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

KELA

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

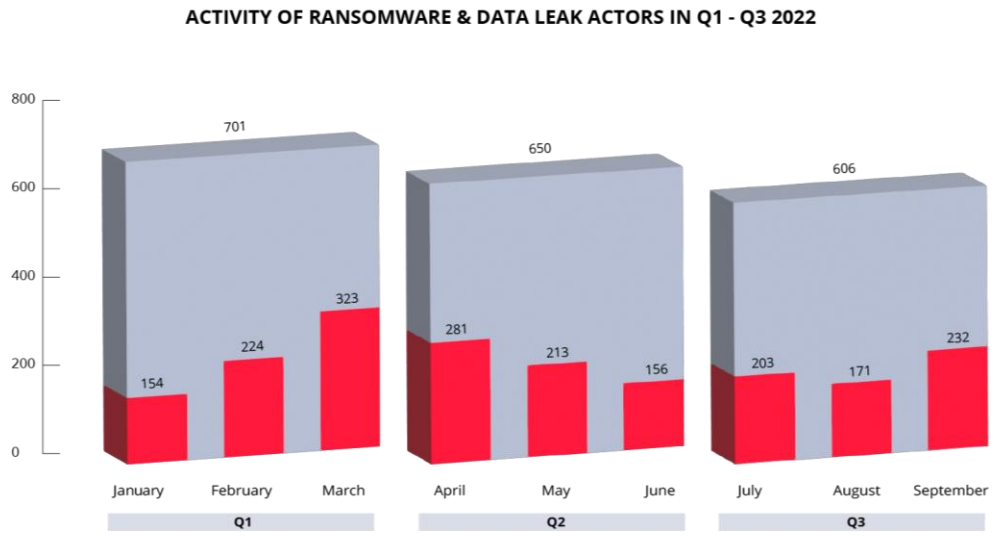
脅威インテリジェンスアナリスト　サリット・ボロホヴ

調査結果の主なポイント

- 2022 年第 3 四半期（2022 年 7 月-9 月期）に、攻撃件数で上位にランクインしたランサムウエアグループ及びデータリークグループは、LockBit、 Black Basta、 Hive、 Alphv（別名 BlackCat）、BianLian でした。うち BianLian は、比較的最近登場したランサムウエアグループです。（以後、本レポートで西暦記載なしの「第 3 四半期」については 2022 年 7 月-9 月期を指すものとします）
- 第 3 四半期にランサムウエアグループ及びデータリークグループの標的となった業界の第 1 位は専門サービスであり、同業界に対する攻撃の 55%は、LockBit、 Alphv、Hive による犯行でした。
- 第 3 四半期にランサムウエアグループ及びデータリークグループの標的となった国の第 1 位は引き続き米国であり、当四半期における被害組織の 40%は米国企業、その次に英国、フランス、ドイツ、スペインが続きました。
- 第 3 四半期には、Yanluowang、 BianLian、 0mega、 Daixin Team、 Donut Leaks などのデータリークサイト及びランサムウエアブログが新たに登場しました。
- 我々が、第 3 四半期に売り出されたネットワークアクセスのうち 570 件超について追跡調査を行った結果、希望販売価格の合計額は約 400 万米ドルとなりました。
- 第 3 四半期に売り出されたネットワークアクセスの平均価格は、約 2,800 米ドル、中央値は 1,350 米ドルとなりました。
- 第 3 四半期に売り出されたネットワークアクセスの総数は、前期とほぼ同じ数字となりましたが、商品の価格はより高額になっていました。また、第 3 四半期に売り出された商品のひと月あたり平均件数は約 190 件となり、前期比で微増となりました。

