脅威アクタープロフィール；Qilin

[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】

Qilin Ransomware （旧称 Agenda ）は、世界で最も蔓延している RaaS(Ransomware-as-a-Service)の脅威へと進化を遂げ、医療分野を含む世界中の重要セクターを標的とした、高圧的な二重脅迫攻撃を専門としています。
2025 年から 2026 年にかけての Qilin の活動は、モジュール式の Rust ベースの暗号化ツール、カーネルレベルのセキュリティ防御を回避するための BYOVD（脆弱なドライバーの持ち込み）の積極的な利用、そして認証情報収集のための悪質なブラウザ拡張機能の展開を特徴としています。
Windows 環境と VMware ESXi 環境の両方を標的とすることで、Qilin は最大限の運用麻痺を実現します。彼らの戦略は、綿密な偵察と脅迫戦術を組み合わせたものであり、世界的なデータプライバシーと組織の継続性に対する重大なリスクとなっています。

【概要】

2026 年初頭現在、Qilin（別名 Agenda）は、世界で最も活発かつ洗練されたランサムウェア・アズ・ア・サービス（RaaS）事業の一つとして確固たる地位を築いています。
当初は中規模レベルの脅威として出現しましたが、2024 年後半から 2025 年初頭にかけて LockBit や ALPHV/BlackCat といった大手競合他社の台頭により、市場は急速に拡大しました。
このグループは 2022 年 7 月に Agenda era という偽名で出現し、当初は Go（Golang）で記述されたランサムウェアペイロードを展開していました。
この初期段階は短命に終わり、2022 年 9 月には Qilin にリブランディングし、大規模な脅威として台頭し始めました。2022 年 12 月、グループがランサムウェアを Rust で書き換えたことにより、技術的な転換点を迎えました。
この移行により、Windows、Linux、VMware ESXi 環境を横断したクロスプラットフォーム攻撃の効率化が実現し、従来のセキュリティソフトウェアによる検知は大幅に困難になりました。
ランサムウェア・アズ・ア・サービス（RaaS）プラットフォームである Qilin は、通常、自ら攻撃を行うことはありません。その代わりに、多様なアフィリエイトネットワーク（実際にネットワーク侵入を実行する独立したハッカーグループ）のソフトウェアプロバイダーとして機能します。

脅威アクタープロフィール；Qilin

グループの活動を通じて、以下の注目すべき関連会社が特定されています。

- **Scattered Spider（Octo Tempest）**： 2024 年後半から 2025 年にかけて、MGM/Caesars 攻撃で知られるこの悪名高いグループは、Qilin の Rust ベースの暗号化ツールを活用し始めました。彼らは高度なソーシャルエンジニアリング（ヴィッシング）とクラウド/SaaS 環境を標的とすることで知られています。
- **Moonstone Sleet（北朝鮮/APT）**： 2025 年初頭、マイクロソフトは北朝鮮の国家支援を受け、Qilin ランサムウェアを展開していたこのアクターを特定しました。これは、国家が犯罪基盤を利用して政権の収益を得るという、稀有な「ハイブリッド」脅威です。
- **FIN12 (DEV-0237)** ::医療現場への迅速な攻撃を専門とする、金銭目的のグループ。Qilin の前身である Agenda を早期に導入し、高圧的な医療恐喝の専門知識を活かして、Qilin の中核関連組織として活動し続けた。
- **STAC4365** ：サプライチェーンを専門とする研究者によって追跡されている。この関連組織は、 2025 年 1 月に大手マネージドサービスプロバイダー（MSP）を侵害し、単一のアクセスポイントを利用して下流の被害者 28 人を同時に感染させたキャンペーンに関与していた。

【活動地域】:

成功した侵入の約 55%は米国に拠点を置く組織を標的としています。残りの攻撃は主にフランス、英国、ドイツ、スペインといったヨーロッパに集中しています。2025 年には、主に韓国と日本を中心とするアジア太平洋地域での攻撃が急増し、この地域は最も急速に活動を拡大した地域となりました。

【攻撃対象産業】

:医療、製造、専門サービス、卸売・小売、公共部門。

【攻撃技術の分析結果】

- 技術的には、Qilin（Agenda） の活動は、低レベルのシステム操作と信頼できる環境の悪用による回避を優先する、高度にモジュール化された「サービス指向」のアーキテクチャを特徴としています。
- Go から Rust ベースのバイナリ（具体的には「Qilin.B」バリアント） への移行により、静的分析やリバース エンジニアリングに対するペイロードが大幅に強化され、Windows および VMware ESXi ハイパーバイザーに対するシームレスなクロスプラットフォーム攻撃が可能になりました。
- 彼らの活動は、カスタムビーコンを使用して動的 API 解決により EDR をバイパスし、偵察のための長い「滞留時間」を特徴としています。
- 中核となる技術的シグネチャは、BYOVD（Bring Your Own Vulnerable Driver）戦術です。

