脅威アクタープロフィール；DevMan Ransomware

[TLP:White]

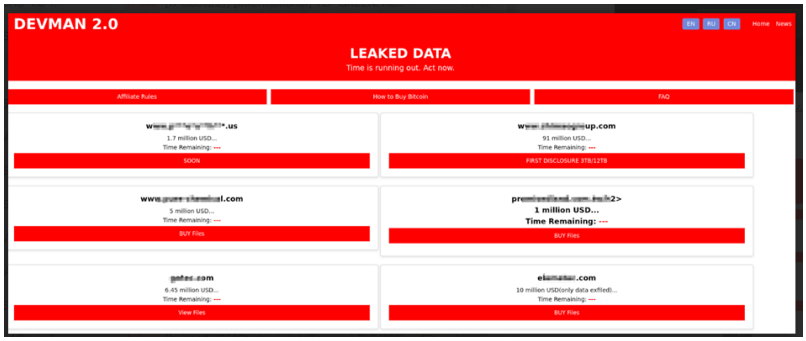
※本資料は Health ISAC が発行したレポートをもとに、Health ISAC Japan で内容を再構成し、一部加筆修正を行ったものとなります。

【エグゼクティブサマリー】

ランサムウェアグループ DevMan は、2025 年 3 月に出現した非常に活発なグループです。彼らは金銭目的の脅威アクターであり、医療分野を含む世界中の組織を標的にしています。

図.:旧 DevMan ランサムウェアのデータ漏洩サイト

図:新型 DevMan ランサムウェアのデータ漏洩サイト(v2)



【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】

ランサムウェア・アズ・ア・サービス型の組織犯罪グループです。

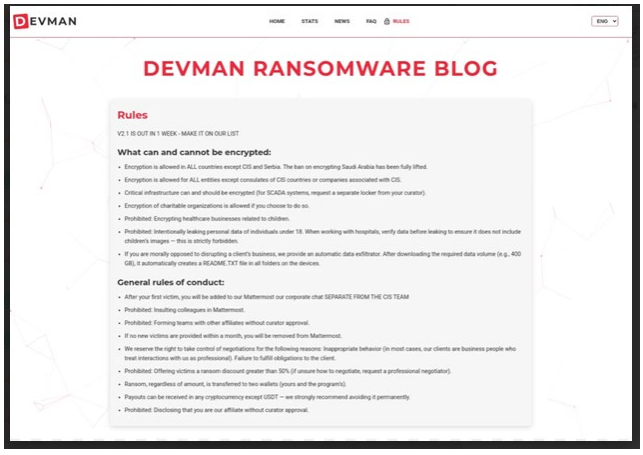
【医療分野への影響】

DevMan の RaaS（ランサムウェアサービス）はランサムウェアの分野では比較的新しい存在ですが、すでに世界中で 86 件の組織を標的にしています。
そのうち 12 件は医療分野に属し、被害者の約 14%を占めています。

【概要】

DevMan ランサムウェアは、特定の国や業種に限定せず、医療、製造、金融、エネルギー、小売など、幅広い分野の組織を対象とするサイバー犯罪グループです。
2025 年には活動を拡大し、英国、フランス、カナダの組織を中心に攻撃が確認されています。
また同年、攻撃の実行を外部の協力者にも広げる仕組みとして、ランサムウェア・アズ・ア・サービス（RaaS）を開始しました。これにより、より多くの攻撃者がこの仕組みを利用できるようになり、被害の拡大が懸念されています。
さらに、情報を暴露するためのサイトも「DevMan 2.0」として刷新され、被害者情報や各種情報を整理して掲載するなど、組織的かつ継続的に運営されていることがうかがえます。

図：DevMan 2.0：データ漏洩サイト － 統計、ブログ、FAQ、およびルール



【活動エリア】

DevMan は特定の業界に限定せず、主に金銭的な利益を重視して攻撃対象を選定しています。その中でも、医療、テクノロジー、公共分野といった、業務停止や情報漏えいの影響が大きい領域が優先される傾向があります。

対象は主に売上高 1 億ドル以上の中堅から大企業であり、支払い能力の高さが重視されていると考えられます。実際に確認された事例の中でも、医療分野は一定の割合を占めてお

り、継続的に狙われています。

地域としては、米国を中心に、ブラジル、フランス、カナダ、さらにアジア太平洋や中東にも広がっており、グローバルに活動している点が特徴です。

【攻撃パターン】

＜①:一般的な攻撃の特徴＞

DevMan ランサムウェアは、既存の攻撃手法（Conti 系）をベースにしつつ、暗号化の速度と検知回避を強化した構成となっています。主な流れは以下のとおりです。

