ebook

最新ランサムウェア脅威レポート

2024年上半期版

2024年9月

コンテンツ

エグゼクティブサマリー

ランサムウェア犯罪業界の規模は2023年下半期にピークを迎え、その活動は横ばいになり始めているという兆候が見られる。

2024年上半期におけるランサムウェア攻撃の件数と被害者による身代金支払額は、2022年上半期や2023年上半期を上回っている。

法執行機関によるテイクダウンなどの措置が長期的にランサムウェアのエコシステムに与える影響はまだ明らかではないが、短期的にはほぼ確実にランサムウェアの活動の低下に寄与するといえる。

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る。

LockbitやALPHVのテイクダウンといった出来事が、「ノマド型」のランサムウェアアフィリエイトたちを、より確立されたRaaSグループへと向かわせた可能性が高い。ランサムウェアグループたちの間には、アフィリエイトをめぐる競争がある。

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。

ランサムウェアの攻撃者のTTP (戦術／技術／手順) は2023年から2024年にかけてはほぼ変化していない。2022年以降、エッジサービスの悪用によるイニシャルアクセスの採用が増加し、また、正規のリモート管理ツールの使用が一貫して頻繁におこなわれている。

Raas (ランサムウェア・アズ・ア・サービス) を使用する サイバー犯罪グループのアーキテクチャ

一部のランサムウェアグループ／ブランドは、イニシャルアクセスから恐喝までのオペレーションが内部で完結する「プライベート」グループとして運営されています。
そのため、RaaS (Ransomware-as-a-Service) モデルが採用されている場所を特定する必要があります。これは、成功したランサムウェアグループのほとんどに当てはまることです。

ウィズセキュアが2023年5月に発行したレポート『The Professionalization of Cyber Crime』では、ランサムウェアがサイバー犯罪の状況に与えた影響について詳しく説明しています。
今回のリサーチで最も重要なことは、ランサムウェアのグループは、ほとんどの場合、もはや単一のグループ名／ブランド名の下で活動する個人の集団であるという明確な定義づけができなくなっている、という点です。私たちはランサムウェアを「亜種ごと」にトラッキングしていますが、こうした理由により、ブルーチームがランサム攻撃前の活動の帰属やTTPのトラッキングをおこなうことが非常に難しくなってきています。

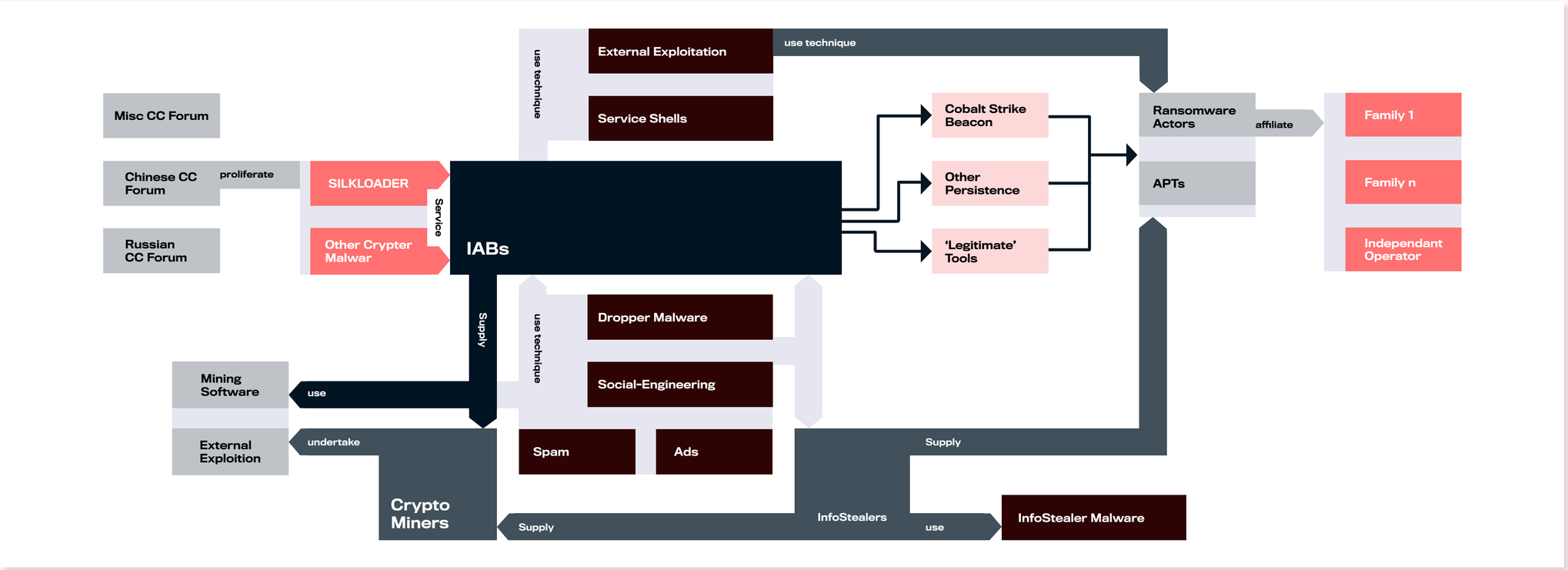


Figure 1: Everything-as-a-Serviceのエコシステム

サイバーセキュリティ業界は、法執行機関 (LEA) の連携による優れた措置により、ランサムウェア業界では圧倒的に組織化されて大きな成功を収めていたLockbitの活動を停止させることができました。しかし、Lockbitのアフィリエイトの多くは、同じように収益化のために存在する別な (または新たな) ランサムウェアグループに移籍しただけ、という結果になりました。

脅威アクター、特にイニシャルアクセスブローカー (IAB) は、インターネット上での悪事を産業化してきました。脅威アクターの参入障壁の1つは、インターネット全体の悪用の試みを成功させるための複雑さだといえます。脅威アクターは、以下のことを行う必要があります：

- 脆弱性がどのように悪用されるかを理解する
- エクスプロイトを武器化する
- トラフィックフィルターを迂回し、大量にスキャン／エクスプロイトする
- 獲得したアクセス／エクイティを記録／維持／整理する
- これらのアクセスを開発および／または販売する

エクスプロイトをリバースエンジニアリングしたり、武器化したりするには、多くのサイバー犯罪者がまだアクセスできないレベルの技術力が必要であり、こうした障壁を取り除くサービスモデルは高い人気を博す可能性が高いです。これはスケーラブルなビジネスモデルであり、IABの数は比較的少ないように見えますが資金力があり、他の脅威アクターたちを幅広くサポートできる有能なサプライヤーという立場で活動していることを意味します。IAB業界は、より広範なランサムウェア攻撃者にとって、迅速な脆弱性の悪用を可能にしました。

業界からの撤退

Lockbitのテイクダウン

本年2月20日、10ヶ国のLEAが参加した共同作戦『Operation Cronos』が、Lockbitのリークサイトに押収通知を掲載しました。皮肉とユーモアに富んだ表現として、Lockbitリークサイトの形式自体がLockbitを茶化すかたちで、LEAの作戦の成功やLockbitのオペレーションについて得た情報を提示するために使用されました。LEAはまた、アフィリエイトのコミュニケーション／コントロールパネルにアクセスし、Lockbitのアフィリエイトを脅すメッセージを残すことができました。

LEAがLockbitにアクセスして得た情報の全容は現在のところ公表されていませんが、判明しているのは、この作戦によって約1億2,000万ドルを保有する数百の暗号資産ウォレットが押収され、34台のLockbitサーバーがコントロール下に置かれ、Lockbitの被害者のために1,000個の復号キーが回収され、同時にLockbitに関与した疑いのあるウクライナとポーランドの2人のハッカーが逮捕されたことです。しかし、この作戦の翌週にはLockbitのリークサイトがオンラインに復活し、テイクダウンの影響は軽微であるかのような長いメッセージが掲載されました。LEAはまた、Lockbitの幹部メンバーの逮捕につながる情報に対して1,500万ドルの報奨金の提供を発表しましたが、これは少なくともLEAが現在そうした情報を入手できていないことを物語っています。

LEAによるLockbitへの最初の措置は、それにより救済された企業／団体の多さや、Lockbitのアフィリエイトに与えた心理的ダメージなどの複数の理由により、大きな成功となりました。しかし、ランサムウェアのエコシステム自体が確立されており、どこかのランサムウェアグループが衰退しても、脅威アクターの一人ひとりは他のRaaSプロジェクトに移籍できるため、この業界からきれいに身を引くよう説得できるとは限らないのが現状です。これについては、『LockbitとALPHVの影響』の項で更に説明します。

本年6月、Lockbitは再構築の段階にあることが示されています。リサーチャーたちは、彼らの恐喝インフラが流動的な状態にあり、ドメインが変わり、サービスを構築するためにこれまでとは異なる技術が使用され、テスト被害者が追加されていることを指摘しています。LEAによる措置以降もLockbitの活動が観測されており、Lockbitがそのオペレーションを強化し、復活に向けて取り組んでいることはほぼ確実です。

本レポート執筆時点では、LEAの作業は、現実世界のアイデンティティをLockbitのアフィリエイトに紐づけることを続けています。これは、ランサムウェア攻撃者のオペレーション上の安全性と、秘密のベールを破る西側当局の能力が真に試されることになるため、重要な作業だといえます。これが成功すれば、特に攻撃的な手法によって、ランサムウェアのアフィリエイト、特にEU／米国と協力する意思のあるLEAが存在する地域で活動するアフィリエイトに対する強力な抑止力となる可能性が高いです。

ヒドラの頭

前述のように、ランサムウェアのアフィリエイトがサイバー犯罪のような『儲かる業界』からの撤退を決しするほどの動機となる要素はほとんどないように思われます。これは、ランサムウェアのブランド数を見るとよくわかります。2023年第1四半期以降、四半期ごとに見ると、少なくとも1人の被害者を計上したランサムウェアブランドの数は、ピークに達した2024年第1四半期まで徐々に増加していることがわかります。

データを月単位で見ると、被害者の一般的なトレンドは比較的横ばいで推移していますが、LEAのLockbitへの措置やALPHVの出口詐欺 (後述) の後に新たなランサムウェアブランドが登場したわけではありません (こちらも後述)。ランサムウェアを取り巻く情勢での不確実性が高まるにつれ、アフィリエイトがより確立されたグループに目を向けたことはほぼ間違いありません。これは2024年6月時点においても同様です。

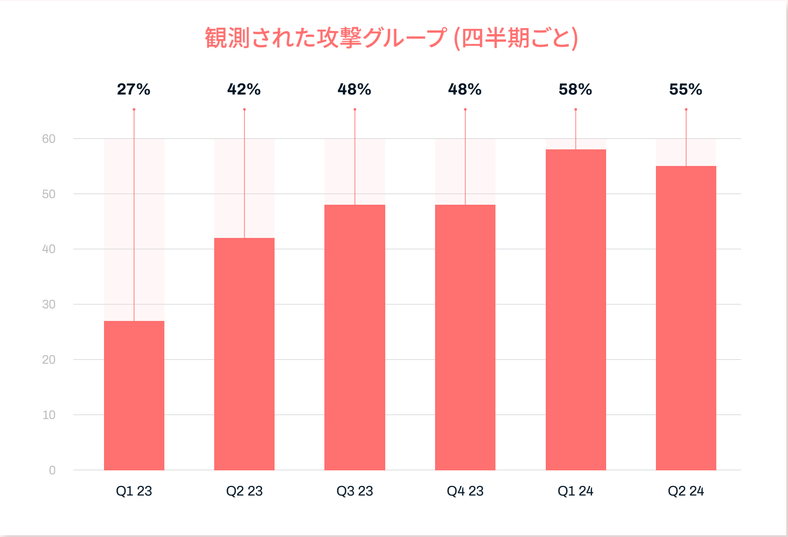


Figure 2: 四半期別のユニークのランサムウェアグループ数

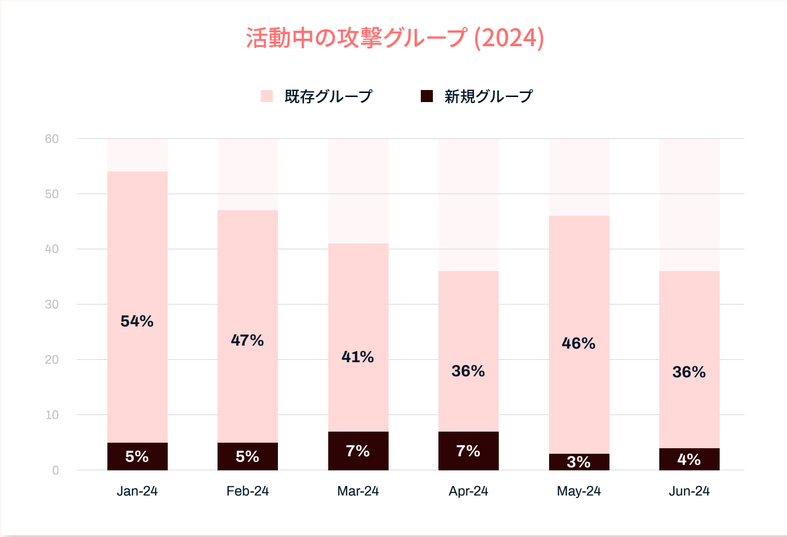


Figure 3: 月別のアクティブなランサムウェアグループ数 (2024年)

