2025年上半期ランサムウェア動向（金融業界）

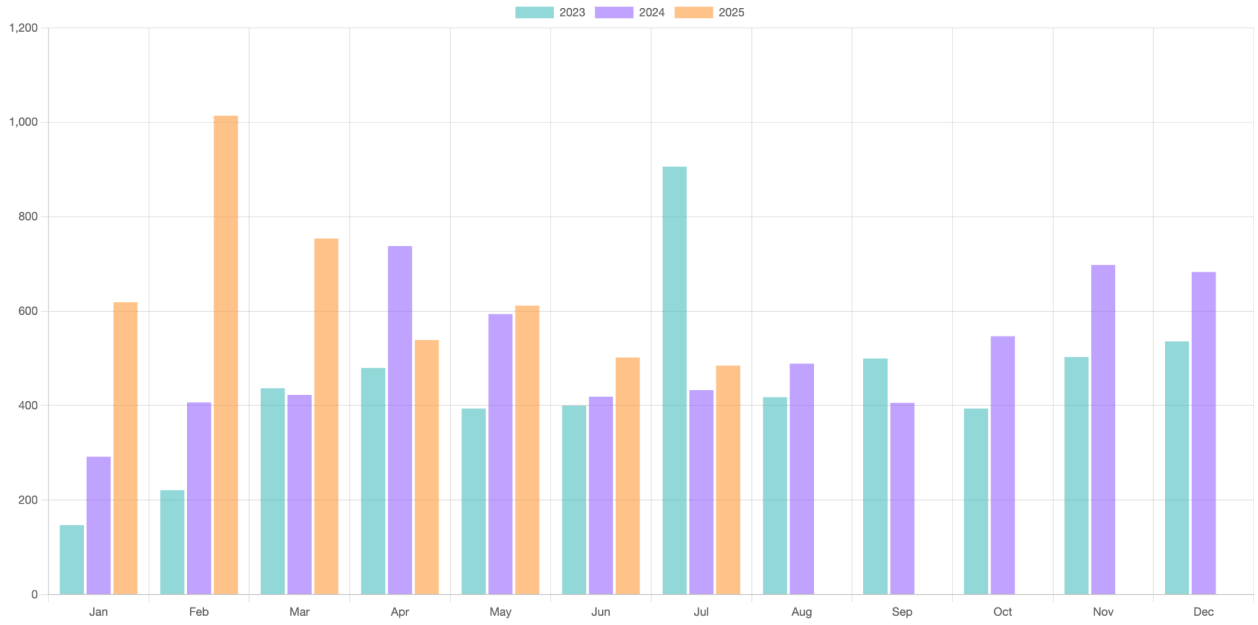
0. 概要

　2025年も上半期が過ぎましたが、国内や海外でもサイバー攻撃の件数は相変わらず増えていると思われます。以下では日本国内および海外の動向と、特に「金融業界」についての攻撃の傾向や、攻撃から守るための手段をピックアップしていきます。

1. 全世界でのランサムウェア動向

1-1. ランサムウェア被害数の傾向

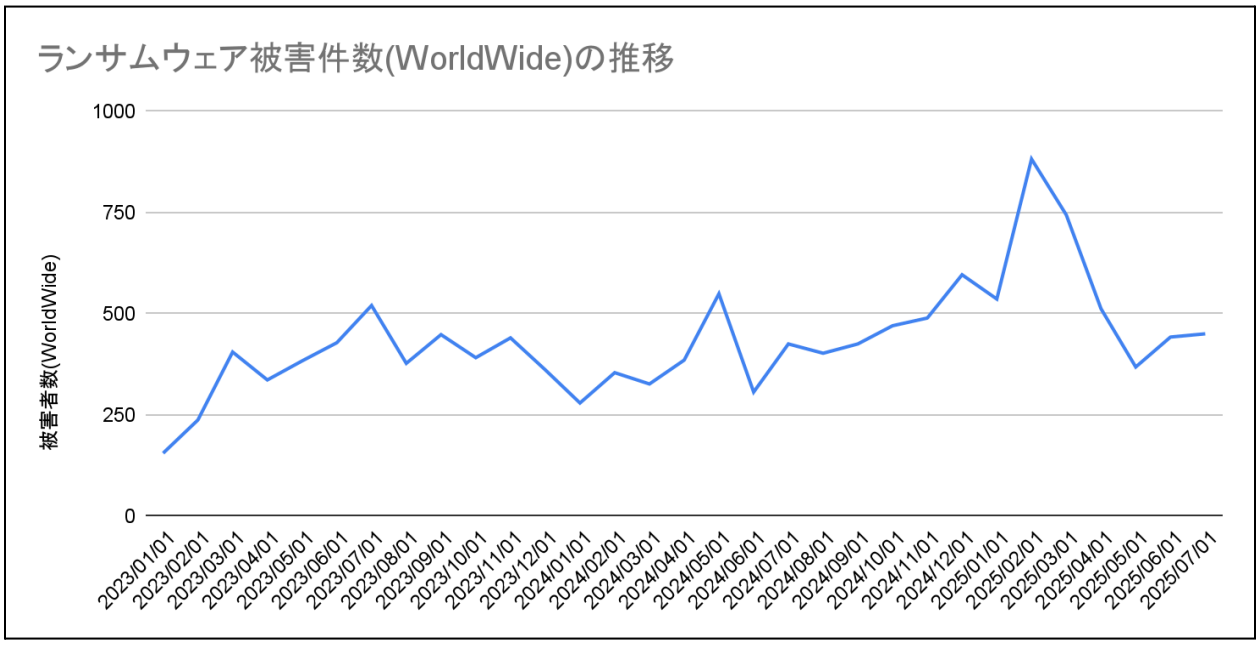
Ransomware.live（ランサムウェアグループの投稿を収集するツールを公開しているサイト）から全体的な傾向が出ています。



ほ

(Ransomware.liveより。2023-2025までのランサムウェア被害件数: 脅迫サイトに張り出された被害者数の推移)

また、BreachSense.com（ランサムウェアグループの投稿を収集するツールを公開しているサイト）で公開されていた情報を元に、2022年から2025年の被害件数をグラフにしたのが下記になります。

