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

KELA

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

KELA サイバー犯罪インテリジェンスセンター

エグゼクティブサマリー

ランサムウエアグループは引き続き進化を遂げ、世界中の組織や企業を脅かしています。2022 年第 2 四半期は、一部のグループにおいて活動量を減少する、または活動そのものを停止するといった動向が観察されましたが、その一方で Black Basta をはじめとする新たなアクターが登場し、企業から金銭をゆすり取っていました。その他、データの窃取やデータリークサイトの運営といったランサムウエアグループの手口を模倣しながらも、実際の攻撃では暗号化ソフトウエアを使用していないアクターも登場しています。

ランサムウエアオペレーションやデータリークサイトを運営しているアクターにとっては、成長の一途をたどるサイバー犯罪エコシステムを活用することで、偵察フェーズや最初の不正アクセスフェースがさらに容易なものとなっています。そしてその中でも、企業のネットワークアクセスを販売している初期アクセス・ブローカー（IAB）は、ランサムウエアのサプライチェーンにおいて重要な役割を果たしています。アンダーグラウンドでネットワークアクセスの供給者となっている彼らを監視することは、ランサムウエア・アズ・ア・サービスのエコシステムの更なる理解につながると言えるでしょう。

KELA が、2022 年第 2 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て得た洞察は以下の通りです。

- 2022 年第 2 四半期のランサムウエアグループ及びデータリークグループの活動は、2022 年第 1 四半期と比較して 7%減少しました。また、我々がこの第 2 四半期に確認した攻撃件数は、ひと月あたり平均 216 件となりました。

- 2022 年第 2 四半期に最も攻撃件数の多か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、Alphv （別名 BlackCat）、Conti、Vice Society であり、いずれのグループも 40 を超える被害組織を公開していました。

- 2022 年第 2 四半期、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トップ 3 は、製造・工業製品、専門サービス、工事・建設となりました。その後には新たに人気の出た標的として、医療・ライフサイエンスや、政府・公共部門が続きました。

- 2022 年第 2 四半期も、ランサムウエアグループ及びデータリークグループが最も標的としたのは米国であり、被害組織の 35%は米国企業、その次に被害組織の多かった国はドイツ、英国、カナダ、イタリアとなりました。この 5 カ国は、第 1 四半期にも標的とされる国のトップ 5 となっていました。

- 2022 年第 2 四半期、REvil（Sodinokibi）や Stormous、Lapsus$など、悪名高いランサムウエアグループやデータリークグループが活動を再開していることが確認されました。

- 2022 年第 2 四半期、一部のデータリークグループ（RansomHouse や Industrial Spy）は新たな収益モデルを導入しており、攻撃者が自らの利益を増やすべく進化を続けている様子がうかがえました。

- 一方でランサムウエアグループも、より高額な金銭を手にするべく新たな手法を取り入れていました。その一例として、最初に攻撃を行った被害組織に加え、そのベンダー企業やパートナー企業、顧客をも攻撃し、複数の企業に対して身代金を要求するといった手口が挙げられます。

- 2022 年第 2 四半期に売り出され、我々がモニタリングしたネットワークアクセスの件数は 550 件超、希望販売価格の合計金額は約 66 万米ドルとなりました。

- 2022 年第 2 四半期に売り出されたネットワークアクセスは、ひと月あたり平均 184 件となりました。

- 2022 年第 2 四半期、ネットワークアクセスを売りに出したアクターの数は約 110 人となりました。また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 40 件以上のアクセスを売りに出していました。

- 2022 年第 1 四半期と同様にこの第 2 四半期も、初期アクセス・ブローカーに標的とされた国の第 1 位は米国となり（被害組織の約 20%）、その後にはブラジル、フランス、英国、イタリアが続きました。

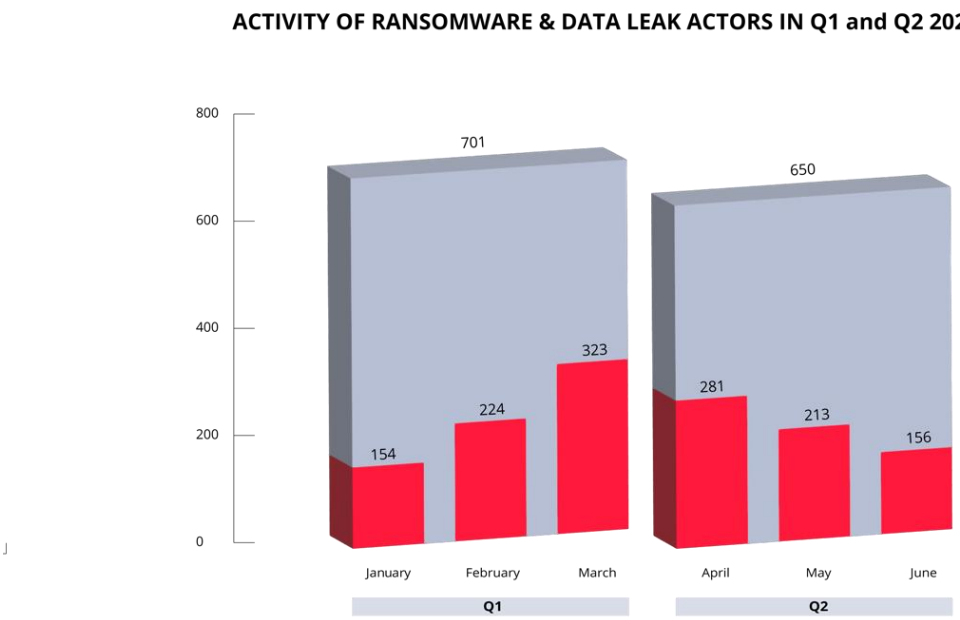
- 初期アクセス・ブローカーに標的とされた業界の第 1 位は、製造・工業製品であり、ランサムウエアグループが標的とした業界の第 1 位と一致する結果となりました。

- 2022 年第 2 四半期を通して見られた傾向の 1 つとして、初期アクセス・ブローカーが新たに発見された脆弱性のエクスプロイトを速やかに活用し、パッチを当てていない組織のネットワークを標的にしていることが挙げられます。我々の調査では、Microsoft Exchange の脆弱性（CVE-2021-42321）や、Confluence Server 及び Data Center の脆弱性（CVE-2022-26134）、VMware 社製 Workspace One Access 及び Identity Manager の脆弱性（CVE-2022-22954）が悪用されていることが確認されました。

- 初期アクセス・ブローカーの多くは、ランサムウエアのサプライチェーンに貢献するのみならず、攻撃にも参加する意思があるようです。2022 年第 2 四半期、我々はそういったアクターの 1 人が、ランサムウエアオペレーターへと進化を遂げていたことを確認しました。

2022 年第 2 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

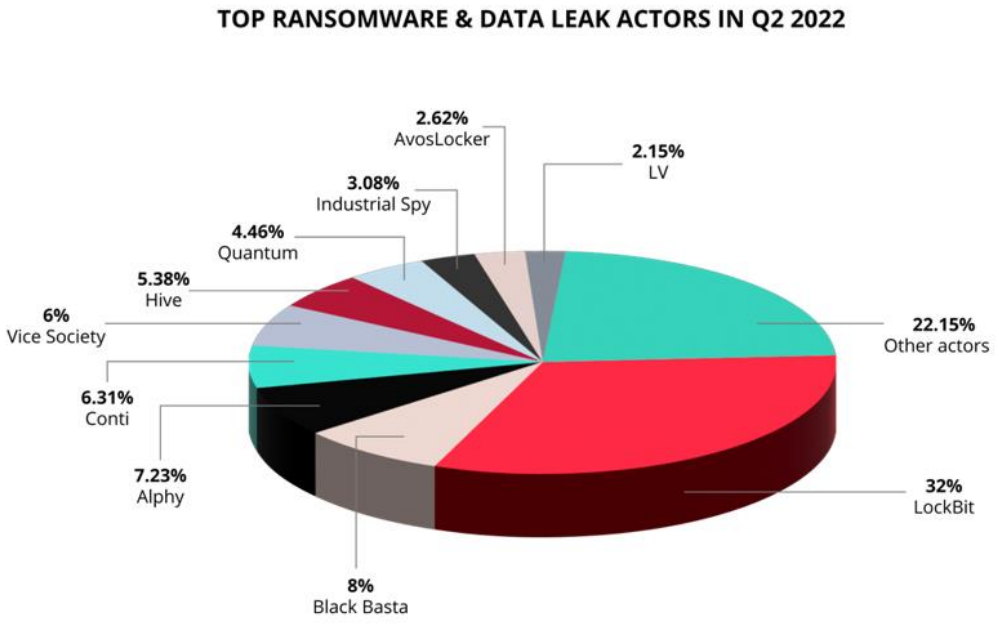
2022 年第 2 四半期、我々は監視対象とするソース（ランサムウエアグループや類似のアクターが運営するデータリークサイトや交渉ポータル、公になっている報告など）で、約 650 の被害組織を特定しました。この数字は、前四半期比でわずかな減少（7%）となっており、また前年同期比でも減少となっています。被害組織のひと月あたり平均数は、第 1 四半期は 232 組織でしたが、2022 年第 2 四半期は 216 組織となりました。



攻撃件数の多かったランサムウエアグループ

2022 年第 2 四半期に攻撃件数の多か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、Alphv**（別名 **BlackCat**）、**Conti、Vice Society** であり、いずれのグループもそれぞれ 40 以上の被害組織を公開していました。その中でも、有名なランサムウエアグループ LockBit は、200 を超える被害組織を公開してトップの地位を守りましたが、比較的最近登場した「Black Basta」も早々に 2 位の座を獲得しました。その他 Vice Society も、前四半期の 2 倍以上の数となる被害組織を公開して比較的上位にランクインしました。Conti は、現在活動を停止していると思われますが、今期（第 2 四半期）当初は活動していたため、今回の調査でもリストの上位にランクインしています。

今回の我々の調査では、第 1 四半期にトップ 5 にランクインしていた Hive と Karakurt の攻撃件数が減少していることが確認されています。Hive については、他のグループに追い抜かれる結果となったものの、同グループが公開している被害組織の数は、前四半期と大きな違いはありません。その一方で Karakurt（Conti の 1 部門）については、攻撃件数が約 90%と大幅に減少していました。ただし、2022 年 7 月における同グループの被害組織数は 45 を超えていることから、現在は活発に活動を展開しているものと思われ、2022 年第 3 四半期においても活発に活動する可能性があります。



LockBit

LockBit は前四半期と同様に、今期も最も活発に活動を展開したランサムウエアグループとなり、同グループが公開した（または検知された）攻撃件数は 200 件を超えました。同グループは過去 1 年の間にその攻撃件数を大きく伸ばし、今や最も進化したランサムウエアグループの 1 つとしての地位を維持しています。最近同グループは、自らのデータリークブログでランサム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「LockBit 3.0」のリリースを正式に発表し、また同グループのオペレーションについても「政治とは完全に無関係であり、金銭のみに関心を持った」活動であると明言して、アフィリエイトに対するルールを改訂しました。同グループが明言したこの方針は、彼らが多岐にわたる業界を攻撃しているという事実にも表れています。またこの発表が行われた投稿には、「団結力があり、経験豊富なペンテスターチームを探している」ことや、「アクセス提供者と連携する用意がある」ことなどが明記されていました。

The oldest international [Ransomware] LockBit affiliate program welcomes you.