2022 年第 3 四半期におけるランサムウエア攻撃・データリークの被害組織

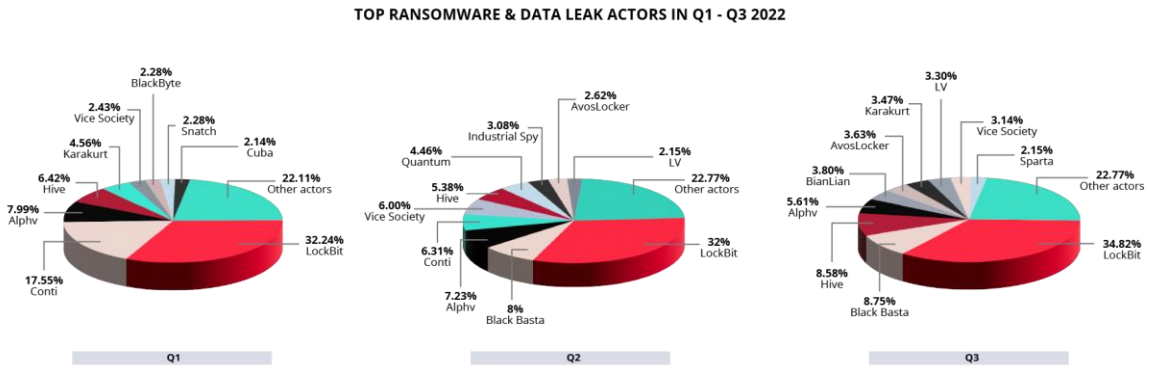
2022 年第 3 四半期、我々は監視対象とするソース（ランサムウエアグループのブログや交渉ポータルサイト、データリークサイト、報道やその他公表されている報告など）で約 600 の被害組織を特定しました。この数字は、前期比で 8%減となります。また前期は、毎月の被害組織数に減少傾向が見られましたが、第 3 四半期については 7 月から 8 月にかけて被害組織数が減少したものの、8 月から 9 月にかけて増加へと転じました。被害組織のひと月あたり平均数については、前期は 216 組織であったのに対し、第 3 四半期は 200 組織となっています。



攻撃件数上位のランサムウエアグループ

2022 年第 3 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及びデータリークグループは、LockBit、Black Basta、Hive、Alphv（別名 BlackCat）、BianLian であり、それぞれ 20 組織から 200 組織を被害組織として公表していました。その中でも有名なランサムエアグループ LockBit は、前期に引き続き 200 を超える被害組織（この数字は、2 位の Black Basta が公表した被害組織の約 4 倍となります）を公開しており、また比較的最近登場した BianLian も、早々にトップ 5 入りを果たしました。

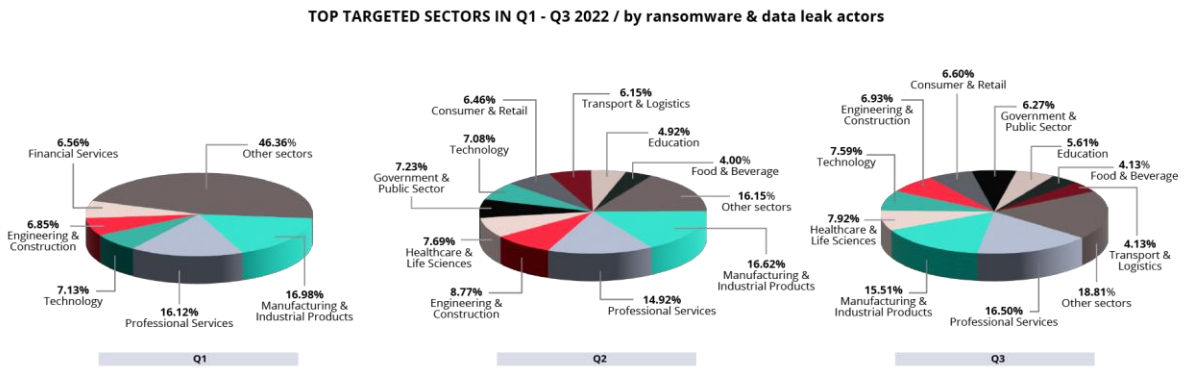
我々が観察を行った結果、Hive の被害組織数が大幅に増加（前期比約 67%増）し、その一方で Alphv の被害組織数が減少（前期比 28%減） していたことが判明しました。Black Basta の活動件数は安定しており、前四半期及び第 3 四半期のいずれも約 50 の被害組織を公表していました。