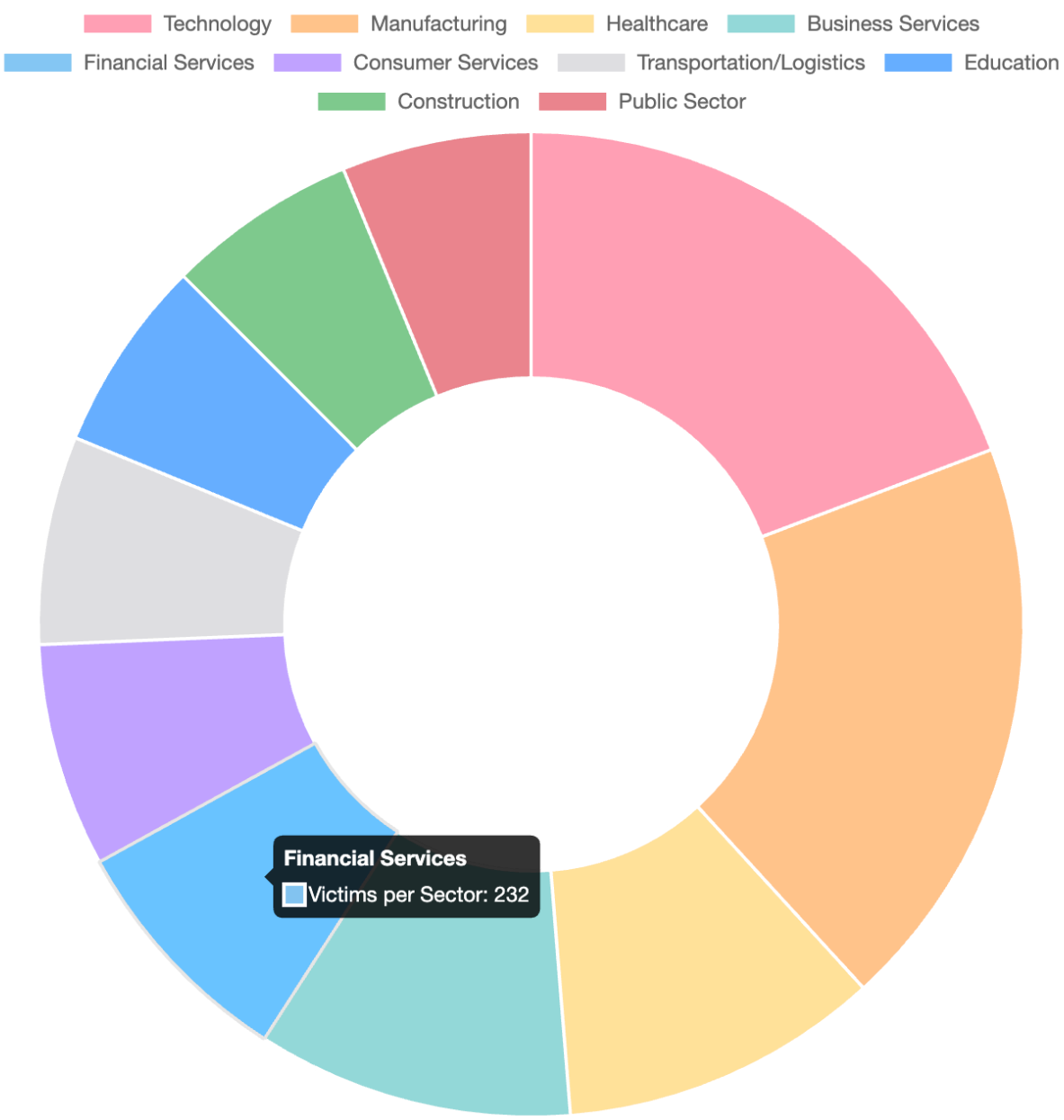


(Breachsense.comより。2023-2025までのランサムウェア被害件数: 脅迫サイトに張り出された被害者数の推移)

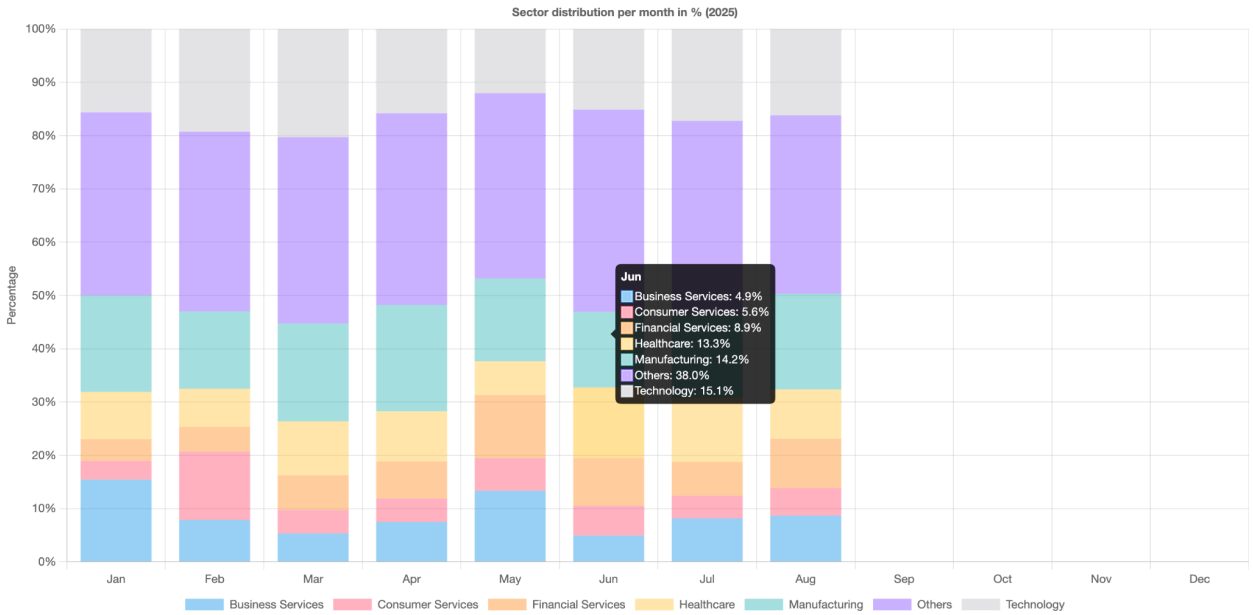
これらから、総じて2023年以降のランサムウェア被害件数は増加率は少ないものの、全体的に増加傾向にあることがわかります。

1-2. 業種の内訳

Ransomware.liveによると、2025年上半期全体での被害業種内訳（円グラフ）は以下になります。



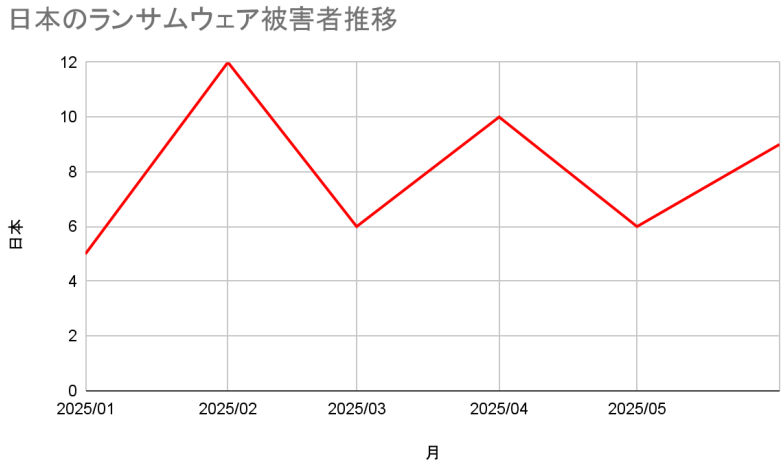
2025年のランサムウェア被害件数において各業種の内訳の推移は下記のようになっています。