We are located in the Netherlands, completely apolitical and only interested in money.
We always have an unlimited amount of affiliates, enough space for all professionals. It does not matter what country you live in, what types of language you speak, what age you are, what religion you believe in, anyone on the planet can work with us at any time of the year.
First and foremost, we're looking for cohesive and experienced teams of pentestors.
In the second turn we are ready to work with access providers: sale or on a percentage of redemption, but you have to trust us completely. We provide a completely transparent process - you can control the communication with the victim. In case when the company was encrypted and has not paid, you will see the stolen data in the blog.
We also work with those who don't encrypt networks, but just want to sell the stolen data, posting it on the largest blog on the planet.

LockBit 3.0 のルール（ソース：LockBit のブログ）

また LockBit は、独自のバグ報奨金プログラムも立ち上げています。これは、同グループのウェブサイトまたはランサムウエアに存在する脆弱性や、同グループのオペレーションに被害をもたらしうる TOX や Tor 上のバグなどを発見して報告してくれた人物に、1,000 米ドルから 100 万米ドルの報奨金を支払うというものです。さらに同グループは、「アフィリエイトプログラムのボス」を特定した人物には 100 万米ドルを支払うとも述べていました（「アフィリエイトプログラムのボス」とは、恐らく LockBit の管理者を指しているものと思われます）。同グループがこういった申し出を行う理由としては、脆弱性やバグ、プログラムのボスに関する情報に

対して金銭を支払うことで、法執行当局へ報告されることを防ごうという意図がある可能性もありますが、LockBit を「曝（さら）す」ことができる者はいないことを鼻にかけ、自慢しているという可能性も考えられます。

その他 LockBit に関して注目すべき出来事としては、米国のサイバーセキュリティ企業「Mandiant」社に対する犯行声明が挙げられますが、これについては世間の注目を集めるための虚言であったことが明らかとなっています。2022 年 6 月、同グループは Mandiant 社の名前とともに 2 本のファイル（メモ「mandiantyellowpress.com」とアーカイブファイル「foxconfortwitter」）を公開しましたが、我々の調査では、それらのファイルに Mandiant 社関連の文書が含まれていなかったことが確認されています。この 2 本のファイルの内容は、LockBit が「Foxconn Baja California」社工場に対して行った攻撃に関連したものであり、その中には LockBit の「サポート担当者」と、Foxconn 社に対する攻撃を実行したアフィリエイトのやり取りのスクリーンショットが含まれていました。またこのスクリーンショットには、アフィリエイトが「『研究者』が自分（アフィリエイト）を Evil Corp に紐づけている」と不満を述べているメッセージが映っていました。

なお先日、Mandiant 社が、LockBit を使用していることが確認されている某脅威アクターの活動について解説を発表し、その中で、この脅威アクターと Evil Corp の活動に共通点が見られるとの見解を述べていました。つまり、LockBit のサポート担当者とアフィリエイトはこの Mandiant 社の発表を受けて、上述のスクリーンショットの中で「我々は Evil Corp とは何の関係もない」と発言していたのです。これらの状況から我々は、LockBit が Mandiant 社の名を被害組織としてブログで公表した理由は、LockBit が同社を攻撃したものとして世間の注目を集め、その注目を逆手にとって自分達が Evil Corp と関連がないことを周知するためであり、Mandiant 社に対する侵害は実際には行われなかったものと判断しています。

Black Basta

ランサムウエアグループ「Black Basta」は 2022 年 4 月に登場して以来、すぐに主要プレイヤーとなりました。なお、同グループのリークサイトや身代金支払いサイト、被害組織へのサポートサービス対応には Conti と類似点があり、両グループのつながりが疑われています。しかし Conti 側は Black Basta とのつながりを否定しており、2022 年 5 月に Conti がペルーの経済財務

省に対する犯行声明を出した際、その投稿の中で「自分達は Black Basta の活動とは関係ない」と明言していました。

ランサムウエアグループ Conti が「自分達は Black Basta とは関係ない」と述べている投稿（ソース：MalwareHunterTeam）

上記の通り、Conti は Black Basta との関係を否定していますが、我々がサイバー犯罪フォーラムを調査したところ、アクターらが参加している複数のディスカッションの中で、「Black Basta は Conti グループのリブランドか、同グループの 1 部門である」との憶測が浮上していることが確認されました。また LockBit のオフィシャルアカウントユーザー「LockBitSupp」も、このような憶測を主張しているユーザーの 1 人であり、2022 年 6 月 28 日にフォーラム XSS で、「Black Basta は Conti のリブランドだ」と発言していたことが確認されています。

この発言を受け、かつて Conti に属していたと主張しているユーザー「ev4ng3liya」は、Black Basta は Conti のリブランドではなく、同グループの 1 部門であると述べていました。その後も ev4ng3liya は、「正式には、Black Basta は（Conti の）1 部門だった。少なくとも、自分が所属していた時はそうだった。今は Black Basta がどっちでもいいけどね」と繰り返していました。ev4ng3liya が XSS に投稿していたその他のメッセージから、我々は高い確率で ev4ng3liya が実際に Conti グループのメンバーであったものと判断しており、ev4ng3liya の上述の発言も考慮しておくべきものと考えています。

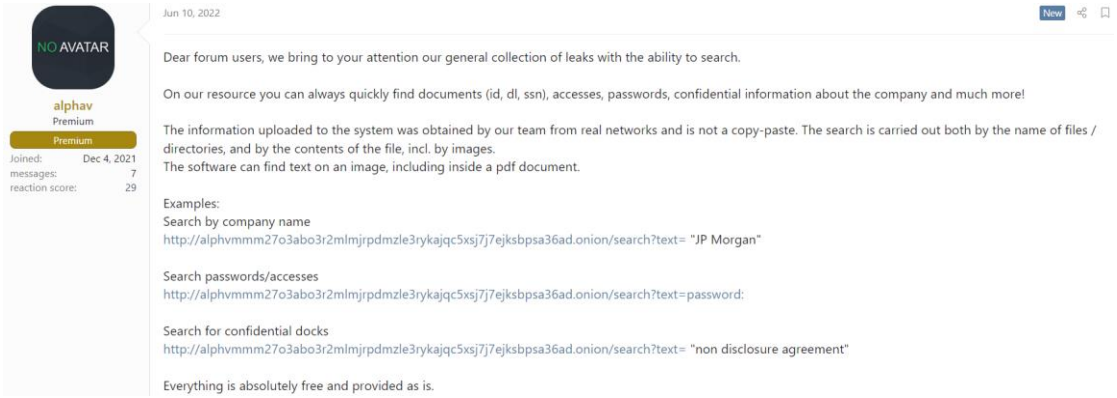
ev4ng3liya が Black Basta は「リブランディングではなく、Hive やその他と同じく 1 部門だ」と主張している投稿（ソース：XSS）

Alphv

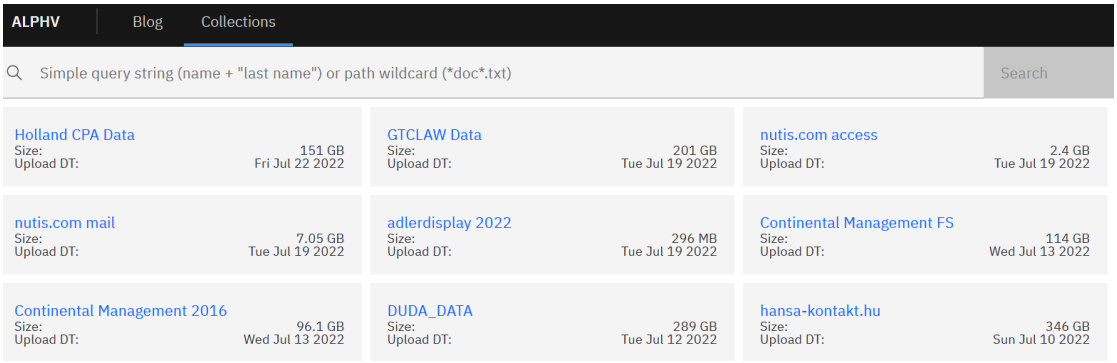
Alphv（別名 BlackCat）は 2021 年 12 月に活動を開始したグループであり、2022 年に入って現在に至るまで、同グループは安定した数の組織を攻撃しています（2022 年第 1 四半期は 60 弱、第 2 四半期は約 50）。2022 年 7 月、Alphv は、同グループが被害組織から窃取した全てのデータを検索できるディレクトリ「Collections」のリリースを発表しました。Alphv が最初に Collections を発表したのはフォーラム XSS であり、この時同グループは、フォーラムの全ユーザーが被害組織のパスワードや文書、アクセス、機密情報を検索・閲覧できるよう、彼らをディレクトリ（Collections）に招待していました。なお Alphv はこの Collections の公開に先立ち、2022 年 6 月 14 日に Collections のテスト版ともいえるバージョンを公開していました。同グループは、米国のリゾート施設「The Allison Inn & Spa（theallison.com）」からデータを窃取して同社専用のウェブサイトを立ち上げ、そこでこのテスト版 Collections を公開していたのです。またこの専用サイトでは、The Allison Inn & Spa の顧客や従業員が、自分の個人情報が侵害されたかをテスト版 Collections で調べられるようになっていました。

Alphv の上述の取り組みは、さらに進化して新たな威嚇手法を取り入れていこうという、同グループの野心を表しています。また今後は、サイバー犯罪者らが Collections の検索バーに入力

した情報（企業の電子メール等）を Alphv が収集し、さらなる不正行為に悪用するのかという点についても関心が持たれるところです。



Alphv のオペレーターが「Collections」を発表している投稿（ソース：XSS）



Alphv の「Collections」（ソース：Alphv のブログ）

Conti よ、さようなら

Conti は、これまで多数の攻撃を実行してきたグループの 1 つです。2022 年第 2 四半期当初は、その被害組織の数は約 40 に上っていましたが、同グループの内部情報がリークされるという事件を皮切りに一連の出来事が続いた後は、活動を停止したものと思われます。なお、Conti の活