ランサムウエアの標的となった業界

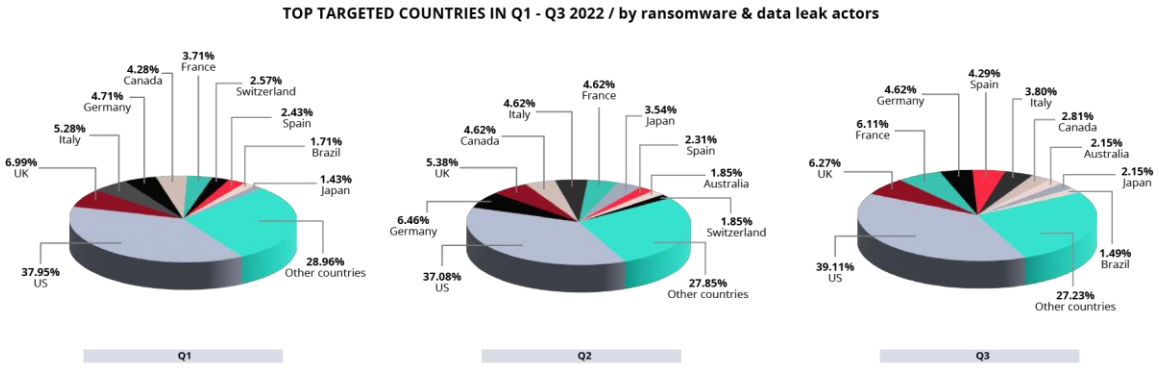
2022 年第 3 四半期に、ランサムウエアグループやデータリークグループの標的となった業界の第 1 位は専門サービスであり、同業界の組織に対する攻撃のうち 55%が、LockBit、 Alphv、Hive による犯行でした。これは、LockBit、 Alphv、Hive が攻撃件数で上位にランクインしているグループであるという事実とも一致しています。また、この業界で標的とされた組織を国別にした結果、米国及び英国が上位にランクインしました。

標的となった業界第 2 位は製造・工業製品、第 3 位は医療・ライフサイエンスとなり、その後にテクノロジー、工事・建設が続きました。



ランサムウエアの標的となった国々

米国は、引き続き標的とされた国の第 1 位となり、2022 年第 3 四半期に発生したランサムウエア攻撃やデータリークの 40%が、米国の組織を標的としていました。2 位は英国、その次にフランス、ドイツ、スペインの順となりました。



悪名高いランサムウエアグループとデータリークグループ

2022 年 8 月 18 日、ランサムウエア LockBit のオペレーターが、米国の決済及びデータ保護サービス企業「Entrust」社に不正アクセスしたと主張しました。しかし LockBit が Entrust 社の情報を公開し始めて間もなく、同グループのデータリークサイトが何者かによる DDoS 攻撃を受ける事態となりました（LockBit 側は、Entrust 社と関連のある人物が攻撃を行ったと主張しています）。

またその後、LockBit はフォーラム「XSS」で、ゼロディ脆弱性を悪用して Entrust 社のネットワークに不正アクセスしたと発言していました。さらに同グループは Entrust 社に報復するべく、同社に対する DDoS 攻撃を実行できるサービスを探しているとも発言し、Entrust 社のデータ 300 GB 相当をトレントトラッカーにアップロードしました。

なお、LockBit の管理者は、Entrust 社への攻撃後に自らが DDoS 攻撃を被る事態となったことを受け、今後はグループとして新たな戦略を導入すると発言していました。同管理者によると、今後はインフラを強化して新たなミラーサイトと DDoS 回避策を導入するとのことであり、また

窃取したデータを保存している TOR 上のインフラに加え、クリアネット上のストレージシステムを開発するとも宣言していました。

さらに同グループは、今後は被害組織に対し、データの暗号化・窃取に DDoS 攻撃を加えた「三重恐喝」戦術を使うとの声明も発表しました。

新たに登場したランサムウエアブログとデータリークサイト

Yanluowang（第 3 四半期に公表した被害組織数：3）

2022 年 7 月、Yanluowang のランサムウエアブログが発見されました。同ランサムウエアは、2021 年 10 月に大企業を狙った高度な標的型攻撃で使用されており、この時の事例で初めてその存在が確認されました。Yanluowang が暗号化したファイルには、「.yanluowang」という拡張子が付けられています。

BianLian（第 3 四半期に公表した被害組織数：24）

2022 年 7 月、我々は それまで存在を知られていなかったランサムウエアグループ BianLian のブログを発見しました。被害を受けたユーザーの報告によると、BianLian が暗号化したファイルには、「.bianlian」という拡張子が付けられています。

