サイバー犯罪の地獄絵図

ランサムウエア攻撃＆データリーク攻撃と
ネットワークアクセスの販売状況
（2022年アニュアルレポート）

KELA

—サイバー犯罪の地獄絵図—
ランサムウエア攻撃&データリーク攻撃と
ネットワークアクセスの販売状況
（2022 年アニュアルレポート）

KELA サイバー犯罪インテリジェンスセンター

目次

エグゼクティブサマリー 2
主な調査結果 2
ランサムウエア攻撃とデータリーク攻撃 2
売り出されたネットワークアクセス 3
ランサムウエアグループ・データリークグループと
初期アクセスブローカーの関係 4
2021 年から 2022 年にかけてサイバー犯罪業界に見られた進化 5
ランサムウエア攻撃とデータリーク攻撃 6
2022 年の概要 6
ランサムウエアグループ・データリークグループのトップ 5 9
標的トップ 5 11
大きなイベント 13
大きなトレンド 18
ネットワークアクセスの販売状況 31
2022 年の概要 31
売り出し商品件数上位の初期アクセスブローカー 32
標的とされた国・業界 32
大きなトレンド 34
**ランサムウエアグループ・データリークグループと
初期アクセスブローカーの関係 38**
進化するサイバー犯罪社会の情勢 （2021 年～2022 年） 42
組織の防御者として活動される皆様への提言 43
**付録 1：ランサムウエアグループ・データ リークグループに関する
弊社データ（四半期別） 45**
付録 2：ネットワークアクセス販売状況に関する 弊社データ（四半期別） 47

エグゼクティブサマリー

近年、個人と組織の両方の間で、ランサムウエア攻撃やデータリーク攻撃に対する懸念が高まっています。これらの攻撃では、ハッカーが、被害者のコンピューターやシステム、ネットワークに不正アクセスしてデータを暗号化し、身代金が支払われるまでシステムを「人質」にとり、身代金が支払われない場合は機密情報を公開するといった行為が行われています。

こういった攻撃の他に、サイバー犯罪ソースで売り出されたネットワークアクセスも、ハッカーの手に渡ってランサムウエア攻撃やデータリーク攻撃に悪用される可能性があることから、これまで以上に注目を集めています。

本レポートでは、2022 年のランサムウエア攻撃とデータリーク攻撃、ネットワークアクセスの販売状況の概要、そしてそれらの活動に見られるトレンドの進化について詳述するとともに、攻撃を阻止してリスクを軽減する方法を解説します。

主な調査結果

ランサムウエア攻撃とデータリーク攻撃

- 2022 年、KELA が様々なプラットフォームを観察した結果、脅威アクターが「ランサムウエア攻撃またはデータリーク攻撃を行った」と主張した被害組織の数は 2,800 にのぼりました。また、被害組織を掲載していたプラットフォームの数は約 60 にのぼり、2022 年に入ってから開設されたものが約 52%を占めました。

- **要求された身代金の平均額は約 370 万米ドル**となりました（KELA が観察した身代金交渉に基づく）。

- **2022 年は、「実際にランサムウエアを使用しているグループ」と「実際にはランサムウエアを使用しておらず、ランサムウエアグループの手口を真似ているだけのグループ」を見分けることがさらに困難となりました。**一部のアクターは、アンダーグラウンドのランサムウエア・アズ・ア・サービスエコノミーに加わらずとも金銭を得られることに気付き、その結果、マルウエアを使うことなく「データリークサイト」や Telegram

チャンネルを使って情報を売買・漏えいするグループが登場しました（「Lapsus$」や「Stormous」など）。

- 2022 年、KELA が追跡調査を行ったランサムウエアグループおよびデータリークグループの**攻撃件数トップ 5** は、「LockBit」、「Alphv」、「Conti」、「Black Basta」、「Hive」となりました。これらグループは、同年に発生した全攻撃の 50%超に関与していました。

- ランサムウエアグループおよびデータリークグループの**攻撃を受けた国のトップ 5** をみ見ると、1 位は米国（40%）であり、その後に英国、ドイツ、カナダ、フランス（それぞれ全体の 4～6%）が続きました。

- 2022 年にランサムウエアグループおよびデータリークグループの標的となった**業界トップ 5** は、1 位が製造・工業製品であり、僅差で専門サービスが 2 位となりました。3 位～5 位にはテクノロジー、工事・建設、医療・ライフサイエンスが続きましたが、それら業界の被害組織数に大差はありませんでした。

- 本レポートでは、2022 年の**大きなイベント**として、ロシア・ウクライナ間の戦争がランサムウエアグループおよびデータリークグループに及ぼした影響と、RaaS オペレーション（Conti、Yanluowang、LockBit）の内部情報漏えいを取りあげています。

- 本レポートでは、2022 年の**大きなトレンド**として、ランサムウエアグループおよびデータリークグループが導入した新たな脅迫手法（被害組織の名をすぐに公表しない、「被害組織の顧客」を被害組織として掲載する、「非公開」のブログ投稿を作成する、被害組織が使用するマネージドサービスプロバイダーを介して攻撃するなど）を取りあげています。その他、**収益力を向上させる目的で導入された新たな機能**に関連したトレンド（ランサムウエアグループとデータリークグループの連携、ネットワークのアクセスや企業データの販売など）についても取りあげています。

売り出されたネットワークアクセス

- 2022 年、KELA は、主要なサイバー犯罪フォーラムで初期アクセスブローカー（IAB）が公に売り出しているネットワークアクセスの数が、著しく増加していることに気付きま

した。売り出されているアクセスのほとんどは、様々な企業のシステムへリモートでアクセスすることが可能となる資格情報であり、**商品（アクセス）数は 2,200 件超、希望販売価格の合計金額は 450 万米ドル超となりました。**

- **売り出し商品数でトップ 3** にランクインした初期アクセスブローカーは、「zirochka」、「orangecake」、「r1z」であり、いずれも 100 件超のアクセスを売りに出していました。

- **初期アクセスブローカーに標的とされた国のトップ 5** は、米国、ブラジル、英国、カナダ、フランスとなりました。

- **初期アクセスブローカーに標的とされた業界のトップ 5** は、専門サービス、製造・工業製品、テクノロジー、消費・小売、工事・建設となりました。

- ネットワークアクセスの販売に関して観察された**大きなトレンド**は、競争を勝ち抜こうと新たな手法を取り入れている初期アクセスブローカーに関するものでした（MSP の顧客に対する不正アクセス、ネットワークの偵察やその後の攻撃を容易にする新サービスの提供、最近公開されたばかりの脆弱性の悪用など）　。

ランサムウエアグループ・データリークグループと初期アクセスブローカーの関係

- 2022 年、KELA は、サイバー犯罪者の間で売り出された**ネットワークアクセスが発端になったと思われるランサムウエア攻撃とデータリーク攻撃**を数件観察しました。それらの攻撃に関与していたグループとしては、「Blackbyte」、「Quantum」、「Hive」、「Alphv」、「REvil（Sodinokibi）の後継とされるグループ」などが挙げられます。

- 最も注目すべきインシデントとしては、オーストラリアの保険会社「Medibank」社への攻撃に関連した出来事が挙げられます。**Medibank 社に対する攻撃は、非公開の Telegram チャンネルで同社のネットワークアクセスが販売された後に発生**しており、それぞれの出来事が発生した時期をもとに考えると、Telegram チャンネルで販売されたアクセスが、Medibank 社への侵入ベクトルとして使用された可能性があります。また、

この攻撃の実行犯であるアクターが同社との交渉内容をリークし、その内容からアフィリエイトと RaaS の協力体制に関する詳細が明らかとなりました。

2021 年から 2022 年にかけてサイバー犯罪業界に見られた進化

- 公に報告されている**ランサムウエア攻撃およびデータリーク攻撃の件数は、2021 年と 2022 年でほぼ同数**となりました（2021 年の方がわずかに多い件数ではあったものの、統計的有意性を示すものでありませんでした）。

- **ランサムウエアグループおよびデータリークグループの攻撃を受けた被害組織を国別にみると、トップ 5 は前年と同様に** 1 位が米国、その後に英国、ドイツ、カナダ、フランスが続き、各国が占める割合に変化はあったものの、全体的な傾向について変化は見られませんでした。これまで KELA が公開したレポートでも言及してきた通り、脅威アクターは利益を最大化するべく裕福な国の企業を攻撃する傾向があり、驚くべき結果ではないと言えるでしょう。

- ランサムウエア攻撃やデータリーク攻撃に関与している脅威アクターの数は、2021 年も 2022 年もほぼ同数となりました（各年とも追跡調査を行ったソースは約 60 件）。

- 2022 年に様々なサイバー犯罪フォーラムで売り出された**ネットワークアクセスの数は、前年比で 70%増**となりましたが、**平均価格および中央価格は前年比で下落**しました。また前年に続き 2022 年も、売り出されたアクセスの大半は米国企業のものでした。

- **当初、ランサムウエアグループやデータリークグループは法執行機関の取り締りを懸念していましたが、2022 年に報告された攻撃件数に減少は見られませんでした。この結果は、概して脅威アクターがランサムウエア攻撃やデータリーク攻撃にともなうリスクを懸念しながらも、依然それらの手口を収益性が高い手法と見なしていることを示唆しています。**KELA は、**初期アクセスブローカーの販売するネットワークアクセスが、**ランサムウエア攻撃の初期侵入ベクトルや、情報窃取・侵害を目的としたネットワークへの不正アクセス手段として、**今後もサイバー犯罪者の間で引き続き人気の高い「商品」になる**であろうと予想しています。

ランサムウエア攻撃とデータリーク攻撃

2022 年の概要

2022 年、KELA は、様々なランサムウエアグループやデータリークグループが、自らのブログやデータリークサイト、身代金交渉用プラットフォームなどで公開した被害組織や、公の報告で公表された被害組織を観察しました。我々が観察した被害組織の数は約 2,800 にのぼり、それら被害組織が掲載されたプラットフォームの数は 60 件弱となりました[1]（注：本レポートで記載する「被害組織」は、攻撃を受けた組織の他に個人も含めた総称として使用している場合があります）。またこの 60 件弱のプラットフォームのうち約 52%は、2022 年に入ってから開設されたものであることが判明しました。ここで重要なポイントは、世界中でランサムウエア攻撃やデータリーク攻撃を受けた実際の被害組織の数は、2,800 よりも大幅に高い数字になるということです。その要因として、まず身代金を支払った組織は、通常は被害組織としてその名を公開されないこと、全てのランサムウエアオペレーションが自らのウェブサイトを公開しているわけではないこと、また被害者が「ホームユーザー」の場合はランサムウエアブログや報道、公のレポートに掲載されないため、その数値化が非常に困難であるということが挙げられます。

2022 年、ランサムウエアグループとデータリークグループは相当な収益を手にしました。我々が、様々なアクターとその被害組織間のやり取り約 80 件を観察した結果、攻撃者が要求した身代金の平均額は 370 万米ドルとなりました。要求した身代金の平均額が最も高かったのはランサムウエアグループ「Conti」（950 万米ドル）であり、その次に「Lorenz」（930 万米ドル）、「Hive」（560 万米ドル）、「AvosLocker」（160 万米ドル）が続きました。また、我々が観察した中で最も高額な身代金を要求していたグループは Hive であり、同グループは 2022 年 2 月に中国の投資会社を攻撃した際、身代金として 5,000 万米ドルを要求していました。なお、観察したやり取りの中には被害組織の名が不明なものが複数あり、またそれらのやり取りの中では、LockBit が身代金の額を 2,800 米ドル～5,000 米ドルの範囲に引き下げていることが観察されました。高い利益を手にしようと目論むランサムウエアグループにとって、こういった身代

[1] 付録 1 の各四半期毎のデータをご参照ください。

金の引き下げは一般的な行為ではありません。したがって、LockBit のアフィリエイトの一部が、企業のみならず「ホームユーザー」をも標的にしているという可能性が考えられます。

また 2022 年は、「ランサムウエアグループ」と「実際には暗号化マルウエアを使用せず、ランサムウエアグループの手口を模倣しているだけのグループ」を区別することが、これまで以上に困難となりました。通常、被害組織を掲載したブログが新たに登場すると、サイバー犯罪者や研究者のコミュニティでは、即座にそれらのブログが「ランサムウエアブログ」と呼ばれるようになっています。しかし一部のグループは、自らが活動するサイトやプラットフォームであえて「ランサムウエア」という言葉を使い、「ランサムウエアブログ」と呼ばれる状況を助長していながら、自分達が実際にカスタム版のランサムウエアを所有している、または一般的に手に入るランサムウエアを使用しているということを証明するにはいたっていません。

