関連会社は、SimpleHelp RMM の脆弱性やその他の公開されているサービスなど、インターネットに接続された脆弱なアプリケーションやパッチが適用されていないソフトウェアを悪用して、初期アクセスを確立します。
初期アクセス	T1566	フィッシング（Phishing）	フィッシング攻撃は、認証情報を収集し、標的となる組織に悪意のあるペイロードを送り込むために利用されます。
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）	Medusa のオペレーターは、PowerShell コマンドを実行してペイロードの準備、偵察活動、防御システムの無効化、ランサムウェアの展開を支援します。観測されたコマンドには、隠し実行フラグを使用したエンコードされた PowerShell コマンドの実行が含まれています。
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	Windows のコマンドシェルとバッチスクリプトは、ランサムウェアのコンポーネントを実行したり、操作を自動化したり、横方向への移動を容易にするために使用されます。

脅威アクタープロフィール；Medusa

戦術	ID	技術	手順 / 観測可能値
		(Command and Scripting Interpreter: Windows Command Shell)	
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)	Medusa の活動には、侵害された環境内で永続的なアクセスを維持するために、不正なローカル管理者アカウントを作成することが含まれます。
永続化	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)	スケジュールされたタスクは、永続性を維持し、悪意のあるペイロードを自動的に実行するために、schtasks を使用して作成されます。
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ダ(Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder)	レジストリの変更とスタートアップエントリは、再起動後も永続的に保持されるように構成されています。
認証情報アクセス	T1003	OS 認証情報ダンピング(OS Credential Dumping)	Medusa の関連会社は、侵害したシステムから認証情報をダンプし、特権昇格を実現して環境全体へのアクセスを拡大する。
権限昇格	T1068	権限昇格のための脆弱性悪用 (Exploitation for Privilege Escalation)	ローカルの脆弱性を悪用したり、特権認証情報を不正に使用したりすることで、管理者権限を取得する。
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)	Medusa のオペレーターは、暗号化作業を開始する前に、アンチウイルス、EDR、バックアップ、および監視ツールを無効化または終了させます。
防御回避	T1112	レジストリの変更 (Modify Registry)	DisableRestrictedAdmin 設定の変更など、レジストリの変更は、セキュリティ制御を弱体化させ、リモートアクセスを容易にするために使用されます。
防御回避	T1027	難読化されたファイルまたは情報	セキュリティソリューションによる検出を回避するために、暗号化された PowerShell コマンドや難読化さ

脅威アクタープロフィール：Medusa

戦術	ID	技術	手順 / 観測可能値
		（Obfuscated Files or Information）	れたスクリプトが使用されます。
防御回避	T1218	システムバイナリプロキシ実行（System Binary Proxy Execution）	certutil.exe や bitsadmin.exe といった正規の Windows バイナリが悪用され、通常のシステム動作に紛れ込みながら悪意のあるファイルをダウンロードして実行する。
探索	T1018	リモートシステムの探索（Remote System Discovery）	Medusa 攻撃者は、内部ネットワークをスキャンして、アクセス可能なシステム、サーバー、および重要なインフラ資産を特定します。
探索	T1087	アカウントの探索（Account Discovery）	ユーザーアカウント、管理者グループ、ドメイン権限を列挙し、価値の高いターゲットと特権アカウントを特定します。
探索	T1083	ファイル／ディレクトリの探索（File and Directory Discovery）	Medusa のオペレーターは、機密ファイル、バックアップ、データベース、共有ディレクトリを、データ流出および暗号化の前に特定します。
探索	T1482	ドメイン信頼関係の探索（Domain Trust Discovery）	Active Directory の信頼関係とドメイン間の関係を列挙することで、企業環境全体にわたるより広範な侵害を容易にします。
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）	管理共有フォルダと SMB は、ランサムウェアのペイロードを配布したり、システム間で横方向に移動したりするために悪用される。
横展開	T1569.002	システムサービス：サービス実行（System Services: Service Execution）	PsExec とリモートサービス実行は、ランサムウェアを複数のホストにリモートで展開するために使用されます。
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）	Medusa のオペレーターは、被害者の環境内で対話型アクセス、手動操作、およびランサムウェアの展開を行うために RDP セッションを使用します。
収集	T1005	ローカルシステムからのデータ（Data from Local System）	機密性の高い業務ファイルや社内文書は、暗号化される前に、侵害されたシステムから収集されます。
収集	T1560.001	収集データのアーカイブ：ユーティリティによるア	収集されたファイルは、転送作業を簡素化するために、外部への持ち出し前にアーカイブ形式に圧縮されます。