月ごとでの差は見られますが、全体を通じて業種に偏り無く攻撃が行われている事がわかります。

1-3. 日本でのランサムウェア被害件数の動向

日本でのランサムウェア被害件数の推移は、以下の様になっています。

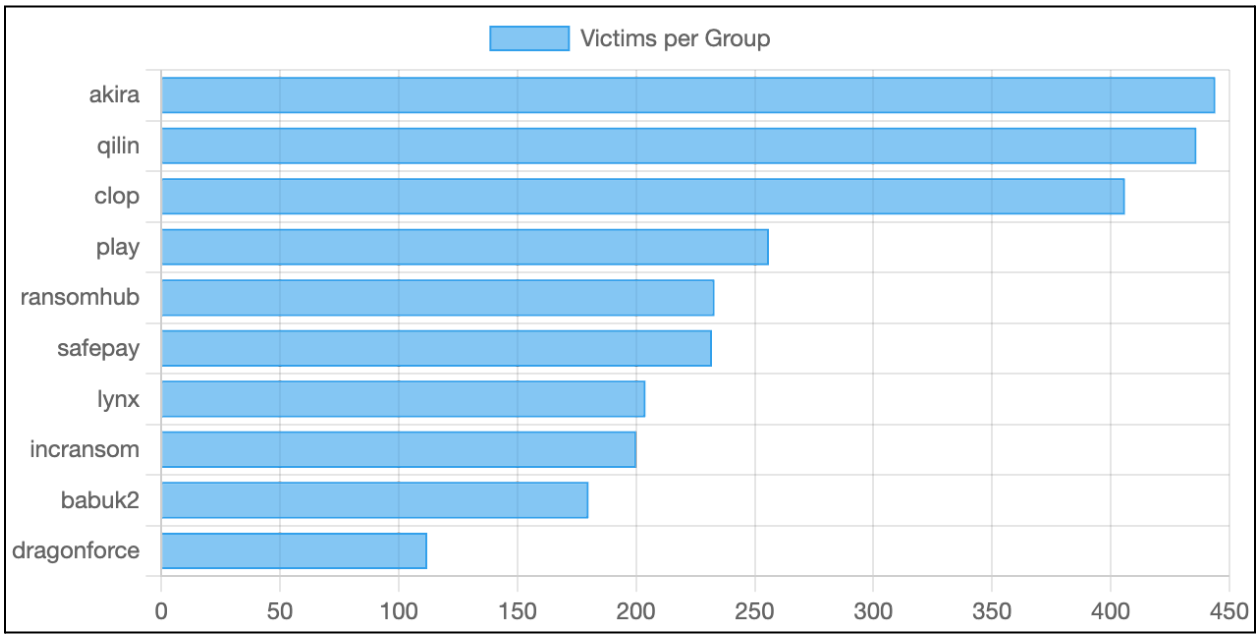


WorldWideからみると日本に対する攻撃は少ない状態ですが、毎月新たに脅迫が行われていることがわかります。

2. ランサムウェアグループの動向

2-1. 全体でのランサムウェアグループの動向

Ransomware.liveのデータによると、各ランサムウェアグループが2025年に被害を与えた件数のTop10は以下のようになっています。



後程各グループについても触れますが、やはりakira/qilin/clop等による被害件数が多くなっています。

2-2. 金融業界に影響を与えたランサムウェアグループ

2025年上半期に、特に「金融業界」に攻撃を加えた代表的なランサムウェアグループとしては

1. Luna Moth
2. Akira,
3. Ransomhub
4. Play
5. Funksec
6. Lynx
7. Medusa
8. KillSecurity
9. SafePay
10. Qilin

が挙げられます。

2-3. ランサムウェアグループの解説(**Top3/日本に被害が出てるもの**)

2-3-1. Luna Moth (Silent Ransom Group)

Luna Moth（別名：Silent Ransom Group、Chatty Spider、UNC3753）に関する情報は以下の通りです。

Welcome to [redacted]!

Your membership is now active

Confirmation #[redacted]

Billed to	[redacted]
Payment method	Credit Card
Subscription price	$79.99
Tax	$5.80
Total monthly payment*	**$85.79**

**After your trial, you'll automatically enroll onto our 40 credits per month plan. You can adjust your plan at any time. Current total is $85.79 including tax.*

Hi [redacted],

Your [redacted] account is prepared for you. Your personal number is [redacted].

Your subscription number is also your invitation code. Invite friends to [redacted] with your subscription number and get up to 3 free months with us.

Have any problems using your [redacted] subscription or want to cancel it? Just call our customer care support at **+1 (619) [redacted]**

You will be able to get each reservation's cancellation window when purchasing (it's usually 36 hours). If you cancel a subscription in time, we will not charge you, and the credits you used to book will automatically be returned to your account. If you cancel late, you won't be able to get a refund.

Always yours,

概要 (Overview)

Luna Mothは、2022年から活動しているサイバー脅威アクターです。このグループは、情報技術（IT）関連のソーシャルエンジニアリングコールや、コールバック型フィッシングメールを利用して、システムやデバイスへのリモートアクセスを獲得し、機密データを窃取した上で被害者を恐喝します。
彼らの攻撃は、暗号化を伴わない恐喝を特徴としており、被害者に数十万ドルの損害を与え、その範囲を拡大しています。従来のアンチウイルス製品に検出されにくいよう、正規のシステム管理ツールやリモートアクセスツールを使用しており、攻撃後の痕跡をほとんど残さないという特徴があります。彼らは、コールセンターや被害者ごとに固有のインフラに投資している、非常に組織化されたグループです。

攻撃対象 (Targets)

Luna Mothは、これまで様々な業界の企業を標的としてきました。

- 2023年春以降、特に米国の法律事務所を継続的に標的としています。これは、法務業界のデータの機密性が非常に高いことに起因すると考えられます。被害者の大半は法律事務所、またはそれに類似した名称を持つ企業です。
- また、医療業界や保険業界の企業も標的にしています。
- キャンペーンの初期段階では、法律業界の中小企業を標的にしていましたが、後に小売業の大規模な標的へと移行していることが観察されています。HPH（ヘルスケアおよび公共衛生）分野では、年間収益が50万ドルから1,000億ドルを超える組織、特に10億ドル以上の収益を持つ被害者が約40%を占めていました。

代表的な被害者 (Typical Victims)

- 米国の法律事務所。
- 医療業界および保険業界の企業。
- 中小規模の法律事務所、および大規模な小売業の企業。
- ヘルスケアおよび公共衛生（HPH）分野の、年間収益が高い組織。

TTP (戦術、技術、手順 - Tactics, Techniques, Procedures)

Luna Mothの攻撃は、主に以下の戦術、技術、手順を用いて行われます。

- 初期侵入 (Initial Access):
    - コールバック型フィッシングメール: 有名なサブスクリプションサービス提供企業を装ったメールを送信します。メールは少額の「サブスクリプション料金」を請求する内容で、不審を抱かれにくいように工夫されています。被害者は偽のサブスクリプションをキャンセルするため、メールに記載された電話番号に連絡するよう指示されます。このメールにはマルウェアが含まれておらず、正規のメールサービスから送信され、PDF形式の請求書が添付されるため、通常のメール保護システムによる検出を回避しやすいです。
    - IT部門を装ったソーシャルエンジニアリング電話: 2025年3月からは、従業員に電話をかけ、自社のIT部門の職員を装う新たな手口も観察されています。その後、従業員にリモートアクセスセッションに参加するよう指示します（メールでリンクを送るか、ウェブページへの誘導）。
- 実行と永続性 (Execution and Persistence):