0mega（第 3 四半期に公表した被害組織数：1）

2022 年 7 月、我々はそれまで存在を知られていなかったランサムウエアグループ 0mega のブログを発見しました。なお、同グループはクリアネットとダークウェブの両方でリークサイトを運営していたものの、それらのサイトはその後すぐに閲覧不可能な状態となりました。同グループのオペレーションでは組織に対して二重恐喝を行い、数百万ドルの身代金を要求していると言われています。

Daixin Team（第 3 四半期に公表した被害組織数：3）

2022 年 8 月、金銭的動機に基づいて活動する Daixin Team が運営している、新たなデータリークサイトが発見されました、同グループが発表した声明によると、彼らはランサムウエアを使用しているということです。Daixin Team はこのデータリークサイトで被害組織名を公表し、機密ファイルをはじめとする（被害組織の）データをリークしています。

Donut Leaks（第 3 四半期に公表した被害組織数：13）

2022 年 8 月、Donut Leaks という名の新たなデータリークサイトが発見されました。このサイトは、ネーミング＆シェーミングブログと、ユーザーがデータをダウンロードできるデータストレージサイトで構成されており、Donut Leaks の被害組織のデータはこの両サイトに投稿されていました。当初、Donut Leaks には 5 つの被害組織が掲載されていましたが、同サイトのストレージサーバーの情報から、サイトの立ち上げ以降、10 組織のデータ（約 2.8 TB）がリークされたものと思われます。

なお、Donut Leaks で公開された被害組織のいくつかは、過去に別のランサムウエアグループ（Hive や Ragnar Locker など）にその名を公開されていることから、このサイトを運営しているアクターは、複数のランサムウエアオペレーションでペンテスターかアフィリエイトとして活動している可能性があります。

Sparta（第 3 四半期に公表した被害組織数：13）

2022 年 9 月、我々は、某脅威アクターが Sparta のブログの URL を公表していたことを発見しました。同グループの素性については明らかとなっていません。

Bl00dy（第 3 四半期に公表した被害組織数：8）

Bl00dy Ransomware Gang（以後「Bl00dy」）という名の新たなランサムウエアグループが、同グループの攻撃を受けたとされている組織の名（米国の医療機関など）を、自らの Telegram チャンネルで公開していることが確認されました。同グループについては、米国の医療機関を標的とする攻撃のいくつかに関与しているとされており、また LockBit 3.0 のランサムウエアビルダーがリークされた後には、Bl00dy が行った攻撃のうち数件で、同ビルダーが使用されていた

との報告が寄せられました。 Bl00dy はこれまで医療機関を標的とした活動を行っており、その際にランサムウエアを展開したとの疑いがもたれています。

MedusaLocker（第 3 四半期に公表した被害組織数：10）

2022 年 9 月、新たなランサムウエアブログの URL がサイバー犯罪フォーラムで拡散されました。サイト名は「ransomware blog（ランサムウエアブログ）」となっており、このサイトを運営しているアクターは、「We will not give ourselves a name. Just watch out for the leakage of your data.（参考訳：我々に名はない。自分達のデータが漏れていないかチェックしたまえ。）」とのメッセージとともに、10 組織を被害組織として掲載していました。

しかし「我々に名はない」というメッセージにもかかわらず、このブログの URL は、ランサムウエアグループ「MedusaLocker （別名 Medusa）」のものとして知られている交渉用ポータル内の、「Open TOR blog（TOR ブログを開く）」ボタンのリンク先にも設定されています。