動が停止にいたる前、同グループのブログやサイバー犯罪フォーラムでは、奇妙な活動が見られました。

例えば 2022 年 5 月には、Conti のオペレーターが自らのブログで、Alphv と LockBit のオペレーターに対する警告（投稿）を公開しており、その内容は Alphv と LockBit が詐欺を行い、非公開のチャットで交わされた情報を窃取し、広告主を騙していると非難しているものでした。またフォーラム「RAMP」では、Conti の代表者が、セキュリティ研究者にアクセスされるリスクを考慮し、今後はオペレーションのチームメンバーを募集しないと発言していました。

ここで興味深い点として、以前 Conti と関連のあった脅威アクター「Danger1488」が、「自分達のチームはネットワークのアクセスを買い取る用意がある」とフォーラム Exploit で発言していたことが挙げられます。Danger1488 は、約 1 年ほどの沈黙していたものの 2022 年 3 月から再び投稿を掲載するようになっており、この変化は「恐らく Conti は活動を停止しており、その結果一部のメンバーが他のランサムウエアオペレーションへ移行している」という報道と一致しています。現在 Conti のデータリークブログや交渉ポータルは閉鎖されており、グループ、またはブランドとしての Conti が永遠に活動を停止したという可能性も考えられますが、同グループの元メンバーは、現在も引き続き別のランサムウエアオペレーションに参加しています。

標的となった業界

2022 年第 2 四半期も、ランサムウエアグループやデータリークグループが標的とした業界の上位には、製造・工業製品と専門サービスがランクインしました。また特に興味深い点として、医療・ライフサイエンスや政府・公共部門が、新たに人気の出た標的として上位に入っていることが挙げられます。医療・ライフサイエンスや政府・公共部門は、いずれもモラルの観点や身代金が支払われる率の低さ、法執行機関の注目を集めることに対する恐れなどから、脅威アクターの間では「論争を引き起こす」標的と見なされていますが、一部の攻撃者の間ではこの認識に変化が生じているようです。

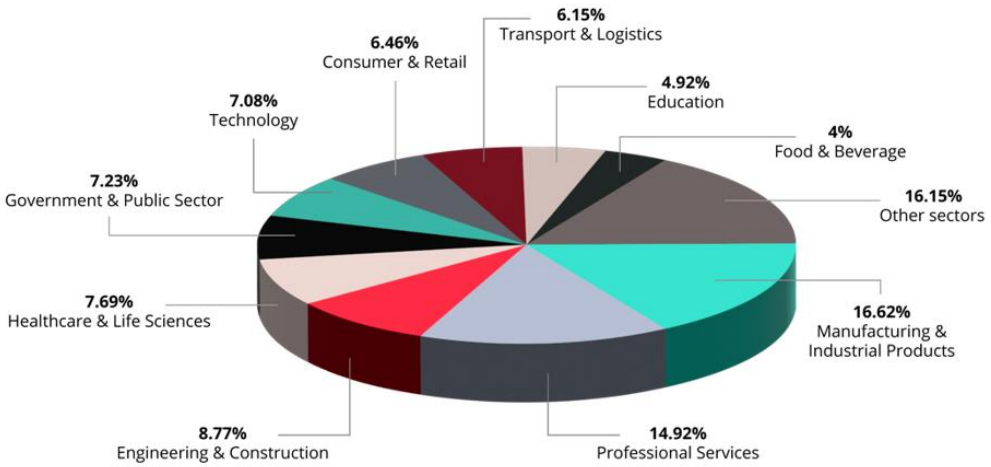
例えば LockBit 3.0 の「ルール」では、医療機関について以下のように主張しています。

「製薬会社や歯科医院、美容外科などの医療関連機関を、非常に慎重かつ選択的に攻撃することは許可されています。<...> また他の組織についても、民間の組織で収益（KELA にて意訳）がある場合は同じ扱いとします。心臓病センターや脳神経外科部門、産婦人科など、ファイルに対するダメージが死につながるような機関での暗号化は禁止されています。<...> データを暗号化せず、医療機関から窃取することは許可されています。そういった情報は、医療上の機密情報である可能性があり、また法に従って厳重に保護されているはずだからです。」

このルールは、一部の脅威アクターの間でその心境が変化していることを示しており、LockBit と Karakurt にいたっては、第 2 四半期における医療関連業界の被害組織のうち約 50%を、彼らが攻撃していました。

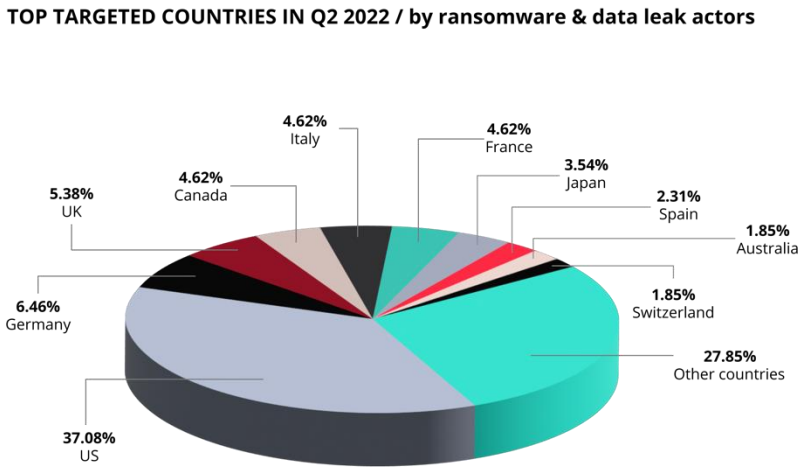
政府・公共部門に対する攻撃については、その 65%超が LockBit または Vice Society、Conti による犯行でした。またこの業界で最も攻撃件数が多かったのは、米国及びコスタリカとなっています（コスタリカは、Conti が最後に攻撃を実行した国でもあります）。

TOP TARGETED SECTORS IN Q2 2022 / by ransomware & data leak actors



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 位となっており、第 2 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 35%は、米国の組織に対して行われていました。その後にはドイツ、英国、カナダ、イタリアが続き、2022 年第 2 四半期に標的とされた国のトップ 5 は、第 1 四半期と同じ結果となりました。



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の活動再開

2022 年第 2 四半期には、悪名高いランサムウエアグループやデータリークグループが活動を再開していることも確認されました。ランサムウエアグループ「**REvil（Sodinokibi）**」は、2022 年 1 月に同グループのメンバーが多数逮捕されて以降活動を停止していましたが、2022 年 4 月 21 日に我々が行った調査では、同グループが Tor 上で運営していたデータリークブログが復活していたことが確認されました（以前のデータリークブログへアクセスすると、新しい URL へリダイレクトされます）。

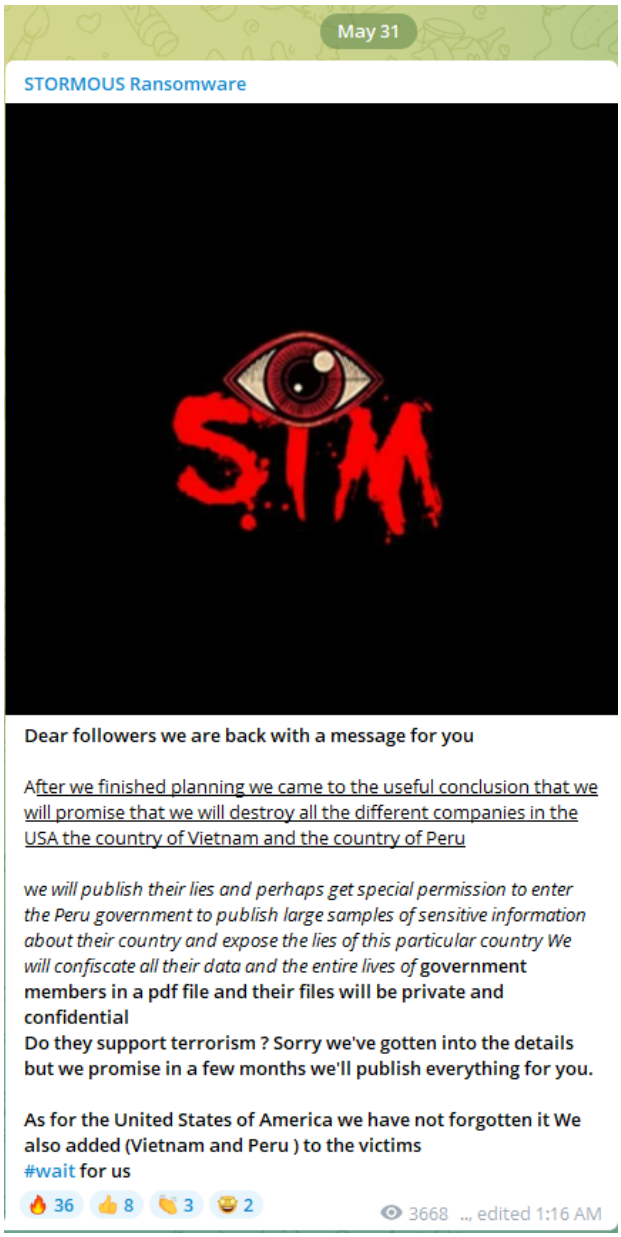
また 2022 年 5 月 1 日には、REvil が使用しているマルウエアの新たな亜種と思われるランサムウエアのサンプルが、研究者によって発見されました。この亜種が生成した身代金要求メモには、REvil の新たなデータリークブログ（前述のブログ）と、このサンプルを使用したアクターの交渉ポータルの URL が掲載されていました。

REvil が復活したとの可能性が浮上して以降、このデータリークブログには新たな被害組織が複数掲載されており、またそれらに加えて、REvil が 2021 年 4 月から 7 月にかけて攻撃していた被害組織もいくつか掲載されています。これまでのところ、REvil に紐づいているこの新たなランサムウエアオペレーションの背後に誰がいるのか、そして REvil の代表者が復活して活動しているのか、それとも他のアクターが、以前活発に活動していた同グループのインフラを利用してオペレーションを運営しているのかなどの点については、いずれについても明らかになっていません。

また我々は、某脅威アクターが、かつて REvil の代表者の 1 人であったユーザーのハンドル名「0_neday（REvil の最初のグループリーダー『UNKN/Unknown』に代わって 2021 年に同グループの代表者となった人物）」や、これに似たハンドル名を複数のサイバー犯罪フォーラムで使用していることを発見しました。このアクターはネットワークアクセスを買い取ると発言し、自分達がランサムウエアオペレーションに属しているかのように振舞っていましたが、かつて REvil のオペレーションに参加していたフォーラムユーザーがこのアクターの投稿に反応していないことから、このアクターは恐らく元の REvil オペレーションとは関連が無いものと思われます。

