脅威アクタープロフィール；Play 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】

Play ランサムウェアは、組織的に運営され、人間が直接操作するタイプのサイバー攻撃グループであり、侵入時に目立たない手法を用いる点に特徴があります。

2022 年の出現以降、認証情報の不正利用や公開されたサービス、正規の管理ツールを悪用することで、企業や医療機関のシステムに侵入しています。

多くのランサムウェアが外部の協力者を広く募る形で運営されているのに対し、Play は限られたメンバーで構成される閉鎖的な体制をとっており、攻撃の手順や運用が統制されているため、再現性の高い効果的な攻撃が行われています。

また、データを暗号化するだけでなく、事前に情報を持ち出し、その公開を示唆することで圧力をかける手法を採用しています。特に医療分野では、業務停止と情報漏えいの双方が重大な影響を及ぼすため、被害組織に対する圧力が大きくなる傾向があります。

【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。

【攻撃動機】

主な目的は金銭の獲得であり、要求額は数千万円から数億円規模に及ぶ場合があります。

【脅威アクターの性質】

データの暗号化と情報公開を組み合わせた脅迫を行う組織なサイバー犯罪集団

【医療分野への影響】

これまでに世界で約 900 の組織が被害を受けており、医療分野は特に頻繁に標的とされています。

脅威アクタープロフィール；Play Ransomware

【概要】

2026 年初頭時点において、Play Ransomware（PlayCrypt とも呼ばれる）は、世界のサイバー犯罪グループの中で確固たる存在感を持ち、組織的に運用されるランサムウェアとして定着しています。

2022 年半ばに出現した本グループは、大規模な外部ネットワークに依存せず、直接的な侵入と高い影響力を伴う攻撃を実行できる点を強みとして、急速に勢力を拡大しました。
本グループは 2022 年 6 月に PlayCrypt の名称で確認されて以降、比較的一貫した名称を維持しています。多くのランサムウェアが外部の協力者を募る形で拡大しているのに対し、Play は閉鎖的かつ厳格に管理された体制で運営されていると考えられています。
この体制により、攻撃手順の一貫性が保たれ、外部からの把握が難しくなるとともに、攻撃の実行がより統制されています。

技術面では、Play は既存のシステム機能や正規の管理ツールを活用し、通常の業務環境に紛れる形で活動します。また、攻撃プログラムを被害組織ごとに調整することで、従来の検知手法を回避しつつ、Windows 環境全体で効果的に攻撃を実行しています。
Play は、人間が直接操作するランサムウェアとして、無差別な攻撃ではなく、計画的な侵入を行います。一般的には、認証情報の不正利用や公開サービスの弱点を利用して侵入し、その後、内部調査や認証情報の収集、ネットワーク内での拡大を経て、最終的にランサムウェアを展開します。

従来のランサムウェア・アズ・ア・サービスとは異なり、Play は広範な外部組織との連携を前提としていません。中央集権的な閉鎖型グループとして運営され、攻撃の各段階は中核メンバーによって一貫して実行されます。この運用により、無駄な動きが抑えられ、再現性の高い攻撃パターンが維持されています。

主な役割は以下のとおりです。

- **侵入担当**： 認証情報や公開サービスを利用して組織内に侵入
- **内部調査担当**： ネットワーク構造や重要システムを把握
- **展開担当**： ネットワーク内で感染を拡大
- **情報持ち出し**： 交渉担当：データの取得と被害者対応
- **開発担当**： 攻撃プログラムの調整・改変

このように役割が分担されていることで、攻撃全体の精度と効率が高められています。

【活動地域】

Play の攻撃は主に北米、特に米国に集中しており、ヨーロッパでも活動が見られます。地理的な偏りはなく、状況に応じて複数の地域を戦略的にターゲットとすることで、グローバルな活動を行っています。

脅威アクタープロフィール；Play Ransomware

【攻撃の特徴】

Play ランサムウェアの特徴は、特別な攻撃手法だけに頼るのではなく、正規のツールや既存の機能を組み合わせて、目立たずに侵入・拡大する点にあります。主な流れは以下のとおりです。

1. **侵入（初期アクセス）**
   - フィッシングメールにより認証情報を取得する
   - 盗まれた VPN や RDP の ID・パスワードを利用してログインする
   - 公開されているサービスを足がかりに侵入する
2. **内部での活動（拡大と維持）**
   - PsExec や SMB などの管理ツールを用いて、ネットワーク内を横断的に移動する
   - PowerShell や WMI といった Windows 標準機能で遠隔操作を継続する
   - SystemBC などを用いて外部との通信経路（バックドア）を維持する
3. **調査と情報収集**
   - Grixba などのツールでネットワーク構成や重要サーバーを特定する
   - Mimikatz を使用して ID やパスワードを取得する
4. **検知の回避**
   - LOLBins（正規ツールの悪用）により通常の操作に紛れる
   - Windows のログを削除し、痕跡を隠す
   - 被害組織ごとにカスタマイズしたプログラムを使用し、検知を回避する
5. **データ持ち出しと暗号化**
   - WinRAR や WinSCP でデータを外部へ送信する
   - データを持ち出したうえで暗号化し、二重に脅迫する
   - vssadmin.exe を用いてバックアップを削除し、復旧を困難にする
6. **実行（影響の発生）**
   - 被害組織ごとに調整されたランサムウェアを実行する
   - 一部のみを暗号化する手法などにより、短時間で広範囲のシステムに影響を与える