ウィズセキュアは2023年に35の新しいランサムウェアグループを観測／追跡しました。また、2023年にトラッキングした67のランサムウェアグループのうち、31のグループは2024年第2四半期には稼働を停止していました。

本年はこれまでに新たに観測されたランサムウェアグループは31ありますが、このうち9グループは第2四半期には全く活動が見られていません。2024年には13の新規グループが5人以下の被害者しか出せておらず、今後これらのグループが生き残っていく可能性は低いと考えます。

『信頼』が果たす役割

Everything-as-a-Serviceのエコシステムがスキルの低い脅威アクターのランサムウェアビジネスへの新規参入におけるハードルを下げる一方で、脅威アクター間の相互信頼という、悪用される可能性があり、なおかつこれまでも悪用されてきた弱点が明らかになりました。LEAによるLockbitへの措置やAlphV/Blackcatに対するLEAのアクションなどが、ほぼ間違いなく脅威アクター間の信頼を損なわせたといえます。

ALPHAVの出口詐欺

本年第1四半期、アメリカのヘルスケア／薬局分野の企業であるChange Healthcare社はALPHVによるランサムウェア攻撃を受け、全米のヘルスケア業界とランサムウェアを取り巻く状況に状況に大きな現実的な影響をもたらしました。この攻撃の数週間後、Change Healthcareへのサイバー攻撃を担当したALPHVのアフィリエイトを名乗る人物が、ロシア語のサイバー犯罪フォーラムに投稿をおこない、Change Healthcareは盗難されたデータの流出を防ぐために2,200万ドルの身代金をALPHVに支払ったが、ALPHVはアフィリエイトに支払うべき取り分を渡しておらず、アフィリエイトのアカウントを凍結し、支払うべき金をプールしてると述べました。Change Healthcareは身代金の支払いを公には認めていませんが、リサーチャーたちが以前ALPHVに関連付けた暗号資産アドレスが、2,200万ドルの支払いを一度受けていることは確認できました。

ALPHVグループの中心メンバーとおぼしき人物が、同じサイバー犯罪フォーラムに、ALPHAVグループは閉鎖され、既にランサムウェアのソースコードの買い手を見つけたと投稿しました。彼らはまた、「FBIに騙された」とも述べていて、ALPHVのWebサイトは、LEAのテイクダウン通知に置き換えられていました。しかしリサーチャーたちは、このテイクダウン通知は、ALPHVが2023年にLEAによって最後にテイクダウンされたときの通知のスクリーンショットに過ぎないことを直ちに指摘しました。

報告されている一連の出来事を見る限り、最も信憑性の高い説明は、ALPHVが出口詐欺をおこない、自発的に廃業したのではなくLEAに取り押さえられたため閉鎖を余儀なくされたと主張した、というものです。ALPHAVメンバーたちが、仲間の犯罪者から盗んだ金を持ち逃げしたことはほぼ間違いありません。Change Healthcareは、盗まれたデータの流出を防ぐために多額の身代金を支払ったにもかかわらず、実際にこの攻撃をおこなったアフィリエイトを自称する人物は、Change Healthcareから盗まれたデータをまだ持っていると述べています。これは、アフィリエイトたちがChange Healthcareを再度攻撃した可能性が非常に高いと思われます。

これは、身代金を支払わない理由として広く指摘されおり、極めて重要なことです。前述のとおり、ランサムウェアの実行者は、自分たちの要求が満たされればインシデントから回復できると被害者側が確信していることを拠り所にしており、こうしたケースは加害者と被害者との間の信頼を損なうことになるものです。これはまた、脅威アクター間の関係や信頼にも影響を及ぼしており、このケースはおそらく、新興RaaSグループたちがRaaSグループの提携支払いモデルを支える重要な原動力となっています。

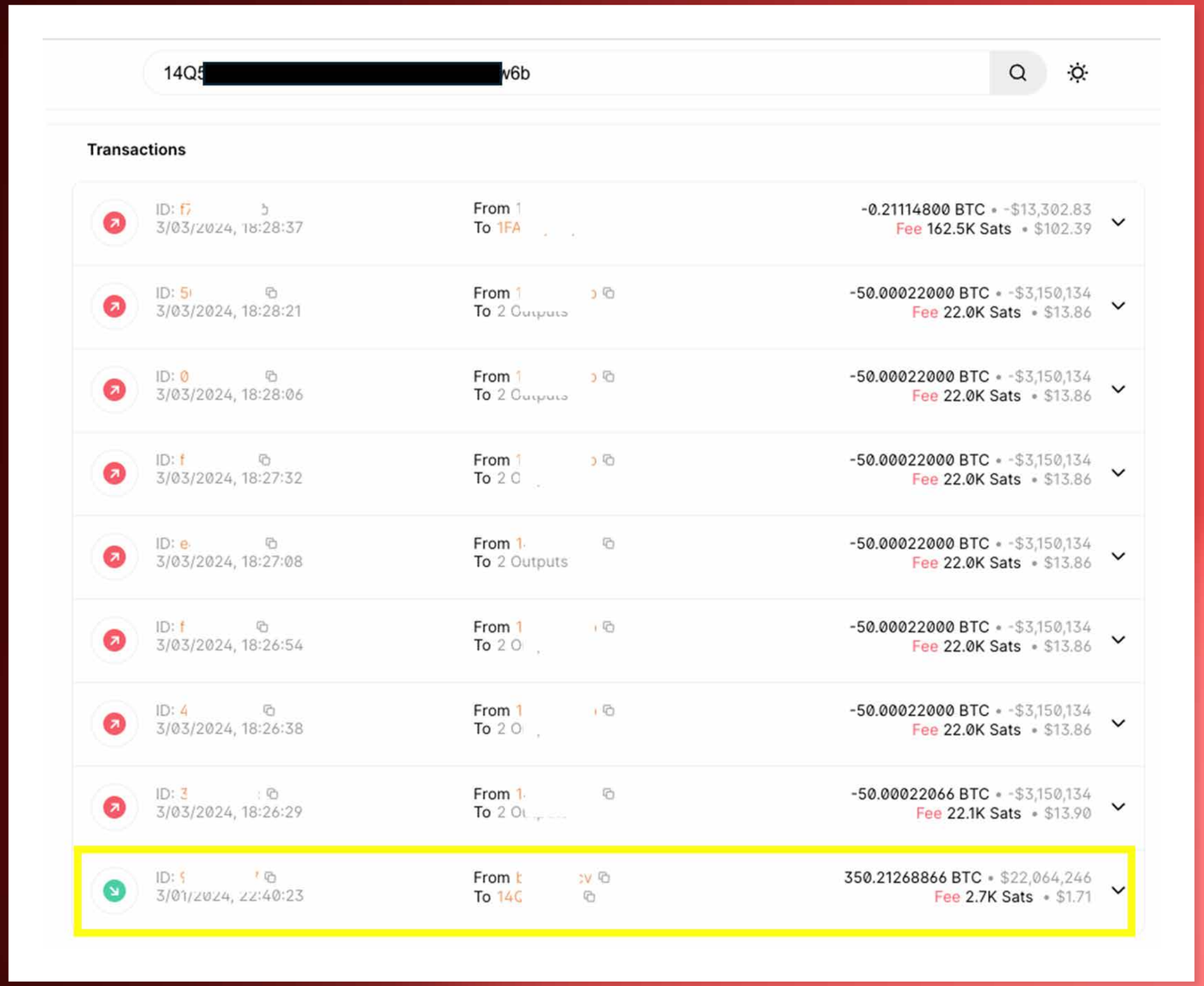


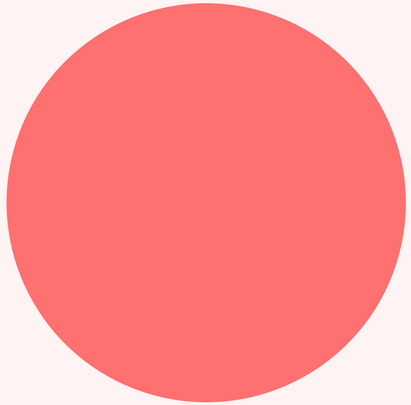
Figure 4: 2,200万ドル相当のビットコイン入金 (Source: Blockchain.com)

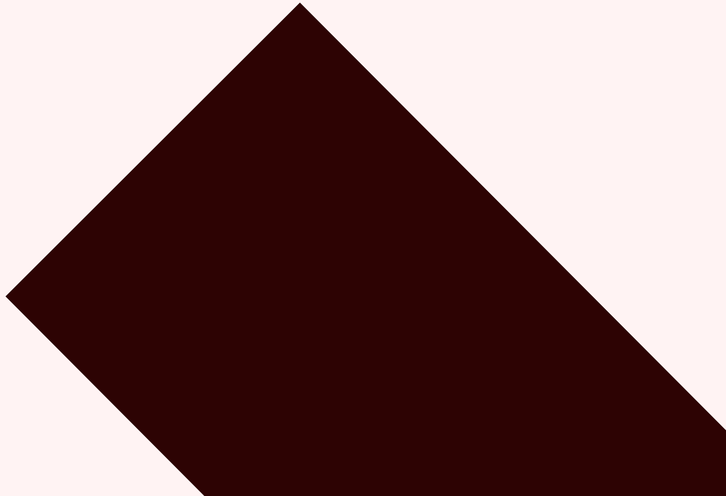
ライバル関係

GuidePoint Securityのリサーチャーによるレポートでは、ランサムウェアのエコシステムを調査し、LockbitとALPHV (LEAは2023年12月にALPHVの侵害サイトを掌握) のアクションおよびALPHVの出口詐欺による最近の衝撃に対するランサムウェアのエコシステムの反応についてのインサイトを提供しています。興味深いことに、Medusa、RansomHub、Cloakのような小規模または新興のランサムウェアグループは、Lockbitのテイクダウンや ALPHVの出口詐欺に直接影響を受けたり失望しているアフィリエイトを自陣に取り込もうとしているようです。

Medusaは気前のいい利益分配率を提供しており、最大90%がアフィリエイトに支払われます。Cloakはアフィリエイトに85%の利益分配を提供し、さらに、アフィリエイトになるための加入金の支払いは不要だと言っています。Lockbitに対するLEAの措置の後、リークサイトに掲載される被害者数が急増したことから、これはMedusaにとって効果的であったようです。

一方、RansomHubは、アフィリエイトが被害者からの支払いを直接受け取り、その後RansomHubに送金することで、RaaSの正統性を崩しています。これは、ALPHVの出口詐欺に失望したアフィリエイトたちを安心させるための試みであるようです。被害者からの支払いは、まずALPHVが管理する暗号資産ウォレットに送られ、その後ALPHVはアフィリエイトの取り分を彼らのウォレットに送るという流れになっていました。これは、Change Healthcareの2回目の身代金がRansomHubに送られたことから、うまくいったようです。RansomHubのリークサイトに掲載される被害者数の増加は、ライバル関係にある他のランサムウェアグループからアフィリエイトを移籍させることに成功した証でしょう。





こうしたややドラマチックなオファーが物語っているのは、LEAによるLockbitとALPHVに対する措置は、即座に直接的にランサムウェアグループを根絶することはできなかったかもしれないが、ランサムウェア業界に大きな圧力をかけ、そのアフィリエイトがRaaSグループに寄せる信頼が非常に低下していることを示すものだということです。サイバー犯罪者同士がお互いを信頼せず協力し合わなければ、攻撃の効果も効率も低下し、企業／団体にとっては防御も容易になるのです。