Stormous も、一旦の活動休止を経て活動を再開したハッカーグループです。同グループは遅くとも 2021 年 4 月から活動しており、自らの Telegram チャンネルで被害組織を公開しています。Stormous はランサムウエアグループを自称していますが、はたして彼ら独自のランサムウエアがあるのか、そしてそもそも彼らがどの種類にせよランサムウエアを攻撃で使用しているのかは明らかとなっていません。また同グループは、これまで複数の有名組織に対して攻撃を行ったと主張していますが、それらの攻撃が実際に行われたのかについて、信ぴょう性が疑われています。さらに同グループが被害組織のものとして公開したデータの一部についても、既にダークウェブ上で公開されていた情報であったことが判明しています。

2022 年第 2 四半期に Stormous が犯行を主張した有名組織の 1 つは、コカ・コーラ社でした。2022 年 4 月 19 日、Stormous は自らの Telegram チャンネルで、次の標的とする組織について投票を行っており、コカ・コーラ社はこの投票結果で標的に選ばれたものと思われます。その後の 2022 年 4 月 25 日、同グループはコカ・コーラ社のサーバーに不正アクセスして 161G を超えるデータを窃取したと主張し、買い手候補となった人物にはデータを見せるとも約束していました。しかし 2022 年 5 月 10 日には、同グループは自らの Telegram チャンネルで活動を休止している旨を発表し、にもかかわらずその 3 週間後には再び活動を開始して、「米国やベトナム、ペルーのあらゆる企業を破壊する」と発言していました。しかし、Stormous はそれほど活発に活動しておらず、活動再開以降に同グループが被害組織として公開したのは、シンガポールのエンジニアリング企業 1 社のみとなっています。

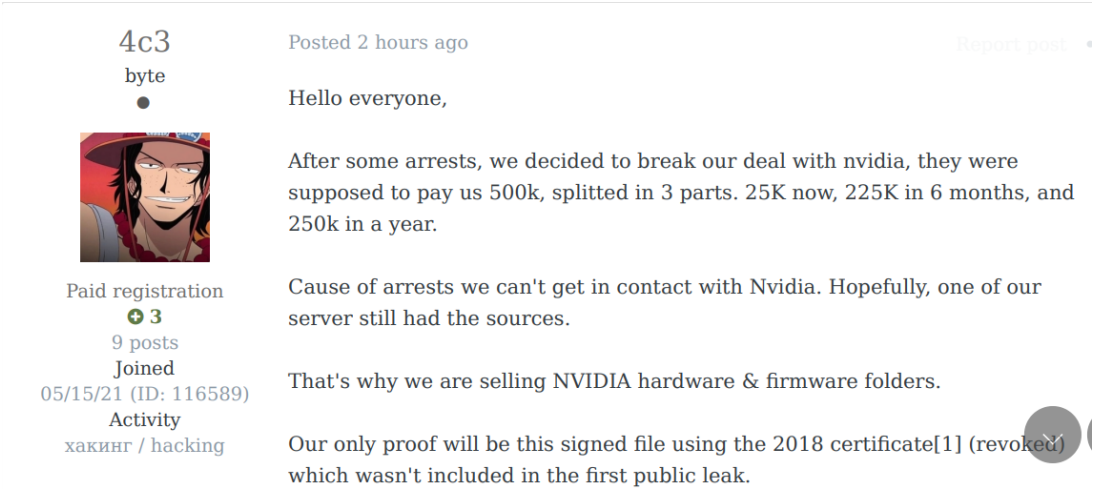


Stormous が活動再開を発表している投稿

Stormous と同じく **Lapsus$**も、有名組織に対する攻撃を主張するグループとして知られていますが、同グループは自らを経験豊富なハッカーグループと証明することができませんでした。Lapsus$は 2022 年第 1 四半期に入って以降、2022 年 3 月にメンバー2 名が逮捕されるまでは、世間の大きな注目を集めることに成功していました。この 2 名の逮捕は、同グループのメンバーが年齢的に若かったことがグループ内で衝突を生む要因となったこと、そして彼らの経験

が浅かったことを物語っています。しかしこの第 2 四半期、同グループのメンバーであったアクター「4c3」が突然活動を再開していました。

2022 年 2 月の時点で、Lapsus$は Nvidia 社に対する攻撃について犯行声明を出していましたが、その 3 カ月後となる 2022 年 5 月 9 日、4c3 が Nvidia 社の「ハードウウエアとファームウエアのフォルダ」を所有していると発言し、それらのフォルダを販売できると主張するメッセージを投稿したのです。とはいえ、4c3 は 2022 年 5 月以降サイバー犯罪フォーラムで活動していないため、Lapsus$が活動を再開したと判断するには未だ疑問の余地が残ります。



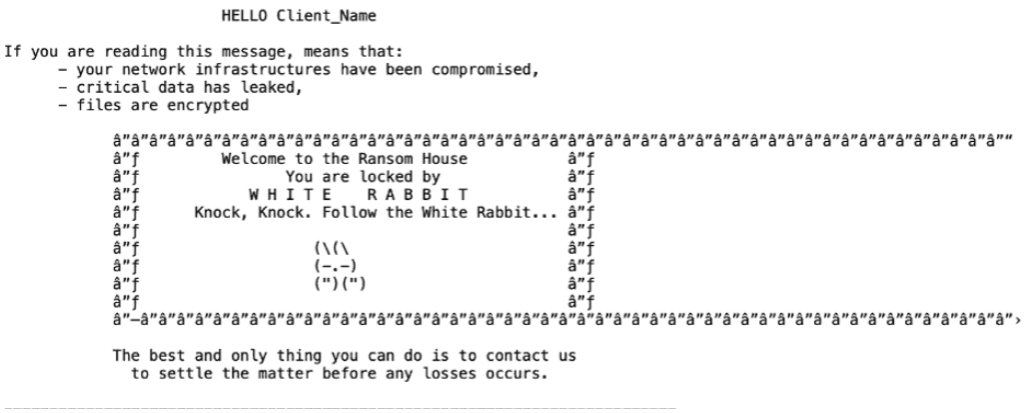
4c3 が Nvidia 社のハードウエアとファームウエアのフォルダを売りに出した投稿

ランサムウエアグループの新たな収益手法

また 2022 年第 2 四半期には、一部のデータリークグループが新たな収益モデルを導入しており、サイバー犯罪者が自らの利益を増やすべく進化を続けている様子がうかがえました。「**RansomHouse**」も、そういったグループの 1 つに該当します。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が発見されたのは 2022 年 5 月に入ってからのことです。同グループがブログに掲載している声明によると、彼ら自身は企業そのものに他する攻撃を行っておらず、他のサイバー犯罪者が攻撃して窃取したものと思われる被害組織のデータを公開しています。RansomHouse のブログでは、「暗号化」と「リーク」という 2 種類のデータが売りに出されており、「暗号化」と「リーク」はそのデータを取得した時の攻撃手法を表しています。

RansomHouse が最近公開した被害組織

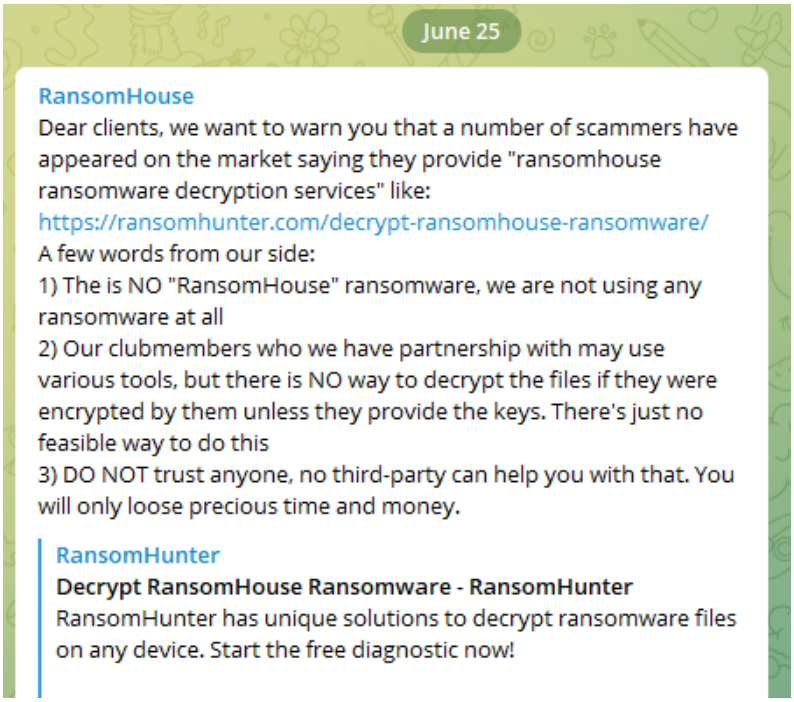
RansomHouse は、自らのサイトで自分達のことを「プロの調停人のコミュニティ」と表現しており、攻撃者と被害組織の「交渉を支援する」と説明していました。その内容によると、同グループは攻撃者と被害組織が話し合いの機会を持ち、十分な情報を得たうえで意思決定を行えるよう双方を手助けするということです。また 2022 年 6 月 25 日、同グループは自らの Telegram チャンネルで、「自分達はランサムウエアグループではなく、暗号化被害を受けた企業に復号ツールを提供できない」と発言していました。しかしその一方で、これまで RansomHouse が、「ランサムウエアを展開することもあるサイ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確認されています。また、同グループ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るのかという点についても、明らかにはなっていません。しかし、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）が残した身代金要求メモを見る限り、RansomHouse は White Rabbit と関連があるようです。