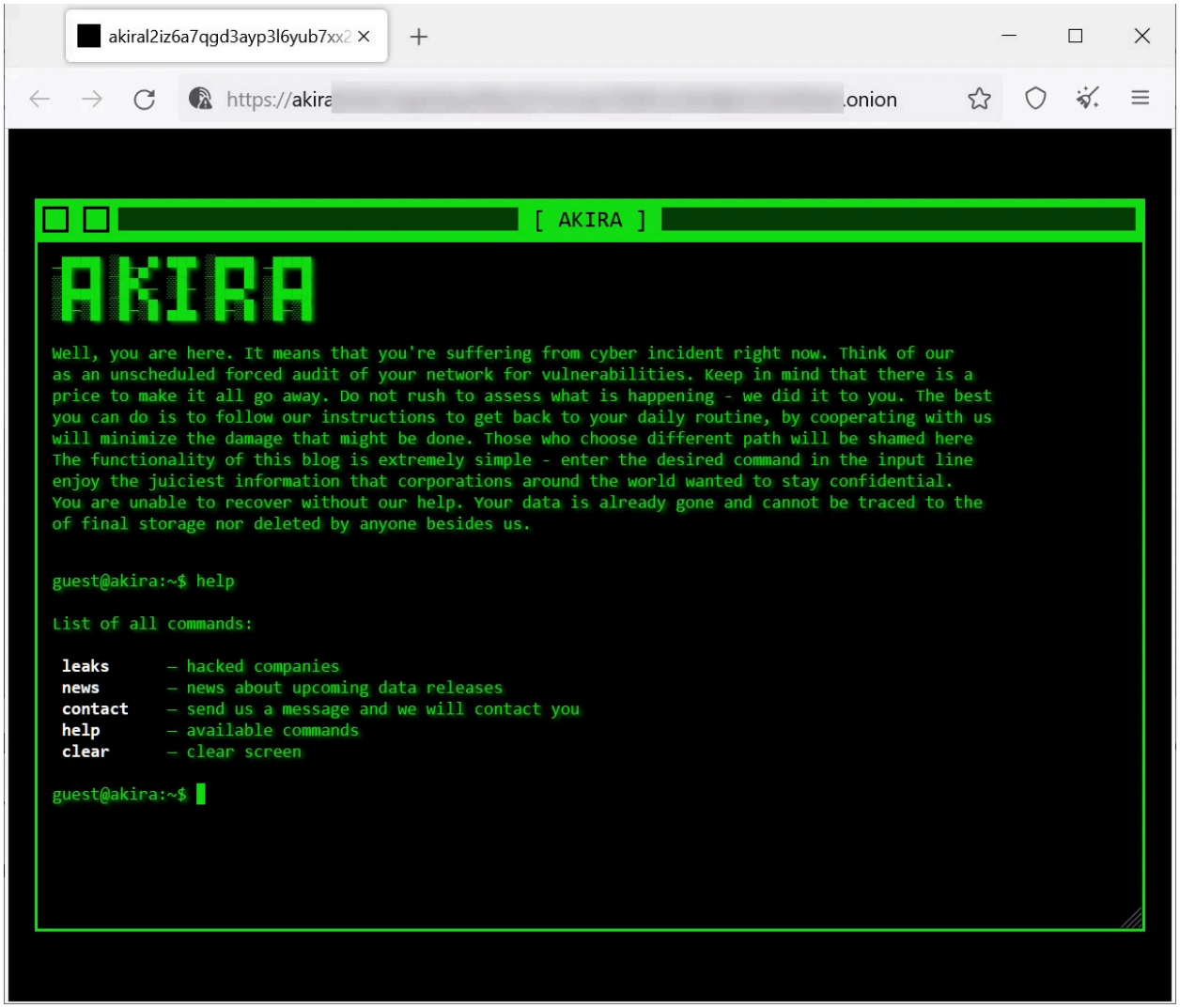
    - 被害者が電話をかけると、脅威アクターが運営するコールセンターに繋がり、オペレーターが対応します。オペレーターは、サブスクリプションのキャンセルを口実に、被害者にリモートサポートツール（例：Zoho Assist、Syncro、AnyDesk、Splashtop、Atera）をダウンロード・実行させます。
    - リモートアクセスを許可されると、アクターはキーボードとマウスを操作し、クリップボードアクセスを有効にし、画面を空白にしてその活動を隠します。
    - その後、Syncroのようなリモート管理ツールをインストールして永続的なアクセスを確立します。
    - 被害者のコンピューターに管理者権限がない場合、アクターは管理者権限を必要としないWinSCP Portableをダウンロード・実行し、永続的なソフトウェアのインストールをスキップします。
- データ窃取と流出 (Data Theft and Exfiltration):
    - アクセス確立後、脅威アクターは被害者のデバイスや接続されたファイル共有から価値のある機密データを特定します。
    - データの流出は、WinSCP (Windows Secure Copy) または隠蔽・改名されたRcloneを介して行われます。
    - 永続的なアクセスが確立された場合は数時間から数週間後に、確立されていない場合は通話中にデータ流出が実行されます。
- 恐喝 (Extortion):
    - データ窃取後、アクターは身代金要求メールを送信し、要求が満たされない場合、データをオンラインで販売または公開すると脅迫します。
    - 被害企業の従業員に直接電話をかけ、身代金交渉に応じるよう圧力をかけることもあります。
    - 被害者データを公開するためのサイトを所有していますが、常に公開するとは限りません。
    - 身代金要求額は、被害組織の収益を調査して決定され、2〜78 BTCの範囲で変動します。迅速な支払いに対しては約25%の割引を提示することもあります。
    - 支払ったとしても、データの削除証明が提供されないなど、約束が履行されないケースも報告されています。
    - さらに、窃取したデータから特定した被害者の顧客やクライアントに連絡すると脅迫し、圧力を高めることもあります。

使っている脆弱性 (Exploited Vulnerabilities)

提供された情報源には、Luna Mothが特定のソフトウェアの既知の脆弱性を悪用しているという明確な記述はありません。むしろ、彼らは攻撃において正規のシステム管理ツールやリモートアクセスツールを使用しているため、従来のアンチウイルス製品による検出を回避しやすいとされています。彼らの攻撃は、マルウェアの使用を最小限に抑え、ソーシャルエンジニアリングの技術に大きく依存することで、検出を避け、効果を最大化しています。

2-3-2. akira

Akiraランサムウェアについて、以下に概要、攻撃対象、代表的な被害者、TTP（戦術、技術、手順）、および使用された既知の脆弱性を日本語でまとめました。



概要 (Overview)