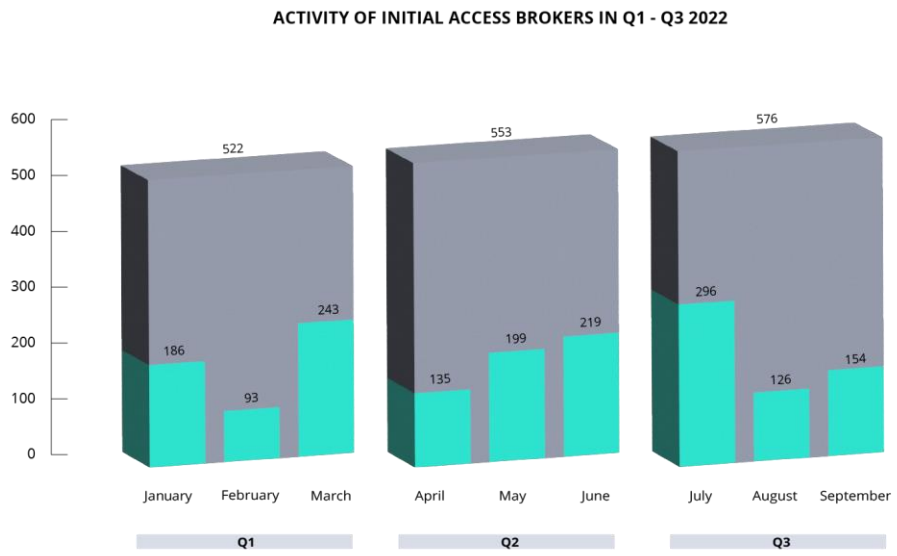
MedusaLocker は、ランサムウエア・アズ・ア・サービスオペレーションであり、2019 年に最初の使用事例が確認されています。

第 3 四半期の「もはやプロとは呼べないランサムウエアグループ」

2022 年 8 月 17 日、我々はランサムウエアグループ BlackByte が、新たなデータリークサイトを立ち上げて活動を再開したことを確認しました。このデータリークサイトは LockBit のブログに似たデザインで構成されており、被害組織に期限延長の機会を与えるという新たな機能も導入されていました。ただし、この新しいサイトに表示されている Bitcoin や Monero のウォレットの「copy address（アドレスをコピー）」ボタンにはウォレットの情報が設定されておらず、このボタンをクリックしても支払先ウォレットの情報が得られない状態になっていました。