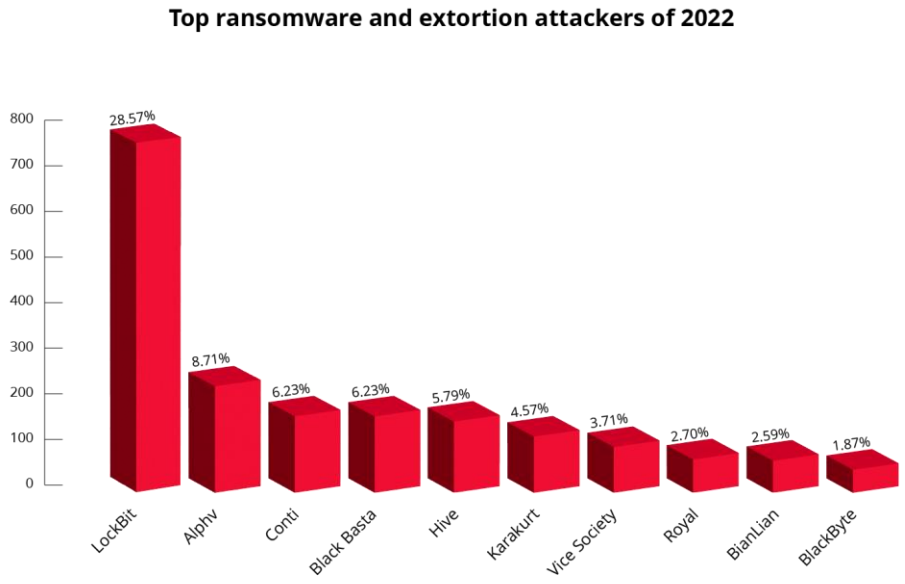
このように、ランサムウエアを展開することなく情報をリーク・販売するサイトが出現しているという状況は、脅威アクターがアンダーグラウンドに広がるランサムウエア・アズ・ア・サービスのエコシステムに参加せずとも、窃取データや侵害行為を収益化できると気付いたことを示唆しています。我々は、マルウエアを使用せずに情報のリーク・販売のみを行っていると思われるサイトを「データリークサイト」と呼んで「ランサムウエアブログ」と区別しています。また、データリークサイトを運営しているサイバー犯罪者については「恐喝アクター」または「データリークアクター（グループ）」と呼んでいます。

恐喝アクターやデータリークアクターの中でも、2022 年に最も大きな注目を集めたグループとしては「Lapsus$」と「Stormous」が挙げられますが、どちらもメディアやサイバーセキュリティ研究者の間ではランサムウエアグループと呼ばれています。また両グループともに、主に Telegram のチャンネルで自らの活動を公表し、有名な組織を攻撃したと主張し、それらの組織から窃取したとされるデータをリークしていました。また時に彼らはランサムウエアを使用していると主張していましたが、この主張が証明されることはありませんでした。さらに、Stormous が攻撃したと主張している被害組織については、過去に他のグループによって侵害され、データをリークされていた事例が多数観察されました。つまり Stormous に関しては、自らを熟練アクターに見せかけるべく、既に他のグループが侵害・リークしたデータを再利用していた可能性が非常に高いものと思われます。

我々は、こういったアクターが、2023 年もランサムウエアグループの「名声」と、その呼び名がもたらす恐怖心に便乗して、成功をおさめるであろうと予想しています。

ランサムウエアグループ・データリークグループのトップ 5

我々が追跡調査を行った攻撃グループのトップ 5 は、2022 年に観察された被害組織に対する攻撃の 50%超に関与していました。最も多くの被害組織を掲載していたのは LockBit のランサムウエアブログであり、同ブログに掲載された被害組織が全体の 3 分の 1 を占めました。また LockBit の被害組織を国別にみると、大半は米国の組織であり、その後にフランス、イタリアの組織が続き、業界別にみると主に専門サービス、製造・工業製品、工事・建設が標的となっていました。



我々は、2021 年に観察されたランサムウエア攻撃のトレンドについて詳述したレポート[2]の中で、LockBit の進化について取りあげましたが、同グループは 2022 年も進化を続け、マルウエアの新バージョンと新たなアフィリエイトプログラムをリリースしていました（マルウエアとアフィリエイトプログラムの名称はいずれも「LockBit 3.0」）。LockBit の代表者はサイバー犯

[2] Beware. Ransomware. 2021 年に確認されたランサムウエアのトップトレンド

罪フォーラムで、ランサムウエア「BlackMatter」のソースコードを購入して LockBit 3.0 用に改良したことを認める発言を行っており、また 2023 年 1 月には、LockBit の RaaS でアフィリエイトが利用できるランサムウエア（「locker」）が 4 バージョンあるとして、その詳細を語っていました。その内容によると、彼らの RaaS で提供されるランサムウエアは、バージョンによって採用している暗号化アルゴリズムや暗号化の速度が異なり、また暗号化できるファイルの量も異なるということでした。さらにそのうちの 1 バージョンについては、リークしたランサムウエア「Conti」のソースコードを使ってビルドされており、同月中にリリースされると説明していました。

また 2022 年、LockBit は「結束力があり経験豊富なペンテスターのチームを探している」、「アクセスを提供してくれる人物と連携するだけの用意がある」と発言していました。これに加え、LockBit のサイトやランサムウエアに存在する脆弱性、または TOX や TOR に存在するバグで同グループのオペレーションにダメージを与えうるものを発見・報告した人物に金銭を支払うという、独自のバグ報奨金プログラムも立ち上げました。同グループの主張によると、支払われる報奨金の額は 1,000 米ドル～100 万米ドルになるということです。

LockBit に関連した出来事の中でも注目すべきものの 1 つは、決済およびデータ保護ソリューションを提供する米国企業「Entrust」社に対して行われた攻撃です。2022 年 8 月、LockBit は Enrust 社に不正アクセスしたと主張し、同社から窃取したとされるデータを公開しましたが、Entrust 社のデータを公開しはじめた直後に、自らのデータリークサイトが DDoS 攻撃に見舞われる事態となりました。この事件について、LockBit は Entrust 社と関連のある人物が DDoS 攻撃を実行したと主張していました。そしてこの攻撃の後、LockBit の管理者は、今後同グループの活動に新たな戦術を導入する旨を宣言しました。この管理者は、グループのインフラを強化して、新たなミラーサイトと DDoS 回避策を実装することを約束しており、いずれも 2022 年内に実装を終えたものと思われます。また LockBit は、自らのサイトに「ファイル共有」機能と「メモ」機能を追加し、同サイトのユーザーがファイルをアップロードして非公開のメモを作成し、限られたユーザー（受信者）のみと共有できる仕組みを確立していました。

LockBit 関連でもう 1 つ注目すべき出来事として、米国のサイバーセキュリティ企業「Mandiant」社に対する攻撃が挙げられます。ただしこれについては、同社が「LockBit と Evil Corp の活動は重複している」と主張したことに対する報復行為であり、またある意味 LockBit の「売名行

為」であったこと、そして実際には LockBit が Mandiant 社を侵害していなかったことが後に明らかとなりました。

LockBit 以外でトップ 5 にランクインしたグループ（Alphv、Conti、Black Basta、Hive）は、いずれも 160 を超える組織を自らの被害組織として主張しており、この 4 グループの被害組織が全被害組織の 27%を占めました。Conti が 2022 年 5 月末に公の活動を停止していたにもかかわらず、2022 年のトップ 5 にランクインしていたという結果は非常に興味深いと言えます。

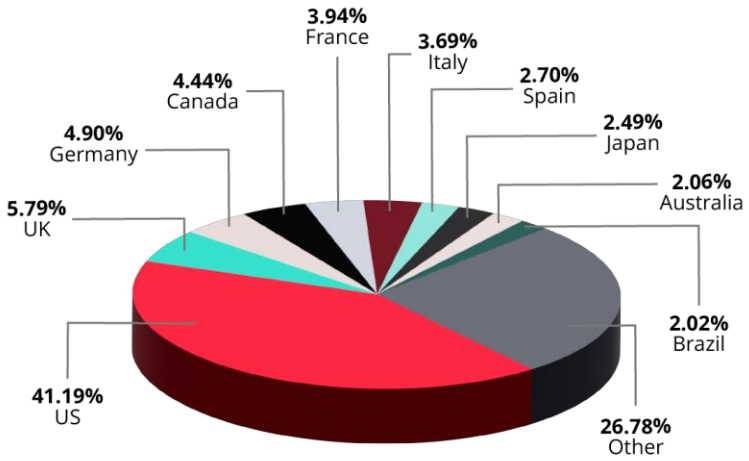
また、2022 年は、攻撃した被害組織を公開するオペレーションが、新たに 30 立ち上げられました。2022 年の攻撃件数トップ 5 で Conti と 3 位を共有した Black Basta も、2022 年に立ち上げられたオペレーションの 1 つです。

標的トップ 5

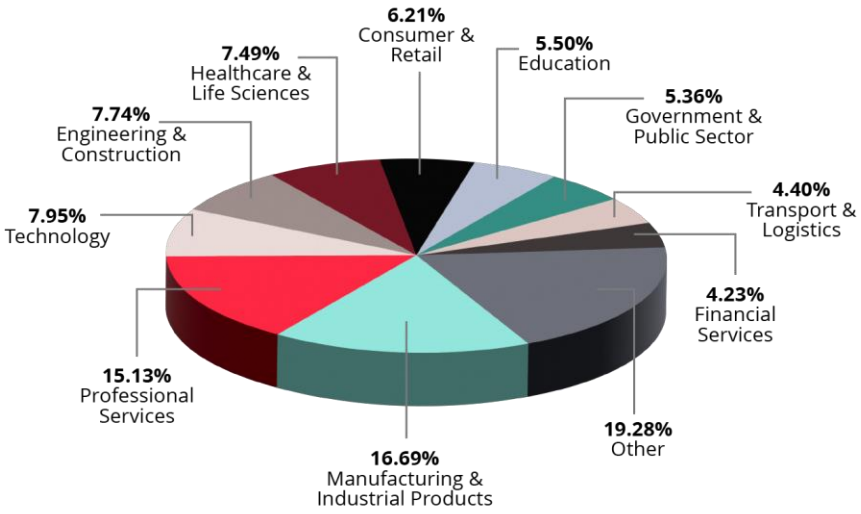
ランサムウエアグループやデータリークグループの攻撃を受けた組織を国別にみると、2022 年を通じて最も攻撃を受けたのは米国の組織であり、被害組織全体の 40%超を占めました。その後には、英国、ドイツ、カナダ、フランスが続きましたが、その割合はいずれも全体の 4%～6%の範囲に留まりました。

また、攻撃を受けた組織を業界別にみると、2022 年に攻撃を受けた業界トップ 5 の 1 位は製造・工業製品であり、僅差で専門サービスが 2 位となりました。3 位～5 位はテクノロジー、工事・建設、医療・ライフサイエンスですが、攻撃を受けた組織の数はいずれの業界もほぼ同数となりました。

Top targeted countries of 2022 by ransomware and extortion actors



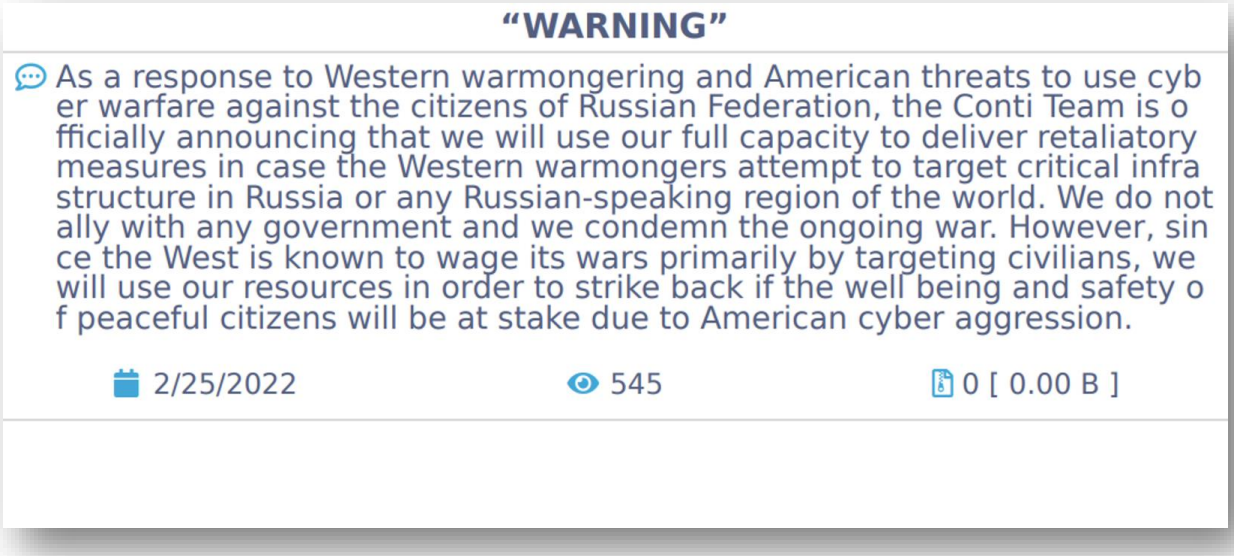
Top targeted sectors of 2022 by ransomware and extortion actors