Akiraは、2023年3月に活動を開始した**RaaS (Ransomware as a Service)** グループです。彼らは二重恐喝モデルを採用しており、データを暗号化する前に窃取し、身代金が支払われない場合は盗んだデータを公開すると脅迫します。当初はWindowsシステムに焦点を当てていましたが、2023年4月以降、VMware ESXi仮想マシンを標的とするLinux版も展開しています。2024年1月1日時点で、Akiraランサムウェアグループは250を超える組織に影響を与え、約4,200万ドル（USD）の身代金を得たとされています。初期のAkiraランサムウェアはC++で書かれ、ファイルに**.akira拡張子を付与しましたが、**2023年8月**からは**Rust**ベースのコードを使用するMegazordを展開し、ファイルに.powerranges**拡張子を付与する攻撃も行っています。Akira_v2と呼ばれる改良版も確認されており、Rust言語で書かれているため、追加機能や暗号化プロセスの速度と効率の向上が見られます。

Akiraは、活動を停止した**Conti**グループとの関連性が示唆されており、コードの重複や資金の混交が見られます。

攻撃対象 **(Targeted Industries)**

Akiraは、幅広い業種や重要インフラに影響を与えています。標的とされた業種は無差別に広範にわたり、以下の例が挙げられます:

- 自動車 (Automotive)
- エネルギー (Energy)
- 教育 (Education)
- IT (Information Technology)
- 航空会社 (Airlines)
- 金融サービス (Financial Services)
- 政府機関 (Government)
- 医療 (Healthcare)
- 製造業 (Manufacturing)
- 不動産 (Real Estate)

特に、Akiraは米国の医療・公衆衛生（**HPH**）分野を標的とする最も活発なランサムウェアグループの第**4**位に挙げられています。

代表的な被害者 **(Typical Victims)**

Akiraは主に北米、ヨーロッパ、オーストラリアの企業や組織に影響を与えています。グループのリークサイトによると、196以上の組織が感染したと報告されています。

TTP (戦術、技術、手順**)**

Akiraランサムウェアのアクターが使用する主なTTPは以下の通りです:

- 初期アクセス **(Initial Access) [T0001]:**
    - 多要素認証（**MFA**）が設定されていない**VPN**サービスを介して初期アクセスを獲得します。
    - **Cisco**の既知の脆弱性（CVE-2020-3259およびCVE-2023-20269）を悪用します。
    - Remote Desktop Protocol (RDP) [T1133] の使用。
    - スピアフィッシング（悪意のある添付ファイルやリンク付き）[T1566.001, T1566.002]。
    - 有効な認証情報 [T1078] の悪用。
- 永続性 **(Persistence) [T0003]:**
    - 新しいドメインアカウントの作成 [T1136.002]（例: `itadm`という管理アカウント）。
    - スケジュールされたタスク、侵害された有効なアカウント、ショートカットの変更、レジストリの実行キー/スタートアップフォルダの利用。
- 探索 **(Discovery) [T0007]:**
    - ドメインコントローラー機能の悪用。

    - Kerberoasting [T1003.001] によるLocal Security Authority Subsystem Service (LSASS) のプロセスメモリに保存された認証情報の抽出。
    - MimikatzやLaZagneといった認証情報スクレイピングツール [T1003] の使用。
    - SoftPerfectやAdvanced IP Scanner [T1016] などのネットワークスキャナーを用いたネットワークデバイスの探索。
    - `net` Windowsコマンドを使用してドメインコントローラー [T1018] やドメイン信頼関係 [T1482] の情報を収集。
    - AdFind、PCHunter64 [T1082]、SharpHound、MASScan、`Get-ADUser`、`Get-ADComputer`の利用。
- 防御回避 **(Defense Evasion) [T0005]:**
    - 検出を避けるためにセキュリティソフトウェアを無効化します。例えば、PowerToolを使用してZemana AntiMalwareドライバー を悪用し、アンチウイルス関連のプロセス [T1562.001] を終了させます。
    - 同じ侵害イベント内で、Windows特有の「Megazord」と「Akira_v2」ESXi暗号化プログラムという**2**種類のランサムウェアを同時に展開する。
    - ログイン画面でアカウントを隠すためのユーザーリストレジストリ変更や、認証情報なしでのログインを許可するためのDisableRestrictedAdminレジストリ変更。
    - BYOVD攻撃を実行するためのTerminatorの利用。
- データ窃取 **(Exfiltration) [T0010]:**
    - FileZilla、WinRAR [T1560.001]（圧縮用）、WinSCP [T1048]、RClone [T1567.002] などのツールを使用。
    - File Transfer Protocol (FTP)、Secure File Transfer Protocol (SFTP)、Megaなどのクラウドストレージサービス [T1537] を介した窃取。
- インパクト **(Impact) [T0040]:**
    - 二重恐喝モデル [T1657] を使用し、データを暗号化する前に窃取します。
    - システムを暗号化 [T1486] します。ファイルには**.akiraまたは.powerranges**拡張子が付与されます。
    - Windowsシステム上でボリュームシャドウコピー **(VSS)** を削除するためにPowerShellコマンド [T1490] を利用します。
    - 身代金要求メモ「`fn.txt`」がルートディレクトリと各ユーザーのホームディレクトリに表示されます。
    - Akira_v2の暗号化プログラムはRustで書かれており、CPUコアの使用数や暗号化プロセスの速度と効率をより細かく制御できる機能を持っています。また、「`vmonly`」による仮想マシンのみの展開や、「`stopvm`」による実行中の仮想マシンの停止機能も確認されています。
    - Veeamバックアップの削除。
- コマンド＆コントロール **(Command and Control) [T0011]:**
    - AnyDesk [T1219]、MobaXterm、RustDesk、Ngrok [T1090]、Cloudflare Tunnelなどの一般的なツールを使用。

