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

KELA

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

脅威インテリジェンスアナリスト　ヤエル　キション

ランサムウエアグループは、2022 年第 1 四半期も引き続き重大な脅威となりました。彼らは、初期アクセス・ブローカー（IAB）をはじめとする様々なサイバー犯罪者と協働し、世界中の企業を攻撃しようと企んでいたのです。KELA は、2022 年第 1 四半期におけるランサムウエアグループや初期アクセス・ブローカーの活動を監視した結果、以下の洞察を得ることができました。

2022 年第 1 四半期のランサムウエア被害組織の総数は、2021 年第 4 四半期の 982 組織から 40%減少して 698 組織となりました。また、最も活発に活動を展開していたグループも、2022 年の初旬以降は Conti から LockBit へと変化しました。ただし、Conti が行った攻撃の件数については 2022 年 1 月に減少傾向がみられたものの、同グループの内部データがリークされた後に再び増加へと転じました。

- **金融セクターが受けた攻撃件数は 46 件に上り、標的とされる業界のトップ 5 にランクインしました。**またそれら攻撃のうち 40%は、LockBit に関連づけられました。
- ランサムウエアグループは、被害組織の名称を明かさないまま自らのブログに掲載するといった、新たな脅迫方法を取り入れていました。
- **2022 年第 1 四半期に売りに出されたネットワークアクセス数は、2021 年第 4 四半期からわずかに増加しました。**我々がモニタリングしたアクセス商品の件数は、2021 年第 4 四半期は 468 件、2022 年第 1 四半期は 521 件超（希望販売価格の合計金額は 110 万ドル以上）となりました。
- ネットワークアクセス商品が売りに出されてから買い取られるまでの販売サイクルは平均で 1.75 日となりました。

我々は、売り出されているネットワークアクセスのうち 150 件以上について、そのアクセスを所有している組織（被害組織）を特定し、またその一部については BlackByte や Quantum、Alphv が実行したランサムウエア攻撃と関連があったことを確認しました。これらを踏まえ、攻撃で使用されたネットワークアクセスを購入したのは、非常に高い確率でランサムウエアアフィリエイトであったと考えられます。

2022 年第 1 四半期に発生したランサムウエア攻撃

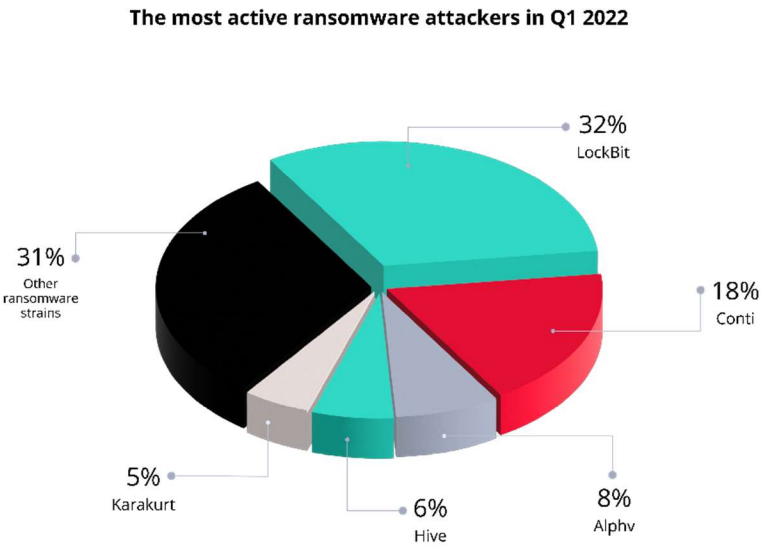
2022 年は、その年明けからロシアによるウクライナ侵攻が始まり、これにあわせて両国及びその支援者がサイバー攻撃を展開する事態となりました。一方、企業や国家機関のネットワーク防御担当者に対しては、ランサムウエア攻撃をはじめとするサイバー攻撃の可能性があるとの警告が出されました。さらにそのような状況の中、Conti をはじめ一部のランサムウエアグループがサイバー戦争への参戦を宣言しました。しかし、ランサムウエアグループのブログや交渉用ポータル、データリークサイトを監視した結果、ロシアのウクライナ侵攻が始まって以降、ランサムウエア攻撃件数が実際には増加していないことが明らかとなりました。それどころか、2022 年の初旬にいたってはランサムウエア攻撃件数が著しく減少しており、2021 年の初旬と同様に減少パターンであったことが判明しました。

2022 年が始まって以降、我々は調査対象とするソースで約 **700** の被害組織を特定しましたが、この数字は 2021 年末と比較すると約 40%の減少となっています。しかしひと月当たりの攻撃件数を見てみると、2022 年 1 月は 149 件であったのが 2022 年 3 月には 325 件へと増加しています。また、2022 年第 1 四半期に我々が観察したランサムウエア攻撃の件数は、ひと月当たりの平均で 232 件となりました。