1. 侵入（初期アクセス）
   - 侵害された RDP や VPN を利用してログインする
   - 公開アプリケーションの弱点（脆弱性）を悪用して侵入する
2. 内部での活動（拡大と維持）
   - 暗号化処理の優先度を上げ、短時間で実行できるようにする
   - AdFind でネットワーク構成を調査する
   - DonPAPI で認証情報（ID・パスワード）を取得する
3. 検知の回避
   - Windows の機能を工夫して呼び出し、セキュリティ製品による検知を回避する
   - セーフモードで再起動し、セキュリティソフトを回避する
4. 水平展開
   - SMB や LDAP を利用してネットワーク内に拡散する
5. **実行（影響の発生）**
   - バックアップ（シャドウコピー）やごみ箱を削除し、復旧を困難にする
   - データベースやバックアップ、セキュリティ関連のサービスを停止する

本攻撃の特徴は、「侵入後に短時間で環境全体を把握し、復旧手段を先に潰したうえで一気に実行する」点にあります。

＜②:具体的な攻撃事例＞

■ CrackMapExec（CME）の悪用

攻撃事例の一つでは、DevMan は、侵入後の内部調査や横展開において、CrackMapExec（CME）を使用しています。このツールは本来、企業のセキュリティ検証（侵入テスト）で用いられる正規のツールですが、攻撃者によって以下のように悪用されました。

- Active Directory の情報収集（ユーザー、端末、権限構造の把握）
- パスワードスプレーやブルートフォースによる認証突破
- PowerShell や WMI 等を用いた遠隔コマンド実行
- パス・ザ・ハッシュ等による水平展開

DevMan は、侵入後に新たに作成した管理者アカウントを用いて、このツールにより重要サー

バーへのアクセス可否を確認し、最終的にドメインコントローラーの管理権限を取得しています。これにより、複数のシステムが連鎖的に侵害されました。

■ 脆弱性（EternalBlue）の悪用とデータ取得
さらに DevMan は、古い脆弱性である MS17-010（EternalBlue）を利用し、侵害した環境内での支配を拡大しています。

- ドメインコントローラーからファイルを取得し、支配状態を確認
- Metasploit（msfconsole）を利用したスクリプトでデータを大量収集
- Powershell コマンドにより C ドライブ内のファイルを広範囲に取得

最終的に、約 7TB に及ぶデータを取得し、加えて実行ファイル（notepad.exe）も持ち出しています。

図：攻撃ログ例

```
msfconsole
use auxiliary/admin/smb/ms17_010_command
set RHOSTS ############
set USERNAME malharbi
set PASSWORD ############
set COMMAND powershell -c 'try { Get-ChildItem -Path C:\ -Recurse -
File -Include *.txt -ErrorAction Stop | Sort-Object LastWriteTime -
Descending | Select-Object -First 1 | Format-List
FullName,LastWriteTime > C[:]\Windows\Temp\file[.]txt } catch { 'No TXT
files found' | Out-File C[:]\Windows\Temp\file[.]txt }'
run
exit
```

```
smbclient //############/C$ -U malharbi%############ -N -c 'cd Windows; get
notepad[.]exe'
```

＜③：DragonForce と DevMan ランサムウェアの関連性＞

2025 年 7 月、新たに見つかったランサムウェアの一部は、既存の「DragonForce」という種類に似ていますが、内容を詳しく見ると DevMan の関与が疑われる特徴が確認されています。このランサムウェアでは、感染したファイルの名前が「ランダムな文字列＋.devman」という形式に変わるため、被害の痕跡として識別しやすい特徴があります。
また、この仕組みは過去の有名なランサムウェア（Conti や DragonForce）をベースに作られており、それを改変したものと考えられています。ただし、一部の改変には不具合もあり、本来表示されるはずの身代金メッセージまで暗号化されてしまうケースが確認されています。
動作の面では、外部と通信せずに単独で動く特徴があり、院内ネットワークの中だけで拡散を試みます。具体的には、同じネットワーク内の他の端末やサーバーを探し、接続できるかを試す動きを行います。