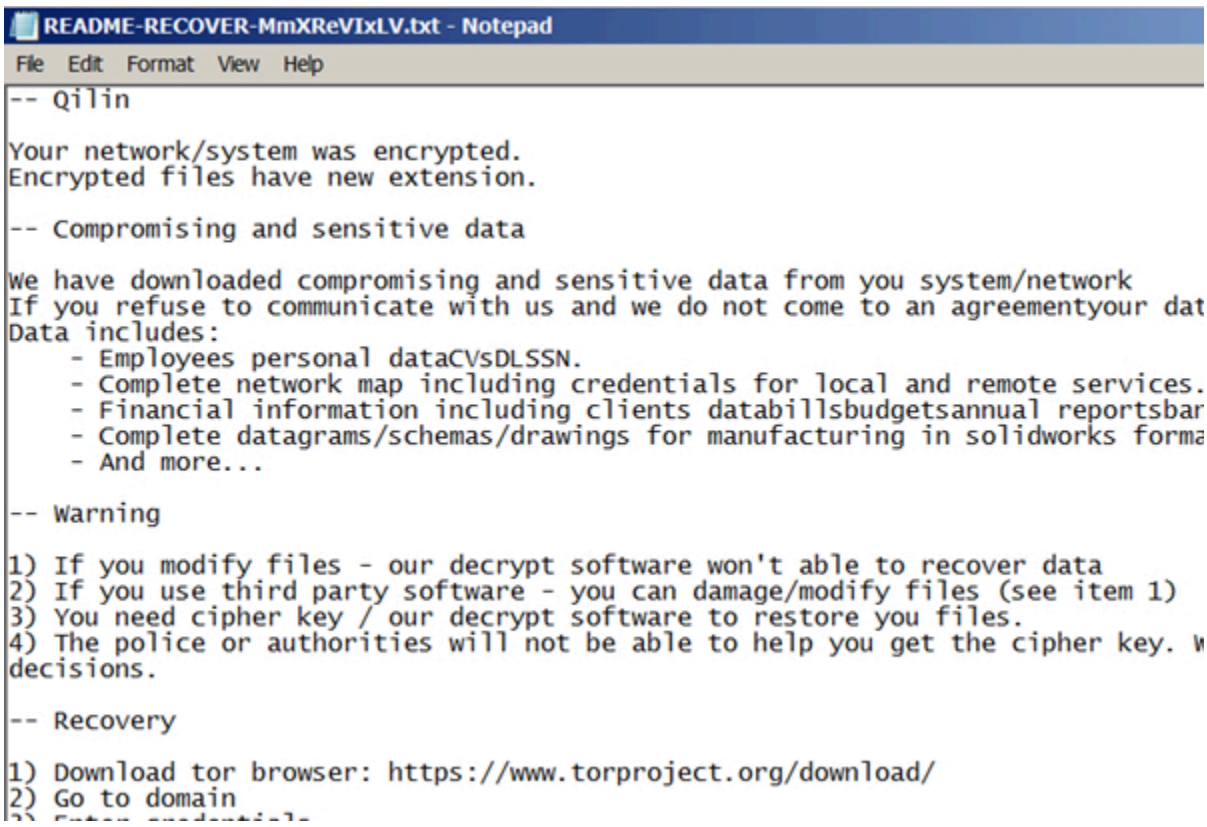
使っている脆弱性 **(Vulnerabilities Used)**

Akiraランサムウェアのアクターが初期アクセスに利用している既知の脆弱性は以下の通りです:

- **CVE-2020-3259:** Cisco Adaptive Security Appliance (ASA) および Firepower Threat Defense (FTD) ソフトウェアのSSL VPNサービスにおけるサービス拒否の脆弱性。
- **CVE-2023-20269:** Cisco ASA および FTD ソフトウェアのリモートアクセスVPN認証バイパスの脆弱性。
- **CVE-2021-21972:** VMware vCenter Server 脆弱性。
- **CVE-2019-6693:** F5 BIG-IP 認証バイパス脆弱性。
- **CVE-2022-40684:** Fortinet FortiGate FortiProxy FortiAuthenticator 認証バイパス脆弱性。
- **CVE-2024-40766:** SonicWall SonicOS リモートコード実行の脆弱性。
- **CVE-2024-37085:** VMware ESXi 権限昇格の脆弱性。
- **CVE-2024-40711:** Veeam Backup & Replication Mount Service 権限昇格の脆弱性。

2-3-3. Qilin

Qilinに関する情報について、以下の通りにまとめました。



概要 **(Overview)**

Qilinは、現在世界で最も活発かつ影響力のあるランサムウェアオペレーションの1つであり、**ランサムウェア・アズ・ア・サービス（RaaS）**として運営されています。

- 起源と変遷: 2022年に「Agent」として開発され、後にRustで再コーディングされました。2022年7月に「Agenda」として運用が開始され、同年9月にはQilinに改名されました。Dark Webの「BianLian」という人物が最初に開発したとされています。
- 流行と現状: 2023年後半には、VMware ESXiインフラストラクチャへの標的型攻撃を通じて人気を獲得しました。2024年にはChrome Stealer機能や堅牢な暗号化・回避戦術を拡大し、2025年には公開されている脅威インテリジェンスレポートで最も普及しているランサムウェアとしてランク付けされています。2024年だけで**5,000**万ドル以上の身代金支払いを得ています。
- 運用モデル: クライアント向けの「Call Lawyer」といった法的サポート、成功した身代金支払いに対するインセンティブと技術など、強固な運用モデルに支えられています。アフィリエイトは、攻撃の収益の15〜20%を受け取ります。
- 言語と所属: 「BianLian」はロシア語と英語の両方で、特にロシアのダークウェブフォーラムでコミュニケーションを取っているのが確認されています。Qilinのマルウェアは、独立国家共同体（CIS）のシステムを標的にしないように設計されており、これはロシアのサイバー犯罪ネットワークと関連する脅威アクターに共通する特徴です。これらのパターンは、ロシア語を話す個人またはグループがQilin RaaSの運営に関与していることを強く示唆しています。Microsoft Threat Intelligenceによると、2024年には北朝鮮の国家アクターである「Moonstone Sleet」もアフィリエイトに含まれるようになりました。
- 二重恐喝: Qilinは、被害者のデータを高速で堅牢に暗号化し、バックアップを削除するだけでなく、データを窃取して二重恐喝を行います。身代金が支払われた後でも、盗んだデータを公開すると脅します。

攻撃対象 **(Targeting Patterns)**

Qilinは、身代金が支払われる可能性が高い3つの主要な垂直分野を戦略的に標的にしています。

- 業界:
    - 製造業
    - 法務・専門サービス
    - 金融サービス
    - 医療
    - 政府機関
    - その他、小売、メディア・ゲーム、石油・ガス、建設・エンジニアリング、テクノロジーなども標的となっています。
- 組織規模: 重要インフラや、大規模な資金力を持つ組織を定期的に標的にしています。彼らは、潜在的な身代金額を事前に見積もるオンラインウェブサイトを利用して、高価値の金融機会に焦点を当てています。小規模な組織も被害に遭っており、どの企業も免れないことを示しています。
- 地理: これまでに25か国以上で攻撃が確認されています。2023年5月には、オーストラリア、ブラジル、カナダ（2件）、コロンビア、フランス、オランダ、セルビア、英国、日本、米国（2件）の12社のデータがQilinのDLSに掲載されていました。米国、英国、カナダ、オーストラリアなど、様々な国の組織が標的となっています。

- システム: VMware ESXiインフラストラクチャ、Windowsマシン、Linuxバージョンも標的となります。

代表的な被害者 **(Notable Victims)**

Qilinの活動は、グループのDLSに被害者データを投稿することにまで及んでいます。

- **2023**年:
    - **Yanfeng Automotive Interiors**: 2023年11月28日に、世界最大の自動車部品サプライヤーの1つであるYanfeng Automotive Interiorsに対するサイバー攻撃の責任を主張しました。
- **2024**年:
    - 米国: Upper Marion Township, Etairos Health, Kevin Leeds, CPA, Commonwealth Sign (2月)。International Electro Mechanical Services (3月)。
    - マレーシア: Felda Global Ventures Holdings Berhad (3月)。
    - サウジアラビア: Bright Wires (3月)。
    - インドネシア: PT Sarana Multi Infrastruktur (Persero) (3月)。
    - スペイン: Casa Santiveri (3月)。
    - 英国: 2024年6月3日には、英国を拠点とする病理診断サービスプロバイダーがQilinランサムウェア攻撃の被害に遭い、ロンドンの複数の主要病院で医療サービスに影響が出ました。
- **2025**年:
    - 米国: 2025年7月1日には、米国の金融アドバイザリー会社がQilinランサムウェア攻撃を受け、機密性の高いデータ約340GBが窃取されたとされています。
- 医療・公衆衛生(**HPH**)セクターへの影響: HC3は、2022年10月以降、世界中で少なくとも15件のQilin/Agendaランサムウェア関連インシデントを確認しており、その約半分が米国のHPHセクター組織に影響を与えています。米国のHPH被害組織の収益は600万ドルから4000万ドルに及んでいます。