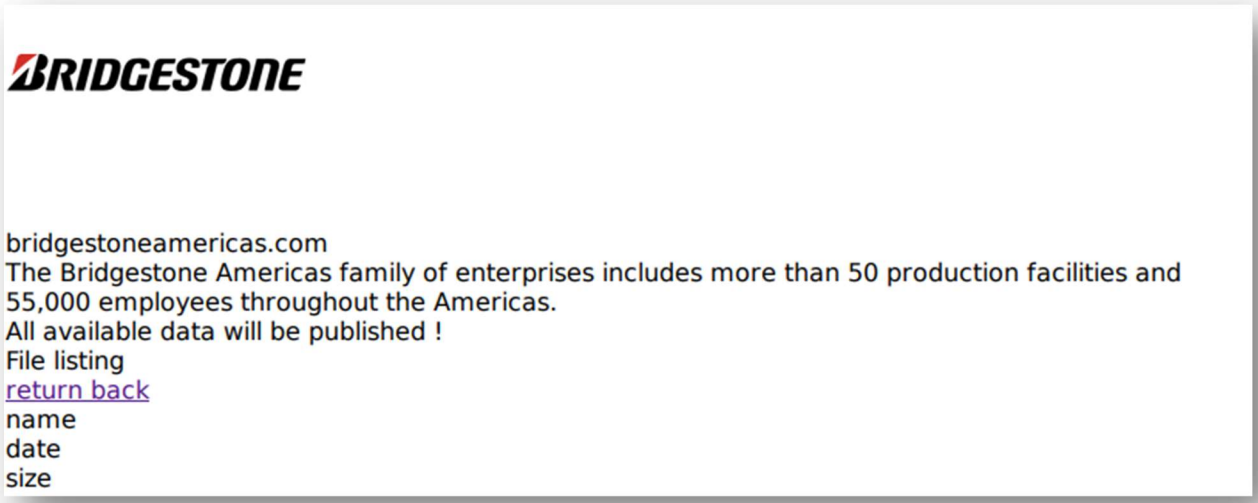
攻撃件数の多かったランサムウエアグループ

2022 年第 1 四半期に攻撃件数の多かったランサムウエアグループは、**LockBit、Conti、Alphv、Hive、Karakurt**（同グループについては最近 Conti の別プロジェクトであることが判明）であり、いずれのオペレーションでも 30 を超える被害組織が公開されていました。一方で、2021

年第 4 四半期に攻撃件数の多さでトップ 10 入りしていたランサムウエアグループのうち、6 グループは攻撃件数が大幅に減少しており、なかでも Conti の攻撃件数が最も大きく減少していました。また **Pysa** は、2021 年第 4 四半期には 81 もの被害組織を攻撃し、同期間において最も大きな成果を上げたグループのトップ 3 にランクインしていましたが、2022 年に入って以降は人目に付くような活動を行っておらず、同グループのブログでも新たな被害者は公開されていません。



LockBit は、Conti に代わって最も活発に活動を展開するランサムウエアグループとなり、彼らの活動は最も注目を集めるオペレーションへと進化しました。2022 年第 1 四半期に同グループが公開した被害組織の数は 226 に上り、2021 年第 4 四半期に同グループが行った攻撃件数に近い数字となっています。彼らは幅広い業界の組織を攻撃しましたが、その大半は製造、テクノロジー、教育、公的サービスセクターの組織でした。



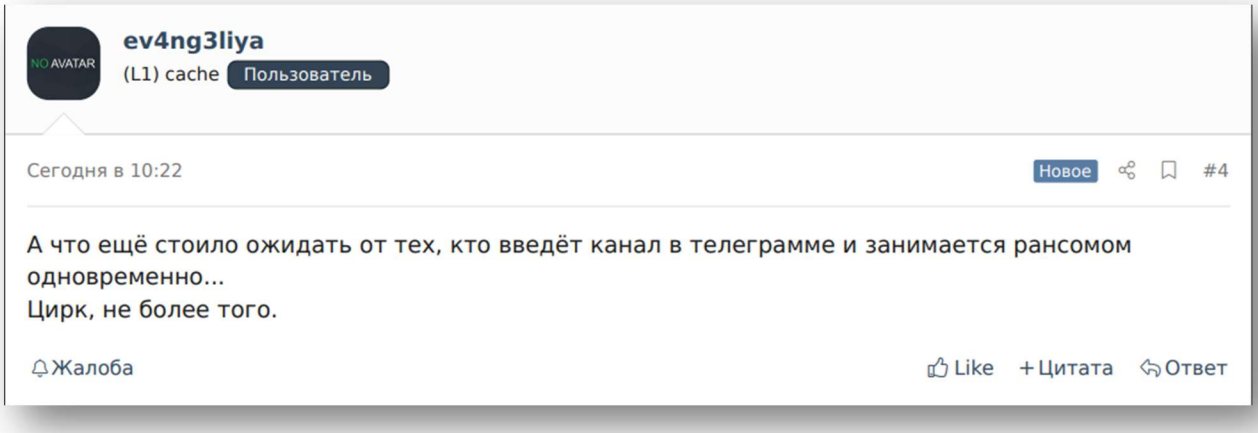
LockBit がタイヤ大手「ブリジストン」の米国法人を攻撃したと主張している投稿