RansomHouse と White Rabbit のメモ（ソース：Bleeping Computer）

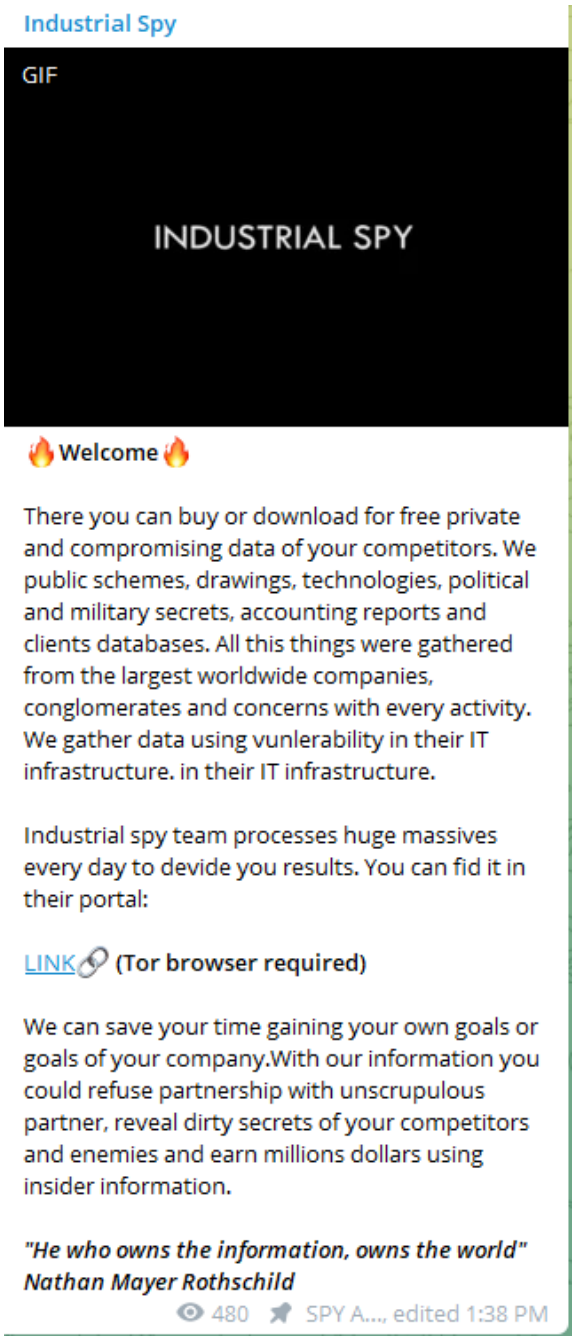
2022 年 4 月以降、RansomHouse は自らのブログで 6 つの被害組織を掲載しています。最も新しく掲載された被害組織は、米国に拠点を置く国際的半導体企業「Advanced Micro Devices（AMD）」社であり、RansomHouse は同社のデータ 450 GB を所有していると主張していました。また同グループは、彼らのパートナーが 1 年前に AMD 社を攻撃したとも述べていました。

ここで興味深い点として、RansomHouse が被害組織を公開しているページのデザインは、ランサムウエアグループ Hive が被害組織を公開しているブログページのデザインと似ていること、そして RansomHouse の同ページの投稿には、Hive と同じく 2 つの日付（攻撃が行われた日と情報がリークされた日）が記載されているということが挙げられます。しかしこれまでのところ、両グループのつながりを示唆する新たな情報は確認されていません。



RansomHouse のアクターが「ファイルの暗号化は行わない」と主張している投稿

その他に、興味深い収益モデルを採用しているサイバー犯罪グループとして、2022 年 4 月 18 日に活動を開始した「**Industrial Spy**」が挙げられます。同グループは、企業の IT 設備に存在する脆弱性を悪用してデータを窃取していると主張しており、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います。



Industrial Spy が企業にデータの提供を呼びかけている投稿

Industrial Spy の説明によると、彼らのマーケットでは商品がその価格に応じて「プレミアム（premium）」、「普通（general）」、「無料（free）」の 3 つに分類されています。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」のセクションに表示され、高額な値段

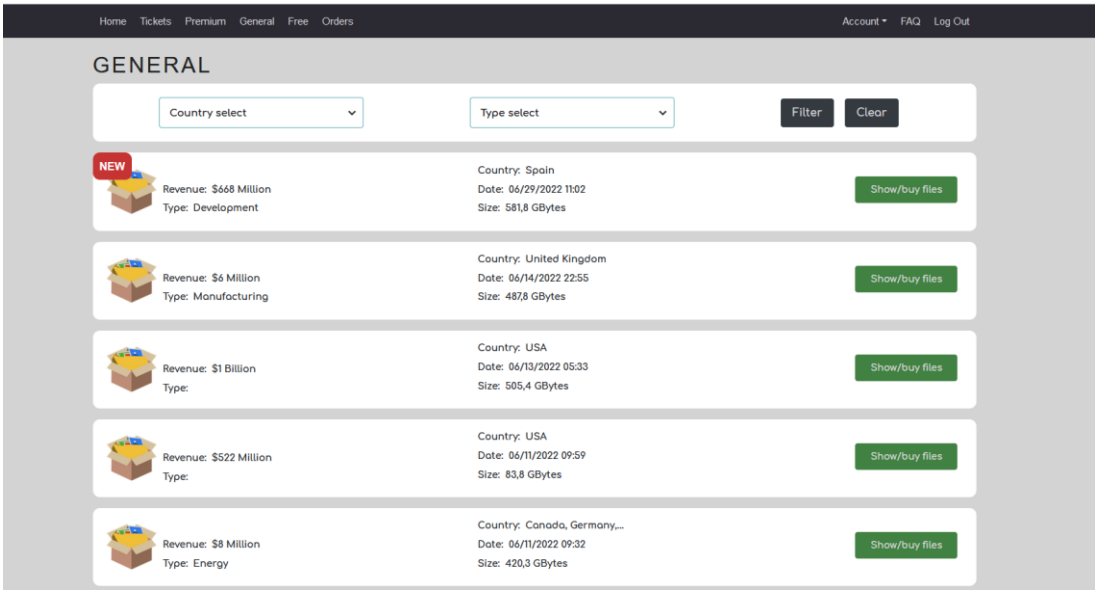
で売り出されます。誰もデータに興味を示さない場合は、その後「普通」セクションへと移動され、値段を下げて売りに出されます。残る「無料」セクションでは、ユーザーが無料でデータをダウンロードすることができる仕組みになっています。

我々がこのマーケットについて分析を進めたところ、これらのセクションで売りに出されているデータ元企業のいくつかは、過去に Hive や Vice Society、Conti、Xing などのランサムウエアグループや、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企業であったことが判明しました。

このマーケットでデータを売り出されている被害組織の大半を、Industrial Spy 自らが攻撃しているのかという点は不明ですが、一部の企業については、サイバー犯罪フォーラムに売り出されたネットワークアクセスが発端となって初期アクセスを取得され、侵害されたようです。その一例を挙げてみましょう。2021 年 11 月 24 日、我々は、脅威アクター「instruktor」がドイツのメディア・オーディオテクノロジー企業へのアクセスを売りに出していることを確認しました。Instruktor によると、この企業の収益は 30 億米ドルであり、「商品」は VMware Horizon を介したアクセスであるということでした。我々は、instruktor がこの企業について公開していた情報（収益や会社に関する説明）をもとに調査を行った結果、アクセスを売りに出されていたのは「Fraunhofer Institute」社であったことを突き止めました。このアクセスは、開始価格 1,500 米ドルでオークション形式にて売り出され、その約半年後の 2022 年 4 月 14 日には、Industrial Spy のマーケットで同社のデータが掲載される事態となりました。

なお、我々が観察している他の事例では、アクセスが売りに出されてから被害組織が公開されるまでのプロセスは約 1 カ月程度であり、Fraunhofer Institute 社のアクセスが売りに出されてから Industrial Spy のマーケットに登場するまで約半年もかかっているのは、ある意味異常な長さとも言えます。そしてこの期間の長さから、Industrial Spy が他のグループと連携していたとしても、真の攻撃者は攻撃を実行してから数カ月経った後で、Industrial Spy にデータを渡したという可能性が考えられます。恐らく真の攻撃者は、まず最初に Fraunhofer Institute 社から身代金を受け取ろうと試み、その後、パートナーを見つけて同社のデータを収益化することに決めたものと思われます。前述の通り、Industrial Spy と同じ類のデータブローカーである RansomHouse が AMD 社のデータを公開したのも、彼らのパートナーが AMD 社に不正アクセスした 1 年後となっています。

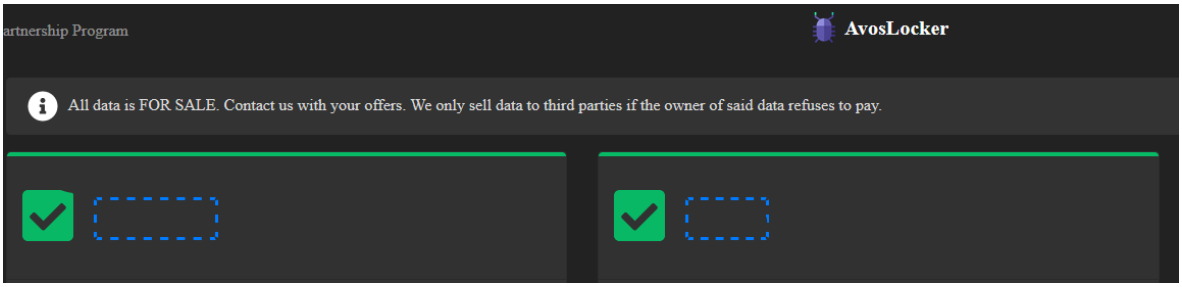
また最近では、Industrial Spy の身代金メモが研究者によって発見されています。この身代金メモは、同グループがデータの窃取のみならず暗号化も行っており、まさに自らの戦術を変えつつあることを示唆していました。



Industrial Spy のブログ

Everest も収益手法を拡大しています。同グループは、2022 年第 2 四半期も前四半期と同じ手法でネットワークのアクセスを販売していましたが、第 2 四半期は企業のデータを販売しようとする新たな動きがみられました。その一例を挙げてみましょう。2022 年 5 月 27 日、我々は調査の中で、Everest のオペレーターがイタリアの製造企業に関するデータを売りに出したことを発見しました。この企業は 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、恐らく企業側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 日には、Everest はこの企業のデータを販売するために新たな投稿を掲載しており、その投稿の中で「侵害の証拠」として、被害企業及び複数のイタリア自動車メーカーに関連したものとされる文書を公開していました。なお、この企業データの販売価格は 3 万米ドルとなっていました。

AvosLocker をはじめとするその他のランサムウエアグループも、身代金の要求以外に何らかの収益方法を引き続き採用しており、その主な手口は、身代金を支払わなかった企業のデータをサイバー犯罪者に販売するというものでした。



AvosLocker が不正アクセスで入手したデータを売りに出している画面

また我々は、**Quantum** が新たな手法を TTP（戦術・技術・手順）に取り入れていることも発見しました。この新たな手法とは、被害組織のデータを一部公開した後も、引き続き身代金の支払いを要求するというものです。その一例を挙げてみましょう。我々は、Quantum とアメリカ合衆国退役軍人省の在フロリダ支局（Florida Department of Veterans' Affairs）のチャットへアクセスすることに成功しました。Quantum は、自らのブログでこの支局（Florida Department of Veterans' Affairs）の名を被害組織として公表するのみならず、すでに同支局のデータの一部を公開していましたが、我々がこのチャットの内容を確認したところ、Quantum が引き続き同支局に対し、自分達に連絡して身代金を支払うよう要求していたことが明らかとなりました（恐らくは、更なるデータの公開を防ぐための身代金と思われます）。

今やランサムウエアグループの努力は、利益を増やすために「データを収益化する手法」を変えるということに留まってはいません。彼らは、「もっと高額な身代金を手に入れる手法」を新たに取り入れています。その一例として、最初に攻撃した標的とは別の企業を攻撃するという手法が挙げられます。2022 年 5 月 14 日、我々は **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チャットへアクセスすることに成功しました。このチャットの中で Hive は、当初同グループは米国の某法律事務所を攻撃していたものの、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、法律事務所に対する攻撃の過程で、このサービス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と述べ