【暴露サイト、感染ファイル等】

- **データ暴露サイト**
  - hxxp://k7kg3jqxang3wh7hnmaiokchk7qoebupfgoik6rha6mjpzwupwtj25yd[.]onion/
  - hxxp://ipi4tiumgzjsym6pyuzrfqrtwskokxokqannmd6sa24shvr7x5kxdvqd[.]onion
  - hxxp://j75o7xvvsm4lpsjhkjvb4wl2q6ajegvabe6oswthuaubbykk4xkzgpid[.]onion
- **暗号化されたファイル拡張子**:
  - .play
  - .PLAY
- **身代金要求の手紙**
  - ReadMe.txt

- [UNIQUE_ID].txt
- play.txt

- **連絡先**
  - [unique_id]@gmx.de
  - [unique_id]@web.de

【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	主なアクセス方法。Play オペレーターは、初期アクセスブローカー（IAB）から入手した、または過去の侵害によって侵害された VPN/RDP 認証情報を使用して、企業環境にアクセスします。
初回アクセス	外部リモートサービス	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 サービスを利用して侵入を試みる。
初回アクセス	公開アプリケーションを悪用する	Play は、一部のキャンペーンにおいて、CVE-2018-13379（Fortinet SSL VPN）、CVE-2022-41040 / CVE-2022-41082（Exchange ProxyNotShell）、CVE-2024-57727（SimpleHelp RMM）などの脆弱性を悪用していますが、その悪用は機会主義的なものであり、認証情報に基づくアクセスに比べれば二次的なものです。
実行	PowerShell	PowerShell スクリプトを実行して、ペイロードの準備、偵察活動の実施、および侵害されたシステム内での横方向の移動の準備を行います。
実行	ネイティブ API	Windows API 呼び出しを使用してペイロードを実行し、操作中に低レベルの制御を維持します。
粘り強さ	レジストリ実行キー / スタートアップフォルダ	攻撃者が制御するバイナリを指す Run/RunOnce レジストリキーを介して永続性を確立します。
特権の拡大	特権拡大のための搾取	BYOVD（Bring Your Own Vulnerable Driver：脆弱性のあるドライバを持ち込む）技術（例えば、メーカの脆弱な署名付きドライバ）を利用して、カーネルレベルのアクセス権を取得し、セキュ

		リティ制御を無効化します。
防御回避	防御を弱体化させる:ツールの無効化／変更	ランサムウェアの実行前に、ウイルス対策／EDR プロセスを無効化または終了させ、検出を回避する。
防御回避	防御機能の無効化:セーフモード起動	エンドポイント保護が無効になっている間に暗号化を実行するため、ネットワーク接続を有効にしたセーフモードでシステムを再起動する（Play の動作に顕著に現れる）。
防御回避	インジケーターの削除:イベントログをクリアする	Windows イベントログをクリアして、悪用、認証情報へのアクセス、および横方向の移動の痕跡を削除します。
認証情報アクセス	OS 認証情報のダンプ	LSASS メモリをダンプして認証情報を収集し、ネットワーク全体で権限を昇格させる。
発見	アカウント発見	Active Directory 環境内のドメインアカウントと特権ユーザーを列挙します。
発見	リモートシステム検出	横方向の移動をサポートするために、到達可能なシステムとネットワーク構造を特定します。
水平移動	SMB/Windows 管理者共有	侵害されたシステム間で、SMB 管理共有（例:ADMIN$）を使用して横方向に移動します。
水平移動	Windows Management Instrumentation (WMI)	システム間でリモートコマンドを実行し、ネットワーク全体に伝達します。
収集	ローカルシステムからのデータ	暗号化前に、機密性の高い企業データ（財務記録、従業員データ、内部ファイルなど）を収集します。
漏洩	C2 チャネルを介した漏出	ランサムウェアを展開する前に、盗んだ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（二重恐喝モデル）。
インパクト	暗号化されたデータ	ネットワークが完全に侵害された後、システム間でファイルを暗号化し、拡張子を「.play」に付加します。
インパクト	システム回復を阻害する	シャドウコピーを削除し、復元メカニズムを無効にすることで、暗号化されたシステムの復元を防ぎます

【推奨対策】

Pkay の攻撃特徴や 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以下に整理します。

脅威アクタープロフィール；Play Ransomware

1. **認証・リモートアクセスの強化（最重要）**
   - VPN／RDP／Citrix などすべての外部接続に MFA を必須化
   - 使い回しパスワードの排除と強固な認証ポリシーの適用
   - 異常ログイン（時間帯・地域・回数）の監視

   Play は「正規ログイン」での侵入が中心のため、入口対策が最も効果的といえます。

2. **ネットワーク分離と横展開の遮断**
   - 重要サーバー（電子カルテ、AD、バックアップ）の分離
   - 端末からコアシステムへの直接アクセスを制限
   - 最小権限の徹底

   侵入後は PsExec や SMB で水平移動して攻撃を拡げるため、1 台の侵害によりシステム環境すべてが停止にならない構造とすることが重要です。

3. **バックアップの隔離と復旧性の確保**
   - 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
   - 復元テストの定期実施

   Play はバックアップを消去したうえでデータの暗号化を行うため、最終的に業務継続のためには復旧できるか否かが重要になります。

Play の特徴（有効な認証情報の悪用／正規ツールでの潜伏／水平展開後に一気に感染実行）から考えると、認証機能の強化により内部へ入らせず、ネットワーク分離等により拡大感染を防止する構成としたうえで、バックアップ保全によりシステムが停止しても早期復旧できるようにすることが重要といえます。

以上