

報道関係者各位

2024 年上半期に中小企業へのランサムウェアによる脅迫件数が増加 – ウィズセキュアがランサムウェア脅威レポートを発行

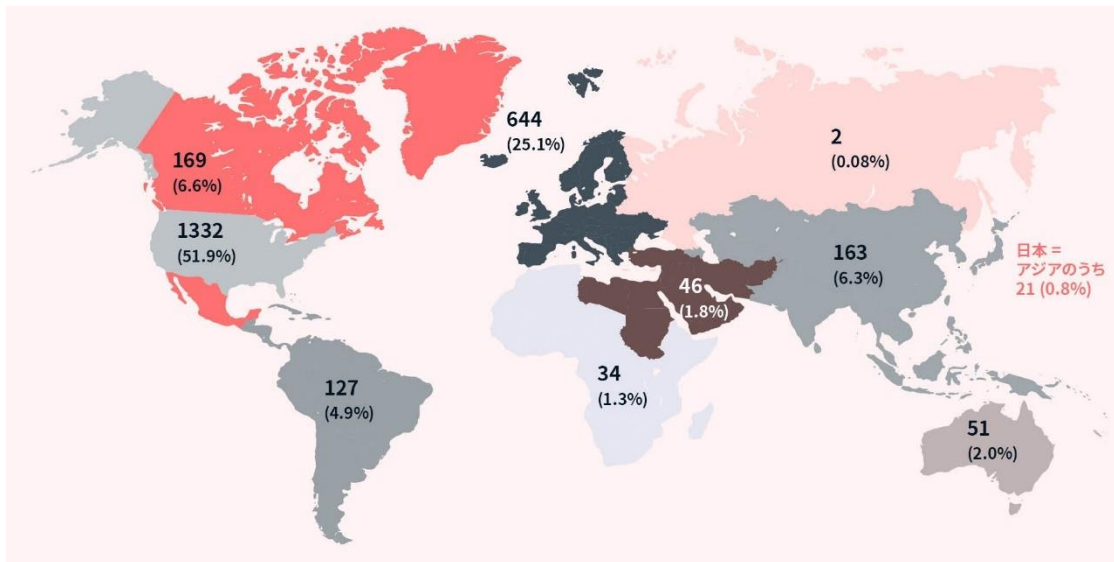
～ 法執行機関による Lockbit のテイクダウン後も順応／進化するランサムウェア業界 ～

2024 年 9 月 4 日
ウィズセキュア株式会社

先進的サイバーセキュリティテクノロジーのプロバイダーである WithSecure (本社: フィンランド・ヘルシンキ、以下、ウィズセキュア) は、2024 年上半期のランサムウェアを巡る情勢やトレンドに関するインサイトをまとめたレポート『最新ランサムウェア脅威レポート 2024 年上半期版』を発行しました。ランサムウェア業界の規模は 2023 年後半にピークを迎えた後、2024 年にはその生産性はほぼ横ばいの傾向を見せています。しかし、2024 年上半期における攻撃件数や身代金の支払い額は 2022 年や 2023 年の同時期と比較して上昇傾向にあります。

以下は本レポートで取り上げているインサイトの一部です:

- 2024 年上半期にランサムウェアのリークサイトに掲載された被害者数は 2,568。地域別ではアメリカが 1 位で 1,332 件 (52%)。次点はヨーロッパの 644 件 (25.1%)。日本は 21 件で 0.8%となっている。
- セクター別の被害では、1 位のエンジニアリング／製造業が 20.59%となっており、2 位の不動産／建設 (9.02%) に倍以上の差をつけている。
- 被害者の企業規模別では小規模組織(従業員 200 名以下) が 2022 年の 50%から 2024 年には 61%に増加している。



(図: 地域別のランサムウェア被害件数分布)

ウィズセキュアで脅威インテリジェンス部門の責任者を務める Tim West (ティム・ウェスト) は、2024 年上半期のトレンドについて、以下のように語っています。

「2024年2月の法執行機関による Lockbit のテイクダウンは主要なランサムウェアグループの活動を阻止する上で重要な役割を果たしましたが、テイクダウンの長期的な影響は依然として不透明であり、ランサムウェアグループはこれに順応し、そして進化しています。私たちは、Lockbit はより強固なオペレーション体制での復活を模索しており、現在は再構築の段階にあることはほぼ間違いないと考えています。」