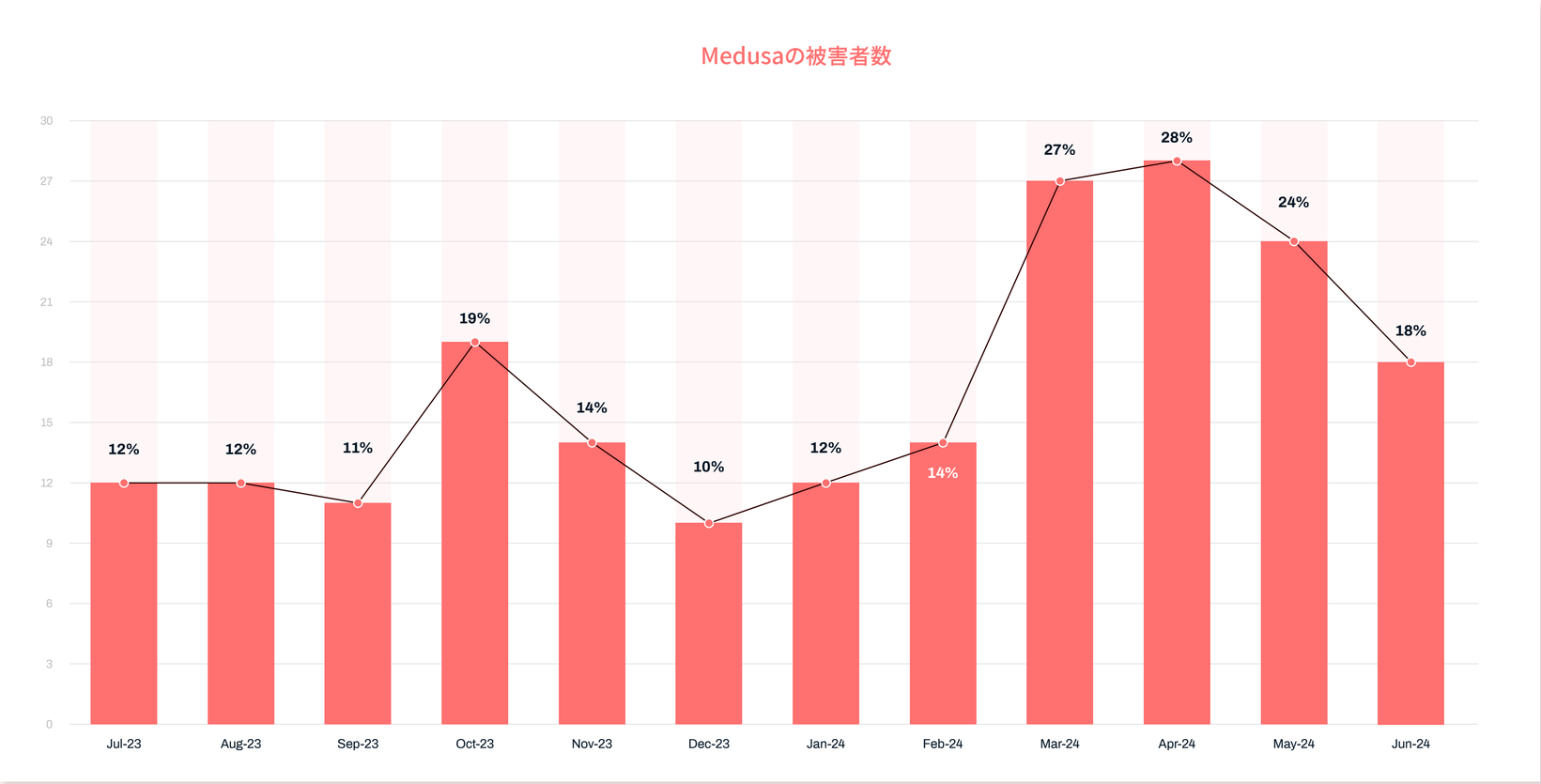


Figure 5: Medusaによる攻撃の被害者数

再感染

ランサムウェアグループは伝統的に、身代金を支払えばデータを復旧できるという信頼を被害者に植え付けることに多くの労力を費やしています。恐喝の成功は、支払えば通常の業務が可能な限り円滑に再開できるという被害者の確信に基づいています。ランサムウェアの支払いを禁止する立法府の主張は、この概念に依拠していますが、それは被害者側の支払い意欲というランサムウェアの運用の核となる原則を損なうことになるのです。

被害者を「改心」させて身代金を支払わせるために、多くのランサムウェアグループは、自らを「ペンテスター」(ペネトレーションテスター: 合法的な攻撃的サイバーセキュリティコンサルタント) として売り込み、顧客にサービスを提供し、侵害がどのように発生したかの詳細を提供し、身代金を支払えばファイルが復号化されることを保証しようとします。

Cybereason社によると、身代金要求を支払った組織の78%以上が2回目のランサムウェア攻撃を受け、その多くは同じ脅威アクターによるものでした。ウィズセキュアのテレメトリーデータと比較すると、この78%という数字は高い割合といえますが、ウィズセキュアは被害者の再感染を確実にトラッキングしています。ランサムウェア攻撃者が被害者に再感染はないと語っていることは信用できないものであり、攻撃者との信頼関係に基づく身代金の支払いを奨励することはありません。これはランサムウェアのランドスケープに直接影響を与えるため、ランサムウェア攻撃者の信頼性の低さについてのリサーチを理解することが重要です。

ランサムウェアに関する統計

被害者のリークサイト

データバイアス

ランサムウェアに関する統計を見る際、エコシステムの分析は望遠鏡を逆から覗くようなもので、データセットごとに見方や視点が異なるという例えがよく用いられます。

このセクションでは、被害者のリークサイトについて見ていきます。このデータセットは、私たちがランサムウェアのランドスケープを理解するために持っている、おそらく最良かつ最も一貫性のあるソースですが、ここで収集されたデータは誤りやすいものではなく、このデータセットに影響を与え、歪ませる要因となる可能性を持つ変数がいくつかあります：

- 攻撃者主導のデータであり、攻撃者の中には不正確なデータを投稿することでインセンティブを得る者も存在する
- このデータセットは流動的で、被害者は頻繁に追加／削除されることがある
- 恐喝の成功も重要な要素であり、身代金を支払う被害者が大幅に増加した場合、ランサムウェアの「総」数は減少しているように見えるかもしれない

とはいえ、賢明な仮定を立て、それを述べることができれば、このデータからいくらかのインサイトを得ることができます。業界で一般的に遵守されている仮定は以下の通りです：

- 被害者の支払い率は前月比でほぼ一定である
- 攻撃者によるリークサイトへの投稿には真実の要素が含まれている

被害者数

ランサムウェアのリークサイトで確認された月別のユニークな被害者の数は、2024年上半期までほぼ横ばいであり、過去12ヶ月ではわずかではあるが減少傾向にあります。

被害者数が2023年の夏に多い原因は、Cl0pのMOVEit大規模エクスプロイトのキャンペーンなどだと考えられます。

LEAによる措置やサイバー犯罪エコシステムの変化にもかかわらず、2024年上半期の数字は2022年と2023年の同時期を上回っています。

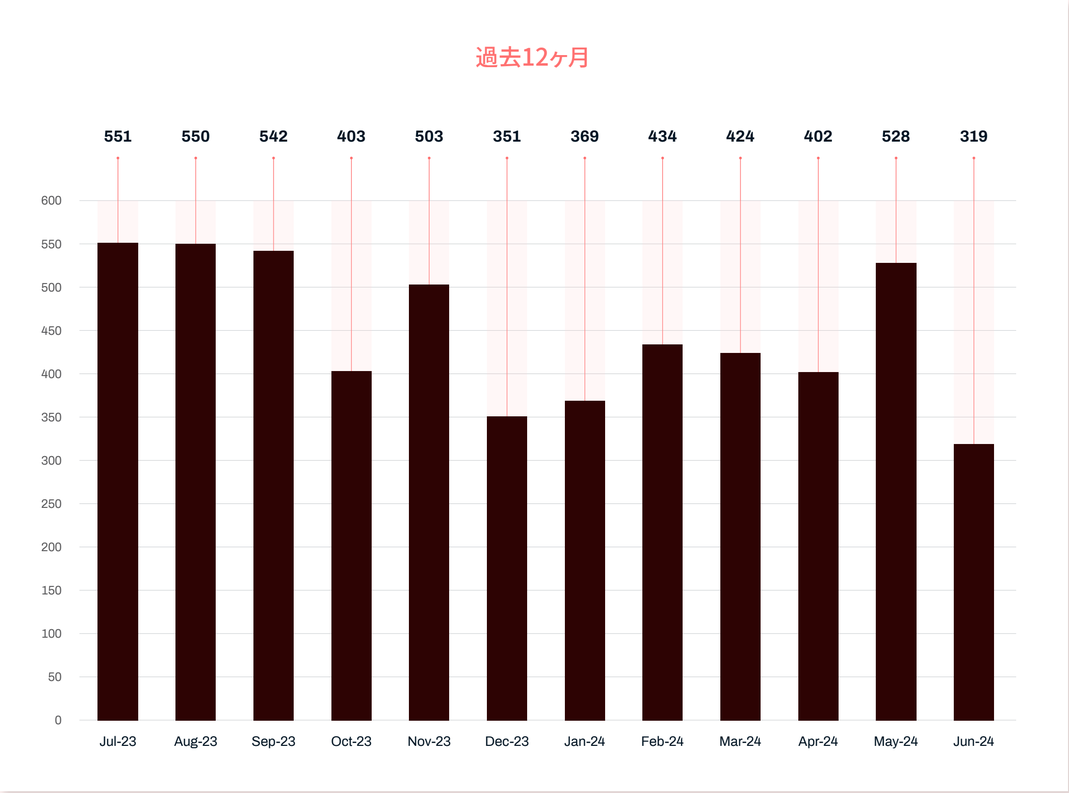


Figure 6: リークサイトに掲載された被害者の数 (過去12ヶ月)

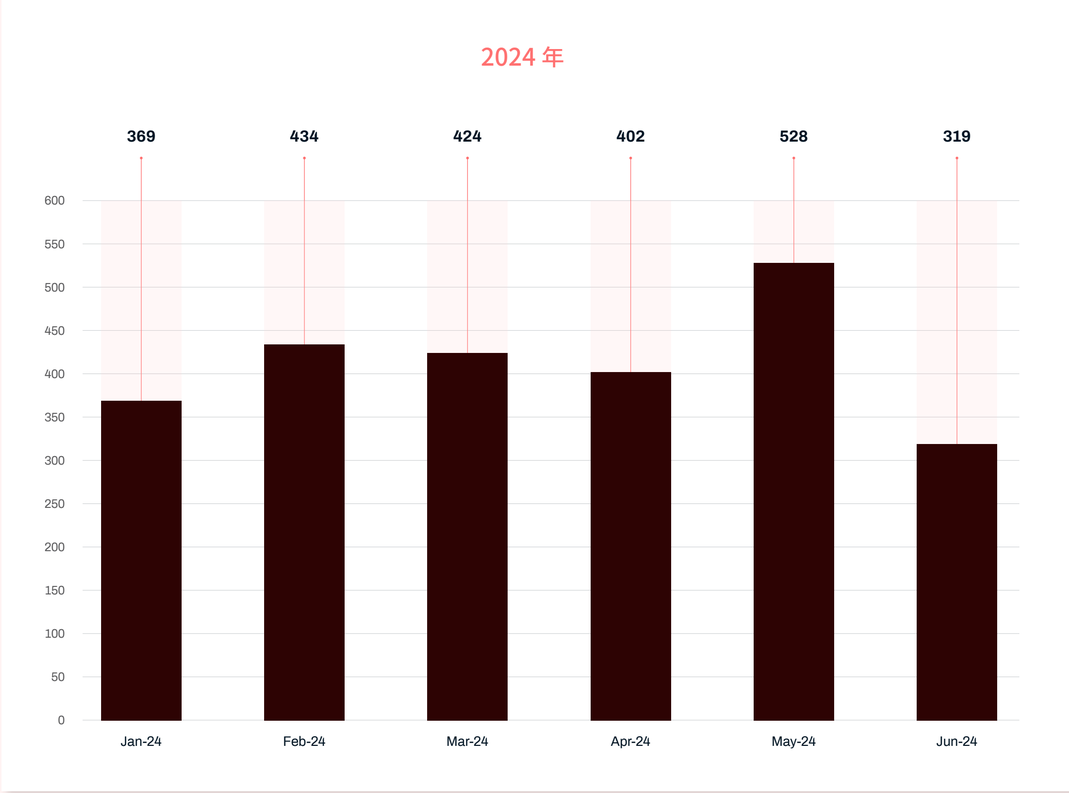


Figure 7: リークサイトに掲載された被害者の数 (2024年)