大きなイベント

ロシア・ウクライナ間の戦争

2022 年は、その年明けからロシア・ウクライナ間の戦争が始まり、これにあわせて両国とその支援者がサイバー攻撃を展開する事態となりました。その結果、国や企業のネットワーク防御担当者には、ランサムウエア攻撃をはじめとするサイバー攻撃を受ける可能性があるとの警告が出されました。一方、Conti や Stormous などのランサムウエアグループやデータリークグループは、サイバー戦争に参戦してロシア側につくことを公言しました。



Conti がロシアに対する支持を表明しているメッセージ（Conti のデータリークサイト）

しかし大半のランサムウエアグループは、ロシアかウクライナのいずれか一方を支持することを避けました。例えば LockBit は、2022 年 2 月 27 日に掲載した投稿の中で、自分達は「素朴で平和な人々」であるがゆえに中立の立場を維持すること、そして自分達の活動が「単なるビジネス目的」であることを明言していました。またこの投稿では、「我々は、いかなる状況においても、いかなる国の重要インフラに対するサイバー攻撃にも決して参加しない」と断言していました。

その他、Alphv（BlackCat）も中立の立場を選択していました。2022 年 2 月 28 日、Alphv のメンバーは、彼らが「共有するエコシステム」に政治を持ち込んだ「Conti とその他の人々・グループを断固非難する」とのメッセージを、グループ内部のサポートチャット経由で公表しました[3]。また同グループは、「インターネットは政治の場所ではない。インターネットの影の側面はなおさらだ」とも発言していました。

ロシア・ウクライナ間の戦争は、サイバー犯罪社会の情勢にも影響を及ぼしましたが（弊社ブログをご参照ください[4]）、データリークグループやランサムウエアグループの主な動機が常に金銭であるという点に変わりはありませんでした。国民国家の支援を受けたアクターの一部については、ロシアまたはウクライナを標的にランサムウエアを展開している様子が観察されましたが、金銭的動機に基づいて活動するグループがそういった活動に参加することはありませんでした[5]。

ロシア・ウクライナ間の戦争が発端となり、ランサムウエアグループやデータリークグループの間で発生した大きな事件の 1 つとして、Conti の内部チャットがリークされた事件が挙げられます。Conti がロシアに対する支持を誓った数日後の 2022 年 2 月 27 日、ウクライナ人研究者と思われる人物が、Conti のメンバー間で交わされたやり取りを Twitter アカウント「ContiLeaks」で公開したのです。

しかし興味深いことに、ロシア・ウクライナ間の戦争に触れる Conti の言葉使いにも、このリーク後の数カ月で変化が生じていました。2022 年 3 月 31 日、同グループは「『2 日以内の制圧』の 2 カ月目を迎えたぞ」と投稿していました。ロシアはキーウを 2 日で制圧すべく計画していたものの、その計画は実現せず、キーウが陥落することはありませんでした。Conti は自らをキーウのこの状況になぞらえ、「自分達は何者かに内部情報をリークされたが、それでもリーク直後にオペレーションを終了することなく、現在も活動しているのだ」ということをほのめかしていたのです。

[3] Dmitry Smylianet の Twitter

[4] ロシアのウクライナ侵攻がもたらしたサイバー犯罪社会情勢の変化

[5] ESET 社研究者の Twitter

RaaS オペレーションの内部情報リーク事件

ランサムウエア・アズ・ア・サービス（RaaS）オペレーションの場合、RaaS の運営側が、攻撃に使用するランサムウエア（「locker」）やインフラストラクチャをアフィリエイト（サイバー犯罪業界のスラングで「adverts」とも呼ばれます）に提供します。サイバー犯罪者は、この RaaS のアフィリエイトを多数集めることによって、自らの活動を拡大することができるようになりました。しかし、優れたビジネスのアイデアには必ず負の側面があります。そして RaaS オペレーションを運営するグループにとっては、プライバシーに関するリスクの増加が負の側面となりました。RaaS オペレーションに参加するメンバーが増加すればするほど、内部の仕組みに関するデータを何者かに窃取・リークされるという可能性も増加します。そして 2022 年、Conti と Yanluowang、LockBit が内部情報をリークされる事態に直面しました。

Conti 内部情報のリーク

先に述べた通り、サイバー犯罪者のデータが漏えいして大きな注目を集めた事例の 1 つとして、ランサムウエアオペレーション Conti の内部で交わされたチャットのリークが挙げられます。リークされた Conti のチャットには、以下の内容が含まれていました。

- Jabber のログ（ContiLeaks が複数に分けて Twitter 上でリーク）。この時 Twitter 上でリークされたログは、q3mcco35auwcstmt[.]onion でホストされた Conti の Jabber サーバーから発信されたものと思われます。また Jabber を使って行われたチャットの大半は、各メンバーが他のメンバーと 1 対 1 でやり取りしていた個別チャットであると思われます。まず第 1 部には 2020 年 6 月 21 日から 2020 年 11 月 16 日までのメッセージが含まれており、第 2 部には一部空白期間があるものの、2021 年 1 月 29 日から 2022 年 2 月 27 日までのアーカイブが含まれていました。
- Rocket.Chat のログ（こちらも ContiLeaks によるリーク）。リークされたログは 6 台の Rocket.Chat サーバーから収集されており、2020 年 8 月 31 日から 2022 年 2 月 26 日までの情報が含まれていました。

我々は、Conti から流出したチャットを分析する中で、特定のランサムウエアグループに属していなかったランサムウエア攻撃者らが集い、進化していった流れを読み取ることができました。

当初彼らは様々なランサムウエアを扱っており、チャットの中ではRyukやConti、Mazeを別々のプロジェクトとして取りあげていました。そしてそんな彼らの活動が、最終的に現在（2021年～2022年）のContiのオペレーションを形成するにいたったのです。グループとしてのContiは高度に組織化されており、ハッカー、コーダー、テスター、リバースエンジニアリングスペシャリスト、クリプター、OSINT スペシャリスト、交渉者、IT サポート、人事などのチームで構成されていました。

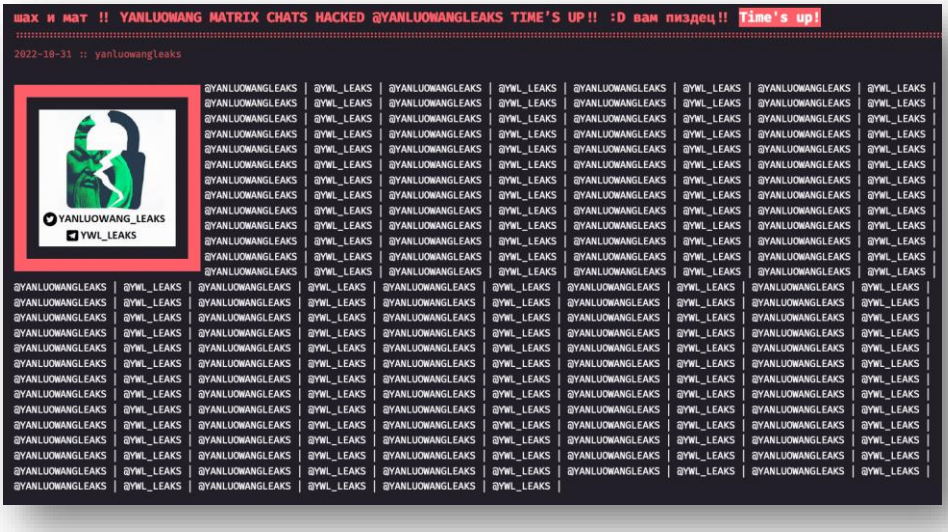
Conti から流出したデータは相当な量にのぼり、企業のネットワーク防御を担当される皆様にとっても有益な情報となることが明らかとなっています。Contiから流出した内部データの詳細な分析については、弊社のレポートをご確認ください[6]。

Yanluowang 内部情報のリーク

グループ内部のやり取りが流出する事態に見舞われたもう1つのグループはYanluowangです。Yanluowangはロシア語話者のランサムウエアグループですが、その活動量は比較的少ないものとなっています（2021年11月～2022年8月に掲載された被害組織は7つのみ）。

2022 年 10 月 31 日、何者かが Yanluowang のブログに不正アクセスし、同ブログで「Yanluowang の Matrix チャットをリークした」と主張する投稿を公開しました（この時の投稿の一部はロシア語で記載されていました）。またこの投稿が公開された同日、今度は「ywl_leaks」と名乗るユーザーが、ロシア語話者の集うサイバー犯罪フォーラム「Exploit」でYanluowangのものとされるチャットを公開し、さらにはTwitterユーザー「@yanluowangleaks」が同じ内容のファイルを Twitter 上で公開しました。そしてその後は、このファイルをダウンロードするリンクが様々なTelegramチャンネルへと拡散されました。リークされたチャットは通信プロトコル「Matrix」を介してやり取りされていたものと思われ、その中には個人チャットが 2 つ、グループチャットが 4 つ含まれていました。またいずれのメッセージもロシア語で記載されており、やり取りが行われた日付は2022年1月～同年9月となっていました。

[6] Conti から流出した 内部データの分析



ハッカーが Yanluowang のブログに残した投稿

Yanluowang から漏えいした情報は、Conti から漏えいした情報よりも量が少なかったものの、ランサムウエアアクターのやり取りの背景情報をより明らかにする情報が含まれていました。Yanluowang のリークの詳細については、本件に関する KELA の Twitter スレッドをご参照ください[7]。

LockBit 内部情報のリーク

2022 年に攻撃した被害組織の数でランサムウエアグループおよびデータリークグループのトップに君臨した LockBit は、常に自らの擁するアフィリエイトの数を自慢していましたが、かつてのライバル Conti がたどった運命から逃れることはできませんでした。2022 年 9 月 21 日、同グループが何者かによる不正アクセスを受け、ランサムウエア「LockBit 3.0」のビルダーが漏えいする事態となったのです。この時のリークでは、未詳のユーザー「Ali Qushji」が、LockBit 3.0 のビルダーを発見したと主張して Twitter で LockBit 3.0 のビルダーを公開し（この Twitter アカウントは現在利用制限がかけられています）、「protonleaks」と名乗るユーザーが同じビルダーのコピーをフォーラム「VX-underground」で公開しました。この Ali Qushji と protonleaks

[7] KELA の Twitter

は、おそらく同一人物であると思われます。さらに、「Persistent」と名乗るユーザーも同じビルダーを BreachedForums で公開していましたが、Persistent については当人がこのリークに関与していたのか、それともリークされていた情報を再公開しただけであるのかは明らかとなっておりません。

LockBit は、フォーラム「XSS」でこのインシデントについて取りあげ、同グループが採用したプログラマーが今回のリーク事件に関与していると主張しました。

またこのリーク事件の後、ランサムウエアグループ「BI00Dy」が複数の攻撃でランサムウエア LockBit 3.0 のビルダーを使用していることが報告されました。これは、今回のようなリーク事件において当然の結末でもあり、2021 年にランサムウエア「Babuk」のソースコードが流出した際にも、その後再三にわたって同ランサムウエア（Babuk）のソースコードが再利用される事態となりました。

ランサムウエアグループ間の競争が激化する時代となり、さらに政治情勢が緊迫する現在、企業でネットワークの防御に従事される皆様におかれましては、サイバー犯罪ソースを注意深く監視し、このようなリーク情報を速やかに検知して防御の一助とされることをお勧めいたします。

大きなトレンド

新たな脅迫手法

ランサムウエアグループやデータリークグループは、データを公開すると脅迫したり、身代金の支払期限を設定したり、起こりうる結末を身代金要求メモに記載するなど、被害組織に恐怖心を引き起こす手口に依存しています。そのため彼らは、被害組織に与える恐怖のレベルを常に引き上げる必要に迫られており、2022 年には攻撃後に新たな種類の活動を導入している様子が観察されました。