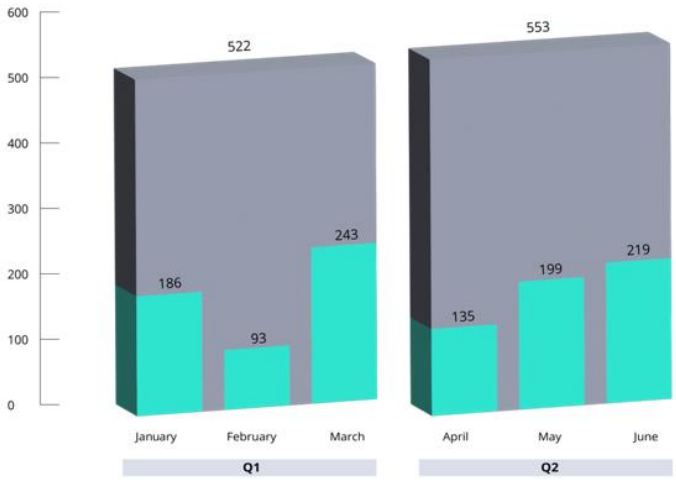
ていました。そしてこの攻撃の後、Hive は法律事務所とサービス事業者の両方に身代金を要求しており、少なくとも一方の被害組織からは身代金の支払いを受けることに成功していました。

2022 年第 2 四半期に売り出されたネットワークアクセス

2022 年第 2 四半期、我々が監視した商品（ネットワークアクセス）は 550 件超、その希望販売価格は合計で約 66 万米ドルとなりました。この金額は、第 1 四半期と比較すると大きく減少しています（2022 年第 1 四半期に売り出されたアクセスの希望販売価格の合計は約 110 万米ドル）。また、売り出されていた商品の平均価格は、第 1 四半期がほぼ 3,000 米ドルであったのに対し、第 2 四半期は約 1,500 米ドルとなりましたが、中央値については第 1 四半期が 400 米ドル、第 2 四半期が 300 米ドルとなり、大きな変化は見られませんでした。したがって、第 1 四半期に売り出されたアクセスは第 2 四半期のものよりも高額ではあったものの、全体的な傾向はほぼ同じであると言えるでしょう。

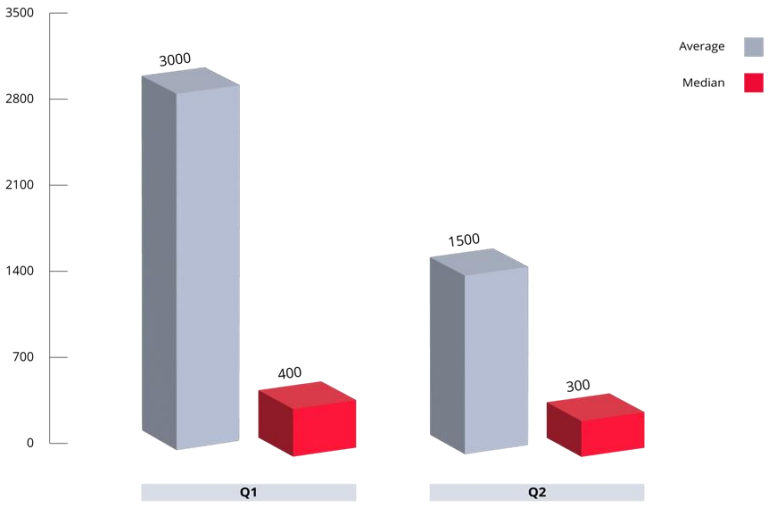
2022 年第 2 四半期に売り出されたアクセスのひと月あたりの平均件数は約 184 件であり、2022 年第 1 四半期に近い数字となりました。この第 1 四半期、第 2 四半期のいずれの件数も、初期アクセス・ブローカーのマーケットが過去 1 年の間に大きく成長したことを示しています（初期アクセス・ブローカーが 2021 年第 2 四半期に売りに出していたアクセス商品の件数は月平均 100 件未満）。

ACTIVITY OF INITIAL ACCESS BROKERS IN Q1 and Q2 2022



また、売り出されていたアクセスのうち、少なくとも 11%が販売者のアクターから売却済みと報告されており、アクセスが売り出されてから買い取られるまでの平均日数は 1.5 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）。ただしここで注意しておくべき点は、全ての初期アクセス・ブローカーが、商品の売買完了を公表するわけではないということです。そのためこの 11%という数字は、売却されたアクセスのあくまで最低件数であると理解しておく必要があります。

PRICES OF NETWORK ACCESS LISTINGS IN Q1 AND Q2 2022



初期アクセス・ブローカーが最も多く売り出していた商品の種類は、RDP や VPN を介したアクセスであり、第 2 四半期もこれまでと同様に、彼らが Citrix 社や Fortinet 社、Pulse Secure 社、そしてそれら企業の VPN 製品について頻繁に言及している様子が観察されました。またこの第 2 四半期には、Confluence Server や SonicVPN を悪用したアクセスも「トレンド入り」しており、これについては各企業が最近公開した脆弱性が原因となって、標的にされているものと思われます。

売り出し件数上位の初期アクセス・ブローカー

2022 年第 2 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、約 110 人となり、第 1 四半期にほぼ近い人数となりました。また、第 2 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 40 件以上のアクセスを売りに出していました。

zirochka

zirochka は、2016 年 7 月からサイバー犯罪フォーラムで活動していますが、ネットワークのアクセスを販売し始めたのは 2022 年 3 月からです。通常、zirochka はドメイン管理者またはローカルの管理者権限を有する端末への RDP アクセスを、比較的低価格で売りに出しています（販売はオークション形式で行われており、開始価格は大抵 100 米ドル未満）。この第 2 四半期は、少なくとも 30 件のアクセスを販売していました。

yesdaddy

yesdaddy は、2022 年 3 月から VPN や RDP を介したアクセスを積極的に販売しており、これまでには「大量のアクセスを定期的に購入してくれる顧客を探している」と発言していたことも確認されています。なお、「Saprano」とのハンドル名を使っているユーザーが掲載している投稿と、yesdaddy の投稿には類似点があることから、我々は中程度の確信をもって yesdaddy が Saprano というハンドル名でも取引を行っているものと判断しています。また Saprano がサイバー犯罪フォーラムに参加したのは 2020 年の末であることから、もしこの両者が同じ人物であった場合には、サイバー犯罪フォーラムにおける yesdaddy の活動歴はより長いものとなります。

orangecake

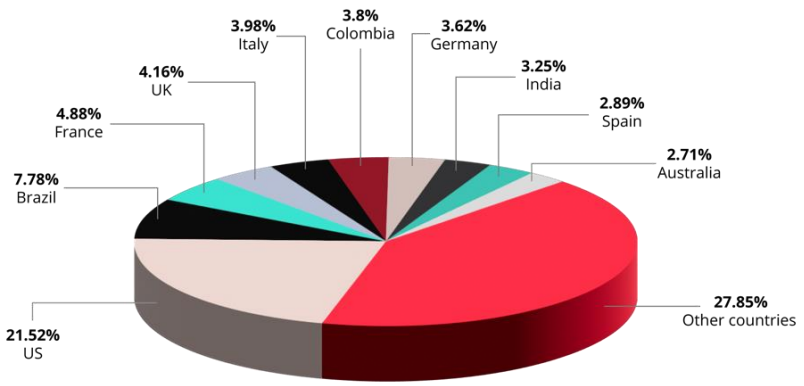
orangecake は 2021 年 9 月に活動を開始して以降フォーラムで高い評価を受けており、ランサムウエアグループと協力体制をとっていることも確認されています。2021 年 10 月には、LockBit がイスラエルの某企業に不正アクセスしたと主張していましたが、この不正アクセスは orangecake が販売したアクセスを利用して行われたものと思われます。orangecake は、主に VPN を介したアクセスを販売しており、その一部では Fortinet が悪用されています。

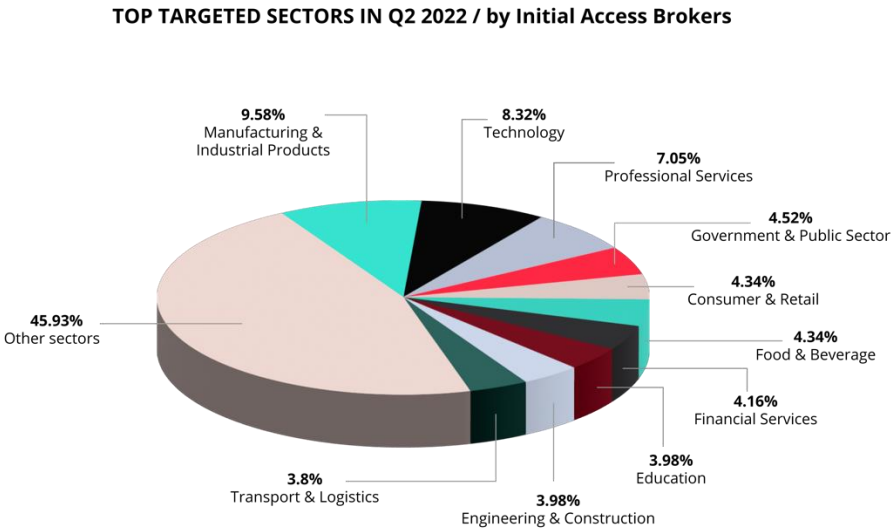
標的とされた国・業界

第 1 四半期と同様に 2022 年第 2 四半期も、米国が初期アクセス・ブローカーに標的とされた国の第 1 位となり（被害組織の約 20%）、その後にはブラジル、フランス、英国、イタリアが続いています。我々は調査の中で、「zirochka」と名乗るアクターがブラジルに対する関心を高めており、これまでにブラジル企業のネットワークアクセスを 20 件以上売りに出していたことを確認しました。第 2 四半期に売り出されていたネットワークアクセスの約 43%は、これら標的トップ 5 の国々の組織で構成されており、第 1 四半期にトップ 5 の国々が占めていた割合に近い数字となっています。

また、初期アクセス・ブローカーに標的とされた業界の第 1 位は、製造・工業製品であり、ランサムウエアグループに標的とされた業界の第 1 位と一致しました。

TOP TARGETED COUNTRIES IN Q2 2022 / by Initial Access Brokers





公表直後の脆弱性を悪用する初期アクセス・ブローカー

2022 年第 2 四半期を通して見られた傾向の 1 つとして、初期アクセス・ブローカーが新たに発見された脆弱性のエクスプロイトを速やかに活用し、パッチを当てていない組織のネットワークを標的にしていることが挙げられます。初期アクセス・ブローカーは、様々な手口で企業のネットワークを侵害しており、その一つとしてソフトウエアに存在するゼロディ脆弱性や既知の脆弱性の悪用が挙げられます。ゼロディ脆弱性のエクスプロイトを阻止するのは困難な作業ですが、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できます。ただし、全ての企業が速やかにパッチを適用できるとは限らないため、初期アクセス・ブローカーにとって攻撃チャンスとなる時間が生まれます。