異なる年における特定の月というフィルターを通して数値を見ることは季節変動の影響を理解するのに役立ちますが、ランサムウェアリークサイトへの被害者の投稿は2023年第3四半期にピークに達し、それ以降の投稿数は比較的一定しているように見えます。

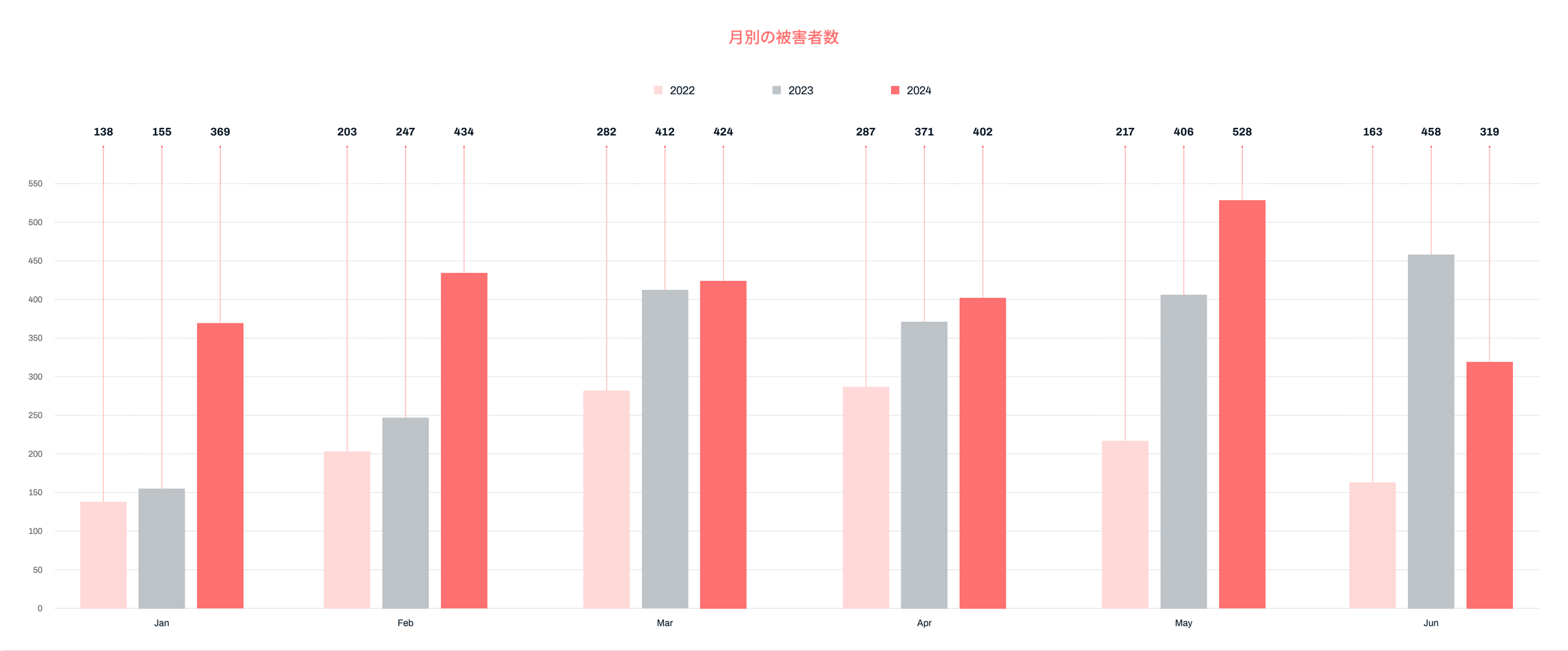


Figure 8: 月別・毎年上半期の被害者数

被害者の規模

ウィズセキュアはランサムウェアのトラッキングサイトであるecrime.chを使用して、詳細なランサムウェアのリークデータを収集しています。それにより、被害者組織の従業員規模別の統計や、被害者の規模の変化を示唆するテーマやパターンが時間の経過とともに存在するかどうかを追跡しています。総数のインフレを補正すると、人口統計には比較的一貫性があり、従業員数によって小規模 (0-200)、中規模 (200-1,000)、大規模 (1,000-5,000)、および超大規模 (5,000人以上) に分類しています。

このデータに若干偏りがあることは本レポートの前半で述べていますが、それを考慮しても、現実世界の出来事がデータにどのような影響を与えるかは明らかです。たとえば、2023年8月には、全体に占める中小企業の組織の割合が低下しています。これは、ファイル転送ソフトウェアであるMOVEitの脆弱性が原因で大規模なエクスプロイトが発生し、通常の月より多数のエンタープライズ規模の企業が影響を受けた時期です。

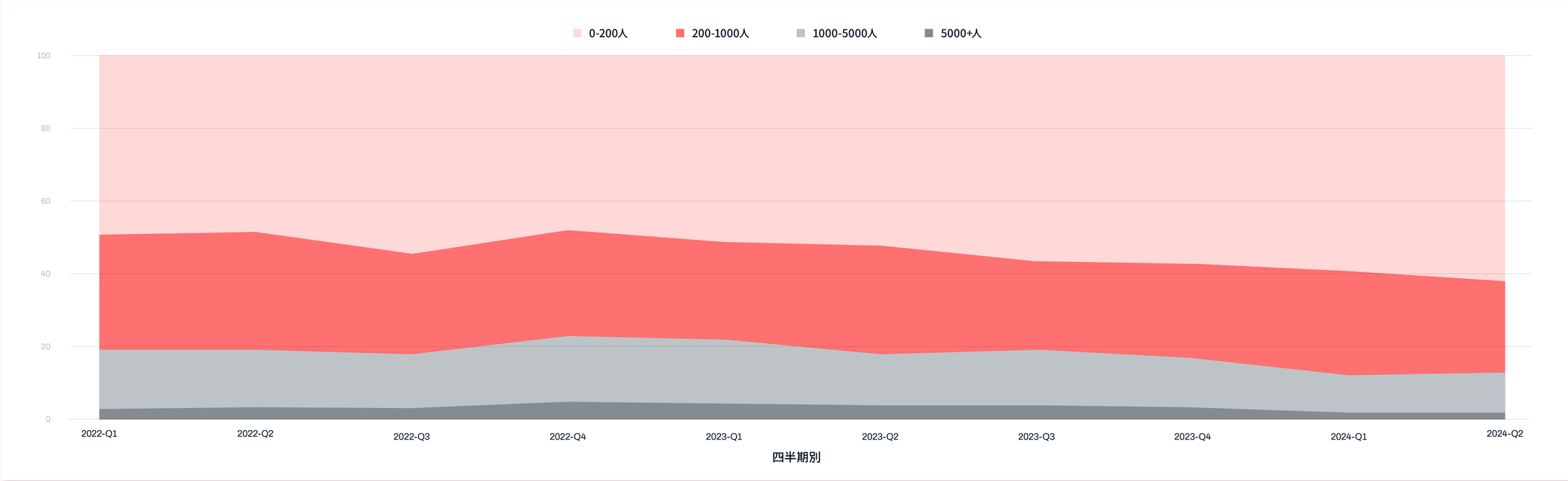


Figure 9: ランサムウェアの被害者の規模（総数に対する割合 (Source: ecrime.ch)

Figure 10では、前年比の割合を示しています。2024年には、小規模の被害者がリークサイトの被害者全体の約61%を占め、被害者の50%がこのカテゴリに属していた2022年以来、前年比で約5.5%増加していることがわかります。この点については、本レポートの以降のセクションで、この結論と相関するCovewareの身代金支払いリサーチにしてさらに詳細に説明します。

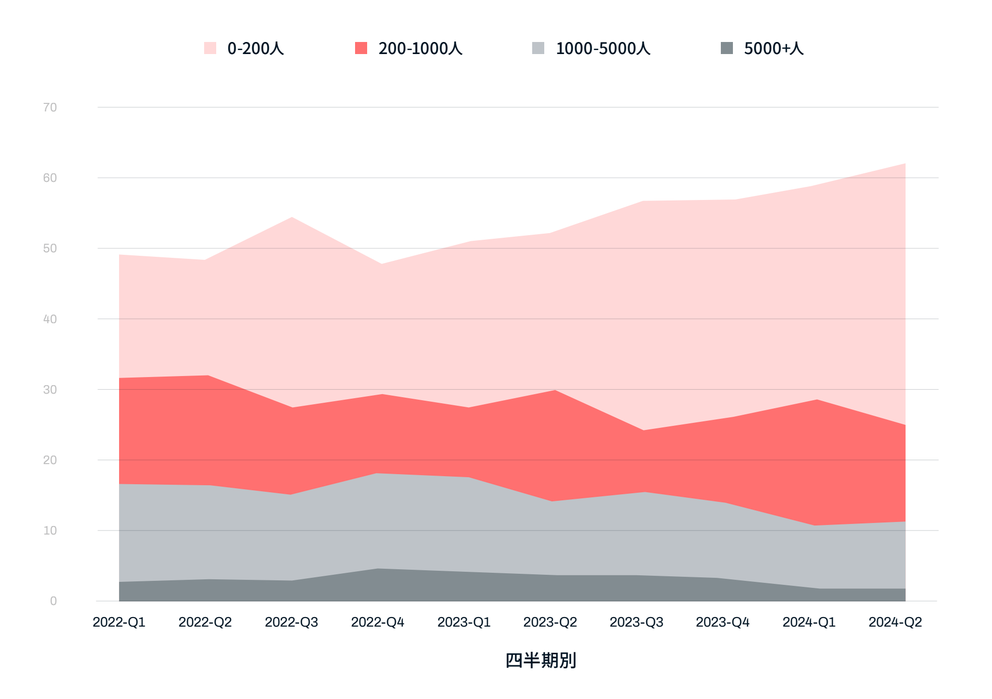


Figure 10: ランサムウェアの被害者の規模 (Source: ecrime.ch)

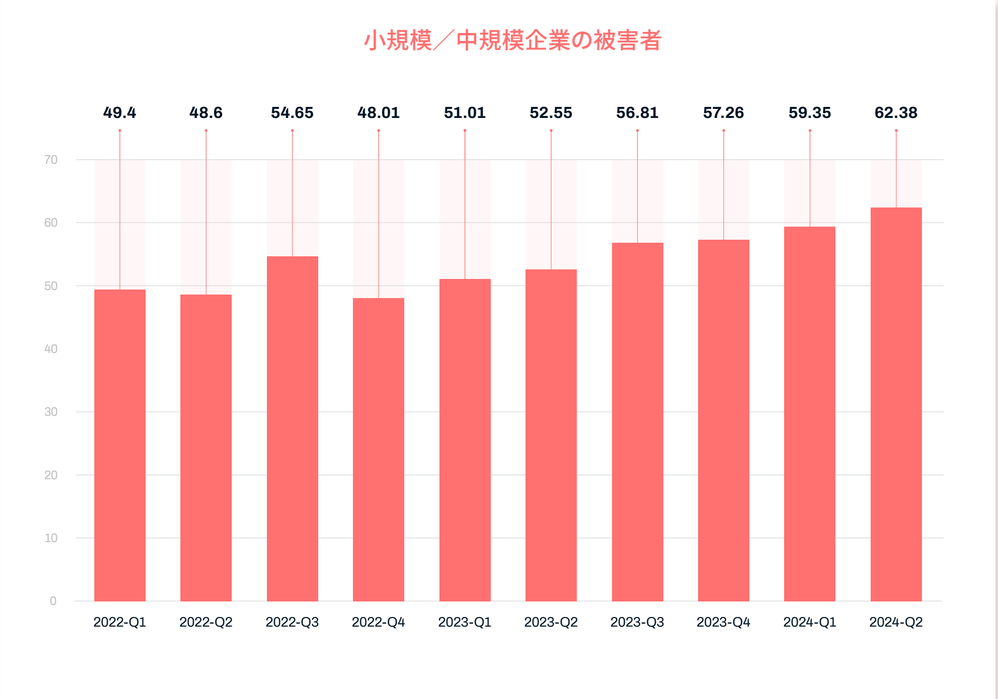


Figure 11: 被害者における小規模／中規模企業の割合 (Source: ecrime.ch)