その一方で、**Conti** の活動は 2022 年 1 月に減少へと転じました。そして 2022 年 2 月にロシアのウクライナ侵攻が始まると、同グループのメンバーの 1 人が、様々な内部チャットで交わされたメッセージ約 39 万 5,000 件、ランサムウエアのソースコード、その他のデータを外部にリークしました。この時リークされたデータは、我々が Conti の組織構造や、彼らのオペレーションにおける活動を垣間見る機会を与えてくれるものとなりました。このリーク事件を受けて Conti は 3 日間にわたり沈黙を続けていましたが、2022 年 3 月になると同グループの被害組織の数は 2 月の倍に増加しました。被害組織の大半は、製造・産業機器や専門サービス、医療関連業界の組織でした。なお Conti は、窃取したデータをもとに恐喝行為を行うグループ「Karakurt」とも関連があり、両グループの活動をあわせると 2022 年第 1 四半期に最も攻撃件数の多かったグループ第 2 位となりました。

Alphv（別名「**Blackcat**」）は、2021 年 12 月に登場したグループです。同グループが最も活発に活動を展開したランサムウエアグループの 1 つと見なされるようになったのは今年に入ってからであり、その標的となったのは、主に**専門サービス、消費・小売、製造業界**の組織でした。2022 年 4 月になると、米連邦捜査局（FBI）が Alphv と関連のある「侵入の痕跡（IoC）」を公開し、また同グループの開発者や資金洗浄者がランサムウエアグループ「DarkSide」や「Blackmatter」と繋がりがあることを公表しました。

攻撃件数が上位にランクインしているランサムウエアグループのうち、一部のグループについては、過去に別グループの攻撃を受けた被害組織を攻撃していることが確認されました。その 1 例を挙げてみましょう。2022 年 1 月 15 日、Conti が米国系の自動車販売会社に不正アクセスしたと主張しました。そしてその後の 2022 年 3 月 22 日には、この自動車販売会社が Alphv のブログで被害者として公開されました。さらに 2022 年 4 月 4 日には、Avos Locker が自らのブログでこの自動車販売会社を被害組織として掲載し、Alphv がブログで公開していたものと同じスクリーンショット、そして Conti がこの会社から窃取したとして公開していたものと同じファイルを公開していました。現時点では、この 3 つのグループが協力体制をとっていたのか、それとも単なる偶然で同じ組織を攻撃したのかは明らかになっていません。しかし最近研究者から寄せられた報告では、Conti が自律的に運営される小規模なランサムウエアグループを立ち上げようとしていたこと、そして他のランサムウエアグループ（Alphv や AvosLocker、Hive、HelloKitty）と協力体制を取ろうとしていたことが明らかになっています。

一方「Lapsus$」はトップの座には至らなかったものの、Okta 社や T-Mobile 社をはじめとする著名な企業を標的としたことで、2022 年第 1 四半期においても引き続き悪名高いサイバー犯罪グループの 1 つとなりました。また同グループについては、10 代のメンバー2 人が上述の企業に対するデータ侵害の容疑で逮捕され、起訴される事態となりました。この逮捕を受け、アンダーグラウンドのフォーラムユーザーの間では、「Lapsus$はランサムウエア攻撃やその他の攻撃を実行するだけの能力がない、間抜け者の集まりだ。だから自分達の身元を明かすという重大な過ちを犯したのだ」といった意見が交わされていました。