TTP (Tactics, Techniques, and Procedures)

Qilinは、標的への影響を最大化するために、被害者ごとに攻撃を調整することがよくあります。

- 初期アクセス **(Initial Access)**:
    - スピアフィッシング: 悪意のあるリンクを含むフィッシングメールを通じて、被害者のネットワークに侵入し、機密データを窃取します。
    - リモート監視・管理(**RMM**)ソフトウェアの悪用: ScreenConnectなどのRMMツールを悪用して、組織の顧客にダウンストリーム攻撃を開始します。
    - 多要素認証(**MFA**)ボンビング、**SIM**スワップ。
    - 公開アプリケーションの悪用: CitrixやRDPなど、公開されているアプリケーションやインターフェースも悪用します。

- 実行と伝播 **(Execution and Propagation)**:
    - QilinはPowerShellやコマンドラインインタープリターイベントを含む様々なスクリプトを実行します。
    - 横方向移動: 初期アクセス後、Qilinは通常、被害者のインフラ内で横方向へ移動し、暗号化に必要なデータを探します。
    - ツール: PsExecやSecureShellを介して実行ファイルを伝播させる能力を持ち、Cobalt Strikeをバイナリの展開に使用します。アフィリエイトはSmokeLoaderや新しい.NETローダー（NETXLOADER）も使用しています。
    - データの収集と圧縮: 攻撃者はWinRARを使用して複数の顧客環境からファイルを収集し、データを圧縮します。
- 暗号化の強化 **(Encryption Enhancements)**:
    - Rust版は、回避されやすく解読が困難な特性があり、Windows、Linux、その他のOS向けにマルウェアをカスタマイズしやすいため、ランサムウェア攻撃に特に効果的です。
    - AES-256-CTR、Optimal Asymmetric Encryption Padding (OAEP)、AES-NI (x86アーキテクチャ向け) などの暗号化標準を使用します。
    - 現代的で高速かつ安全なストリーム暗号通信のためにChaCha20も使用します。
    - 暗号化されたファイルのファイル名拡張子の変更、特定のプロセスやサービスの終了、様々な暗号化モードのサポートなど、カスタマイズオプションを提供します。
    - 各被害者には独自の32文字のパスワードと、ランサムウェアメモに独自のチャットIDが割り当てられます。
- 防御回避と影響 **(Defense Evasion and Impact)**:
    - 証拠の削除: Windowsイベントログをクリアし、自身の実行ファイルを削除して、フォレンジック調査やインシデントレスポンスを妨害します。
    - バックアップの破壊: Windows Volume Shadow Copy Service (VSS) のバックアップを削除し、復旧を妨害して身代金支払いを強制します。
    - アンチウイルスソフトウェアの終了を試みたり、プロセスインジェクションを実行したり、レジストリに変更を加えて永続化を図ったりします。
    - ブートオプションをSafe Mode with networkingに変更し、エンドポイントセキュリティを回避します。
    - コードの難読化、関数の名前変更、制御フローの変更、文字列の暗号化などの方法を用います。
- データ窃取と流出サイト **(Data Exfiltration and Leak Sites)**:
    - 攻撃者がWinRARでデータを収集した後、IncognitoタブでGoogle Chromeを介して**easyupload.io**に.rarファイルを窃取しました。
    - Tor上でデータ漏洩サイト（DLS）を運用し、被害者に圧力をかけます。
    - 2024年5月には、Qilinランサムウェアに関連する脅威アクターが「WikiLeaksV2」というデータ漏洩サイトを公開インターネット上に開設しました。

使用している脆弱性 **(Vulnerabilities Used)**

Qilinは、過去に以下の脆弱性を悪用しています。

- **CVE-2023-27532**: Veeam Cloud Backupサービスの脆弱性で、非認証ユーザーがローカルのVeeam設定データベースから暗号化されていない資格情報を要求できるものです。これはMITRE ATT&CK ID T1190の一部として悪用されました。

4. 代表的な被害事例

4-1. 国内（三つ以上）

1. 証券口座乗っ取り事件

証券口座の乗っ取り問題について、経緯、被害状況、原因をまとめました。

証券口座乗っ取り問題の概要

証券口座の乗っ取りは、近年増加しているサイバー犯罪の一種で、顧客の口座が不正に操作され、意図しない株式売買が行われる被害が多発しています。

経緯

- 被害の発覚と拡大:
    - 2025年1月以降、証券口座のIDやパスワードが盗まれ、身に覚えのない株式などの売買が行われる被害が相次いで確認されています。
    - この問題は、楽天証券や野村証券など、大手・中堅・ネット証券を問わず広がり、確認された証券会社は一時**17**社に上りました。
    - 金融庁や日本証券業協会（日証協）が事態を重視し、金融担当大臣からも証券会社への補償対応が指示されました。
- 補償対応の進展:
    - 被害者への補償を巡っては、大手証券4社が顧客に明確な過失がない場合、株式を買い戻すなどの方針を示しました。
    - GMOクリック証券は、2025年8月5日にインターネット証券として初めての全額補償を発表しました。被害者には市場で保有していた株式を買い戻すよう依頼し、同社が購入代金を支払います。6月以降の不正売買被害は確認されておらず、5月までに被害にあった顧客が補償の対象とされています。
    - SBI証券、楽天証券、松井証券といった大手ネット証券は、7月25日に原則として被害額の2分の1を補償すると発表しました。対面大手証券の方針決定から約1カ月遅れたのは、金融庁との対話の不調が背景にあったとされています。
    - 三菱UFJモルガン・スタンレー証券やみずほ証券などの対面大手5社は、不正に売却された株の返還（原状回復）を決めています。

    - 日本証券業協会は、顧客への補償方針が未定の会社に対し、早期の対応を求めています。
- 対策の強化:
    - 日本証券業協会は、2025年7月15日に「インターネット取引における不正アクセス等防止に向けたガイドライン」の改正案を公表し、フィッシングに耐性のある多要素認証の必須化などの項目を新たに盛り込みました。

被害状況

- 累計被害額:
    - 2025年1月から5月末までの期間では、不正売買額が**5,240**億円に達しました。
    - 2025年1月から6月末までの半年間では、不正取引による被害額は合計で**5,700**億円を超えました。内訳は、株式などの売却額が約3,044億円、買い付けられた金額が約2,666億円です。
    - 2025年1月から7月末までの期間では、不正取引金額が合計で約**6,205**億円に上っています。
- 件数:
    - 2025年1月から5月末までの不正アクセス件数は**10,422**件、不正取引件数は**5,958**件でした。
    - 2025年1月から6月末までの不正取引件数は**7,139**件でした。
    - 2025年1月から7月末までの不正アクセス件数は**14,069**件、不正取引件数は**8,111**件でした。
- 被害ペースの変化:
    - 単月で見ると、4月は2,932件、売買額2,915億円、5月は2,329件、売買額2,105億円でしたが、**6**月は件数が**783**件、売買額は**381**億円と、被害ペースが大幅に縮小しました。
    - 5月末から6月末にかけての累計増加率は、件数が12%増、売買額が7%増にとどまり、被害が沈静化の兆しを見せています。
    - 不正取引があった証券会社も、5月の16社から6月は7社に減少しました。
    - 新NISA口座も標的となっています。