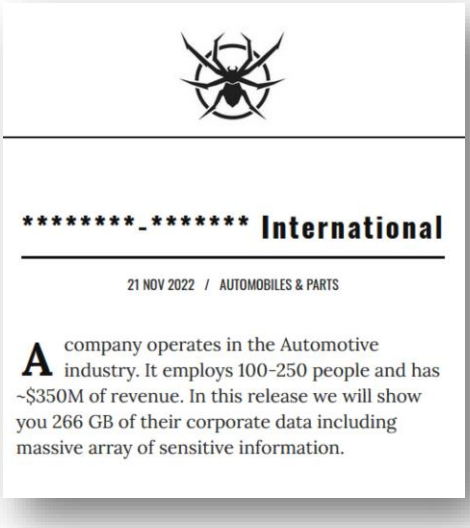
被害組織の名をすぐに公開しない

2022 年、複数のグループが、「完全な名称を記載しないまま、被害組織を公開する」という手口を採用していました。例えば「Midas」は自らのデータリークサイトで、複数の被害組織を

「new company（新しい会社）」という名称で掲載していました（被害組織が身代金を支払わなかった場合は、投稿を編集して組織名を記載します）。

ランサムウエアグループ「Lorenz」も同じ手法を採用しており、2022 年全体を通して同グループは自らのブログで、被害組織を「new target company（新たな標的企業）」として公開していました。Lorenz のブログでは、被害組織が身代金を支払わなかった場合、その名を記載した新たな投稿を作成して公開しているものと思われます。

また、この手法をゲーム化しているグループも複数確認されました。例えば「Karakurt」は被害組織の名を 1 文字ずつ公開しており、「BianLian」は被害組織の名を部分的に公開して訪問者に推測するよう促していました。



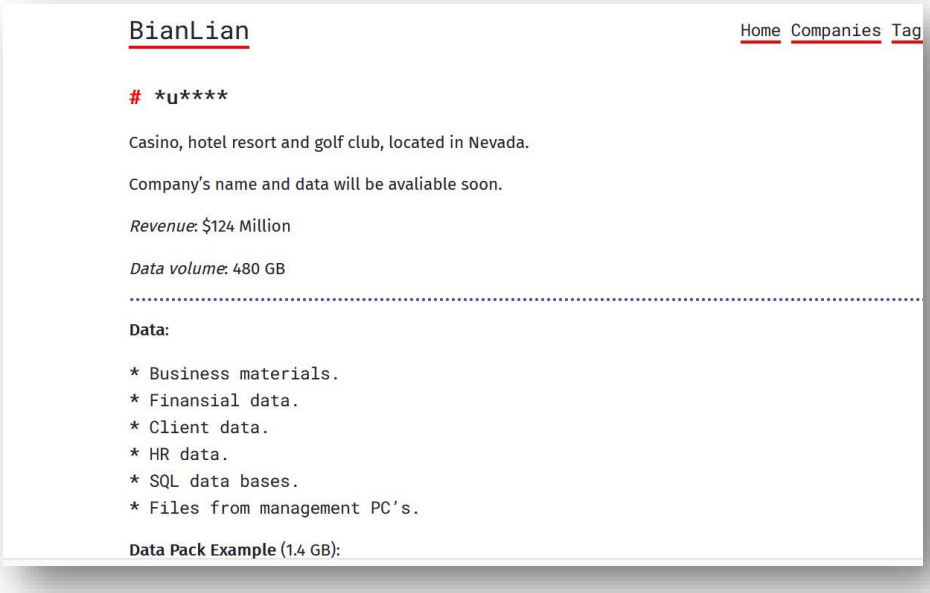
Karakurt が被害組織名を編集して公開した投稿

C***-****F** International**

21 NOV 2022 / AUTOMOBILES & PARTS

A company operates in the Automotive industry. It employs 100-250 people and has ~$350M of revenue. In this release we will show you 266 GB of their corporate data including massive array of sensitive information.

Karakurt が被害組織名の数文字を明らかにした投稿



BianLian

Home Companies Tag

*u****

Casino, hotel resort and golf club, located in Nevada.

Company's name and data will be avaliable soon.

Revenue: $124 Million

Data volume: 480 GB

Data:

* Business materials.
* Finansial data.
* Client data.
* HR data.
* SQL data bases.
* Files from management PC's.

Data Pack Example (1.4 GB):

BianLian が被害組織名の 1 文字を明かしている投稿

とはいえ、ほとんどの事例では、これらのグループがその名を完全に公開する前に、被害組織を特定することが可能です。

「被害組織の顧客」を被害組織として掲載

ランサムウエアグループは、被害組織の顧客やパートナー企業に連絡を取り、彼らに攻撃の事実を伝えることで被害組織にさらなるプレッシャーを与えるという手口も頻繁に利用しています。2022 年 KELA は、「Clop」がこの手法を大々的に取り入れ、被害組織の顧客に電子メールを送信していることを発見しました。顧客に送られたメールには、「If [the victim] does not contact us then we gonna start to publish the data on the onion website（［被害組織］が我々に連絡してこなければ、TOR 上のサイトでデータを公開するぞ）」"という文章が含まれており、被害組織が交渉を開始するよう仕向ける狙いがあったものと思われます。

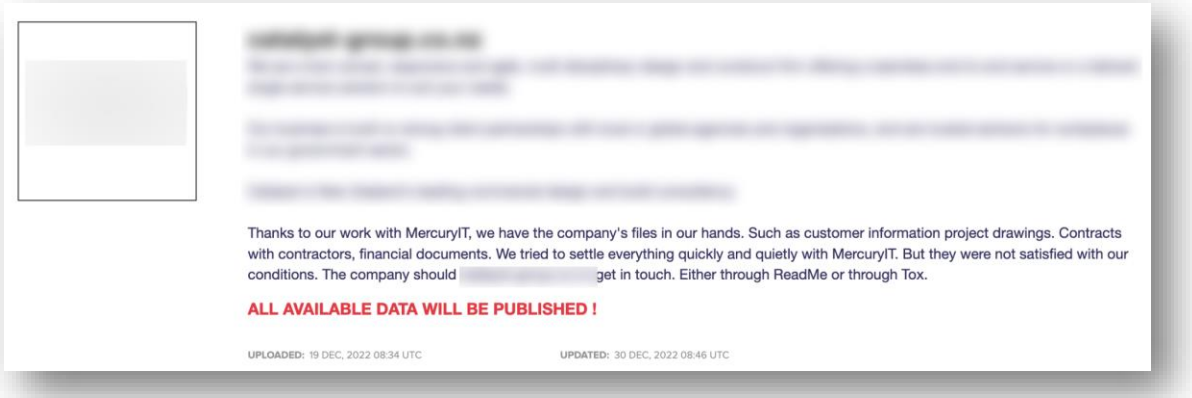
また 2022 年は、直接の被害組織ではなく第三者を被害組織として公表する事例の増加が観察されました。例えば LockBit の場合は、被害組織から窃取したファイル内にある（被害組織の）顧客やベンダー企業、パートナー企業に関する情報を探して、攻撃のさらなる収益化を試みていました。そしてファイルの中に収益の高い企業の情報が確認されると、LockBit はその企業を被害組織として公表し、実際の被害組織から窃取した情報を「攻撃の証拠」として提供し、身代金を要求していました。このような事例の場合、攻撃を行ったという主張が「フェイクニュース（その企業のネットワークや資産そのものは、実際には不正アクセスを受けていなかったという事実）」であったことが証明されたとしても、被害組織として公開された企業の評判に影響が生じることは不可避であり、またその企業に関するファイルそのものは実際に流出・公開されているがゆえ、対応を取る必要も生じます。

これに該当するパターンとして、2022 年 7 月、LockBit がイタリアの税務当局「Agenzia Entrate」に不正アクセスしたと主張した事例が挙げられます。しかしその数日後、イタリアの IT 企業「Gesis」社がイタリアのメディアに連絡を取り、不正アクセスを受けたのは自社であること、そして Agenzia Entrate が同社の顧客であったことを公表しました[8]。また、この時「侵害の証拠」として公開されたスクリーンショットを我々が検証した結果、リークされたファイルは確かに Gesis 社に関するものであることが判明しました。

これと同様の事例は 2022 年 12 月にも発生していました。この時 LockBit は、ニュージーランドの非営利保険会社である「Accuro」社に不正アクセスしたと主張していました。しかしその

[8] Attacco informatico all'Agenzia delle Entrate

時すでに、Accuro 社はサイバー攻撃を受けた旨を公表しており、同社がウェブサイトに掲載した声明によると「実際に攻撃を受けたのは Accuro 社ではなく、同社が利用する外部の IT インフラプロバイダー『Mercury IT』社であり、この時に Accuro 社のデータも流出した」ということでした[9]。そして実際、2022 年 12 月の LockBit のブログには、他のニュージーランド企業とともに Mercury IT 社が被害組織として掲載されていました。なお、LockBit がブログの投稿の中で、「Mercury IT の協力のおかげでこの会社のファイルを手に入れることができた」と主張していたことから、ブログに掲載されていた他のニュージーランド企業は、おそらく Mercury IT 社のインシデントから派生した被害組織であるものと思われます。



LockBit がニュージーランドの企業を被害組織として公開している投稿 （ただし、同社に関するファイルは、IT 企業「Mercury IT」社から窃取したものと思われる）

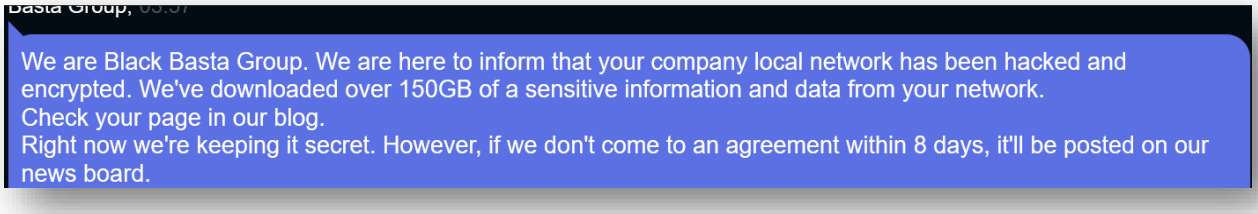
「非公開」のブログエントリ

我々は、Conti から流出したデータを分析する中で、同グループが被害組織に関する「非公開」のブログエントリを作成していることを発見しました。この非公開のエントリは、検索ではヒットしない秘密の URL を介してのみ閲覧できる投稿です。彼らは非公開のブログエントリを被害組織に公開して、データがどれほど簡単に公開されうるかを示すことで被害組織を脅迫していたのです。被害組織が身代金の支払いに合意した場合、そのエントリが公開されることは

[9] Cyber incident impacting Accuro

ありませんでしたが、交渉が決裂した場合にはエントリが一般に公開され、被害組織の名が明かされました。

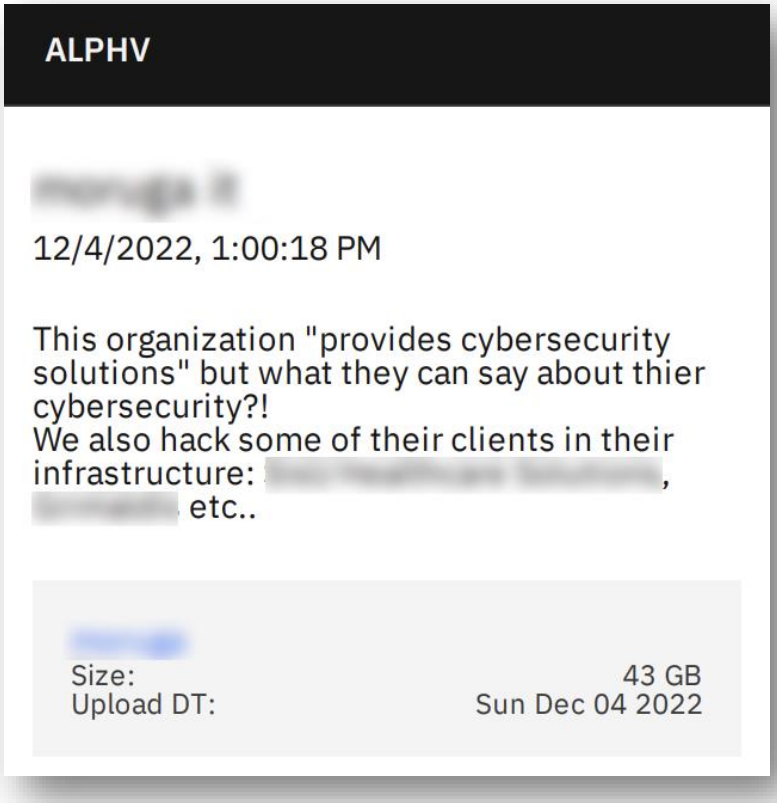
BlackBasta もこの手法を取り入れており、同グループは交渉の間、被害組織だけが閲覧できるブログ投稿を作成していました。