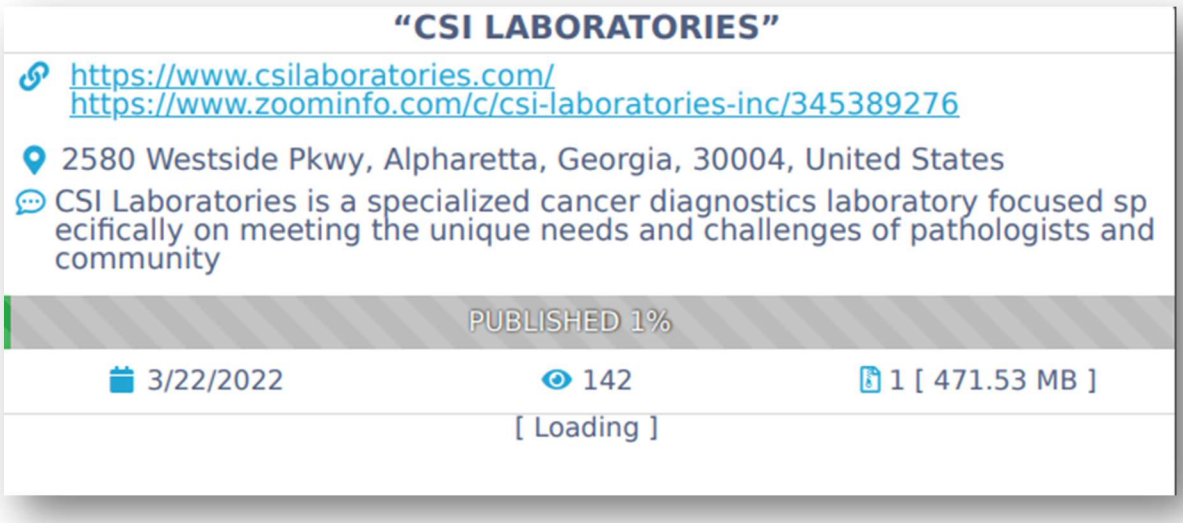


Lapsus$のオペレーターの身元が判明したことについてコメントしている脅威アクターの投稿。
「Telegram のチャンネルで活動しながらランサムウエア攻撃にも足を突っ込むような奴らに、
サーカス以上のものを期待できるわけがないだろう」

標的となった業界

ランサムウエアグループの標的となった業界の上位には、製造・工業製品、専門サービス、テクノロジーがランクインしました。また金融も、標的となった業界の 5 位にランクインしており、同業界における被害組織の数は 2021 年第 4 四半期と比較して 40%増となりました。興味深いことに、標的となった業界トップ 10 のうち、被害組織の数が増加したのは金融業界のみとなっています。金融業界に対する攻撃の 40%は、LockBit によって行われたものでした。

パンデミックが続く中、研究者やジャーナリストは、医療業界に対するサイバー攻撃についても綿密な観察を行ってきました。一部のランサムウエアグループにいたっては、医療業界に対する攻撃を禁じると公言していましたが、それにもかかわらず 2022 年第 1 四半期にランサムウエア攻撃を受けた医療機関・組織の数は 41 にのぼりました。また、それら攻撃の 34%は、Conti や Karakurt に関連していました。



ランサムウエアグループ「Conti」が、米国のがん診断企業「CSI Laboratories」に
不正アクセスしたと主張している投稿

標的となった国々

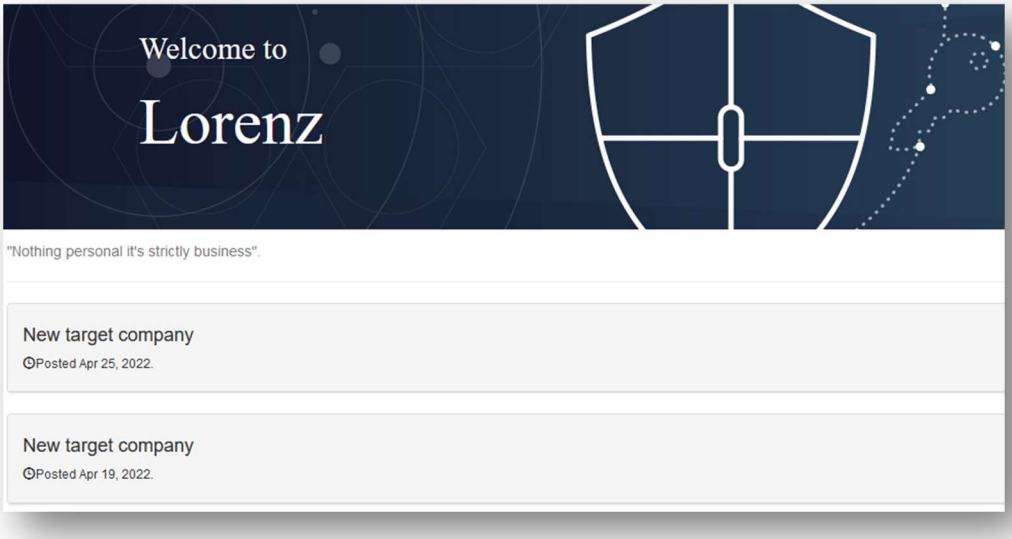
米国は最も標的とされている国であり、2022 年第 1 四半期にランサムウエア攻撃を受けた被害組織の 40%が米国企業、その次に被害組織の多かった国は英国、イタリア、ドイツ、カナダとなっています。この結果は、2021 年第 4 四半期と比較するとわずかに変化したものとなっています。2021 年第 4 四半期には、標的とされる国のトップ 5 にフランスがランクインしていましたが、2022 年にはフランスに代わってイタリアがランクインしました。

ランサムウエアグループの新たな恐喝手法

我々は、一部のランサムウエアグループが新たな恐喝手法を採用していることを発見しました。そのうちのひとつは、具体的な名称を明かさない状態で被害組織を自らのブログに掲載するというものです。Midas を例に挙げると、同グループは自らのデータリークサイトで被害組織を「New Company」と名付けて公開していました。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、被害組織の名称を追記するものと思われます。

Midas が被害者を「新会社」と名付けている投稿

ランサムウエアグループ「**Lorenz**」も同じ手口を採用しており、自らのランサムウエアブログで被害組織を「新たな標的企業」と名付けて公開しています。



Lorenz が被害者を「新たな標的企業」と呼んでいる投稿

さらに **Everest** のデータリークサイトのオペレーターも、同じ手口を採用していました。同グループのサイトでは、カナダに拠点を置くサプライヤー企業が被害組織として公開されており、1 万 500 人を超えるカナダ人の個人情報が含まれている同社データ（96 ギガバイト相当）をリークするという脅迫文が併せて掲載されていました。