戦術	ID	技術	手順 / 観測可能値
		ーカイブ（Archive Collected Data: Archive via Utility）	
情報窃取	T1041	C2 チャネルを介したデータ窃取（Exfiltration Over C2 Channel）	Medusa の関連組織は、暗号化活動を開始する前に、被害者のデータを攻撃者が管理するインフラストラクチャに持ち出す。
情報窃取	T1567	Web サービスを介したデータ窃取（Exfiltration Over Web Service）	盗まれた被害者のデータをアップロードするために、ウェブベースのインフラストラクチャとリモートサービスが利用されている。
C2（コマンド＆コントロール）	T1090	プロキシ（Proxy）	TOR インフラストラクチャと匿名プロキシサービスは、攻撃者の通信や情報漏洩活動を隠蔽するために使用される。
C2（コマンド＆コントロール）	T1071.001	アプリケーション層プロトコル：Web プロトコル（Application Layer Protocol: Web Protocols）	HTTP および HTTPS 通信は、コマンド＆コントロール通信、ペイロード配信、および被害者との交渉に使用されます。
インパクト	T1486	データ暗号化による影響（Data Encrypted for Impact）	Medusa は被害者のシステムを暗号化し、暗号化されたファイルに.medusa.MEDUSA や.[victim_ID].[medusa]などの拡張子を追加します。
インパクト	T1490	システム復旧の妨害（Inhibit System Recovery）	復元作業を妨害するために、シャドウコピー、バックアップ、および復旧メカニズムが削除または無効化されます。
インパクト	T1657	金銭的窃取（Financial Theft）	Medusa は、身代金の支払いを要求すると同時に、盗んだ被害者のデータを公開すると脅迫するという二重の恐喝行為を行う。
初期アクセス	T1078.002	有効なアカウント:ドメインアカウント（Valid Accounts: Domain Accounts）	管理アカウントの障害やシステム変更が発生する可能性があり、インシデント対応および復旧作業を妨げる可能性があります。

【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、国内医療機関において特に優先すべき三つの対策例とその理由を示します。

脅威アクタープロフィール；Medusa

1. **診療系ネットワークへ到達可能な VPN・リモート保守経路の防御（初期侵入対策）**
   - 診療系ネットワークへ接続する保守用 VPN、RDP、Citrix、ScreenConnect 等の外部接続経路を棚卸し
   - VPN、RDP、Citrix、リモート管理サービスへの MFA 適用と、ベンダー共用アカウントの廃止
   - ScreenConnect、Fortinet、SimpleHelp RMM 等の外部公開・リモート管理基盤について迅速な脆弱性対応を実施
   - 保守接続を常時開放せず、接続元、接続時間、接続対象システムを必要最小限に限定
   - 漏えい認証情報、不審地域、営業時間外、通常と異なるベンダーアカウントからの接続を監視

   Medusa は、フィッシングや侵害済み認証情報に加え、公開 VPN、RDP、Citrix、ScreenConnect や Fortinet 製品などの脆弱性を利用して初期侵入します。 また、MFA が適用されていない外部リモートサービスを積極的に悪用することが確認されています。そのため、Medusa 対策では、一般的な情報系端末のフィッシング対策だけでなく、**診療系へ直接到達できるリモート保守経路を最優先で統制すること**が重要です。

2. **Active Directory・管理者権限・正規管理ツールの監視強化（横展開・全体感染対策）**
   - 管理者アカウント、ローカル管理者、サービスアカウントを分離し、権限を必要最小限に制限
   - Mimikatz や OS 認証情報ダンピング、異常な管理者アカウント作成・権限昇格を監視
   - PsExec、PowerShell、RDP、AnyDesk、ScreenConnect、SMB 等の利用を許可された管理端末・担当者に限定
   - Active Directory のアカウント・ドメイン信頼関係の大量列挙や、不審なネットワーク探索を監視
   - 情報系 NW、診療系 NW、サーバー・管理 NW を分離し、不要な RDP、SMB、Windows 管理共有を制限

   Medusa は、侵入後に Mimikatz 等で認証情報を収集し、管理者権限を獲得したうえで、PsExec、PowerShell、AnyDesk、ScreenConnect、RDP 等の正規ツールを利用して横展開します。 また、SMB や Windows 管理共有、リモートサービス実行を利用して複数のシステムへランサムウェアを配布する傾向も確認されています。 国内医療機関では、診療系ネットワーク内部に電子カルテ、画像、検査、部門システム、ファイルサーバー等が集約されている場合があり、内部管理通信が広く許可されていると、一つの侵害から診療系全体へ被害が拡大する可能性があります。そのため、**「外部から遮断しているから安全」と考えるのではなく、診療系内部でも認証情報・管理通信・管理ツールを厳格に制御すること**が重要です。

3. バックアップ保護と患者情報の窃取・外部送信の検知（診療停止・二重恐喝対策）

- 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、バックアップ管理権限を通常の AD 管理権限から分離
- シャドウコピー削除、バックアップサービス停止、EDR・アンチウイルス停止等の操作を重点監視
- Rclone、大量圧縮、Web 経由の大量データ送信等を検知し、通常業務では不要な外部転送を制限
- 電子カルテ、共有ファイル、データベース等における患者情報・機密情報への大量アクセスを監視
- 電子カルテ・部門システムの復旧試験、紙運用を含む IT-BCP 訓練を定期的に実施

Medusa は暗号化前に機密情報を収集し、Rclone 等を用いて外部へ持ち出したうえで、バックアップやシャドウコピーを削除・無効化し、その後に暗号化を行います。 また、EDR やアンチウイルス、バックアップ、監視ツール自体を停止させることも確認されています。患者情報の流出だけでも重大な医療安全・信用・経営上の被害となるうえ、電子カルテや部門システムの停止は診療継続そのものに直結します。そのため、「盗まれたことに気付く」「復旧手段を破壊させない」「暗号化されても診療を再開できる」という三つの観点を同時に確保する必要があります。

以上