原因

- 手口:
    - 主な手口は、日本の証券口座の認証情報を狙ったフィッシング詐欺です。
    - 被害者は証券会社を装ったメールやSMSを受信し、不安や緊急性を煽るメッセージとリンクから偽サイトへと誘導されます。
    - 偽サイトでログインID、パスワード、個人情報、さらには取引パスワードまで詐取されます。
    - 詐欺に使われるメール、SMS、偽サイトは非常に巧妙で、人間が見抜くことが困難なほど完成度が高いとされています。
    - 不正SMSの送信元は、国際電話番号や、モバイルマルウェアに感染した端末からの送信など、多岐にわたり、約84%が1日しか使われないなど、常に変化しています。
    - 詐欺メールは、デバイス設定やスマホ認証（FIDO）の案内、さらには不正取引の補償に関する発表に便乗するなど、手口を変化させています。

    - 偽サイトのURLは、Google翻訳のリダイレクト悪用、短縮URL、Unicode文字の混在、ホモグリフ攻撃など、迷惑メールフィルタや不正URL対策を回避する巧妙な技術が使われています。
    - 多要素認証を突破するため、「リアルタイム型」（AiTM攻撃によるリアルタイムフィッシング）へと進化しており、ワンタイムパスワードの同時窃取や、電話番号認証のための発信誘導などが行われます。
    - **インフォスティーラー（Infostealer）**と呼ばれる情報窃取型マルウェアによる認証情報の窃取も懸念されています。
- 攻撃者の特徴と目的:
    - 複数の詐欺集団が関与していると考えられており、短期間で様々な攻撃ツールや手口が入れ替わっています。
    - 不正アクセスの発信元は中国である疑いが強いとされています。
    - 盗んだ認証情報を悪用し、国外から遠隔操作で株式を売買します。
    - 乗っ取られた口座は、口座内の株を勝手に売却した資金で超安値の別の株を大量購入し、株価をつり上げる**「相場操縦」に利用された可能性**があります。
    - 新NISAなど日本での投資ブームに便乗し、人々の関心を集めやすいテーマを悪用しています。
    - 証券会社が注意喚起した後も攻撃は継続しています。
- 対策の限界と課題:
    - 多要素認証が必須化された後も被害は減っておらず、多要素認証も万全ではなく突破される危険性があります。
    - 一般的なワンタイムパスワードは、攻撃者がID、パスワードと同時に窃取できるため、フィッシングに耐性がないとされています。

6. 考察

狙われる場所

今回代表的な脅威アクターを取り上げてみましたが、攻撃パターンは大きく分けて

1. 外部に面したデバイスを攻撃するケース
2. フィッシング・Vishing等を用いて、人間を対象に攻撃を仕掛けるケース

があります。

6-1. 外部に面したデバイスを攻撃するケース

Akira, Quilinをみると、攻撃に際して特に重要となる「初期アクセス」時において、外部に面したデバイスを攻撃するケースとしては以下のものがあげられます。

- 初期アクセス **(Initial Access)**:
    - 公開アプリケーション・リモート監視・管理（**RMM**）ソフトウェアの悪用
        - Remote Desktop Protocol (RDP) [T1133] の悪用。
        - ScreenConnectなどのRMMツールを悪用して、組織の顧客にダウンストリーム攻撃を行う。
        - 多要素認証（**MFA**）が設定されていない**VPN**サービスを悪用。
    - 多要素認証（**MFA**）を狙った攻撃
        - 多要素認証ボンビング
        - **SIM**スワップ
    - **Cisco**の既知の脆弱性（CVE-2020-3259およびCVE-2023-20269）を悪用します。
    - 有効な認証情報 [T1078] の悪用。

- 使用する脆弱性
    - **CVE-2020-3259:** Cisco Adaptive Security Appliance (ASA) および Firepower Threat Defense (FTD) ソフトウェアのSSL VPNサービスにおけるサービス拒否の脆弱性。
    - **CVE-2023-20269:** Cisco ASA および FTD ソフトウェアのリモートアクセスVPN認証バイパスの脆弱性。
    - **CVE-2021-21972:** VMware vCenter Server 脆弱性。
    - **CVE-2019-6693:** F5 BIG-IP 認証バイパス脆弱性。
    - **CVE-2022-40684:** Fortinet FortiGate FortiProxy FortiAuthenticator 認証バイパス脆弱性。
    - **CVE-2024-40766:** SonicWall SonicOS リモートコード実行の脆弱性。
    - **CVE-2024-37085:** VMware ESXi 権限昇格の脆弱性。
    - **CVE-2024-40711:** Veeam Backup & Replication Mount Service 権限昇格の脆弱性。
    - **CVE-2023-27532**: Veeam Cloud Backupサービスの脆弱性。

これらについて対処する必要があります。

6-2. 外部に面したデバイスを攻撃するケース

Luna Mothの攻撃では初期アクセスとして以下の様なものが使われます。

- 初期アクセス **(Initial Access)**:
    - コールバック型フィッシングメール: 有名なサブスクリプションサービス提供企業を装ったメールを送信します。メールは少額の「サブスクリプション料金」を請求する内容で、不審を抱かれにくいように工夫されています。被害者は偽のサブスクリプションをキャンセルするため、メールに記載された電話番号に連絡するよう指示されます。このメールにはマルウェアが含まれておらず、正規のメールサービスから送信され、

PDF形式の請求書が添付されるため、通常のメール保護システムによる検出を回避しやすいです。
    - IT部門を装ったソーシャルエンジニアリング電話: 2025年3月からは、従業員に電話をかけ、自社のIT部門の職員を装う新たな手口も観察されています。その後、従業員にリモートアクセスセッションに参加するよう指示します（メールでリンクを送るか、ウェブページへの誘導）。

また、Akira, Qilinに関しても

- 初期アクセス **(Initial Access)**:
    - **Akira:** スピアフィッシング（悪意のある添付ファイルやリンク付き）[T1566.001, T1566.002]。
    - **Qilin:** スピアフィッシング: 悪意のあるリンクを含むフィッシングメールを通じて、被害者のネットワークに侵入し、機密データを窃取します。

とスピアフィッシングを用いて直接従業員を騙すような手口が見られます。

6-3. 対応策

まず、6-1でまとめた様な「外部に面したデバイスを狙った攻撃」に関しては、
- Attack Surface管理
- 脆弱性管理

などが有効になります。

また、6-2でまとめた様な「スピアフィッシングなどの人間を狙ってくる攻撃」に関しては
- 従業員に対する教育
- 多要素認証をできる限り導入し、盗まれた際のリスクを減らす

などが有効になります。

7. 結論（まとめ、Conclusion）

2025年上半期もランサムウェアグループによる被害は止まるところを知りません。また近年ではスピアフィッシングなどの人間を狙う攻撃にAIを加えて、より巧妙に騙す手口が続出しています。

これらの攻撃に対応するためには、技術的な解決ともにユーザへの教育が不可欠となっています。