BlackBasta が投稿した「交渉プロセス」の詳細

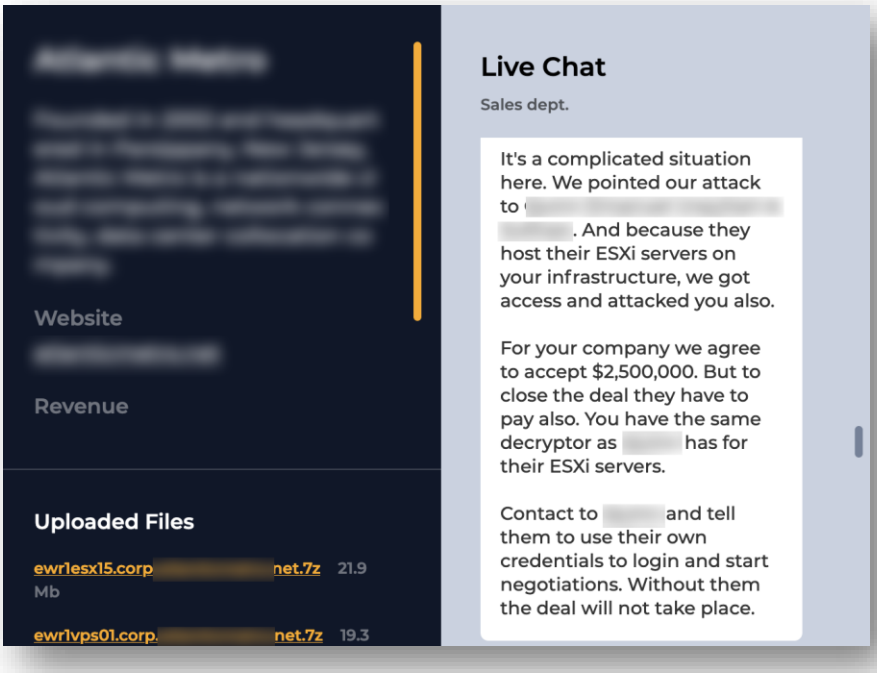
マネージドサービスプロバイダーを介した攻撃

前述の通り、ランサムウエアグループやデータリークグループは、被害組織のみならずその顧客やベンダー企業、パートナー企業をも脅迫するために、ありとあらゆる手段を駆使しています。そしてそれゆえに、場合によっては彼らの主張が事実ではないということが判明したり、実際の脅威の程度が主張されていたよりも低いものであるという場合があります。とはいえ、いずれの攻撃も被害組織と関連のある企業に劇的な影響をもたらしうるということを、覚えておくことが重要です。例えば、ランサムウエアグループやデータリークグループが、ある組織から窃取したデータを利用して、別の組織を侵害することもありえるのです。



Alphv が某企業を攻撃したと主張し、またその企業の顧客をも攻撃したと主張している投稿

またマネージドサービスプロバイダーも、自らの顧客を通じて攻撃される可能性があります。2022 年 6 月、我々はランサムウエア「Hive」の代表者と米国の某マネージドインフラサービス事業者の間で交わされたチャットにアクセスすることができました。Hive はこのチャットの中で、当初彼らは米国の某法律事務所を攻撃していたこと、そしてその法律事務所が使用している ESXi サーバーがこのサービス事業者のインフラ上で管理されていたことから、同事業者のネットワークにもアクセスできるようになったことを説明していました。そしてこの攻撃の後、Hive は法律事務所とこのサービス事業者の両方に身代金を要求し、少なくとも一方の被害組織から身代金の支払いを受けることに成功しました。



Hive が顧客を介してMSP プロバイダーを攻撃した手口について説明している様子（Hive のチャット）

その他にも 2022 年 12 月には、ランサムウエアグループ Alphv が、米国の某マネージドサービスプロバイダーに不正アクセスしたと主張し、さらに自らのブログ投稿の中で、「some of their clients in their infrastructure（マネージドサービスプロバイダーのインフラを使用している一部顧客）」にも不正アクセスしたと発言していました。

したがって、企業においては自社のみならず、侵害された場合には関連する全ての企業に影響が生じるであろう、第三者の脅威エクスポージャーについても監視することが重要です。

収益力を向上すべく導入された新たな機能

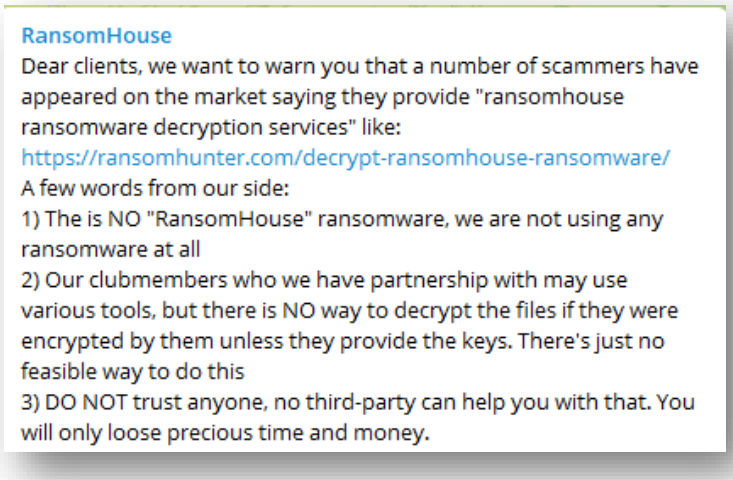
2022 年、一部のデータリークグループが新たな収益化モデルを導入し、利益を拡大すべく引き続き進化を遂げていました。

ランサムウエアグループとの連携

2022 年、ランサムウエアグループとデータリークグループがさらなる協力体制をとっている様子が観察されました。その 1 例として、「RansomHouse」が挙げられます。RansomHouse の活動が最初に確認されたのは 2021 年 12 月ですが、同グループのデータリークブログについては 2022 年 5 月頃に開設されました。RansomHouse は、このブログで自らを「プロの調停人の集まり」と表現し、攻撃者と被害組織の「交渉を支援する」と説明していました。その内容によると、RansomHouse は攻撃者と被害組織が話し合い、「十分な情報を得たうえでの意思決定」を行えるよう双方を手助けするということでした。またこのブログでは、「暗号化」と「リーク」という 2 種類のデータが販売されており、「暗号化」と「リーク」は、同グループが各データを取得した時の攻撃手法（「暗号化」はランサムエア攻撃、「リーク」はデータ窃取）を表しているものと思われます。

その他に RansomHouse に関する情報としては、2022 年 6 月 25 日に同グループが自らの Telegram チャンネルで、「自分達はランサムウエアグループではない。だから、暗号化被害を受けた企業に復号ツールを提供することはできない」と発言していたことが観察されています。しかしその一方で、これまでに同グループが「ランサムウエアを使えるサイバー犯罪グループとパートナーシップを確立した」と発言していたことも観察されています。RansomHouse が自らのサイトで言及している「交渉」の詳細条件や、同グループがランサムウエアグループなどのパートナーから身代金の一部を受け取っているのかという点については明らかにはなっていませんが、RansomHouse は被害組織に金銭を要求するメモの中で、度々サイバー犯罪グループ「White Rabbit（ハッカーグループ『FIN8』と関連のあるグループ）」や「Mario ESXi ransomware」について言及していることが観察されており、また同グループの攻撃では、以前漏えいした Babuk のソースコードを流用したマルウエアが使用されているものと思われます[10]。

[10] MalwareHunterTeam の Twitter



RansomHouse がランサムウエアグループと協力体制をとっていることを示唆している投稿

（RansomHouse の Telegram チャンネル）

同様の手法は、2022 年 12 月に立ち上げられたデータリークサイト「Unsafe Security Blog」でも採用されていました。同サイトを運営しているアクターは、協力体制をとってデータのリーク・販売を行おうとハッカーに誘いをかけ、また「自分達はあくまで『購入者と販売者をつなぐプラットフォーム』である。ブログ上にあるデータは全て攻撃を実行したハッカーに帰属する」と明言していました。さらに彼らは、データの売買における交渉も有償で対応すると説明していました。

我々は、この Unsafe Security Blog に掲載された被害組織のうち 3 つは、過去に Alphv（別名 BlackCat）や REvil（別名 Sodinokibi）による攻撃を受けていたことを確認しました。この 3 組織のうち、過去に Alphv の攻撃を受けていた被害組織については、Unsafe と Alphv がそれぞれ違う「攻撃の証拠（ファイル）」を公開している事例もありましたが、Unsafe が公開したデータの中に、Alphv が公開していたファイルに加え、新たな写真などが含まれている事例もありました。これらの事例と、Alphv が被害組織から窃取した全データを公開していたわけではないということをあわせて考えると、Alphv と Unsafe が協力体制をとって、被害組織のデータを販売しているという可能性が浮かび上がります。

一方、過去に REvil の攻撃を受け、後に Unsafe のブログに掲載された被害組織については、Unsafe が公開したファイル（攻撃の証拠）の中に、REvil によって公開されていた文書の他、新たなテキストファイルなども含まれていました。しかし、REvil のサイトは約 1 年前からダウンしているため、双方のファイルを厳密に比較することはできません。

また、上記と類似の収益化モデルを採用しているグループとして、2022 年 4 月に登場した「Industrial Spy」が挙げられます。同グループは、不正アクセス先企業のデータを販売するマーケットプレイスを運営しており、販売しているデータについては、「企業の IT インフラに存在する脆弱性を悪用して、自らが収集した」と主張しています。しかし同グループについては早々に、データの販売のみならず暗号化も行うようになったとの報告が寄せられています[11]。

Industrial Spy の説明によると、同グループのマーケットでは商品が価格に応じて「プレミアム（premium）、「一般（general）」、「無料（free）」の 3 つに分類されているということです。データが売り出されると、まず最初の 1 週間は「プレミアム」セクションに表示され、高額な値段で売り出されます。誰もそのデータに興味を示さない場合は、その後「一般」セクションへと移動され、値段を下げて売りに出されます。残る「無料」セクションでは、ユーザーが無料でデータをダウンロードすることができる仕組みとなっています。なお、我々がこのマーケットについて分析した結果、これらのセクションでデータを売り出されている企業のいくつかは、過去に Hive や Vice Society、Conti、Xing などのランサムウエアグループに被害組織としてその名を公開されたり、Marketo をはじめとするデータリークサイトで被害組織として掲載されていたことが判明しました。

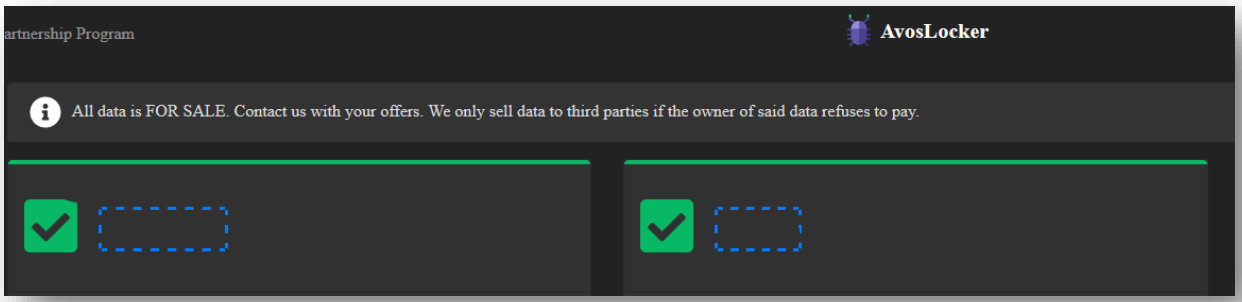
ネットワークアクセスや企業データの販売

また 2021 年末には、「Everest」が自らのサイトに新たな商品を導入していました。同グループは、組織のネットワークアクセスを所有していると主張し、商品として販売するようになっていたのです（同グループは、2022 年全体で 10 社を超える企業のアクセスを売り出しました）。これに加えて Everest は、企業データを販売するという新たな試みも取り入れていました。例えば 2022 年 5 月、我々は、Everest がイタリアの某製造企業に関連するデータを売りに

[11] Industrial Spy data extortion market gets into the ransomware game

出している状況を観察しました。この製造企業は、2021 年 12 月 22 日に Everest のデータリークサイトに掲載されていましたが、おそらく同社は身代金を支払わなかったものと思われます。その後の 2022 年 6 月 14 日、Everest はこの企業のデータを販売するべく新たな投稿を掲載し、その投稿の中で「侵害の証拠」として、被害企業および複数のイタリア自動車製造企業に関連するものとされる文書を公開しました。この企業データの販売価格は 3 万米ドルに設定されていました。