これは、カーネルレベルのアクセスを許可し、セキュリティプロセスを終了させます。Qilin は、悪意のある Chrome 拡張機能を通じて GPO 主導の認証情報収集を行う先駆者でもあります。

- 最後に、マルチスレッド暗号化機能は、ハードウェア アクセラレーションによって速度を最適化し、多くの場合、セーフ モードでの再起動を強制し、フォレンジック ログを消去して、回復不可能な影響を最大限に与えます。
- 技術的には、Qilin (Agenda) の活動は、低レベルのシステム操作と信頼できる環境の悪用による回避を優先する、高度にモジュール化された「サービス指向」のアーキテクチャを特徴としています。

【攻撃特徴】

- **コアペイロードとマルウェア**
  - **The Encryptor (Go & Rust)**:もともと Go で書かれていましたが、グループは 2022 年後半に、より洗練された Rust バリアントに移行しました。Rust により、暗号化が高速化され、リバース エンジニアリングが困難になります。
  - **ローダー**: SmokeLoader や、NETXLOADER と呼ばれるカスタム .NET ベースのローダーなどのマルウェア ローダーを使用してペイロードを配信します。
  - **資格情報窃取マルウェア**: 2024 ～ 2025 年に彼らの武器庫に新たに加わるユニークなものとして、ブラウザーに保存されている資格情報を収集し、さらなるネットワーク侵害や将来の攻撃を容易にする PowerShell ベースのカスタム Chrome 拡張機能窃取マルウェアが挙げられます。
- **初期アクセスとエクスプロイト**
  - **フィッシング**:詐欺的な電子メールには、正規のツールのトロイの木馬バージョンが配信されることがよくあります。
  - **資格情報の不正使用**:特に MFA のない環境では、盗まれた VPN または RDP 資格情報が主な攻撃手段となります。
  - **悪用される一般的な脆弱性**: CVE-2024-21762 および CVE-2024-55591 (Fortinet)、CVE-2023-27532 (Veeam)、および CVE-2024-27198 (JetBrains TeamCity)。
- **横方向の移動と持続性**
  - **RMM ツール**:永続的なアクセスを維持するために、ScreenConnect、AnyDesk、Splashtop などのリモート監視および管理ツールを乗っ取ったりインストールしたりします。
  - **管理ツール**:ネットワークを移動するために、PsExec (多くの場合、ランダムな文字列に名前が変更されます)、WinRM、SMB、および WMI を頻繁に使用します。
  - **GPO 操作**: Qilin は、ドメイン コントローラー上のグループ ポリシー オブジェクト (GPO) を頻繁に変更して、ドメイン内のすべてのマシンにランサムウェアまたはスクリプトを自動的に展開します。
- **防御回避**

- **脆弱なドライバーの持ち込み** (BYOVD):通常、正規のドライバーを導入して脆弱なドライバーをカーネル レベルのアクセスを取得し、EDR およびウイルス対策ソフトウェアを強制的に無効にします。
- **ログの消去**:攻撃者は、痕跡を隠蔽するために専用のスレッドを使用して、Windows イベント ログと PowerShell 履歴を定期的に消去します。
- **Mimikatz**:埋め込みモジュールは、LSASS メモリをダンプし、より多くの資格情報を収集するために使用されます。

- **情報流出と恐喝**
  - **抽出ツール**: Rclone、WinSCP、FileZilla、Cyberduck、FreeFileSync を使用して、MEGA などのクラウド ストレージや専用のファイル共有サイト (easyupload[.]io など) にデータを移動します。
  - **「弁護士に電話」機能**: 2025 年に交渉ポータルに追加された独自の機能により、関連会社は「法律顧問」を呼び出し、データ漏洩の法的および規制上の結末を被害者に脅迫することができます。
  - **VSS 妨害**:他のランサムウェア グループと同様に、vssadmin[.]exe を使用してボリューム シャドウ コピーを削除し、被害者がバックアップなしでシステムを簡単にロールバックできないようにします。

【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
初期アクセス	公開アプリケーションを悪用する	CVE-2024-21762 (Fortinet)、CVE-2023-27532 (Veeam)、および CVE-2025-61882 (Oracle E-Business Suite) の積極的な悪用。
初期アクセス	スピアフィッシング添付ファイル	AI 生成の「ディープフェイク」メールとデジタル ツインを活用して、非常に説得力のあるフィッシング詐欺を作成します。
初期アクセス	有効なアカウント: ドメインアカウント	VPN および Citrix ポータルを対象とする初期アクセス ブローカー (IAB) から「ウォーム」アクセスを購入します。
初期アクセス	信頼関係	2025 年には、ScreenConnect などの RMM ツールを使用して複数のクライアントに同時にランサムウェアをプッシュする MSP レベルのサプライ チェーン攻撃が急増します。
実行	パワーシェル	svchost[.]js または PowerShell ローダーを実行して、ランサムウェアの Rust 亜種を展開します。
実行	クライアント実行のた	WSL (Windows Subsystem for Linux) を悪用して、