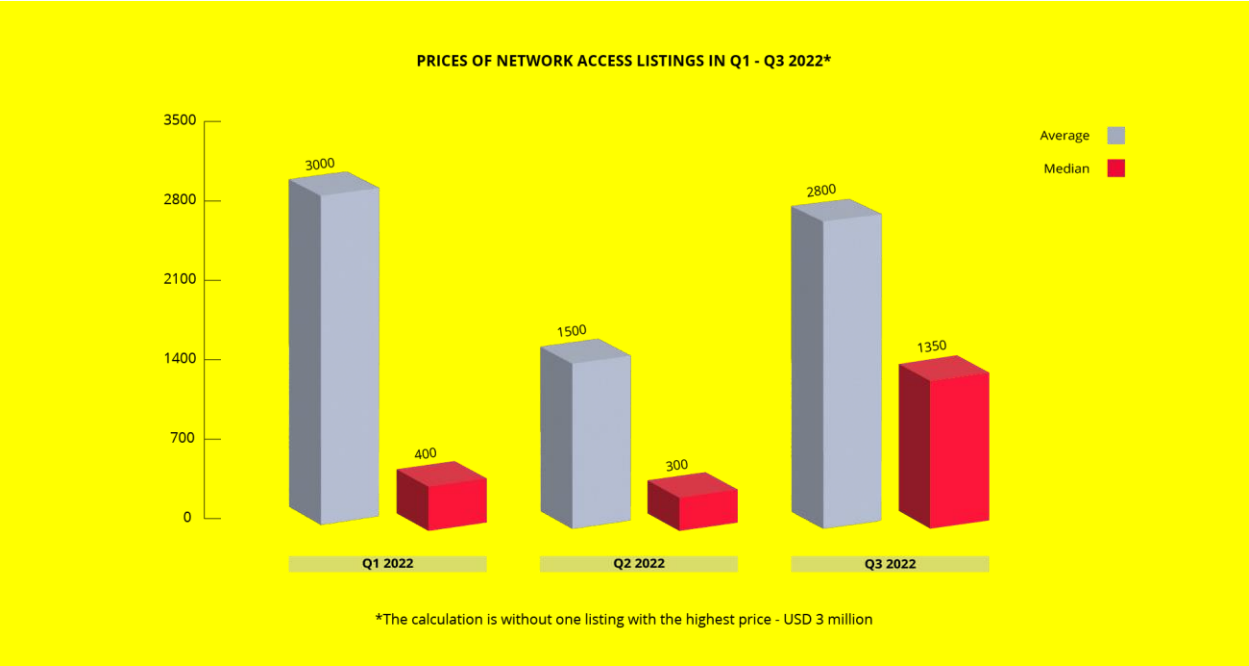
2022 年第 3 四半期に売り出されたネットワークアクセス

2022 年第 3 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 570 件超、その希望販売額は合計約 400 万米ドルとなりました。なお、この中には 300 万米ドルという価格で売り出された商品が 1 件含まれています。この 400 万米ドルという金額は、前期比でみると著しい増加と言えますが（第 2 四半期の希望販売額の合計は約 66 万米ドル）、300 万米ドルという価格がつけられた 1 商品を除外すると、第 2 四半期と第 3 四半期の金額にそれほど差はありません。そのため、第 3 四半期のデータについてはこの 300 万米ドルの商品を除外して算出しています（これについては、当該商品を売りに出したアクターが、信頼に足りる人物とは思われないという事実も考慮した上での対応となっています）。



売り出されていたネットワークアクセスの平均価格については、第 2 四半期が約 1,500 米ドルであったのに対し、第 3 四半期は約 2,800 米ドルとなりました。また、中央値も大きく増加しており、第 2 四半期が 300 米ドルであったのに対し、第 3 四半期は 1,350 米ドルとなりました。第 2 四半期と第 3 四半期に売りに出されたアクセスの総数がほぼ同じ件数であったことから、この第 3 四半期においては、アクターらはより高額なアクセスを売りに出していたということ

がわかります。第 3 四半期に売りに出されたネットワークアクセスのひと月あたり平均件数は約 190 件であり、前期比で微増となりました。



また今回の追跡調査の結果では、ネットワークアクセスが売りに出されてから買い取られるまでの平均日数は 1.6 日となりました（買い取り状況の確認については、販売者が公開していたコメントなどの情報に基づいています）。脅威アクターが最も多く売りに出していた商品は、RPD や VPN を悪用したネットワークアクセスでした。

売り出し件数上位の初期アクセス・ブローカー

2022 年第 3 四半期にネットワークアクセスを売りに出していたアクターの数は約 110 人であり、第 2 四半期とほぼ同じ人数となりました。また、第 3 四半期に最も多くネットワークアクセスを売りに出していた初期アクセス・ブローカーの上位 3 人は、それぞれ 40 件～100 件のアクセスを売りに出していました。

r1z

r1z がサイバー犯罪フォーラムに参加したのは 2019 年 7 月ですが、同アクターがネットワークアクセスを販売し始めたのは、2022 年 7 月に入ってからのことです。r1z は、主にリモートコー

ド実行（RCE）の脆弱性を悪用したネットワークアクセスを売りに出しており、第 3 四半期には約 100 件の商品を売りに出していました。同アクターが悪用している脆弱性の 1 つは、「CVE-2022-22954（VMware Workspace One Access & Identity Manager に影響を及ぼす脆弱性）」です。なお、同アクターはフォーラム「Exploit」では出入り禁止となっており、フォーラム「XSS」で活動しています。

Salvador_Dali

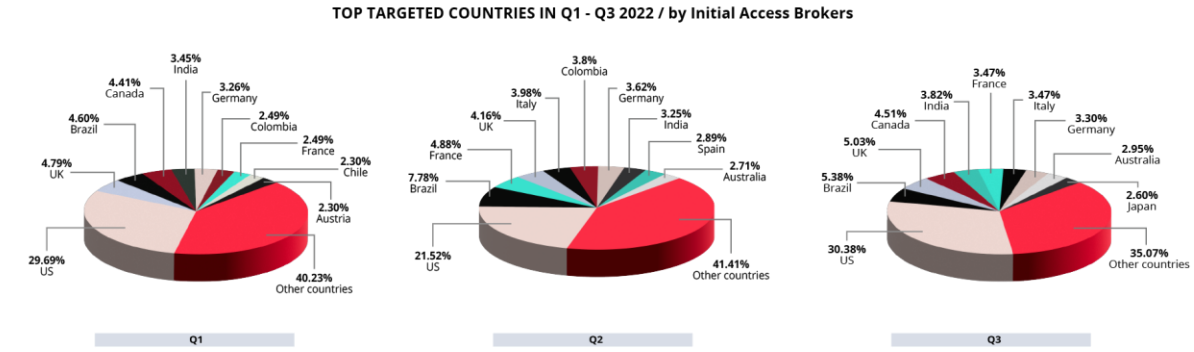
Salvador_Dali は、2022 年 5 月からネットワークアクセスを販売しており、主に米国企業を標的としています。同アクターは、売り出しているほとんどの商品についてアクセスの種類や価格を記載していませんが、被害組織の名は公表しています。