その他には、AvosLocker が収益力の向上にむけて新たな機能を導入していることも確認されました。現在、同グループの投稿には「購入」ボタンが表示されており、身代金の支払いを拒否した企業のデータをユーザー（サイバー犯罪者）が購入できる仕組みになっています。また画面には、購入したいデータの希望購入金額を同グループに連絡するよう、指示が表示されています。



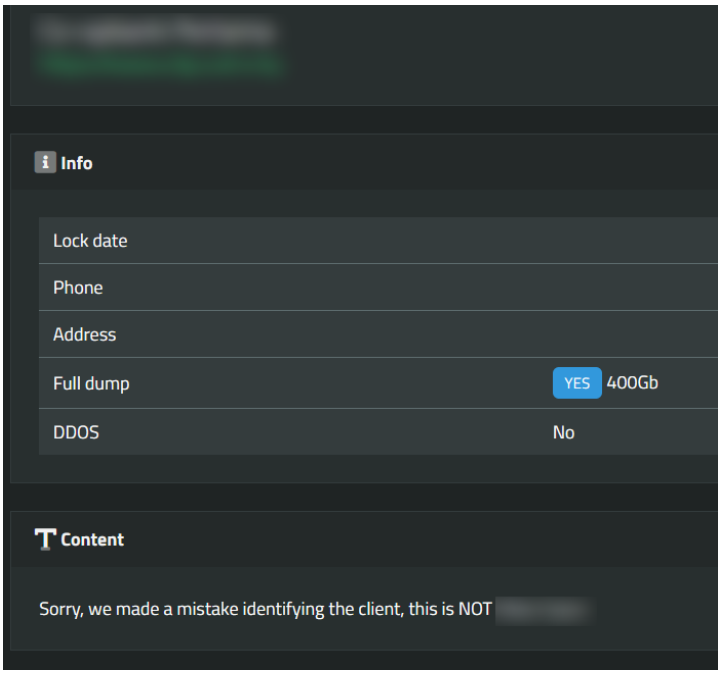
AvosLocker が被害組織のデータを売り出している投稿

失敗

組織の成長にともなう痛みや従業員の不手際というものは、もはやランサムウエアグループやデータリークグループであっても逃れることのできない呪いとも言えるでしょう。その 1 例として、ランサムウエアグループが被害組織の身元特定を誤るという事例が挙げられます。どうやら、ランサムウエアグループの OSINT 担当部門や被害組織公表担当チーム、アフィリエイト

は、攻撃した組織を時に別の組織と取り違えることがあり、2022 年、我々はそのような事例をいくつか観察することができました。

例えば 2022 年 4 月 14 日、ランサムウエア「Suncrypt」のオペレーターが、「持続可能な生産ソリューションを提供する某スウェーデン企業」に不正アクセスしたと主張していました。しかしその後、このオペレーターは「被害組織を誤認した」とのメッセージを掲載し、真の被害組織はマレーシアの協同組合銀行であると被害組織に関する情報を訂正していました。なお、このマレーシアの協働組合銀行は、先に被害組織として名を挙げられたスウェーデンの企業とは何の関係もありませんでした。



Suncrypt が自らの誤りを認めているメッセージ

もう 1 つ事例を挙げてみましょう。LockBit は、米国の IT サービス・コンサルティング企業「Orion Innovation」社に不正アクセスしたと主張しました。しかし LockBit がリークしたファイルを我々が分析した結果、含まれているデータは同グループの主張を裏付けるものではないことが判明しました。Orion Innovation 社のものとされたファイルは、実際には米国の某学区

と、その学区にサービスを提供している某企業（幼稚園～高校向けテクノロジーソリューション企業）に関連するものだったのです。

この 2 つの事例に関しては、各ランサムウエアグループが被害組織を誤認した理由は明らかとなっておらず、おそらくは偶然間違ったものと思われます。しかしその一方で、誤認の理由が明らかとなった事例も確認されています。2022 年 11 月、データリークグループ「Snatch」が、日本の某アプリ制作会社を被害組織として自らのリークサイトに掲載しました。またそこには、この会社のロゴと説明も記載されていましたが、同グループが公開した「proof pack（侵害した証拠の一式）」を我々が調査した結果、日本のアプリ制作会社に似た名称でビジネスを展開するイラン企業（自動車会社）が真の被害組織であることが判明しました。

これらの事例は、ランサムウエアグループやデータリークグループの主張については慎重に評価すべきであること、そしてソースを注意深く監視する中で目にした全ての情報を額面通りに受け止める前に、まずソースそのものを検証する必要があることを浮き彫りにしています（これについては弊社ブログでも詳述しています[12]）。

ネットワークアクセスの販売状況

2022 年の概要

2022 年、我々は、主要なサイバー犯罪フォーラムで初期アクセスブローカーが公に売り出しているネットワークアクセス数が著しく増加している様子を観察しました。それらアクセスの大半は、様々な企業のシステムへリモートでアクセスできる資格情報という形で売り出されていました。我々が追跡調査した「商品」の数は 2,200 件を超え、希望販売価格の合計額は 450 万米ドル超[13]となりました。多数の企業が、引き続き何らかの形でリモートワークを採用している現状を踏まえると、この増加は憂慮すべき傾向であり、組織のサイバーセキュリティ研修で職員や従業員に十分周知・説明しておくべき内容であると言えるでしょう。

[12] 完全に信用できるアクターなど存在しない— ソース検証の重要性

[13] 付録 2 の各四半期毎のデータをご参照ください。

売り出し商品件数上位の初期アクセスブローカー

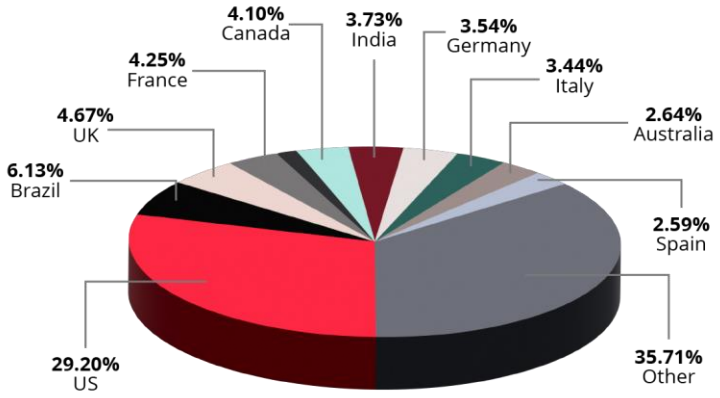
2022 年に売り出した商品数でトップ 3 にランクインした初期アクセスブローカーは「zirochka」、「orangecake」、「r1z」であり、いずれも 100 件超のアクセスを売りに出していました。彼らは、我々が過去に執筆・公開したレポートにも登場しています。この 3 名の後に続いた初期アクセスブローカーは、「paranoia」、「wwsgrep」、「Salvador_dali」であり、いずれも 70 件超のアクセスを売りに出していました。脅威アクターのプロファイルについては、KELA のサイバー犯罪インテリジェンスプラットフォームでご覧いただけます（こちらの画面でプラットフォームの無料アカウントを作成のうえ、ご覧ください）。

標的とされた国・業界

サイバー犯罪プラットフォームで売り出されていたネットワークアクセスの大半は、米国企業のものでした。また、2022 年全体を通した観察の中でも際立っていた点として、我々が追跡したアクセスのうち、被害組織の国が明記されていなかったものが 150 件を超えていたということが挙げられます（これらのアクセスは、国の代わりに地域が記載されているものと、地理的情報が全く含まれていないものに分かれました）。米国の他にネットワークアクセスを売り出された国の上位は、ブラジル、英国、カナダ、フランスでした。

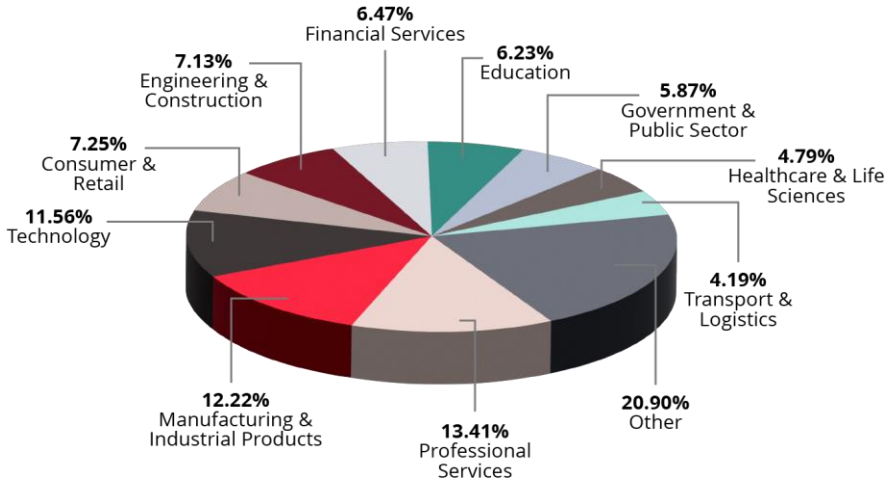
また、被害組織の業界が公開されていたアクセスを分析した結果、被害組織の大半は、専門サービス、製造・工業製品、テクノロジー業界に属しており、その後に、消費・小売、工事・建設業界が続きました。

Top targeted countries of 2022 by IABs*



* where the country name was disclosed by the IAB

Top targeted sectors of 2022 by IABs*



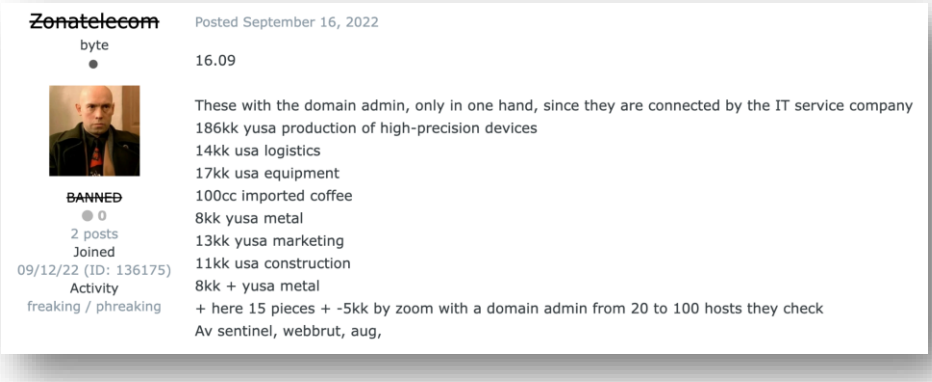
* where the sector was disclosed by the IAB

大きなトレンド

初期アクセスブローカーのサービスに対する需要は現在も続いていますが、彼ら自身も、競争に打ち勝つための新たな手法を模索しています。我々が観察したところ、初期アクセスブローカーはこれまでとは異なる被害組織（MSP の顧客など）を侵害したり、新しいサービスを提供して競争に勝ち抜こうとしていました。また、最近公表されたばかりの脆弱性に対するエクスプロイトが公開されると、そのエクスプロイトを悪用することで自らの「商品」やサービスを拡大するという手口も取り入れられていました。

マネージドサービスプロバイダー（MSP）の顧客を侵害

ランサムウエアグループやデータリークグループと同じく、高度なスキルを持つ初期アクセスブローカーの一部は第三者を介して企業を攻撃しています。我々が 2022 年に観察した状況から、第三者を介した攻撃では、マネージドサービスプロバイダー（MSP）が攻撃者の間で魅力的な標的になっているものと思われます。その 1 例として、2022 年 9 月に脅威アクター「Zonatelecom」が、米国企業 12 社のアクセスを売りに出した事例が挙げられます。Zonatelecom の説明によると、この 12 社のアクセスは、みな同じ IT サービスプロバイダーで「繋がっている」ということでした。



Zonatelecom が同じ IT サービスプロバイダーを利用している企業数社のアクセスを売り出した投稿（ロシア語からの自動翻訳）

我々は、脅威アクターが今後ますます MSP や IT 企業を標的にし、それら企業を介してその先にいる顧客を攻撃するであろうと予測しています。

新たなサービス

一部の初期アクセスブローカーは、今やアクセスのみならず、購入者（攻撃者）がネットワークの偵察や、その後の攻撃をより容易に実行できるよう支援するサービスも提供しています。例えば 2022 年 4 月には、脅威アクター「apollo12」が、収益 400 億米ドルを有する自動車部品製造企業のアクセスを売り出しました。apollo12 はこの投稿の中で、商品は VPN を介したアクセスであると説明するとともに、「不正アクセス先のネットワークには、『CVE-2017-0144（EternalBlue で悪用可能な Microsoft Windows SMB プロトコルの脆弱性）』に脆弱な端末が使用されている」と、購入者がさらなる侵害を行う際に役立つであろう情報を提供していました。