	めのエクスプロイト	Windows のみのセキュリティを回避し、Windows ホスト上で ELF (Linux) 暗号化プログラムを実行します。
実行	ネイティブ API	盗んだ資格情報を使用して LogonUserW を呼び出し、横方向の拡散のための正当なログオン セッションを作成します。
粘り強さ	レジストリ実行キー / スタートアップフォルダ	%Public% フォルダ内の enc[.]exe を指す 'aster' という名前の RunOnce エントリを作成します。
権限昇格	権限昇格のための悪用	BYOVD: 脆弱な署名付きドライバー (Zemana、Toshiba、TPwSav[.]sys など) を展開して、カーネルレベルで EDR/AV を強制終了します。
防御回避	防御を弱める: ツールを無効化/変更する	upd[.]exe (AV アップデータの偽装) を使用して avupdate[.]dll をサイドロードし、セキュリティ プロセスを終了します。
防御回避	防御を弱める: セーフモードブート	セキュリティ ソフトウェアが非アクティブな間に、システムをセーフ モードとネットワークで再起動してファイルを暗号化します。
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	PowerShell と wevtutil[.]exe を介して Windows イベント ログを大量にクリアします。
防御回避	難読化ファイル: ソフトウェアパッキング	Rust ベースの暗号化プログラムは高密度にパッケージ化されており、関数名の削除を使用してリバースエンジニアリングに抵抗します。
資格情報アクセス	OS 資格情報のダンプ: LSASS メモリ	統合された Mimikatz モジュールは、管理者権限を取得すると資格情報をダンプします。
発見	クラウドサービスダッシュボードの検出	SharePoint、O365、Azure ポータルを検索して、バックアップと機密データ リポジトリを見つけます。
横方向の移動	リモートサービス: SMB/Windows 管理共有	埋め込まれた PsExec モジュールを使用して、すべての Active Directory に参加しているホストにランサムウェアをコピーして実行します。
流出	Web サービス経由の漏洩: クラウドへの漏洩	Rclone と WinRAR を使用して、大量のデータ (多くの場合 1 TB 以上) を MEGA、EasyUpload、またはそれらのプライベート Tor ストレージに流出させます。
インパクト	影響度に応じて暗号化されたデータ	AES-256-CTR または ChaCha20(旧 CPU の場合)と RSA-4096 を使用します。「スキップステップ」暗号化をサポートし、極めて高速です。
インパクト	システム回復を禁止する	ボリューム シャドウ コピーを削除し (vssadmin[.]exe delete shadows /all /quiet)、最初にオフサイト バックアップをターゲットにします。

インパクト	内部の改ざん	GPO 経由でドメイン全体のデスクトップの壁紙を身代金メッセージに変更します。

【推奨対策】

- **防御回避に対する強化** :(特に BYOVD に対する): Microsoft の脆弱なドライバー ブロックリストを実装し、ドライバー署名の強制を実施し、EDR/AV に「改ざん防止」と「プロセス保護」を構成し、可能であればカーネル モード アクティビティを監視します。
- **ID およびアクセス管理**: Qilin は、機密データやバックアップコンソールを探すために、数週間（平均 19 日間）かけて水平方向に移動することがしばしばあります。多要素認証（MFA）を適用し、管理者アカウントとリモートアクセスアカウントにハードウェアトークンを導入し、特権アクセス管理（PAM）の一環としてジャストインタイム（JIT）アクセスを実装し、業務上必要のないワークステーションではコマンドおよびスクリプトインタープリター（PowerShell、WMI など）の実行を制限します。
- **GPO 監査:グループ ポリシー オブジェクトの変更**: 特に「実行」キー、スケジュールされたタスク、またはブラウザー拡張機能に影響する変更について、リアルタイム アラートを設定します。
- **脆弱性と攻撃対象領域の管理**:重要なパッチを優先し、Windows Subsystem for Linux (WSL) を無効にし、リモート監視ツールの使用を監査および制限します（「許可リスト」を使用して、会社が承認した RMM バージョンのみが実行できるようにします）。
- **データの復元力とバックアップ セキュリティ**:バックアップ サーバーがプライマリ Active Directory ドメインに参加していないことを確認し、エンドポイント ファイアウォール ルールまたは EDR ポリシーを使用して vssadmin[.]exe および wmic シャドウコピーのリモート実行をブロックすることで、VSS のリモート削除を無効にします。

【関連情報】

- https://www.halcyon.ai/threat-group/qilin

以上