その一例を挙げてみましょう。「r1z」は 2019 年から活動しており、フォーラム XSS で販売者として高い評価を得ているユーザーです。2022 年 6 月、我々はこのユーザーが 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」とあわせて売りに出していたことを確認しました。しかしその 3 カ月前の時点で r1z は、「**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のです。これらの事実を総合して考えると、r1z は CVE-2021-

42321 を実際に悪用できる独自のエクスプロイトを持っており、後々、r1z が自らそのエクスプロイトを使用して、アクセスを取得するようになったと考えることができます。

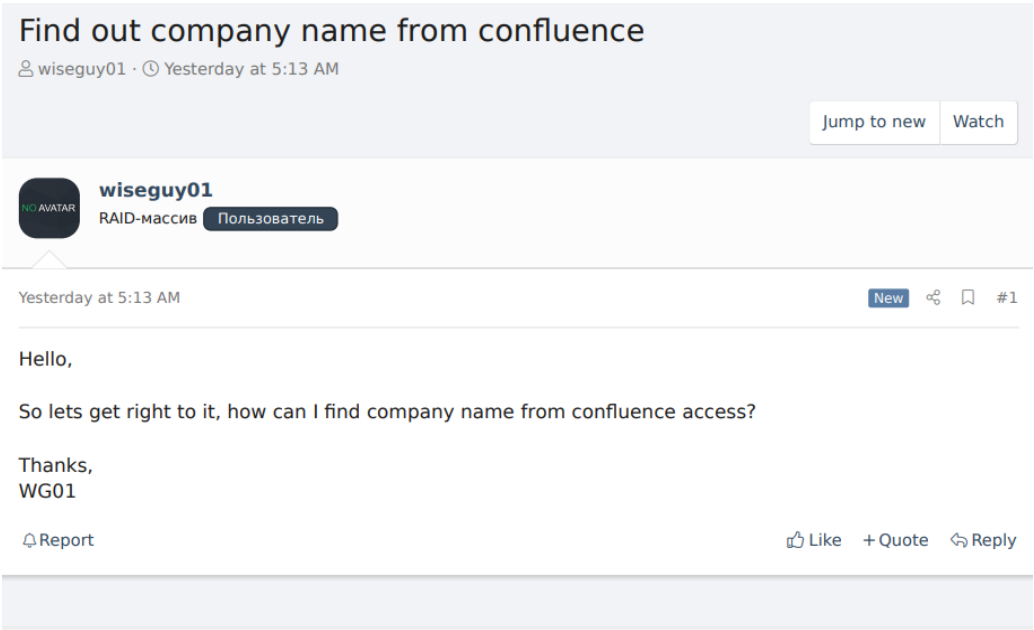
また同じく 2022 年 6 月、r1z は米国企業へのアクセス 50 件（いずれも「Confluence」経由）を売りに出しており、さらにこの時には脆弱な端末 1 万台のリストも売りに出していたことが確認されました。r1z が公開したスクリーンショットを見ると、このアクターが、Confluence Server 及び Data Center に影響を及ぼす重大なリモートコード実行の脆弱性（**CVE-2022-26134**）を使ってサーバーにアクセスしていたことがわかります。となると、r1z が売り出していた脆弱な端末のリストには、恐らくこの脆弱性を悪用できる端末が含まれていたものと思われます。

その他にも今回の調査期間からは外れますが、2022 年 7 月、r1z が別の投稿で企業のネットワークに存在するリモートコード実行の脆弱性を売りに出していたことが確認されています。そしてその一方で、同じく 7 月、「nopiro」と名乗るアクターが「r1z が売り出している脆弱性情報を『リークする』と主張していたことが確認されました。またこの時 nopiro は、このリモートコード実行の脆弱性の影響を受けると思われる企業と URL のリストも提供していました。我々が確認したところ、この時 r1z や nopiro が悪用していた脆弱性は、「**CVE-2022-22954**（VMware 社製 Workspace One Access 及び Identity Manager に影響を及ぼす脆弱性）」であったと思われます。なお、同脆弱性については、既に PoC（概念実証）のコードが公開されています。

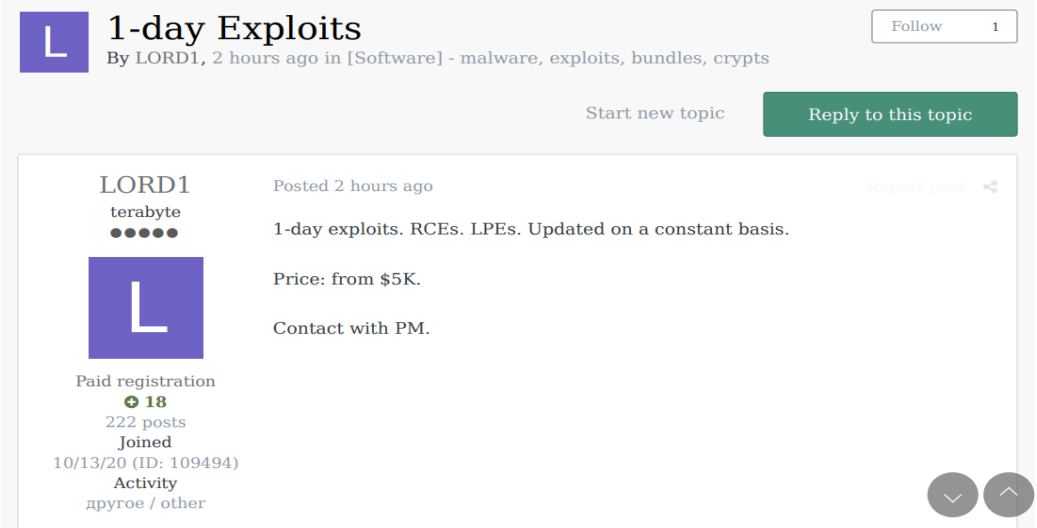
我々の知る限り、ランサムウエアオペレーターやデータリークグループは初期アクセス・ブローカーから頻繁にアクセスを購入していますが、今後は「今すぐ購入できるアクセス」のみならず、潜在的被害者に関する情報や、実際に使用可能なエクスプロイトにも関心を示し出す可能性があります。潜在的被害者に関する情報としては、特定の脆弱性に対して適切な対策を取っていない企業のリストなどが挙げられますが、そういったリストは、市販のツールやカスタムツールを使ってインターネットをスキャンするだけで作成することができるのです。また、実際に使用可能なエクスプロイトがあれば、既知の脆弱性を悪用しようと企むアクターは、より簡単に攻撃を実行することが可能となります。

そしてサイバー犯罪フォーラムは、ランサムウエアアクターと初期アクセス・ブローカーの双方に、そういった製品を供給する場となっています。その一例として、「wiseguy01」と名乗

るアクターが、Windows や Linux 機器に使用されている脆弱な Confluence サーバーのアクセスを売りに出していたことが挙げられます（恐らく上述の事例と同じ脆弱性「CVE-2021-42321」に対して脆弱であると思われます）。wiseguy01 は、それぞれの専用サーバーのアクセスを、50 ドルという価格で売りに出していましたが、その一方で、各サーバーを使用している企業の名を見つける方法を模索していました。恐らくは、不正アクセスを更なる段階へとすすめるにあたり、収益の高い企業を特定したかったものと思われます。



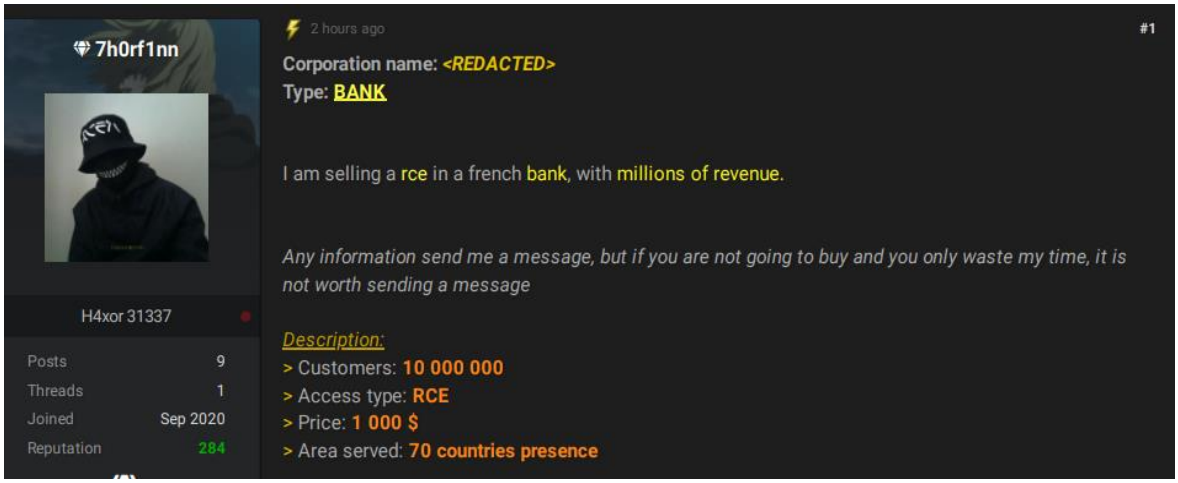
また我々の調査では、ワンディ脆弱性のエクスプロイトが継続的に売り出されていることも確認されました。これはまさに、初期アクセス・ブローカーや他のアクターが、自社環境に速やかにパッチを適用しなかった企業を標的として狙っていることを証明しています。例えばフォーラム Exploit では、「LORD1」と名乗るアクターが、定期的にリモートコードの実行やローカル権限昇格のエクスプロイトを 5,000 ドルからの価格で売りに出しています。