本レポートでは、ランサムウェアグループのアーキテクチャを検証し、アフィリエイトを自陣に引き入れるためにグループ間の競争が激化していることについても取り上げています。法執行機関による Lockbit や ALPHV への措置の後、「ノマド型」のアフィリエイトが、他のグループに移籍して活動しています。West はこうした状況について次のように説明しています。

「ALPHV の出口詐欺では、アフィリエイトが本来得るはずであった報酬を ALPHAV が支払いませんでした。そのため、サイバー犯罪コミュニティ内の信頼は著しく低下しています。アフィリエイトの勧誘のために、Medusa は利益の最大 90%を、Cloak は 85%をそれぞれアフィリエイトに分配するとしています。こうした背景もあり、ランサムウェアのエコシステム内のパワーバランスがさらに複雑なものになってきています。」

本レポートで確認された顕著な傾向として、今年の WithSecure の過去のリサーチでも述べられているように、エッジサービスの悪用による初期アクセスの採用が増加していること、またランサムウェアグループによる正規のリモート管理ツールの頻繁な使用が挙げられます。また、身代金を支払った企業／団体のかなりの割合が、その後、同じまたは別のランサムウェアグループによって再び標的にされたというデータもあり、再感染という根強い問題にも触れています。そして、攻撃の対象が大企業から中小企業へとシフトしはじめているというデータを得ることができました。West はこうした中小企業への攻撃の増加について、こう締めくくっています。

「2022 年以降、ランサムウェアのリークサイトに掲載される企業のうち、中小企業が占める割合が大きくなってきています。身代金の支払い率は低下し、1 件あたりの身代金支払額も小さくなってきていますが、攻撃グループがターゲットでの収益を保つために脅迫の件数は増加しています。大企業と違い、中小企業はサイバー保険に加入していないところが多く、身代金の額は少なくとも、攻撃者にとっては狙いやすいターゲットだといえます。」



『最新ランサムウェア脅威レポート 2024 年上半期版』(日本語) の全文は以下のページからご覧いただけます:

https://www.withsecure.com/content/dam/with-secure/ja/resources/202409_WithSecure_Ransomware_Landscape_JP_Light.pdf

ウィズセキュア Web サイト:

<https://www.withsecure.com/jp-ja/>

ウィズセキュアプレスページ:

<https://www.withsecure.com/jp-ja/whats-new/pressroom>

WithSecure™について

ウィズセキュアは、多くのヨーロッパ企業に選ばれるサイバーセキュリティパートナーです。世界中の IT サービスプロバイダー、MSSP、ユーザー企業から、中堅・中小企業を保護するアウトカム(成果)ベースのサイバーセキュリティソリューションにおいて大きな信頼を勝ち取っています。ウィズセキュアはヨーロッパにおけるデータ保護の規制に準拠し、プライバシー、データ主権、コンプライアンスに注力しています。



当社は 35 年以上の経験を持ち、ユーザー企業の消極的／保守的なサイバーセキュリティ対策から積極的／先進的なアプローチへのパラダイムシフトのサポートのためのポートフォリオを持っています。ウィズセキュアはパートナーとの協力的な成長へのコミットメントに基づく柔軟な商業モデルを提供し、ダイナミックなサイバーセキュリティの世界において両者の成功を保証します。

ウィズセキュアの最先端のポートフォリオの中心となるのは、AI を搭載したテクノロジー、人の専門知識、コ・セキュリティ (共同セキュリティ) サービスをシームレスに統合する Elements Cloud です。さらに、エンドポイントおよびクラウドの保護、脅威の検出と対応、エクスポージャー管理にまたがるモジュール式の機能により、中堅・中小企業ユーザーのセキュリティ対策を強固なものとしします。

1988 年に設立されたウィズセキュアは本社をフィンランド・ヘルシンキに、日本法人であるウィズセキュア株式会社を東京都港区に置いています。また、NASDAQ ヘルシンキに上場しています。詳細は www.withsecure.com をご覧ください。また、X (旧 Twitter) アカウント @WithSecure_JP https://twitter.com/WithSecure_JP でも情報の発信をおこなっています。