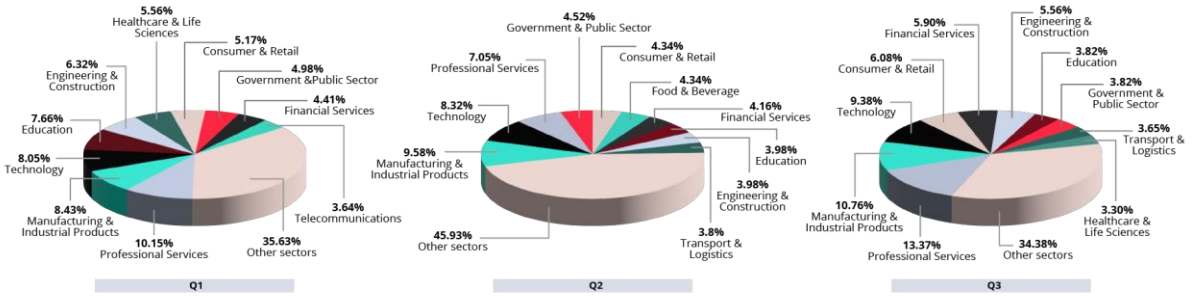
Orangecake

Orangecake は 2021 年 9 月から活動しており、主に VPN 及び RDP を介したアクセスを売りに出しています。同アクターはフォーラムで高い評価を受けており、ランサムウエアグループと協働している様子も観察されています。（Orangecake の詳細な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。サインアップまたはログインの上ご利用ください）

標的とされた国・業界

2022 年第 2 四半期に引き続き第 3 四半期も、初期アクセス・ブローカーの標的となった国の第 1 位は米国となり（被害組織の約 30%）、その後にはブラジル、英国、カナダ、インドが続きました。また、第 3 四半期に売り出されていたネットワークアクセスの約 50%は、これら 5 カ国の組織のものでした。初期アクセス・ブローカーの標的となった業界の第 1 位は専門サービスであり、その次に製造・工業製品、テクノロジーが続きました。





注目の事例

最も高い収益を有していた被害企業

2022 年 7 月 5 日、我々は、脅威アクター「qx56」が収益 600 億米ドルを有する電力関連企業へのアクセスを売りに出したことを確認しました。

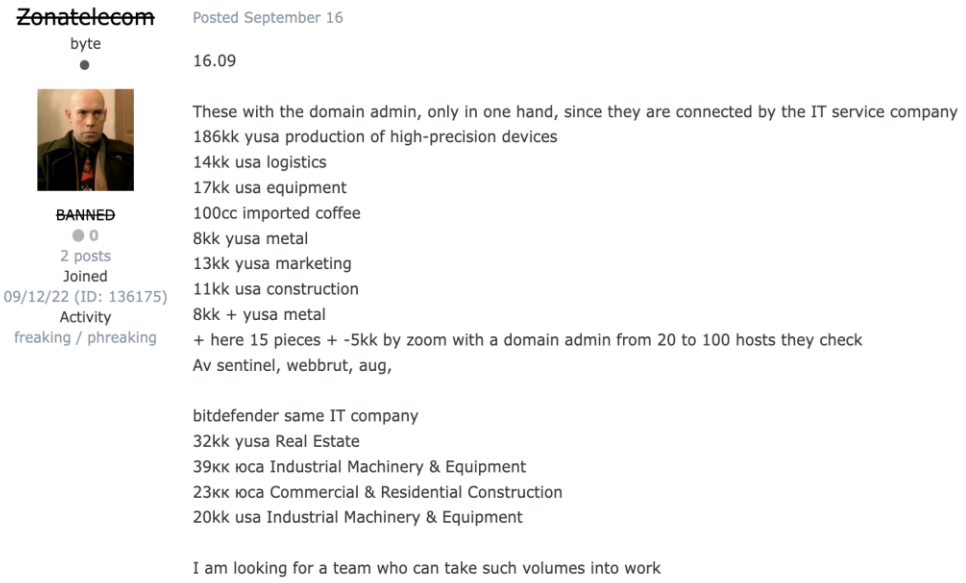
我々は、qx56 が記載していた被害組織に関する説明および収益と、一般入手可能な情報を照合した結果、被害組織がフランスの公益事業会社であることを特定しました。同アクターの説明によると、このアクセスを使って、ドメイン管理者権限が付与された端末にログインできるということでした。このアクセスは、開始価格 2 万米ドルでオークション形式にて売り出され、2022 年第 3 四半期に売り出された中で最も高い収益を有する（被害組織の）商品となりました。