Supplies Company Data Leak in British Columbia, Canada

96 gigabytes of internal company data. Including over 10,500 personal records of Canadian citizens (DOB, SYN, Email, phone, addresses, signature samples). The company has been notified of the attack and we are awaiting a response in a next few days . Otherwise the date will be published

Everest の投稿

Everest や Lorenz は被害組織の名称を曖昧にしていますが、Conti の場合はリークされた同グループのチャットから、特定の URL でのみアクセス可能な非公開のブログ投稿を作成していたことが判明しました。この非公開の投稿には被害組織に関する情報が掲載されており、アクターはその投稿を被害組織に閲覧させ、いかに簡単に（被害組織の）データへアクセスすることができるのかということを示して脅迫しています。被害組織が金銭の支払いに応じた場合には投稿が公開されることはありませんが、もし交渉が成立しなかった場合には、投稿が一般公開され、被害組織の名前が公表されます。

疑わしいデータリークサイト

2021 年、我々は、熟練したハッカーグループのふりをしながら実際には過去のリークデータを再公開しているアクターの存在を検知し、監視していました。そして 2022 年第 1 四半期に

おいても、過去にダークウェブで流通していたリーク情報を部分的に再利用することで悪名を高めていると思われるデータリークサイトを発見しました。

その 1 例を挙げてみましょう。2022 年 1 月 17 日、「**LeakTheAnalyst**」と名乗るアクターが RaidForums で、ハッカーグループ「LeakTheAnalys」が 5 年間の沈黙を経て復活したと発表しました。LeakTheAnalyst（別名ハッカーグループ 31337）」が最初のオペレーションを立ち上げたのは 2017 年であり、当時同グループは不正アクセスした企業の機密データを公開していました。しかし LeakTheAnalyst が FireEye 社を攻撃した後の 2017 年 10 月、メンバーの 1 人であったハッカーが逮捕され、同グループは活動を停止しました。

そして 2022 年 1 月 24 日、LeakTheAnalyst が今度は F5 ネットワーク社とその顧客に不正アクセスしたと主張しました。被害者の大半は F5 ネットワーク社の顧客でしたが、同グループが公開したスクリーンショットから、F5 ネットワーク社が不正アクセスされたのは 2016 年であることが判明し、恐喝に使用されているデータが過去の攻撃で窃取されたものである可能性が浮上しました。ダークウェブ上で同グループについて言及しているチャットの内容は、LeakTheAnalyst の信頼性が低いことを示唆しており、同グループのサイトには素晴らしい機能があるものの、価値あるデータは含まれていないといった主張も確認されています。また現在 LeakTheAnalyst のものとされている新しいサイトについても、5 年前に LeakTheAnalyst として活動していた同じアクターが運営していると判断できるだけの証拠は確認されていません。

その他に広範に議論されるようになったグループとして、「**STORMOUS**」が挙げられます。STORMOUS は自らをランサムウエアグループと名乗っており、2021 年 4 月 30 日には、Telegram でチャンネル「STORMOUS RANSOMWARE」を作成しました。同グループは、自分達は企業を攻撃してデータを窃取するランサムウエアグループであると主張していますが、彼らが Telegram チャンネルで公開した約 10 の被害組織は、それまでに他のランサムウエアグループによる不正アクセスを受けていました。また、STORMOUS が一部の被害組織について公開したファイルは、他のランサムウエアオペレーションのブログで公開されていたファイルと全く同じものでした。同グループは 2022 年 3 月 21 日に自らのサイトを立ち上げましたが、彼らについては他のアクターがリークした情報を再公開して、自らを熟練したランサムウエアグループに見せかけようとしているだけのグループであると推測されます。STORMOUS が独自の攻撃を展開しつつ、過去のデータ侵害を利用して自分達の活動を宣伝しているという可能

性も考えられますが、これまでのところ、研究者が同グループに関連するランサムウエア攻撃を確認したという事例は報告されていません。

2022 年第 1 四半期に売り出されたネットワークアクセス

脅威アクターは、引き続きアンダーグラウンドのフォーラムで、様々な不正行為に利用可能な初期アクセスを販売しています。2022 年第 1 四半期、我々は 521 件を超える商品を監視し、その希望販売価格は累計で 110 万ドルを超えました。また売りに出されていたネットワークアクセスのうち、少なくとも 11%については販売者のアクターから売却済と報告されていました。我々が観察したところ、初期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 1.75 日となりました（販売者が公開していたコメントなどの情報に基づく）。ただしここで重要となるのは、全ての初期アクセス・ブローカーが、商品（アクセス）の売買完了を公言するわけではないということです。