被害者における中規模企業の割合は比較的一定しており、2022年には30%、2023年には27%、2024年には29%となっています。その一方、リークサイトに掲載される大規模および超大規模の被害者は減少しています。

- Large: 16.5% (2022) -> 10.9% (2024)
- Extra Large: 3.25% (2022) -> 3.5% (2023 - 増加は恐らくMOVEitの影響によるもの) ->1.5% (2024)

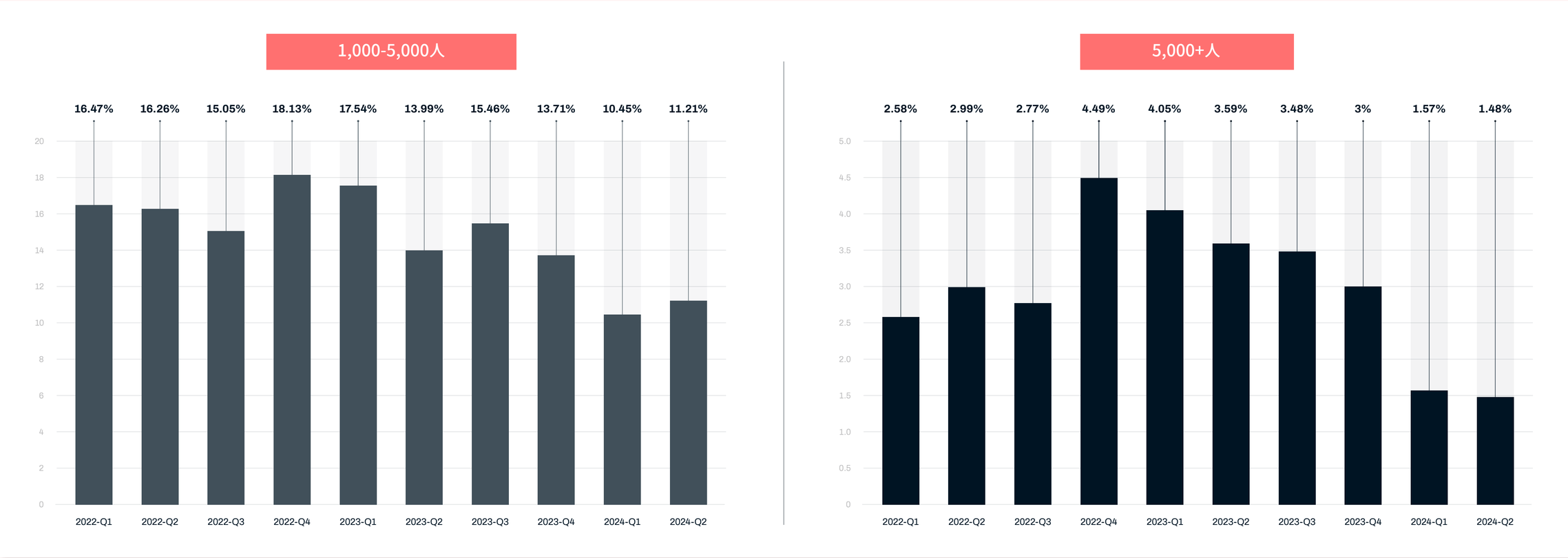


Figure 12: 被害者における大規模企業／超大規模企業の割合の減少 (Source: ecrime.ch)

このデータから導き出される結論は、データが示唆するほど単純ではないかもしれません。1,000人以上の従業員を抱える組織が直面するランサムウェアのリスクは減少しているという結論に至りたくなるかもしれませんが、ここで私たちの重要な原則の1つ、つまり「支払い率は比較的一定している」という原則を再検討する必要があります。月ごとに見ればこれは妥当な仮定ですが、前年比で見ると、2022年の状況は2024年の状況とは大きく異なっていたことに注意する必要があります。総数はるかに少なく、活動しているランサムグループの数は少なく、また、その後サイバー保険市場は急速に変化しました。

サイバー保険は大企業にとって現実的なリスク軽減のための戦略となっています。サイバー保険市場規模が毎年数十億ドル単位で増加していることから、この層の支払い率の上昇によってこれらの数字が歪められる可能性が現実的にあることを認識する必要があります。

地域別データ

ヨーロッパと中東でのLockbitとALPHVによる混乱の影響はむしろポジティブなものとなり、事件後の数ヶ月で地域別データとしては明らかに影響が減少しました。Figure 13では、被害者全体におけるこれら地域での被害の減少を明確に示しています。

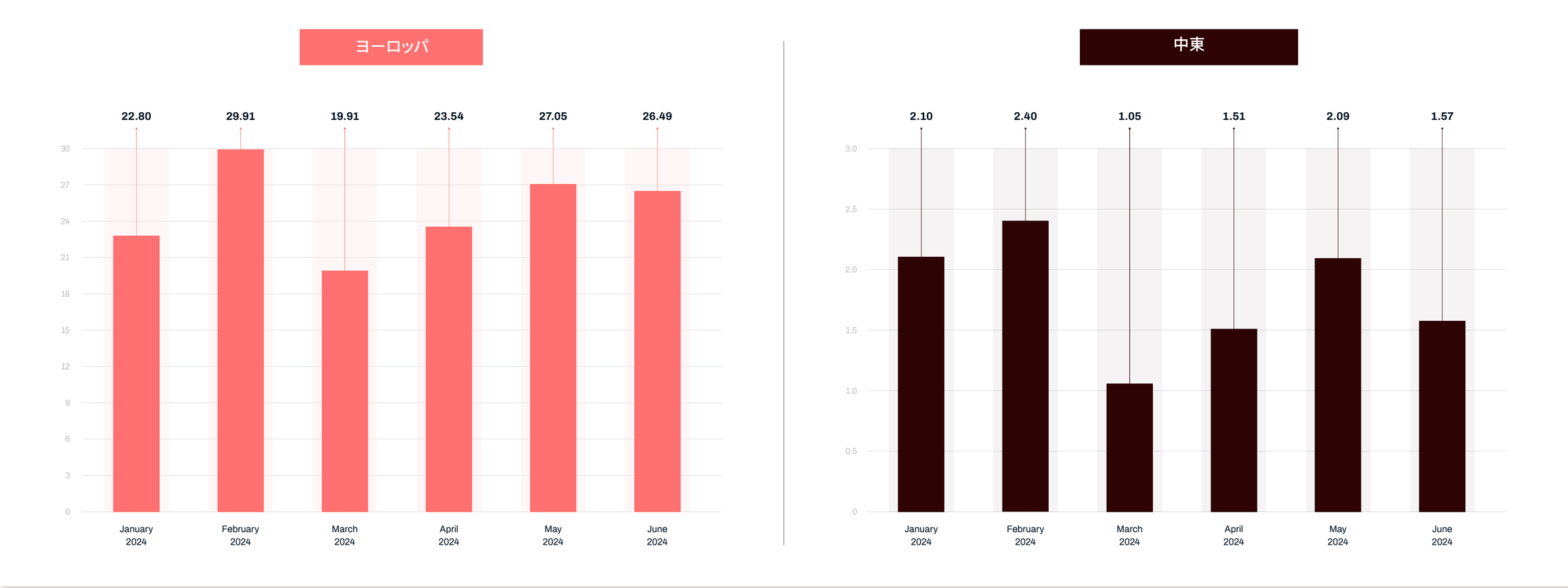


Figure 13: 被害者におけるヨーロッパと中東の割合

最も被害が多かった地域はアメリカで、リークサイトに投稿された被害者の52%を占めています。ヨーロッパは全体の25%となっています。

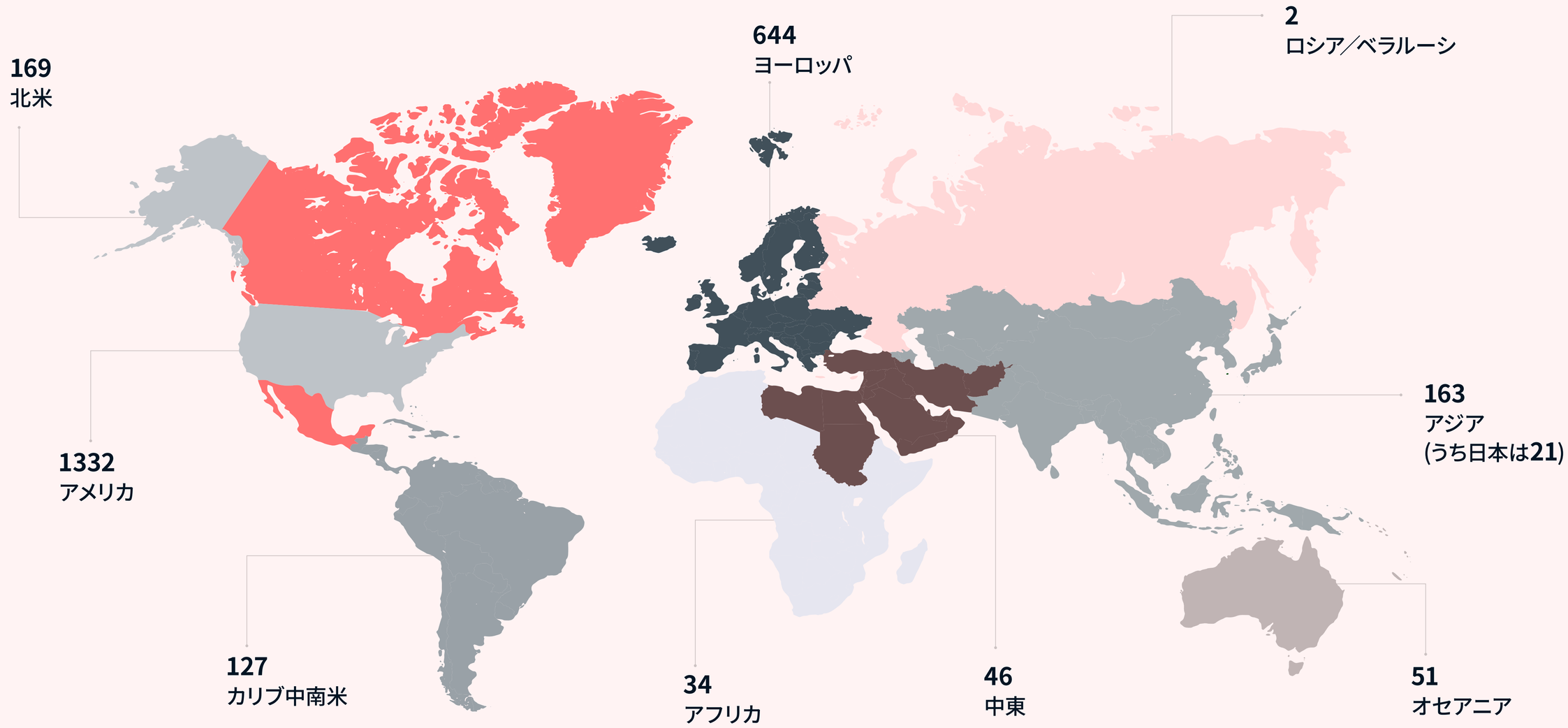


Figure 14: 地域別の被害者分布

Figure 15: 月ごとの被害者の地域別割合

Figure 15: 月ごとの被害者の地域別割合

LockbitとALPHVの影響

LEAの措置により、大規模なランサムウェアグループが分裂し、既存のグループが強化されたり、新しいグループが誕生したことはほぼ確実です。しかし多くの個人のアフィリエイトの完全なトラッキングはできないため、データに基づいてリサーチ結果を抽出することしかできません。2023年7月に初めて確認されたBlackSuitについては、Lockbitに対する LEA の措置とALPHVの出口詐欺を受けて、リークサイトに投稿された彼らの被害者が急増しました。また、増加したのはBlackSuitの被害者だけではありません。それまで20社分以上のリーク投稿をしたことがなかったMedusaは27社へと増加しました。INC Groupは3月から数が増えており、QuilinとHunters Internationalは2024年初頭に初めて増加が見られ、それ以降も増加が継続しています。アフィリエイトの支払いモデルの変更がRansomHubとMedusaにもたらした成功については、このレポートの前半ですでに取り上げたとおりです。