最も高額商品となった欧州の某銀行

2022 年 7 月 11 日、我々は脅威アクター「4JWHaYQKdra9KHQ」が、欧州に拠点を置き 200 億米ドルの収益を有する某銀行へのアクセスを売りに出したことを確認しました。4JWHaYQKdra9KHQ の説明によると、このアクセスはリモートコード実行の脆弱性を悪用したものであり、ドメイン管理者権限が付与された端末にログインできるということでした。このアクセスは 300 万米ドルで売りに出されており、第 3 四半期に売り出された中で最も高額な商品となりました。ただし、同アクターは確固たる評判を得ていないため、この商品が主張通りのものであると信用することはできません。

脅威アクター「Zonatelecom」が IT プロバイダーを利用して複数の米国企業に不正アクセス

2022 年 9 月 16 日、我々は、脅威アクター「Zonatelecom」が米国企業 12 社へのアクセスを売りに出したことを確認しました。Zonatelecom の説明によると、この 12 社へのアクセスは同じ IT サービス企業で「繋がっている」ということでした。この商品からもわかるとおり、サイバー犯罪社会の脅威アクターがマネージドサービスプロバイダー（MSSP）のソリューションを悪用し、その先にいる顧客を攻撃するという事例が増加しています。



Zonatelecom が同じ MSP を利用している企業数社へのアクセスを売りに出した投稿。なお、同アクターは教育業界を標的にしていたことを理由に、フォーラム「Exploit」では出入り禁止となっている。

結論及びリスク低減策

2022 年第 3 四半期は、ランサムウエアグループやデータリークグループが精力的に活動を展開する一方で、新たなグループが登場しました。その一方で初期アクセス・ブローカーにも、彼らの商品に対する需要が続く状況を背景に、より多くの商品を売り出し、価格を引き上げている傾向が見られました。組織や企業のネットワーク防御に従事される IT 担当者やサイバーセキュリティ担当者の皆様には、ランサムウエアグループをはじめとするサイバー犯罪者に立ち向かうにあたって、以下に投資することが求められています。

- 主要な利害関係者と従業員全員に対し、サイバーセキュリティについての啓蒙活動及びトレーニングを行い、主要メンバーが自分の資格情報や個人情報を安全に使用する方法について確実に理解できるようにします。このトレーニングでは、疑わしいアクティビティ（詐欺メールや、認証されていない個人または電子メールアドレスから送信された異常なリクエストなど）を特定するための具体的な方法を明示することも必須となります。このようなサイバーセキュリティトレーニングを組織全体に対して行うことで、従業員のミスにより不正アクセスを受ける機会が大幅に低下します。
- 日常的に脆弱性を監視して適切にパッチを適用し、組織のネットワークインフラストラクチャ全体を常時保護し、初期アクセス・ブローカーやその他のネットワーク侵入者による不正アクセスを防止します。
- 主要な資産に的を絞った自動モニタリングを活用し、アンダーグラウンドのサイバー犯罪エコシステムに台頭する脅威を即時に検出します。組織の資産をスケーラブルに常時自動監視することで、アタックサーフェス（攻撃対象領域）を常時最小化することが大幅に容易になり、かつサイバー攻撃の試みを阻止することにもつながります。

KELA のソリューションは、アンダーグラウンドで密やかに繰り広げられるサイバー犯罪者の活動をリアルタイムで監視し、組織や企業でネットワークの防御に従事される皆様に、価値の高い重要なインテリジェンスをご提供しております。脅威アクターが採用する新たな戦術について学び、理解を深め、適切な防御措置を取り、脅威の先手を打ったアプローチを実現する一助として、是非 KELA のサイバー犯罪インテリジェンスをご活用ください。