2022 年第 1 四半期に売り出されたアクセスの件数は、ひと月当たりの平均件数が約 173 件となり、2021 年第 4 四半期の 156 件より高い件数となっています。また、各月に売り出されたアクセスの件数を見てみると、2022 年 2 月の件数は 1 月の件数の約 50%程度に減少しましたが、3 月になると再び増加へと転じ 243 件が売りに出されていました。

脅威アクターの多くが売りに出していたのは RDP や VPN を介したアクセスであり、彼らは、Citrix 社や Fortinet 社、Palo Alto 社の VPN 製品について頻繁に言及していました。

売り出し件数の多かった初期アクセス・ブローカー

2022 年の第 1 四半期にネットワークアクセスを売り出していた脅威アクターの数は 116 人であり、2021 年第 4 四半期と比較して 15%増となりました。また、2022 年第 1 四半期に最も多く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、いずれも 30 件以上のアクセスを売りに出していました。

Novelli

Novelli は、2019 年からサイバー犯罪フォーラムで活動しており、毎月数十のネットワークアクセスを売りに出しています。Novelli は通常、固定価格で売り出している 1 商品の一部として、様々な企業の RDP アクセスを提供しています。彼は 2021 年第 1 四半期に続き、2022 年第 1 四半期においても最も活発に活動している初期アクセス・ブローカー第 1 位の地位を維持しました。

Pumpedkicks

Pumpedkicks は、「**Mont4na**」というハンドル名でも活動しており、主に SQL の脆弱性と企業のログイン資格情報を販売しています。ただし最近では、米国組織の VPN アクセスも売り出すようになっており、その一部には米国政府機関や公共部門のアクセスも含まれています。

Chiftlocal

Chiftlocal は、2022 年 3 月からフォーラム「Exploit」で活動している新参者の脅威アクターです。本人の主張によると、彼が売り出しているアクセスのほとんどは、オーストラリアや米国に拠点を置く企業のものだということです。

最も標的とされた国・業界

通常、初期アクセス・ブローカーは侵害した組織の名称を明かさず、それ以外の詳細情報（国、収益、業界など）を提供します。最も標的とされているのは米国であり、「Pumpedkicks」と名乗るアクターが米国に対する関心を高めていることも確認されました（Pumpedkicks は、米国企業のネットワークアクセスを 30 件以上も売りに出していました）。また、標的とされている国のトップ 5 は、米国、英国、ブラジル、カナダ、インドであり、売りに出されているネットワークアクセスの約 47%は、このトップ 5 の国々の組織のものとなっています。ブラジルとインドは、一般的に攻撃者の間で最も人気のある標的というわけではありませんが、2022 年第 1 四半期に入って一部のアクターがこの 2 カ国を集中的に狙いはじめた結果、両国が標的の上位にランクインしました（例えばブラジルは、主にアクター「Novelli」により標的とされていました）。

初期アクセス・ブローカーの標的となった業界の上位については、ランサムウエアグループの標的となった業界の上位と同様のパターンが確認されました。ただし、教育セクターについてはこのパターンから外れており、ランサムウエアグループが狙う業界のトップ 5 からは外れているものの、初期アクセス・ブローカーが標的とする業界のトップ 5 に入っています。これについては LockBit の代表者が以前主張していたように、ランサムウエアグループが収益性の高い企業に特化していることが理由となっている可能性が考えられます。かつて LockBit の代表者は、「我々は自分達のような輩、『ビジネスシャーク』を攻撃したいんだ」とも発言していました。したがって、教育機関は初期アクセス・ブローカーからの攻撃を受ける可能性はあるものの、ランサムウエアグループの目には魅力のない標的と映っていると言えるでしょう。

注目すべき事例

2022 年第 1 四半期に我々が発見した中でも、特に注目すべき事例として以下が挙げられます。

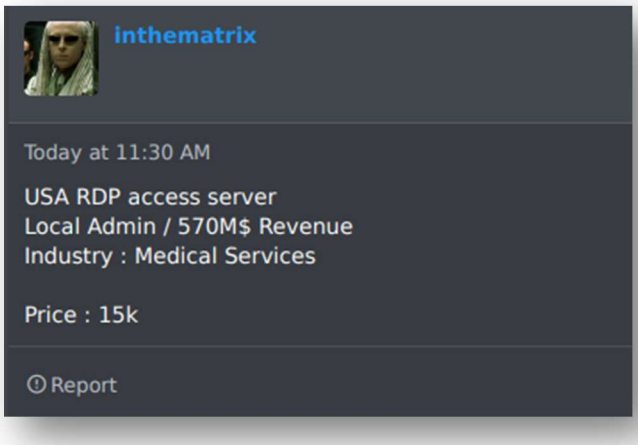
米国の自動車メーカー

2022 年 2 月 10 日、我々は脅威アクター「samyurch」が、米国に拠点を置き **300 億米ドル**の収益を有する「一流の自動車メーカー」へのアクセスを売りに出したことを発見しました。samyurch の説明によると、そのアクセスを使ってユーザー権限レベルの端末に 2 要素認証なしでログインできるということでした。このアクセスはオークション形式で売りに出され、その開始価格は **1 万 5,000 米ドル**となっていました。