LORD1 がリモートコード実行やローカル権限昇格の脆弱性用のワンディ・エクスプロイトを売りに出している投稿（価格は 5,000 ドルから）

ランサムウエアオペレーターに転身した初期アクセス・ブローカー

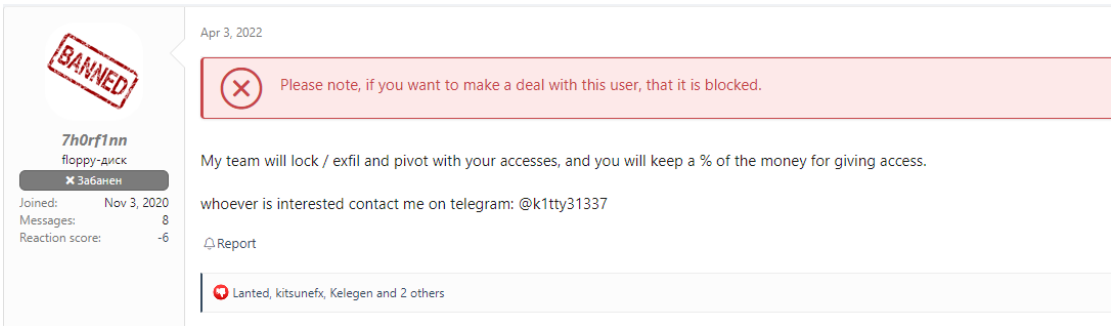
我々は、ランサムウエアグループや初期アクセス・ブローカーが共同で行う活動を継続的に監視しており、初期アクセス・ブローカーが販売したネットワークアクセスが発端となったランサムウエア攻撃についても調査を行っています。そしてそういった監視活動や調査の結果から、多くのアクターは、ランサムウエアのサプライチェーンに貢献するのみならず、攻撃にも参加する意思があるものと思われます。2022 年第 2 四半期、我々はそういったアクターの 1 人「7h0rf1nn」が、まさにランサムウエアオペレーターへと進化してゆくプロセスを観察しました。7h0rf1nn は 2020 年以降、様々な企業のネットワークに存在するリモートコード実行の脆弱性や Web シェルを販売していました。



7h0rf1nn が初期アクセス・ブローカーとして活動していた時の投稿

（ソース：Raidforums、2021 年）

しかし 2022 年 4 月、我々は、7h0rf1nn がフォーラム XSS で活動スタイルを変化させ、他のサイバー犯罪者から提供されたアクセスを使って「作業」すると申し出ていたことを確認しました。7h0rf1nn はこの投稿の中で、「不正アクセスした企業からデータを窃取し、さらにその企業のネットワークを『ロック』できるチームを擁している」と述べており、このチームの活動は十中八九、ランサムウエアを展開することを意味しています。また 7h0rf1nn は同じ投稿の中で、協力者には利益の一部を支払うとも述べていました。しかしこういった主張は、まさにランサムウエアグループの結成を意図するものであったため、その後 7h0rf1nn は、ランサムウエアの宣伝を禁じる XSS では出入り禁止となりました。

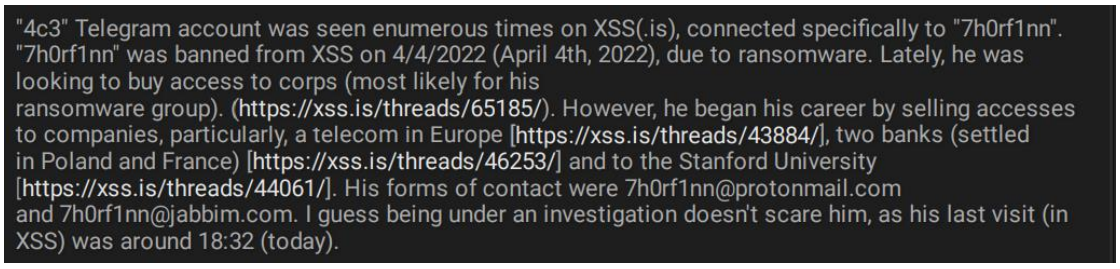


7h0rf1nn がランサムウエアオペレーションに向けてチームを結成しようとしている投稿

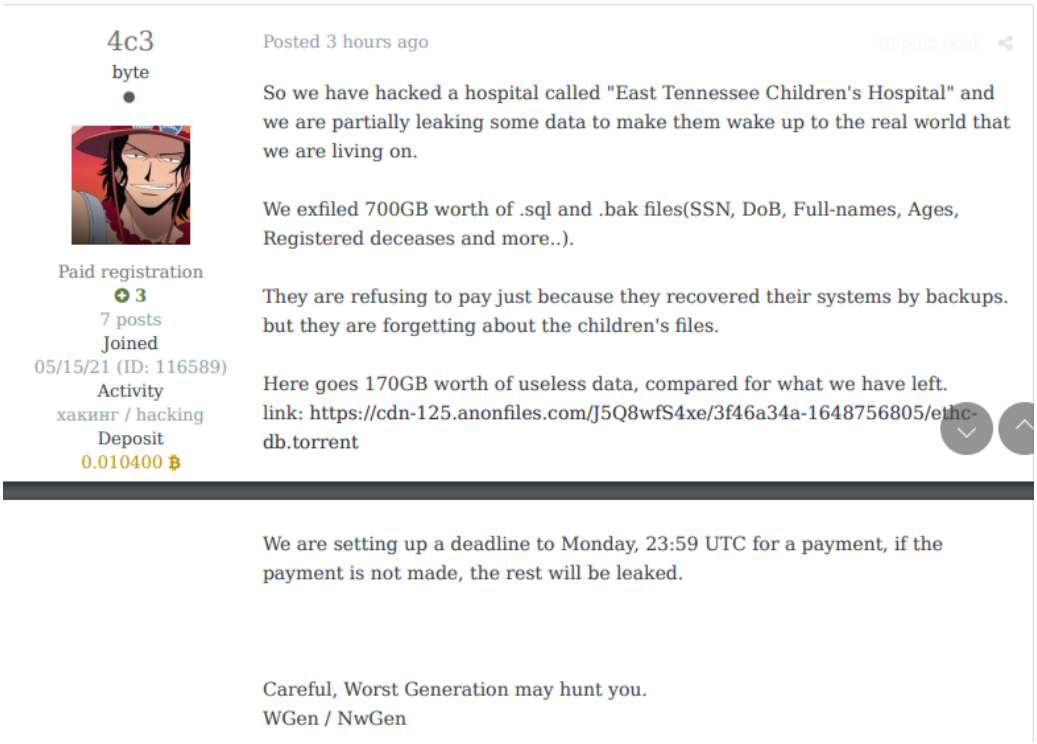
7h0rf1nn の進化の道のりは、まだ始まったばかりのようです。2022 年 6 月 2 日には、7h0rf1nn がフォーラム Exploit で、Web アプリケーションの悪用方法を学びたいと述べ、他のユーザーに支援を求めていたことが確認されました。しかしフォーラムのユーザーからは、7h0rf1nn の経験値に対する疑問の声が上がっており、もし 7h0rf1nn が熟練したアクターであれば、フォーラムにある Web アプリケーションの悪用関連情報を自分で見つけることができるはずだと返されていました。

7h0rf1nn が web アプリケーションの悪用方法を学びたいと述べている投稿

なお、フォーラム Breached で活動しているアクターの多くは、7h0rf1nn が Lapsus$の元メンバーである 4c3 とつながっているのではないかと推測しています。そして 4c3 自身も 2022 年 3 月に、新たなオペレーション「Worst Generation（WGen/NwGen）」の立ち上げを発表しています。しかしこれまでの我々の調査では、Worst Generation をランサムウエアオペレーションやその他のマルウエアと結びつけるにいたる、新たな投稿は確認されておりません。



Breached のユーザーが 7h0rf1nn と 4c3 のつながりを発見したと述べている投稿



Lapsus$の元メンバーが立ち上げた新たなオペレーション

「Worst Generation（WGen/NwGen）」

注目すべき事例

2 度の不正アクセスを受けていたアジアのレストランチェーン

2022 年 5 月 31 日、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売りに出したことを確認しました。Bloomsday の説明によると、このアクセスは VPN や RDP を介したものであり、ドメイン管理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。またその販売価格は 2 万米ドルとなっていました。

そしてその後の 2022 年 6 月 26 日、我々は、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売りに出したことを確認しました。iFrame の説明によると、このアクセスも VPN や RDP を介したものであり、ドメイン管理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。またその販売価格は 4,000 米ドルとなっていました。

我々は、それぞれの脅威アクターがレストランチェーンについて提供していた詳細情報をもとに調査を進め、その結果、両方のアクター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。どちらも VPN や RDP を介しており、ドメイン管理権限が付与された端末にログインできるアクセスと説明されていましたが、両者の価格が大幅に違うことから、我々は iFrame と Bloomsday は別々のアクターであると判断しています。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得ること、そしてその結果として「複数」の事態が引き起こされ得ることを証明しています。

収益数十億ドルを有するインド企業

2022 年 6 月 4 日、我々は、脅威アクター「black_palm」が収益 956 億米ドルを有するインド企業へのアクセスをオークション形式で売りに出したことを確認しました。black_palm の説明によると、このアクセスは VPN を介したものであり、オークションの開始価格は 1 万米ドルとなっていました。これは、大手企業のアクセスが売りに出されていた事例の 1 つですが、売り出されたその翌日には販売が終了していたことから、恐らくは購入者が決まったものと思われます（ただし、このアクセスが使用不可能になったという可能性も考えられます）。

最も高額なアクセスとなった英国企業

2022 年 4 月 2 日、我々は、脅威アクター「5MRBID」が、3 億 5,000 万米ドルの収益を有する英国企業のアクセスを売りに出していたことを確認しました。5MRBID の説明によると、このアクセスを使ってドメイン管理権限のある端末にログインできるということであり、その販売価格は 3 万 5,000 米ドルとなっていました。これは我々が観察した限り、第 2 四半期に売り出された中で最も高額なアクセスです。この高額な価格設定にもかかわらず、5MRBID はアクセスに関する詳細情報をほとんど公開していませんでしたが、それでもこの商品は数日後に売却されていました。

ペイロードの配信態勢が整えられた米国銀行

2022 年 6 月 3 日、我々は、脅威アクター「Jesus-Like」が、収益 6 億米ドルを有する米国銀行のアクセスを売りに出したことを確認しました。Jesus-Like の説明によるとこの商品は、同行

の Active Directory ドメインに属する、NT authority/system 権限が付与された端末へのアクセスであるということでした。この事例で興味深い点は、Jesus-Like が同行のアクセスを売り出すのみならず、さらなる攻撃を著しく容易にできる準備が整っていると主張していたことです。Jesus-Like は、同行の端末にリバースシェルを仕込んでおり、「Metasploit Framework」を介してコードを実行できる態勢を整えていたのです。また Jesus-Like は、要望に応じて購入者の悪意あるペイロードをロードするという、新たなサービスも販売していました。このアクセスの販売価格は、8,000 米ドルとなっていました。

結論

2022 年第 2 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の活動はわずかに減少しましたが、その一方で新たなグループが次々に登場し、既存のグループも進化を遂げていました。また初期アクセス・ブローカーも、彼らの商品に対する需要が続く状況を背景に、ランサムウエア・アズ・ア・サービスのサプライチェーンにおける地位をさらに強固なものにしています。組織のネットワーク防御を担当される皆様には、サイバー犯罪者に一歩先んじてランサムウエア攻撃を回避するために、アンダーグラウンドにおける彼らの活動を監視されることをお勧めいたします。