もう 1 つ事例を挙げてみましょう。2022 年 6 月、脅威アクター「Jesus-Like」が、収益 6 億米ドルを有する某米国銀行のアクセスを売りに出しました。Jesus-Like の説明によると、この商品は「被害組織の Active Directory ドメインに属し、NT authority/system 権限が付与されている端末」のアクセスであり、その販売価格は 8,000 米ドルとなっていました。なお、この事例で興味深い点として、Jesus-Like が同行のアクセスを売り出した際、「さらなる攻撃を簡単に実行できる準備が整っている」と主張していたことが挙げられます。その説明によると、Jesus-Like は同行の端末にリバースシェルを仕込み、「Metasploit Framework」を介してコードを実行できる態勢を整えているということでした。また Jesus-Like は、要望に応じて購入者の不正なペイロードをロードする、新たなサービスも販売していました。

Jesus-Like が新たなサービスを潜在顧客に提示している投稿（ロシア語からの自動翻訳）

公表直後の脆弱性を悪用

我々は、別々の初期アクセスブローカーが同じ標的を攻撃している様子を度々目撃しています。それらの事例について調査を進めてみると、ほとんどの場合は、彼ら（初期アクセスブローカー）が被害組織の数を最大化しようと公表直後の脆弱性を悪用し、公開されているエクスプロイトや Dorks（高度な検索演算子を用いた検索手法）を使っていたという結果にたどり着きます。こういった手口を使う初期アクセスブローカーは高度なスキルを持っていないものと思われ、また慎重に標的を選ぶよりも、数多くの企業を侵害するというやり方を好んでいます。

2022 年 5 月、我々は、脅威アクター「Bloomsday」が、収益 4 億米ドルを有するベトナムのレストランチェーンのアクセスを 2 万米ドルで売り出したことを確認しました。そしてその翌月となる 6 月、今度は脅威アクター「iFrame」が、収益 3 億 9,100 万米ドルを有するレストランチェーンのアクセスを4,000 米ドルで売り出したことを確認しました。両者ともに、商品はVPN や RDP を介したアクセスであり、購入者はドメイン管理権限が付与された端末にログインすることができると説明していました。

我々は、Bloomsday と iFrame がそれぞれレストランチェーンについて記載していた詳細情報をもとに調査を進め、この 2 人が売り出したアクセスが同じレストランチェーンのものであることを突き止めました。なお、両者が提示した価格には大きな差があることや、彼らの過去の活動を踏まえ、我々は iFrame と Bloomsday が同一人物ではないと判断しています。彼らが同じレストランチェーンのアクセスを売り出すにいたった理由としては、両者が同じ既知の脆弱性を利用して偵察活動を行い、被害組織のネットワークに不正アクセスしたという可能性が考えられ、この筋書きであれば、アクセスが売り出された時期が近かった点についても説明がつきます。この事例はまさに、1 つの企業が同時に複数のサイバー犯罪者の標的となりうること、そしてその結果として「複数」の事態が引き起こされうることを証明しています。

今度は、2019 年から活動し、フォーラム XSS で高い評価を得ているユーザー「r1z」の事例を取りあげてみましょう。2022 年 6 月、r1z は、SonicVPN を介したアクセス 30 件と Microsoft Exchange を介したアクセス 50 件を「実際に使えるエクスプロイト」とともに売りに出していました。しかしこの 3 カ月前には、r1z が「CVE-2021-42321（Microsoft Exchange のセキュリティ上の脆弱性）のエクスプロイト」を販売できると発言していたことが観察されており、こ

れらの事実をまとめ合わせると、「r1z はまず最初に、CVE-2021-42321 を悪用できる独自のエクスプロイトを手に入れた。そしてその後、r1z 自身がこのエクスプロイトを使ってアクセスを入手するようになった」という可能性が考えられます。

その他にも r1z については、上記と同じような手口で、Confluence Server と Data Center に影響を及ぼす重大なリモートコード実行の脆弱性（CVE-2022-26134）や、VMware 社製 Workspace One Access と Identity Manager に影響を及ぼす脆弱性（CVE-2022-22954）を悪用していることが観察されています（前者については同アクターが公開したスクリーンショット、後者については別のアクターがリークした一連の資格情報に関する調査で発覚しています）。ただしこれらの事例については、r1z は、一般公開されているエクスプロイトを使用しているものと思われます。

ゼロディ脆弱性のエクスプロイトを阻止する場合は、その作業も困難なものとなりますが、上述の事例で悪用されていたようなワンディ脆弱性については、セキュリティアップデートを常時チェックして、速やかにパッチを適用することでリスクを低減することが可能となります。

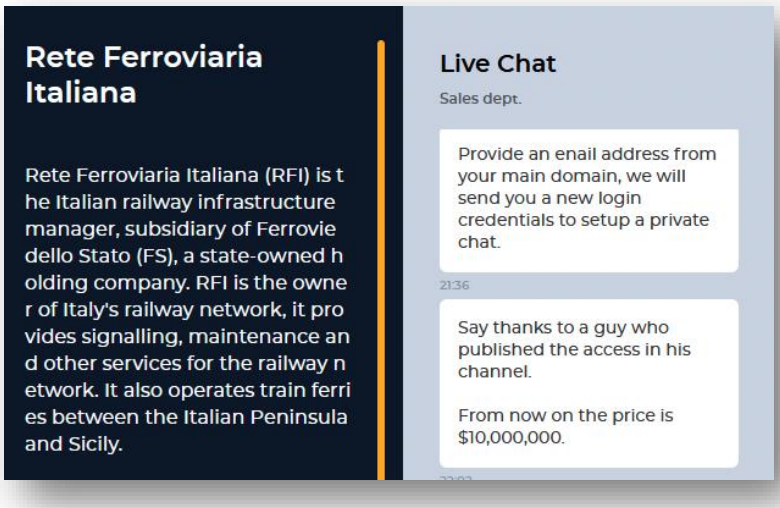
ランサムウエアグループ・データリークグループと初期アクセスブローカーの関係

ネットワークのアクセスが売買された後に起こるであろう結末は、ランサムウエア攻撃だけではありませんが、それでも RaaS のサプライチェーンで、今や初期アクセスブローカーが必須の存在になっていると認識しておくことは重要です。前述した Conti のリークでは、同グループが身代金の一部と引き換えに、初期アクセスブローカーのサービスを利用していたとわかる内容が確認されました。

我々は Conti から漏えいしたチャットの中で、Conti と某アクターの間で交渉が行われていたことを発見し、このアクターが使用していた Jabber アカウントをもとにさらなる調査を進めました。そしてその結果、このアクターがロシア語話者の集うサイバー犯罪フォーラム XSS や Exploit、RAMP で活動しているユーザー「RDPCorp」であることが判明しました。この RDPCorp は、「あらゆるネットワークアクセス」を定価で購入してランサムウエアグループに転売し、身代金の一部をその代金として受け取っていました。また RDPCorp は Conti と「労働

条件」を話し合う中で、ドメイン管理者権限を持つアクセスの場合は身代金の 35%、ユーザー権限のアクセスの場合は 15%を支払うよう要求していました。そして交渉の結果、Conti はユーザー権限のアクセスのみ購入するということで合意していました。その他にも Conti は、初期アクセスブローカーから大量のネットワークアクセスを定価で購入することなどを、チャット内で話し合っていました。

ランサムウエアグループやデータリークグループの中には、被害組織と身代金交渉を行う中で、初期感染ベクトルの詳細を明らかにするグループも存在します。そしてそういったグループのおかげで、我々はランサムウエアグループやデータリークグループと、初期アクセスブローカーが緊密に連携している様子を観察することができました。例えば Hive は、イタリアの鉄道会社「Rete Ferroviaria Italiana」社と身代金交渉を行う中で、「Say thanks to a guy who published the access in his channel.（【Rete Ferroviaria Italiana 社の】アクセスをチャンネルで公開していたヤツに礼を言うんだな）」と、初期アクセスブローカーの活動のおかげで攻撃を実行できたと取れる内容を発言していました。



Hive が侵害経路を被害組織に明かしているメッセージ

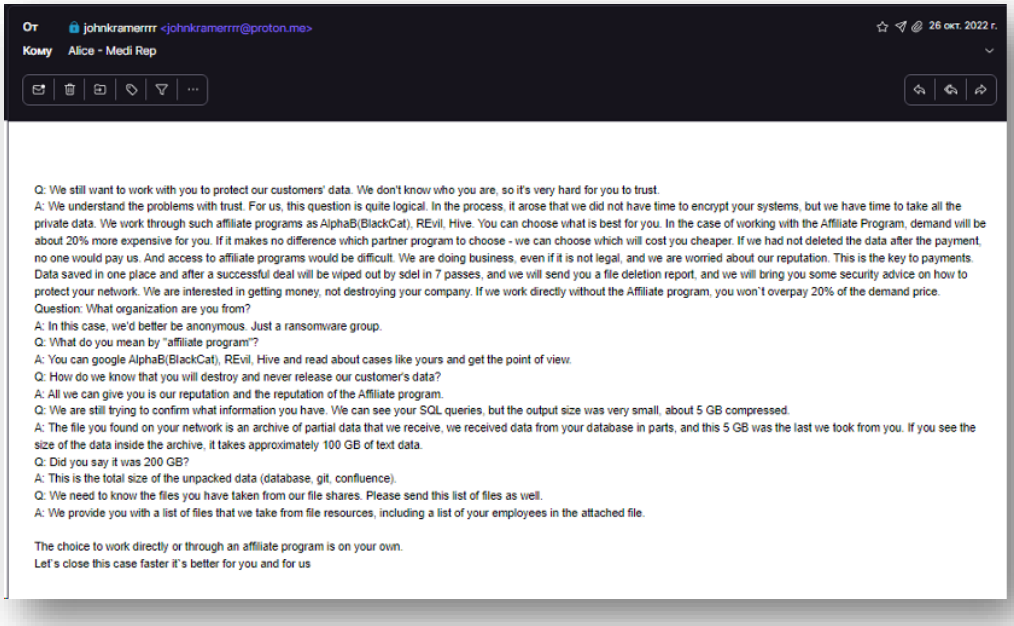
2022 年、我々は、サイバー犯罪者の間で売り出されたネットワークアクセスに端を発したと思われるランサムウエア攻撃やデータリーク攻撃を複数観察しました。それらの攻撃に関与して

いたグループとしては、REvil（Sodinokibi）の後継とされるグループ、Blackbyte、Quantum、Hive、Alphv が挙げられます。また、最も注目を集めたインシデントはオーストラリアの保険会社「Medibank」社に対する攻撃と関連していました。

2022 年 9 月、脅威アクター「c0xeec」が、オーストラリアに拠点を置く保険会社「Medibank」社のアクセスを、自らが運営する非公開の Telegram チャンネル「0x_dump」で売りに出しており、またその後同チャンネルで交わされたチャットの内容から、このアクセスが 2 日以内に何者かに買い取られたことが判明しました。そしてその 1 カ月後となる 10 月、Medibank 社がサイバー攻撃を受けたことが公表されました（公表当初、このサイバー攻撃はランサムウエア攻撃と考えられていました）。これらの出来事を時系列にして考えると、9 月に c0xeec が販売した Medibank 社のネットワークアクセスが攻撃の初期感染ベクトルとして使われた可能性が考えられます。

そして 2022 年 11 月、今度は REvil（Sodinokibi）とされるランサムウエアグループのオペレーターが、身代金を支払わないとして Medibank 社を非難する投稿を公開しました。ここで、REvil の背景情報を少し説明します。REvil のメンバーが多数逮捕されて以来、同グループの活動は停止していましたが、我々は、2022 年 4 月に REVil の TOR サーバーが復旧していることを確認しました。この TOR サイトには、REvil が過去に攻撃した被害組織がいくつか掲載されており、またその様子から、同サイトを運営しているアクターのうち、少なくとも何人かはランサムウエア REvil の複数バージョンを使用できているものと思われました。

Medibank 社を非難する投稿を掲載して間もなく、REvil は同社データの一部を公開し、さらには攻撃を実行したアフィリエイトと同社の間で行われた交渉のスクリーンショットも公開しました。このスクリーンショットに映し出されていた交渉の様子から、実行犯のアフィリエイトは Medibank 社に対して単独で攻撃を実行し、攻撃後に REvil へ連絡をとったことが判明しました。当初このアフィリエイトは Medibank 社に対し、「RaaS プログラムを介さず、自分（攻撃者）に直接身代金を支払う」、または「Alphv（BlackCat）や REvil、Hive などのアフィリエイトプトグラムを介して身代金を支払う」という 2 つの選択肢を提示しており、「アフィリエイトプログラムを使う場合は、窃取したデータの削除費用が 20%増額となる」とも説明していました。