Figure 16は、2024年上半期の前述のRaaSグループと、LockbitおよびALPHVをめぐる事件以降の被害者数の顕著な増加を示しています。

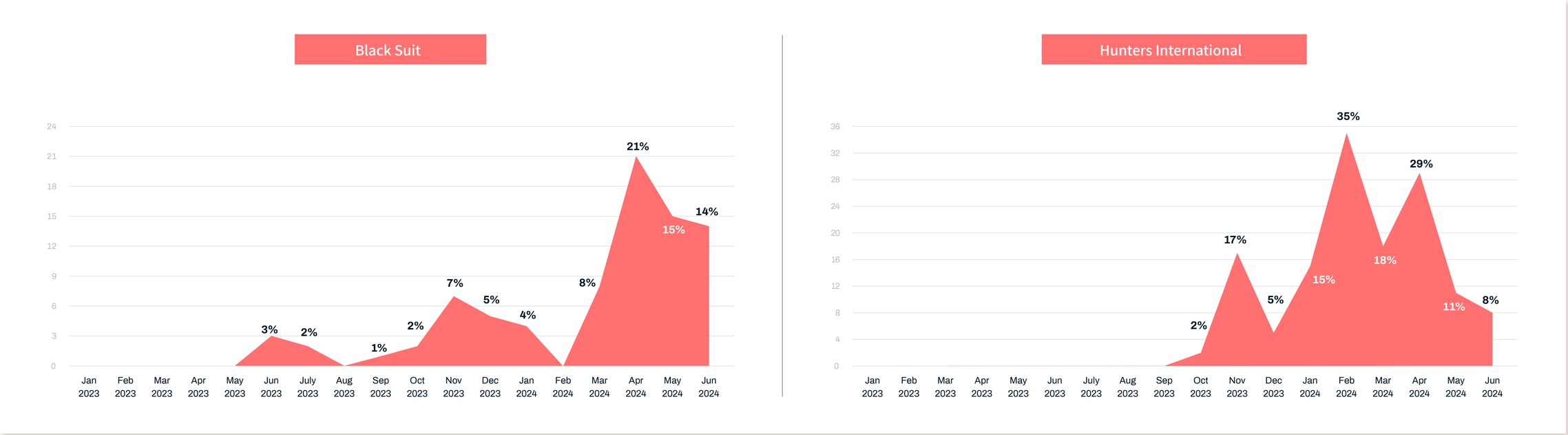


Figure 16: Lockbit／ALPHVの事件後のRaaSグループの活動

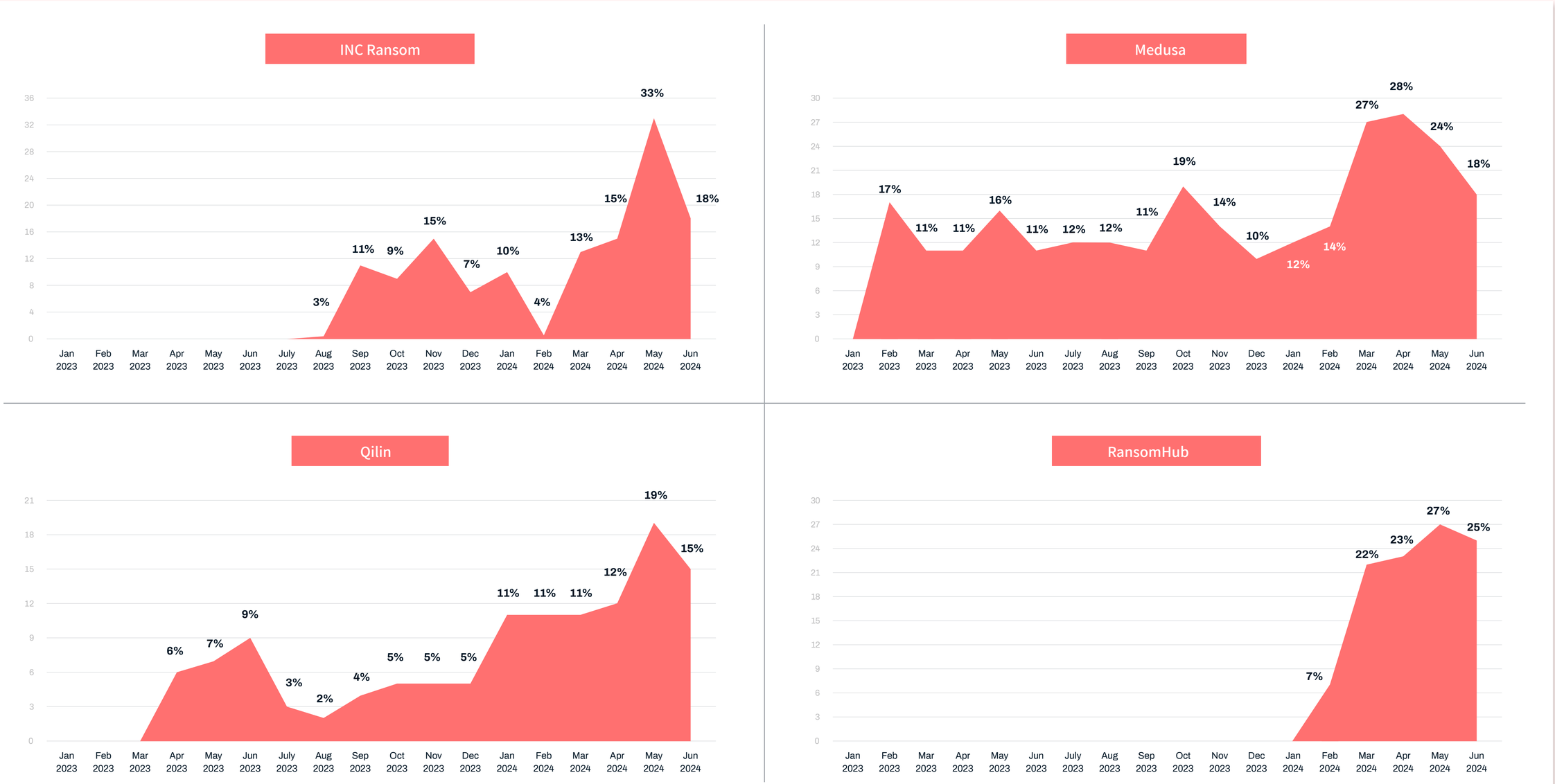


Figure 16: Lockbit/ALPHVの事件後のRaaSグループの生産性の向上

身代金支払いに関する統計

Covewareが発表した統計によると、2023年第4四半期のランサムウェアの身代金支払い率は29%に低下し、身代金の平均支払額は同年第3四半期と比較して33%減少して568,705ドルとなりました。Covewareは、これは被害者の平均従業員数の縮小によるものであり、2023年第3四半期と比較して32%の減少し、平均231人であったと報告しています。Covewareは、これは特に小規模のターゲットを狙う「スモールゲーム」志向の脅威アクターの数の増加に関連している可能性があると述べています。Covewareのデータは2023年第4四半期を具体的にカバーしていますが、Chainalysisが最近発表した2023年全体の統計によると、2023年の身代金支払総額は2022年と比較して2倍になり、2021年と比較して10〜15%増加して11億ドルに達しています。

これらの統計を組み合わせると、ランサムウェアは攻撃側にとっては総コストが高い反面、被害者からの支払い率が低く、そのためより多くの組織に攻撃を仕掛ける必要があるということになります。ただし、これら2つのリサーチは調査期間が異なることに注意し、状況の複雑さと私たちが持っている情報にギャップがあることを改めて強調したいと思います。

ランサムウェアのターゲット

ほとんどの場合、ランサムウェアの攻撃者は特定のセクターや業界をターゲットにしてはいないようです。例外はありますが、一般論として、あるグループのアフィリエイトが特定のセクターを優先的にターゲットとしているとしても、即座にそのグループ全体がその傾向にあるとは断定できません。

ターゲットとなる業界

エンジニアリング／製造業は、2024年上半期に最も影響を受けたセクターであり、観測されたすべての被害者の20.59%を占めました。

セクター	割合
エンジニアリング／製造業	20.59%
不動産／建設	9.02%
医療サービス	7.17%
金融サービス	7.02%
IT／ソフトウェア	6.82%
ビジネスサービス	6.09%
小売	5.63%
運輸／物流	5.05%
法律サービス	3.97%
教育	3.89%
その他	24.75%

Table 1: セクター別の被害者の割合

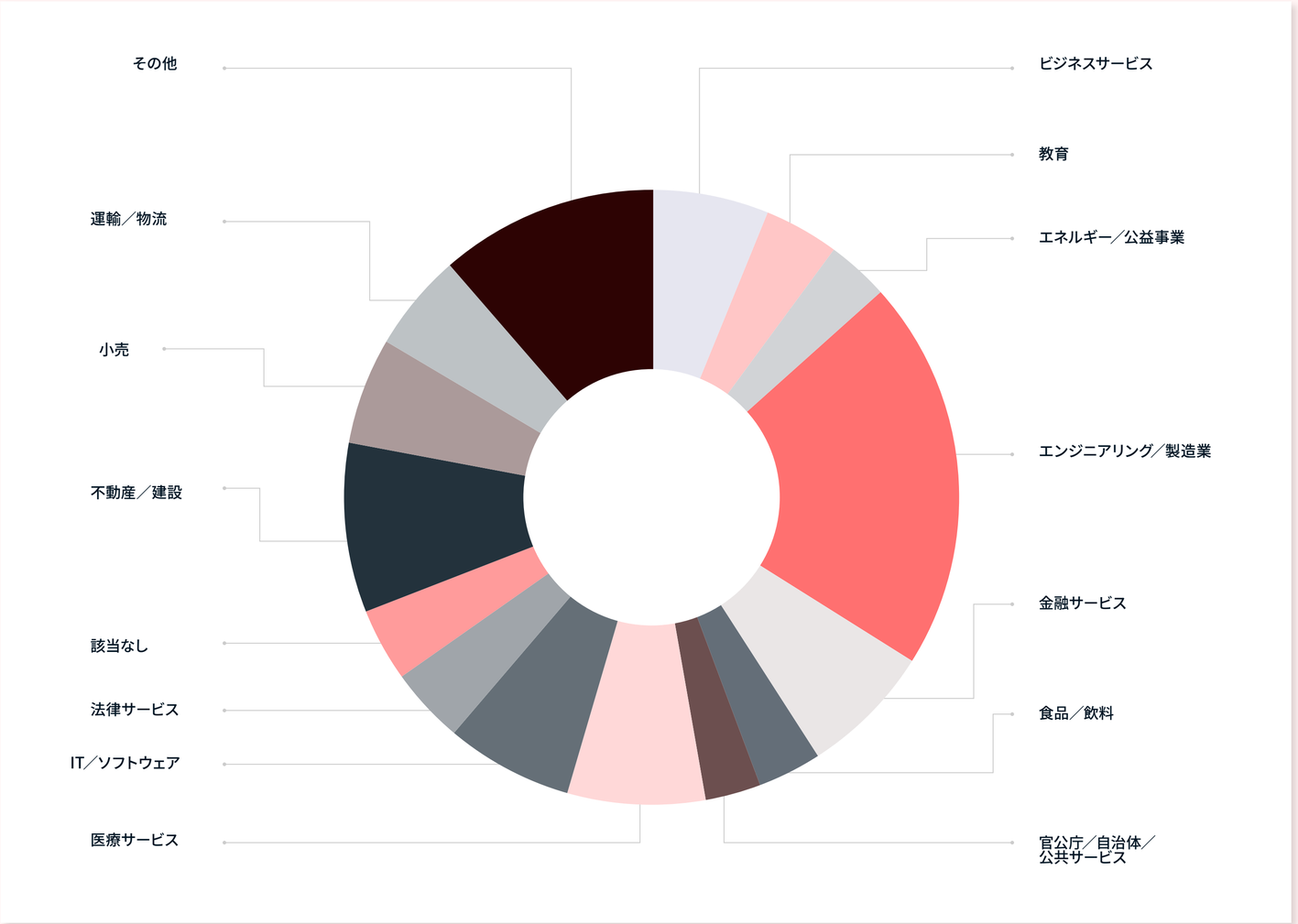


Figure 17: ランサムウェアの被害を受けたセクター

呪縛からの解放

2021年のColonial Pipeline社へのランサムウェア攻撃を受けてLEAがダークサイドに対しておこなった措置の結果、制裁回避のためにランサムウェアグループ集団間での協調的な取り組みがあったようです。ランサムウェアグループの多くは、当局による措置を回避すべく、医療機関への攻撃はおこなわないとの声明を出してました。しかし2023年には、多くのランサムウェアの亜種グループがこうした姿勢を放棄し、特に西側の医療関連の企業／団体をターゲットにすることに何の躊躇もしないようになりました。2回にわたるChange Health社に対する恐喝の成功により、犯罪グループはヘルスケア業界をターゲットにすることをより優先するようになるだろうという仮説がありましたが、データはそれが実際に起こったということは示唆していません。本年1月から5月にかけて、ヘルスケア業界の被害者数はわずかに増加していますが、被害者全体のうちのヘルスケア業界の割合は2024年を通して比較的一定のままとなっています。