米国の一流自動車メーカーへのアクセスを売りに出したアクターの投稿

米国の医療サービス企業

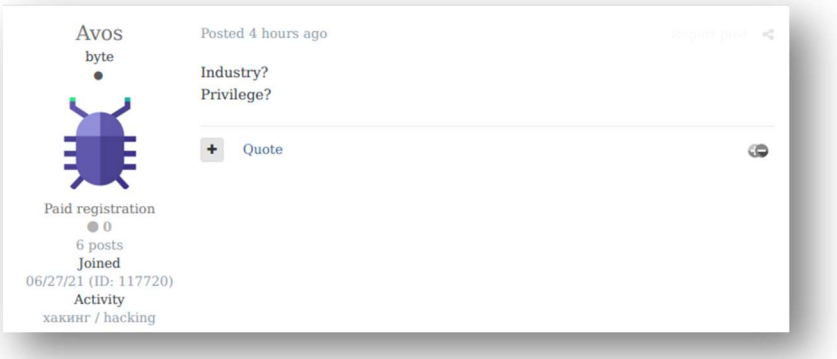
2022 年 2 月 1 日、我々は脅威アクター「inthematrix」が、米国に拠点を置き 5 億 7,000 万米ドルの収益を有する医療サービス企業のアクセスを売りに出したことを発見しました。inthematrix の説明によると、この商品は RDP を介したアクセスであり、ローカルの管理者権限レベルの端末にログインできるということでした。このアクセスは **1 万 5,000 米ドル**で売りに出されていましたが、2022 年 2 月 3 日には販売が終了していました。



医療サービス企業のネットワークアクセスを売りに出したアクターの投稿

ドイツの大手スポーツウエア企業

2022 年 2 月 23 日、脅威アクター「blackkkjackkkk」が、**230 億米ドル**の収益を有し数千人の従業員を擁するドイツ企業のアクセスを売りに出しました。このアクセスはオークション形式で売りに出され、その開始価格は **9,000 米ドル**となっていました。ランサムウエアグループ「**AvosLocker**」を代表しているユーザーがこのアクセスを購入することに関心を示しており、被害企業の業界やアクセスの権限レベルなど質問していました。



Avos の代表者がアクセスの買い取りに関心を示している投稿

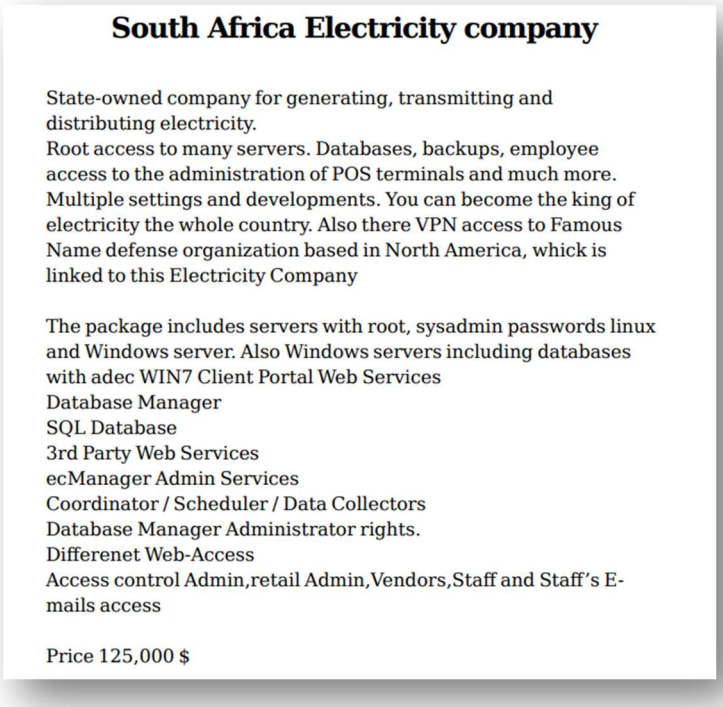
英国のフィンテック企業

2022 年 1 月 14 日、我々は、脅威アクター「BigShady」が、英国に拠点を置き 5,000 万米ドルの収益を有するフィンテック企業のアクセスを売りに出したことを発見しました。BigShady の説明によると、この商品は AWS （Amazon Web Services）のアカウントを介したアクセスであり、管理者権限が付与されているとのことでした。このアクセスは、**1 万米ドル**で販売されていました。

英フィンテック企業の AWS アカウントのネットワークアクセスを売りに出したアクターの投稿

南アフリカの電力企業

我々は、サイバー犯罪グループ「Everest」が、引き続き被害者のネットワークアクセスを売りに出していることを確認しました。2022 年 3 月 20 日、同グループは南アフリカに拠点を置く電力企業のアクセスを売りに出し、この商品（VPN 経由のアクセス）を使って管理者権限のある端末にログインできると説明していました。このアクセスは、**12 万 5,000 米ドル**で売りに出されていました。