さらに、実行時には一時的にシステム内部に情報を記録し、その後すぐ削除することで、調査しても痕跡が残りにくい仕組みが使われています。

【暴露サイト、感染ファイル等】

- **データ暴露サイト**
  - hXXp[:]//qljmlmp4psnn3wqskkf3alqquatymo6hntficb4rhq5n76kuogcv7zyd[.]onion (Primary)
  - hXXp[:]//devmanblggk7ddrtqj3tsocnayow3bwnozab2s4yhv4shpv6ueitjzid[.]onion
- **暗号化されたファイル拡張子:**
  - .devman
  - .devmanv1
  - .6-8 Random Alphabetical Characters (例., .yAGRTb)
- **SNS:**
  - . X (Twitter) - @Inifintyink
  - TOX ID - 9D97F166730F865F793E2EA07B173C742A6302879DE1B0BBB03817A5A04B572FBD82F984981D
- **身代金要求テキスト:**
  - README[.]devmanv1[.]txt
  - README.[8_random_chars].txt
  - !!!_README_!!!.txt

(図:身代金要求テキスト)

【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	パッチが適用されていない RMM ツール（SimpleHelp CVE-2024-57726 ）および VPN ゲートウェイ（Fortinet/Cisco）を標的としています。
初回アクセス	有効なアカウント	RDP 経由で外部境界を迂回するために、初期アクセスブローカー（IAB）から認証情報を購入する。
実行	Windows 管理計測	WMI を使用して、ドメインに参加しているすべてのワークステーション上でランサムウェアのバイナリをリモートで起動します。
実行	共有モジュール	実行には必須の引数「-code [password]」が必要です。引数がない場合、バイナリはサンドボックスを回避するために不活性状態のままになります。
維持	Windows サービス	暗号化ツールをシステムサービスとしてインストールするか、 -detached フラグを使用してバックグラウンドプロセスとして実行します。
維持	レジストリ実行キー / スタートアップフォルダ	HKCU¥Software¥Microsoft¥Windows¥CurrentVersion¥Run を変更して、再起動後も実行が継続されるようにします。
特権の拡大	特権拡大のための搾取	セキュリティサービスを終了する前に、ローカルの脆弱性を悪用して SYSTEM 権限に昇格します。
防御回避	セーフモード起動	AV/EDR を無効にするために、ネットワーク接続ありのセーフモードで強制的に再起動します（bcdedit /set {default} safeboot network）。
防御回避	難読化されたファイルまたは情報	実行時に API ハッシュを使用して Windows 関数を解決することで、静的解析からその意図を隠蔽します。
防御回避	仮想化／サンドボックス回避	IsDebuggerPresent を使用してデバッガーの存在を確認し、仮想化された分析環境が検出された場合はシャットダウンします。
発見	リモートシステム検出	SMB と LDAP のプロービングを統合。 -ldap フラグを使用してドメインをマッピングし、 -sub を使用して特定のサブネットをターゲットにします。
発見	アカウント検出: ドメインアカウント	AdFind と DonPAPI を使用して、ドメイン管理者の認証情報と DPAPI で保護された秘密情報を収集します。
水平展開	SMB/Windows 管理者共有	ネットワーク共有への自動拡散。Impacket （wmiexec）モジュールを使用して、ネットワーク上を「ファイルレス」で移動します。

漏出	クラウドリポジトリへのデータ流出	暗号化の前に、機密データ（PDF、SQL、Docx）を Mega[.]nz または AWS S3 バケットに移動するために、Rclone または Rsync をデプロイします。
インパクト	データの暗号化	ECDH（Curve25519） + AES/ChaCha20 を使用します。速度向上のため、断続的暗号化（5MB を超えるファイルの 20%）を実装しています。
インパクト	システム回復を阻害する	vssadmin delete shadows /all /quiet を実行し、SHEmptyRecycleBinA を使用してごみ箱をクリアします。

【優先的に実施すべき対策】

DevMan の攻撃特徴や TTP を考慮した観点より、以下に優先的に行うべき三つの対策例とその理由を整理します。

1. **認証情報の保護**
   - 多要素認証（MFA）の導入
   - 強固なパスワード管理（使い回し防止・定期変更）

   攻撃者は「正しい ID とパスワードで入り込む」ことを攻撃の起点にしているため、入口を突破されないようにすることが重要です。

2. **新旧脆弱性の対策**
   - VPN やサーバーの定期アップデート（パッチ適用）
   - 古いシステムや未修正の弱点の洗い出し
   - 不要な外部公開サービスの停止

   攻撃者は古い脆弱性も含めた調査を行い、侵入を図るため、最新パッチのみならず、過去の脆弱性の見落としも含めて精査・対応が必要です。

3. **内部の監視と早期検知**
   - 不審なログインや権限変更の監視
   - 院内ネットワーク内の不自然な動きの検知
   - エンドポイント監視（EDR 等）の導入

   攻撃者は侵入後、静かに内部を調べて一気に拡大することから、「気づいた時には全体停止」という事態になります。そのため、侵入されたとしても早めに検知すべく監視を行う必要があります。

以上