実行犯のアフィリエイトが、Medibank 社担当者から寄せられた多数の質問に回答している様子

Medibank 社は、このアフィリエイトが名を挙げたランサムウエアグループについて調査した後、「It may be that your affiliation with those groups can help to build trust.（あなたがそれらのランサムウエアグループと提携している方が、我々としても信頼しやすいと思う）」と返答していました。そして同社は、より信頼できるであろうとの思いからアフィリエイトプログラムを介して交渉することを選択しました。しかしその後、この交渉は失敗に終わり、Medibank 社のデータが公開される事態となりました。また、我々が両者のやり取りを分析した結果、このアフィリエイトが実際には Medibank 社のシステムを暗号化していなかったこと、そして同社から窃取したデータはたった 200 GB であったことが判明しました。本件の詳細については、KELA のサイバー犯罪インテリジェンスプラットフォームでご確認いただけます（こちらの画面で無料アカウントを作成のうえ、ご覧ください）。

進化するサイバー犯罪社会の情勢（2021 年～2022 年）

KELA は、日々大量のデータを収集し、分析を行っています。そして今回、収集されたデータをもとに 2021 年と 2022 年に観察されたトレンドを比較しました。その結果で特に興味深かった点として、2022 年に公表されたランサムウエア攻撃とデータリーク攻撃の件数が、2021 年のものと非常に近い数字であったことが挙げられます（KELA の観察に基づいた数字となります。また、2021 年の方がわずかに多い件数ではあったものの、統計的有意性を示すものでありませんでした）。

また、攻撃を受けた国や業界のトップ 5 にも同じ傾向がみられました。ランサムウエア攻撃やデータリーク攻撃を受けた国は、2021 年に続き、2022 年も米国が他国を大きく引き離して 1 位となり、2 位が英国、その後にドイツ、カナダ、フランスが続きました。これらの国が占める割合やその順位は 2021 年と比較して変化があったものの、全体的な傾向に変わりはありませんでした。これまでに詳述した通り、脅威アクターはできる限り大きな収益を手にするべく「より裕福な」国の企業を攻撃することを好むため、傾向に変化がないのも驚くべきことではないと言えるでしょう。2022 年に攻撃を受けた主な業界も、その大半は 2021 年と変わっておらず、製造・工業製品、専門サービス、テクノロジー、工事・建設が引き続き 1 位～4 位の座を守り、2021 年に 5 位であった消費・小売のみ、2022 年は医療・ライフサイエンスにその順位を譲りました。

観察結果でもう 1 つ興味深かった点として、ランサムウエア攻撃やデータリーク攻撃に関与した脅威アクター（グループ）の数も、2021 年と 2022 年でほぼ同じ同数であったことが挙げられます（両年とも追跡調査したソースは約 60 件）。ただし、彼らのオペレーションの中には「廃業」するものもあれば、リブランドするものや、新たに登場するものもあり、活動しているアクターはその年によって若干異なっています。また、我々が 2022 年に観察したオペレーションの約 52%は、同年中に立ち上げられていました。これまでのところ、ランサムウエア攻撃やデータリーク攻撃の分野でコンスタントに活動しているグループは LockBit であり、同グループがオペレーションで主張していた被害組織の数をみると、2021 年は 2 位（1 位は Conti）、

2022 年は 1 位となりました。ただし 2022 年については、Conti が活動を終了したことが影響しています。

当初サイバー犯罪者らは、西側諸国の法執行機関がランサムウエアグループやデータリークグループに対して取るであろう措置について懸念していましたが、観察結果に表れた数字が概して彼らの思いを代弁しています。2022 年に公表された攻撃の件数が減少していないというこの調査結果は、脅威アクターが依然としてこの類の攻撃を実入りの良い活動と見なしており、また潜在的リスクに対する彼らの関心が若干薄れていることを意味しています。

次に、ネットワークアクセスに関する調査結果を説明します。我々が様々なサイバー犯罪フォーラムを観察した結果、2022 年に売り出されたネットワークアクセスの数は、前年比 70%増となりました。しかしその一方で、2022 年の平均価格および中央価格は前年比で下落し、平均価格については 2021 年の 4,600 米ドルが 2022 年は 2,900 米ドルに、中央価格については 2021 年の 500 米ドルが 2022 年は 300 米ドルに減少しました。

2022 年にサイバー犯罪者が売り出したアクセスは、2021 年に続き、米国企業のアクセスが最多となりました。また当然のことながら、アクセスに最も悪用されていた「製品」は RDP や VPN のプラットフォームであり、これらの製品がいかに手軽に組織の初期侵入経路となりうるかを物語っています。

我々は、ランサムウエア攻撃の初期侵入ベクトルや、情報窃取・侵害を目的としたネットワークへの不正アクセス手段として、サイバー犯罪者の間でこの種の「商品」に対する関心がさらに高まるか、少なくとも現在のレベルを維持するものと予想しています。

組織の防御者として活動される皆様への提言

2022 年、サイバー犯罪のエコシステムは全体的により高度になり、より複雑さを増しました。ランサムウエアグループやデータリークグループは、このエコシステムを利用することで攻撃のプロセスをこれまでよりも容易なものにするとともに、その規模を拡大しています。また、売りに出されているネットワークアクセスが、彼らにとって「見込み客（標的）」の重要なソースとなっていることが判明しています。

組織のネットワーク防御に従事される皆様がサイバー犯罪者の一歩先を行くためには、堅牢なセキュリティ戦略が必要となります。その一環として、セキュリティ強度の高いパスワード、多要素認証、最新のソフトウエア、ファイヤーウォールを導入すること、そしてサイバー犯罪者を正確に理解することが求められます。

また、脅威アクターの活動を理解して最新の脅威の先を行くためには、サイバー犯罪脅威インテリジェンスを利用することが鍵となります。これについては、脅威アクターやサイバー犯罪ソースを監視して、以下の点を理解することが含まれます。

- アンダーグラウンドで展開されている様々な種類のサイバー犯罪活動
- 脅威アクターが使用しているマルウエアやハッキングツールの種類
- 脅威アクターが悪用している脆弱性
- 脅威アクターが標的としている業種
- 特定の企業のアタックサーフェス・エクスポージャー

さらに、オンライン上で身を守る方法について従業員にトレーニングを行うことも重要です。各従業員が、オンラインの作業に潜むリスクとその回避方法を理解しておく必要があります。また、攻撃が発生した場合の戦略（従業員や顧客への通知など情報伝達に関する計画や、事後処理の対応計画など）を策定しておくことも重要です。

上記のアプローチを採用することで、組織として積極的な防御を実現し、現実に即したセキュリティ戦略を策定し、サイバー犯罪者の一歩先を行くことが可能となります。

付録 1：ランサムウエアグループ・データリークグループに関する弊社データ（四半期別）

2022 年第 1 四半期

2022 年第 1 四半期のランサムウエア被害組織とネットワークアクセスの販売状況
をご参照ください。

2022 年第 2 四半期

2022 年第 2 四半期のランサムウエア被害組織とネットワークアクセスの販売状況
をご参照ください。

2022 年第 3 四半期

2022 年第 3 四半期のランサムウエア被害組織とネットワークアクセスの販売状況
をご参照ください。

2022 年第 4 四半期

2022 年第 4 四半期、我々は監視対象とするソース（ランサムウエアグループのブログや交渉ポータルサイト、データリークサイト、報道やその他公表されている報告など）で、約 730 の被害組織を特定しました（以後、西暦記載なしの「第 3 四半期」については 2022 年 7 月-9 月期、「第 4 四半期」については 2022 年 10 月-12 月期を指すものとします）。この数字は前四半期比で 20%増であり、第 4 四半期ひと月あたりの被害組織は平均 240 組織となりました。

第 4 四半期に攻撃件数で上位に挙がったランサムウエアグループおよびデータリークグループは、第 3 四半期にトップ 3 にランクインしていた LockBit、Alphv（別名 BlackCat）、Black Basta であり、いずれのグループも 60 を超える組織を「シェイミング（被害組織の名を公開して辱める行為）」して上位プレイヤーの地位を維持しました。詳しく見ると、1 位の LockBit は、2 位の Alphv の 2 倍に近い被害組織を公表してトップの座を守りました。ただし、LockBit が第 4 四半期に公開した被害組織の数は 146 であり、前四半期比で 30%減少しました。2 位は Alphv であり、その後には、新たに立ち上げられたデータリークサイト Royal が 73 の被害組織を公開し

て 3 位となりました（Royal は、2022 年 10 月に「シェイミング」を始めたばかりであるにもかかわらずこの成績をおさめましたが、同サイトの運営については、2022 年 1 月に存在が発見されたランサムウエアオペレーションが関与していると思われます）。続いて 4 位は Black Basta となり、5 位は Karakurt と BianLian（第 3 四半期に登場した新しいグループ）が「同点」でランクインしました。

ランサムウエアグループやデータリークグループの攻撃を受けた組織を国別にみると、前四半期に続いて第 4 四半期も米国が 1 位となり、全被害組織の 43%を占めました。米国は、2022 年のいずれの四半期でも 1 位となっていましたが、43%という割合は 2022 年の四半期ベースで最高となっています。また、2 位はカナダ、その後に僅差で英国、ドイツ、オーストラリアの組織が続きました。

2022 年第 4 四半期、ランサムウエアグループやデータリークグループに標的とされた業界の 1 位は製造・工業製品であり、被害組織全体の 17%を占めました。同業界を攻撃したグループは主に LockBit と BlackBasta であり、攻撃の約半分は彼らが関与していました。また、製造・工業製品業界で標的とされた組織を国別にみると、米国が 1 位（60%）となりました。第 4 四半期に標的とされた業界の 2 位には、1 位との僅差で専門サービス（15%）が続きました。専門サービス業界を攻撃したグループは主に LockBit（攻撃の 25%は同グループが関与）であり、その後に BlackBasta が続きました。また同業界で標的とされた組織を国別にみると、やはり米国が 1 位となりました。

第 4 四半期にランサムウエアグループやデータリークグループの標的となった業界の 3 位～5 位は、テクノロジー、工事・建設、医療・ライフサイエンスであり、全被害組織の 23%を占めました。

付録 2：ネットワークアクセス販売状況に関する弊社データ（四半期別）

2022 年第 1 四半期

2022 年第 1 四半期のランサムウエア被害組織とネットワークアクセスの販売状況
をご参照ください。

2022 年第 2 四半期

2022 年第 2 四半期のランサムウエア被害組織とネットワークアクセスの販売状況
をご参照ください。

2022 年第 3 四半期

2022 年第 3 四半期のランサムウエア被害組織とネットワークアクセスの販売状況
をご参照ください。

2022 年第 4 四半期

2022 年第 4 四半期、我々が追跡調査を行った商品（ネットワークアクセス）は 590 件超、希望販売価格の合計金額は約 180 万米ドルとなりました。

また、第 4 四半期に売り出されていたネットワークアクセスの平均価格は約 4,400 米ドルであり、前四半期よりも高い数字となりました。ただし、第 4 四半期に売りに出された中で最も高額なアクセス（70 万米ドル）を除外すると、第 4 四半期の平均価格は第 3 四半期に近い数字となります。また、第 4 四半期に売り出されたネットワークアクセスの中央値価格は 300 米ドル、ひと月当たり平均件数は 200 件となりました。最も売りに出されていたアクセスの種類は RDP を悪用したもの、または RDP と VPN の両方を悪用したものでした。

2022 年第 4 四半期、我々は、ネットワークアクセスを売り出していた初期アクセスブローカー 100 人超を監視しました。売り出し件数で 1 位となったアクターは「paranoya」と「wwssgrep」の 2 名であり、それぞれ 70 件のアクセスを売り出していました。3 位は 60 件超のアクセスを

売り出した「sganarelle（別名 sganarelle2）」、4 位は約 30 件のアクセスを売り出した「nixploiter」であり、5 位には 12 月 30 日に 27 件ものアクセスを一括で売り出した「Kane_lynch」がランクインしました。

初期アクセスブローカーの標的となった国の1位は今回も米国であり、同国のアクセスは約165件にのぼりました（観察したアクセスの 3 分の 1）。その後にブラジル、フランス、カナダ、イタリアが続きましたが、各国のアクセスは22件〜32件となっています。

また、第 4 四半期に初期アクセスブローカーの標的となった業界のトップ 5 は、専門サービス、テクノロジー、製造・工業製品、消費・小売、工事・建設であり、いずれの業界も被害組織の数は27を超えていました。しかし、同四半期に観察されたネットワークアクセスの3分の1については、業界に関する記載がありませんでした。