South Africa Electricity company

State-owned company for generating, transmitting and distributing electricity.
Root access to many servers. Databases, backups, employee access to the administration of POS terminals and much more. Multiple settings and developments. You can become the king of electricity the whole country. Also there VPN access to Famous Name defense organization based in North America, whick is linked to this Electricity Company

The package includes servers with root, sysadmin passwords linux and Windows server. Also Windows servers including databases with adec WIN7 Client Portal Web Services
Database Manager
SQL Database
3rd Party Web Services
ecManager Admin Services
Coordinator / Scheduler / Data Collectors
Database Manager Administrator rights.
Differenet Web-Access
Access control Admin,retail Admin,Vendors,Staff and Staff's E-mails access

Price 125,000 $

Everest のオペレーターが南アフリカの電力企業のネットワークアクセスを売りに出した投稿

ネットワークアクセスがランサムウエア攻撃にいたるまで

初期アクセス・ブローカーが販売している商品の一部は、ランサムウエア業界において重要な役割を果たしています。ランサムウエアグループは、標的とする組織の侵入口を積極的に探しており、侵入口を手に入れた後は攻撃に利用しています。2021 年、我々は、商品として売り

出されたネットワークアクセスが発端となってランサムウエア攻撃が引き起こされた事例を複数紹介しました。それらの事例で、アクセスが売り出されてからランサムウエア攻撃へと発展するまでの期間は、平均して 1 カ月以内となっていました。2022 年第 1 四半期、我々は **BlackByte** や **Quantum**、**Alphv** が初期アクセス・ブローカーからアクセスを購入していることを確認しており、彼らは購入したアクセスを十中八九、自分達の攻撃で使用しているものと思われます。

東南アジアの石油ガス企業（BlackByte）

BlackByte は、2021 年 8 月にオペレーションを立ち上げたグループであり、これまでに同グループがランサムウエア攻撃に利用するアクセスを初期アクセス・ブローカーから購入していたことが観察されています。2022 年 2 月には、米連邦捜査局（FBI）が BlackByte に関する警告を発表し、同グループに関連付けられた IoC を公開しました。

そして 2022 年 1 月 11 日、我々は、脅威アクター「White_Album」が 2 億 5,700 万米ドルの収益を有する公益企業のアクセスを 1,000 米ドルで売りに出したことを確認しました。そしてその後の 2022 年 2 月 6 日には、BlackByte がこの企業に不正アクセスしたと主張しました。この攻撃については、同グループのアフィリエイトがアクセスを購入したことが発端となっている可能性が考えられます

西アジアに拠点を置く航空会社への攻撃（Quantum）

Quantum は、2021 年 8 月に登場したランサムウエアグループであり、ランサムウエアオペレーション「MountLocker」と関連があります。Quantum はデータリークサイトを運営しており、当初は同リークサイトで Dopple Paymer や Xing など他のランサムウエアグループの被害組織の情報を投稿していました。しかし 2021 年 11 月以降は、Quantum 独自の被害組織のものと思われる情報を公開するようになりました。

2022 年 1 月 10 日、我々は、脅威アクター「fatman_Dark」が西アジアに拠点を置く航空会社のアクセスを売りに出したことを確認しました。この時 fatman_Dark は商品について、VPN を介したアクセスであると説明していました。そしてその後の 2022 年 2 月 7 日、Quantum のオペレーターが、この航空会社に不正アクセスしたと主張しました。

米系 IT 企業への攻撃（Alphv）

2022 年 3 月 28 日、我々は脅威アクター「vcc_expert」が、3 億 4,000 万米ドルの収益を有する米系 IT 企業のアクセスを売りに出したことを確認しました。vcc_expert によると、この商品は RDP を介したアクセスであり、ユーザーレベルの権限を持つ端末にログインできるとのことでした。商品はオークション形式で売りに出されており、開始価格は 1,000 米ドルとなっていました。そしてその後の 2022 年 4 月 5 日、ランサムウエアグループ「Alphv」がこの企業に不正アクセスしたと主張しました。この事例については、アクセスが売りに出されてから犯行声明が出されるまでの期間が 1 週間という短い時間であったことを考慮すると、それぞれのインシデント（アクセスの販売と攻撃の実行）が発生したのは単なる偶然であったという可能性が考えられます。例えば、売り出されていた初期アクセスと同じアクセスを Alphv が偶然自力で発見して攻撃に利用した、又はこの企業に侵入できる別のベクトルを利用して攻撃したといった可能性です。

結論

我々の調査結果をまとめると、2022 年第 1 四半期も引き続き、初期アクセス・ブローカーの提供する商品に対して需要があったことが判明しました。さらに売却されたアクセス商品の一部については、ランサムウエアグループの攻撃で悪用されていました。ネットワークの防御を担当される皆様には、サイバー犯罪者らに一歩先んじてランサムウエア攻撃を防ぐために、こういったアクセスの売買活動を監視されることをお勧めいたします。

サイバー犯罪に特化した KELA の脅威インテリジェンスプラットフォームを、是非ご活用ください。