ヘルスケアは最も相互に関連した産業の1つであることに留意することは非常に重要です。イギリスの研究所への攻撃や、ルーマニアの約100の医療機関に影響を与えたPhobosによる攻撃で見られるように、1つの医療機関が受けた被害が他の多くの医療機関に影響を与える可能性があり、したがってヘルスケア産業への体系的な影響は、データリークサイトで予測される範囲をはるかに超える可能性があります。

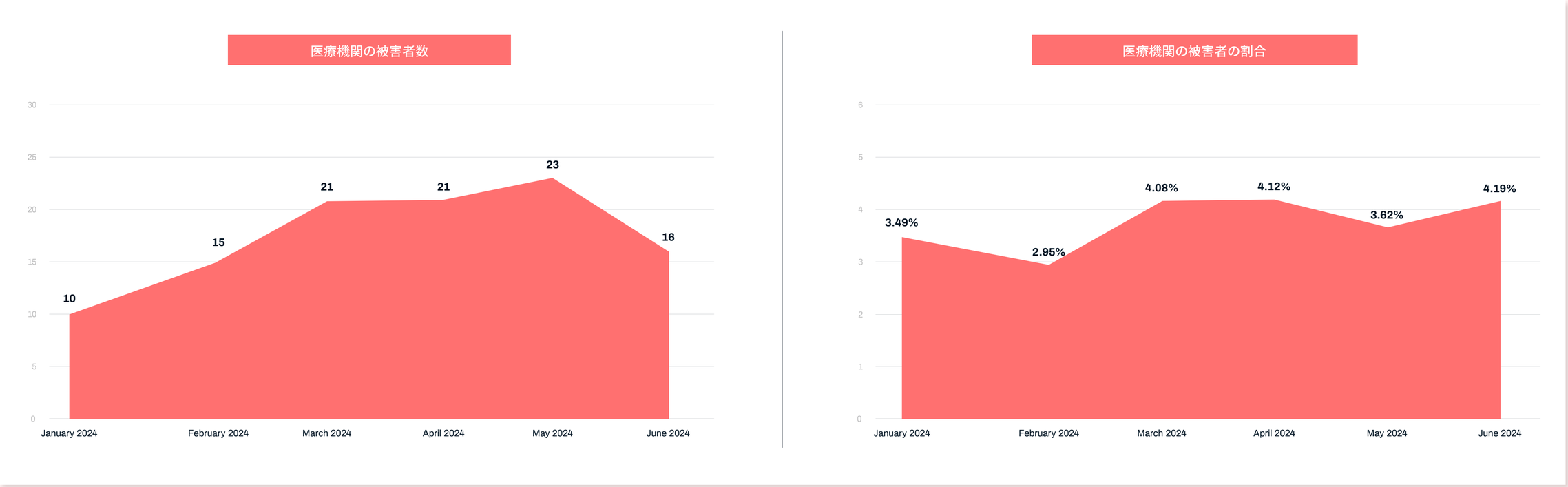


Figure 18: 医療機関の被害者の総数と実際の割合

また、2023年後半から2024年初頭にかけて、イギリス、アメリカ、フランス、オーストラリアの官公庁／自治体／公共サービスの分野において大きな傾向が見られます。攻撃グループによる『自主的なターゲットの制限』が崩れ去っていっていると考えるのが現実的ではないでしょうか。特に、犯罪者がLEAによる措置を防ぐための手段としてその制限を自らに課していただけなのであればなおさらです。西側諸国によるロシアおよびロシアの金融システムに対する制裁により、ロシアの個人に対して西側のLEAがおこなえる能力も制限される可能性があり、脅威アクターが西側当局の手の届く範囲に資産を保有する可能性は低くなっています。

官公庁／自治体／公共サービスの分野は一旦攻撃を受けるとメディアでの露出が目立ちますが、実際にはランサムウェアのターゲットとなることは少なく、その割合は被害総数のわずか3.05%となっています。とはいえ、関連する被害は、LEAによるBlackCat/ALPHVやLockbitへの措置や、その後これらのグループの活動が低下した期間と一致するパターンに従っているように見える。

Figure 19は、全ての被害における官公庁／自治体／公共サービス分野の被害者の割合と被害数を示しています。どちらも、Lockbit/ALPHVに対する措置の直後に顕著な減少を示しています。

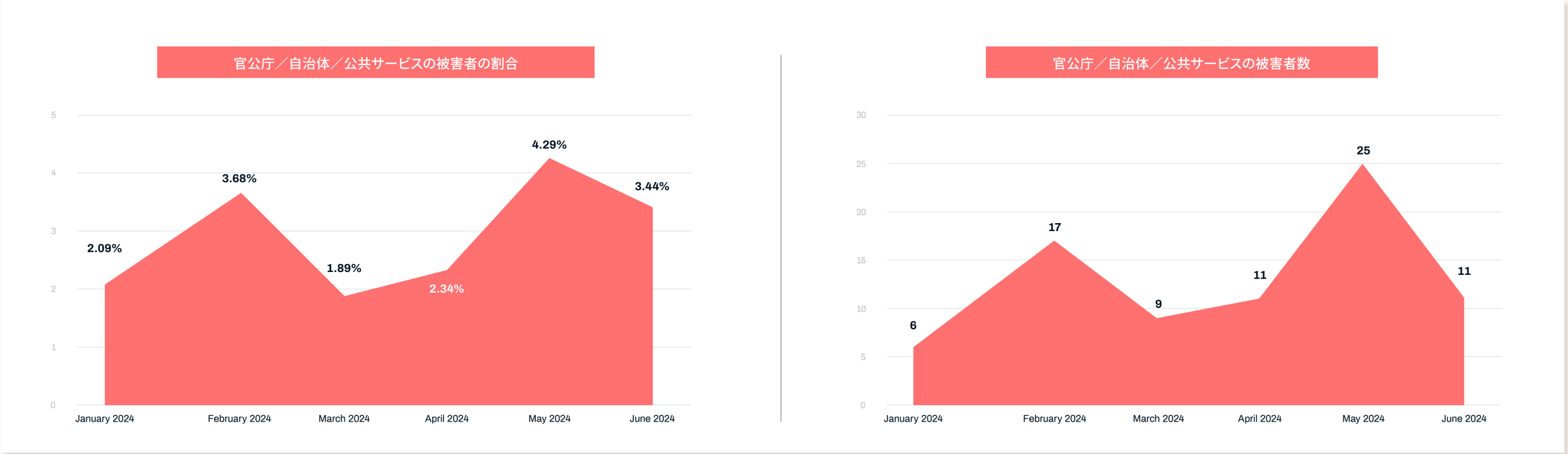


Figure 19: 官公庁／自治体／公共サービスの被害の割合および件数

2024年上半期において他のセクターに関する明らかなインサイトはほとんどありませんが、エンジニアリング／製造業のセクターではわずかながら着実に減少し、IT／ソフトウェアの業界では被害者が増加しています。これらはFigure 20に示されています。

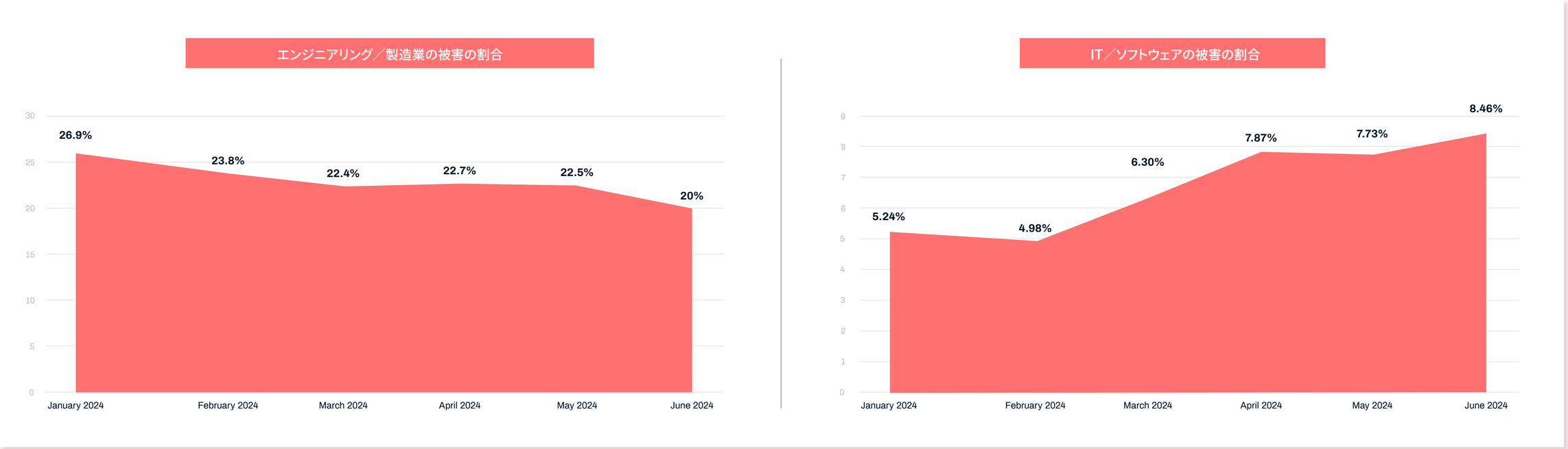


Figure 20: エンジニアリング／製造業の被害の割合の減少とIT／ソフトウェアの被害の割合の増加

FBIによるレポート

FBIは、ランサムウェアを含むさまざまな種類のサイバー犯罪に関する統計を含む、2023年のサイバー犯罪に関するレポートを発表しました。被害者から報告されたインシデントに基づく数字によると、2022年と比較して、報告されたランサムウェア攻撃は18%増加して2,825件となり、ランサムウェア攻撃による損失は74%増加しました。(注: これは発生した損失であり、支払われた身代金ではありません)

さらに懸念されるデータは、報告された2,825件の攻撃のうち、1,193件が重要インフラに対するものであり、それが前年比37%増となっていることです。報告されたランサムウェアによる損失は3,430万ドルから5,960万ドルへと74%増加しましたが、これは2023年の投資詐欺による損失45億7,000万ドルと比較すると比較的小さな金額です。投資詐欺のほとんどは暗号資産に関するもので、報告された損失の39億6,000万ドルを占めています。これは、2022年と比較して投資詐欺による損失が38%増加し、暗号資産投資詐欺が53%増加したことを意味します。

FBI は被害者の特定のサブセット、つまり、サイバー攻撃の被害に遭った際に報告を義務づけられている、または自発的におこなっているアメリカ国内の企業／団体に関するデータを収集しているという点に留意する必要があります。これらの数字から、ランサムウェアによって生み出される利益は投資詐欺のそれよりも急速に増加している、という結論を導き出すことができます。ただし、これらのデータは複雑なものであり、十分注意を払う必要があります。

ランサムウェアの戦術

イニシャルアクセス

データ収集の際に侵入ベクトルを特定するのは必ずしも容易ではありません。2024年に攻撃者が使用するベクトルの種類に大きな変化が見られるとは考えていませんが、戦術が使用される頻度の傾向は継続的に変化しています。Table 2は、ウィズセキュアのインシデントレスポンスチームが観測したイニシャルアクセスの戦術を順不同で示しています。

T1566.002	Phishing: Spearphishing Link
T1133	External Remote Services
T1190	Exploit Public-Facing Application
T1078	Valid Accounts
T1566.002	Spearphishing Link
T1566.001	Spearphishing Attachment
T1566.003	Spearphishing via Service

Table 2: 観測されたイニシャルアクセスのベクトル

大規模エクスプロイト

2024 年上半期にウィズセキュアのインシデントレスポンスチームが観測した中では、全ケースの約45%を占める、公開アプリケーション (MITRE ATT&CK ID T1190) の悪用が最も一般的な感染ベクトルでした。このインサイトは業界の他の企業にも共有されており、2024年第1四半期後半に発表されたSymantec社のリサーチでも、ランサムウェアの主な感染ベクトルがボットネットから脆弱性の悪用に変わったと述べられています。

エクスプロイト

CISA KEV (既知の脆弱性の悪用) によると、2024年にリストに追加された脆弱性は4つあり、そのうち3つは当局によって10.0 CVSSと評価されています。これは、脆弱性の深刻度スコアとして可能な最高スコアです。これは、CISAに報告されたケースでのみ明示的に観測されていない、新たに悪用された脆弱性のみです。このリストに含まれるテクノロジーはエンタープライズスケールのものです。

- モバイルデバイス管理サービス
- データサーバー
- VPNサーバー
- リモート管理ツール

これは、ランサムウェア攻撃者にとって1日でエクスプロイトが利用可能になりつつあること、そして a) 大規模向けに そして b) ネットワークセキュリティ専用に設計されたツールの脆弱性を侵害する障壁が低下していることをさらに実証しています。

サプライチェーン攻撃

2023年、ウィズセキュアの脅威インテリジェンスチームは、サプライチェーンの脅威を詳述したホワイトペーパーを発表しました。そのホワイトペーパーは、サプライチェーンを介したラテラルムーブメントによってもたらされる脅威を正確に表現していますが、サプライチェーンの脅威の要素がレポートで言及された限界を超えて発展している領域が1つあり、Log4jは「特別なケース」とされています。懸念される現実は、エンタープライズサービスに直接存在するか、エンタープライズサービス内に含まれる未知または文書化されていないソフトウェアライブラリに、CVSS CRITICALの脆弱性が多数存在することです。ここでは、ソフトウェアサプライチェーンの外部に公開されている要素の悪用を「T1190 エクスプロイトパブリックアプリケーション」と見なし、2024年2月のScreenConnect (CVSS 10.0) の脆弱性で観察されたイベントのように、信頼関係を通じてツールまたはアクセスのラテラルムーブメントが発生した場合に引用する「サプライチェーン攻撃」とは見なしません。

2024年第1四半期、ルーマニアの約100の医療機関が一連のPhobosランサムウェア攻撃の影響を受けました。短期間での攻撃の量と、被害者 (全てルーマニア国内の医療機関) の密接な論理的関連性は、原因がサプライチェーン攻撃であることを強く示唆していました。これは現在、ルーマニアのサイバー防衛機関によって確認されています。攻撃キャンペーンは、統合医療管理システムプラットフォームであるRomanian Soft CompanyのHipocrate Information Systemへの侵害から始まりました。幸いなことに、ほとんどの医療機関は過去1〜3日間のバックアップを持っていますが、それでも一部のデータは失われます。これは医療においてはクリティカルな問題となります。最近数ヶ月間、多くの国で医療機関をターゲットとした攻撃が増加していますが、これはおそらく、システム運用の中断が生死に関わる結果をもたらすためです。実際、アメリカのサイバー当局は最近、ALPHVランサムウェアグループによる標的型ランサムウェア攻撃に関して医療分野に警告を発しました。

個人情報 (ID) 攻撃

I個人情報を狙う攻撃も非常に一般的です。インフォスティーラー型マルウェアはダークウェブのマーケットプレイスで安価に入手でき、ブルートフォース攻撃、パスワードスプレー攻撃、クレデンシャルスタッフィング攻撃などの手法は、特に追加のセキュリティレイヤーが有効になっていないクラウドサービスへのイニシャルアクセスによく使用されます。

インサイダー脅威

ウィズセキュアではインサイダーによるリスクが依然として存在し、アンダーグラウンドフォーラムで積極的に採用の募集がかかり、そして宣伝がなされていることを認識しています。

二重目的ツール

二重目的ツールの使用が増えると、悪意のあるアプリケーションや正規ツールのインストールがマルウェア対策の制御を回避し、正規に使用されるテレメトリーに紛れ込む可能性があるため、ネットワーク防御者にとって大きな問題となります。ウィズセキュアのインシデントレスポンスチームによって観測されたリモートアクセス／永続化／流出用のツールはTable 3に含まれています。

リモートアクセスツール	流出
PDQ Connect	rclone
Action1	rsync
AnyDesk	winSCP
TeamViewer	SFTP
Atera	Megaupload
Syncro RMM	FileZilla
SplashTop	cURL
NetSupport	
NinjaRMM	
ScreenConnect	
RustDesk	
SimpleHelp	
QuickAssist	

Table 3: RaaS攻撃者によって使用された二重目的ツール

環境

現在、ランサムウェア攻撃者がWindows環境に特化した亜種を持るわけではないという例は数多くあります。多くのランサムウェアファミリーには、LinuxおよびESXiサービスをターゲットとする亜種があり、これは 2024年においても目新しいことではありません。

こちらも2024年には目新しいことではありませんが、クラウドサービスもランサムウェア攻撃者の標的になりつつあります。ネットワークが境界のないクラウドアーキテクチャに移行するにつれて、IDへの攻撃が新たな戦場となります。IDおよびアクセス管理会社であるOkta社は、「前例のない」クレデンシャル スタッフィング攻撃について警告するレポートを2024年4月に発表し、その中で次のように述べています。

2024年3月18日から4月16日にかけて、Cisco社のDuo SecurityとCisco Talos社は、複数のモデルのVPNデバイスに対する大規模なブルートフォース攻撃を観測しました。

2024年4月19日から4月26日にかけて、Okta社のアイデンティティ脅威リサーチチームは、同様のインフラと思われるものから、ユーザーアカウントに対するクレデンシャルスタッフィング活動の急増を観測しました。

攻撃者は暗号化よりもデータの盗難 (および削除) を好む傾向があるため、クラウドサービスはランサムウェア攻撃者にとって非常に魅力的なターゲットです。

恐喝

恐喝の手法の傾向について考えると、2023年から2024年第1四半期末までの間では大きな変化はありません。多くの攻撃者はデータの盗難と身代金のみを好む一方、データの持ち出しを試みることなく「従来の」暗号化ツールを引き続き導入する攻撃者もいます。ランサムウェア攻撃者にとって、おそらく二重脅迫が依然として最も望ましい結果ですが、脆弱なファイル転送システムやクラウド環境を標的にするなど、アフィリエイトがデータの盗難を優先している例は数多くあります。これは、暗号化対策機能やネットワークセグメンテーションの性能が向上していることも一因であると考えられますが、攻撃者が効率的に活動できることも一因となっています。

検出を回避しつつ慎重にネットワークに侵入するには時間が必要であり、企業向けセキュリティツールが導入されている場合、有能なランサムウェア攻撃者だけがそれを実行できます。よりシンプルな「強奪」攻撃の後に、企業が盗まれた機密データの回復のために身代金を支払う可能性が依然として高い場合、暗号化ツールをドロップするためにシステム全体を侵害することは、おそらく時間の無駄と見なされます。

脅迫の圧力をさらに強めようとする攻撃者も存在します。DDoS攻撃の脅迫、メディアや株主への通知などです。ウィズセキュアではこれらの戦術の有効性に関するデータを持っていませんが、これらは被害者にとってほぼ間違いなく3次的な懸念事項です。多くのランサムウェア攻撃者は依然として自分たちを「有能」かつ「プロ意識」を持つ存在に見せかけ、攻撃のターゲットを「身代金ビジネスのクライアント」と見ています。

ロシアだけの問題ではなく

東ヨーロッパとロシアは、ランサムウェア攻撃の発信源として頻繁に挙げられますが、これは、ランサムウェアのバイナリーに実行ガードレールが組み込まれ、ランサムウェアが展開されたコンピューターがキリル文字を使用している場合にランサムウェアの起動を阻止することが多く、ロシア語のサイバー犯罪フォーラムが多数存在するためと考えられます。しかしこうしたケースは減少してきており、ランサムウェア攻撃が世界中からおこなわれていることに留意することが非常に重要です。

アメリカやヨーロッパでアフィリエイトが逮捕された例は数多くありますが、アメリカやヨーロッパと犯罪人引き渡し条約を結んでいない他の国を拠点に活動しているランサムウェアグループも存在します。RA World (2023年夏に初めて観測) は、中国を拠点とする侵入セットであるDEV-0401/EMPORER DRAGONFLYと重複していると考えられるランサムウェアグループです。ウィズセキュアは、イランの攻撃者によって運営されている可能性が高い「Phalcon」ランサムウェアも観測しています。サイバーセキュリティ業界は、主にCIS (独立国家共同体) 諸国を拠点とするアフィリエイトを好んで利用する大規模なランサムウェアアフィリエイトモデルにも注目しています。ロシアとCISの圏外で活動している、漏洩済みのランサムウェアのソースコードや使い捨てのメールアドレスを利用できる、独立系の報告されていない「小動物ハンター」が相当数いることはほぼ間違いありません。

国家ハッカーによるランサムウェア

ランサムウェアは蔓延しており、その有用性は金銭的利益だけにとどまりません。業界には、国家が支援する破壊的な攻撃がランサムウェアを装った例があります。これは現在、ロシアとウクライナの紛争から距離を置いて活動しているほとんどの企業／団体にとっては、現実的にはありそうもない脅威モデルですが、しかし地政学的緊張が高まるにつれて変化していきます。ロシアとウクライナの紛争に参加していない国の民間組織であっても、ロシアの国家ハッカーによるランサムウェア攻撃キャンペーン『Prestige』の影響を受けています。Microsoft社はポーランドの組織の詳細を公開しており、ウィズセキュアでもエストニアのネットワークでのPrestige関連のインプラントを検出しました。

ヨーロッパにおいて、そしてイランとイスラエル、中国と台湾において地政学的な緊張が高まっているなか、こうした脅威モデルを再検討する必要がでてくるでしょう。

国家が支援する攻撃グループによるCNE/CAN (コンピュータネットワークエクスプロイト／攻撃) イベントを考慮する際、収益を生み出すために侵入セットを実行している北朝鮮は例外的な存在となります。北朝鮮が直接開発したランサムウェアファミリーもありますが、これらは長い間観測されていません。北朝鮮で活動するアクターたちが、RaaSモデルを利用して攻撃を実行している可能性の方がはるかに高いです。ウィズセキュアは、北朝鮮によって実行された侵入とランサムウェアアフィリエイトによる侵入の重複を検出しました。

まとめ

ランサムウェアは全世界で大きな問題であり、何百もの組織に影響を与え、数十億ドルの損害をもたらしています。ランサムウェアはほとんどの組織のネットワーク、特に中小規模の組織のネットワーク
にとって最も重大なリスクであると考えられます。

成熟／発達したランサムウェアエコシステムが存在しますが、最近の出来事により、その中で活動するグループ間の信頼が損なわれている可能性があります。より大きな成功を収めたランサムウェアグループは、高度に組織化／構造化された合法的なビジネスを厳密に模倣した方法で運営されたものです。LEAによる措置の後でも、多くのランサムウェアグループが廃業した可能性は低く、代わりに既存の比較的知名度の高くないグループに移籍したものと考えられます。それは2024年にリークサイトに投稿される被害者の数が依然と大差ないことが主な理由です。LEAの措置がランサムウェアのエコシステムに大きな影響を与えたことはほぼ間違いありません。現時点では、その長期的な有効性について結論を出すのは時期尚早ですが、短期的には顕著なプラスの影響がありました。Lockbitは復活の兆候を示しており、ほぼ間違いなく活動の再編成／再構築／強化を目論んでいます。

ランサムウェア攻撃者は、「大物狩り」という概念から離れつつあるようです。小規模から中規模の組織がランサムウェアのリークサイトに投稿されることが増えていますが、これは小規模組織では特に利用できないリスク軽減戦略 (サイバー保険など) を通じて、大企業が攻撃者の要求に応えることができることが一因である可能性があります。小規模ではあるが頻繁な恐喝の試みは、ランサムウェア攻撃者にとってより効率的な投資収益率を反映している可能性もあります。

攻撃者がイニシャルアクセスにエッジサービスの脆弱性を悪用するケースが増えているなか、堅牢なエクスポージャー管理プロセスと成熟したセキュリティツールを持つ組織は、ランサムウェア攻撃による被害をより効果的に軽減する態勢が整っています。

2024 年上半期には、ランサムウェアの活動が低下していることを示す前向きな兆候がありますが、業界と西側当局は可能な限りランサムウェア攻撃者たちに圧力をかけ、攻撃の実行をより困難なものにしていく必要があります。

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。

https://www.withsecure.com/jp-ja/home

WITH secure™