KELA

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

KELA Cybercrime Intelligence ©

目次

エグゼクティブサマリー

2021年においてもランサムウエア攻撃は、世界中の企業や組織を脅かす脅威の中でも最も注目を集めました。重要なインフラストラクチャ（Colonial Pipeline社）や食品加工産業（JBS Foods社）、保険（CNA社）をはじめとする多数の業界で大規模なランサムウエア攻撃が展開され、被害者となった企業は業務の一時停止を余儀なくされました。またそれらの攻撃を受けて、ランサムウエアグループに対する法執行機関の圧力が激しさを増していますが、その一方でランサムウエア攻撃に従事する脅威アクターも進化を続けています。彼らはその技術をより洗練させると同時に、成長するサイバー犯罪エコシステムを広範に活用して、自らのオペレーションに利用できる新たなパートナーやサービス、ツールを模索しています。

本レポートでは、2021年に確認されたランサムウエア攻撃の被害者となった組織についてKELAの知見を詳述するとともに、ランサムウエアグループの活動（攻撃やサイバー犯罪フォーラムでの活動状況）をまとめました。また、ランサムウエアアクターとその他のサイバー犯罪者たちの協力関係に関する独自の調査結果も記載しております。

主な調査結果

被害者学

- 我々は2021年、ランサムウエアの活動件数は大幅に増加しました。KELAのソース（ランサムウエアブログ、ランサムウエア身代金交渉用ポータル、データリークサイト、公式の報告など）で確認されたランサムウエア被害者の数は、1,460から2,860となり、約2倍に増加しています。

- データリークサイトは、被害者の名前を公開する「ネイミング＆シェイミング」ゲームに参加しています。データリークサイトを運営するアクターもデータを窃取し、ランサムウエアブログと同様のウェブサイトを運営していますが、彼らがランサムウエアを使ってデータを暗号化することはありません。

- 我々が2021年に監視していたランサムウエアブログ及びデータリークサイトの65%は、同年中に新設されたサイトでした。

- 最も標的とされた国々と欧州や北米の先進国市場（米国、カナダ、フランス、英国、ドイツ）には相関性がみられます。

- 最も攻撃を受けた業界として、製造・工業製品、専門サービス、テクノロジー、土木建築、消費財・小売が挙げられます。

- 2021年中に別々のランサムウエアグループから攻撃を受けた（すなわち2021年に2回ランサムウエア攻撃を受けた）企業の数は約40社にのぼります。また、2020年に1回目のランサムウエア攻撃を受け、2021年に2回目の攻撃を受けた企業の数は17社にのぼります。

- データリークサイト（MarketoとSnatch）のオペレーターは、多数のランサムウエアグループ（Conti、Ragnar Locker、その他多数）と同じ被害者を公表しており、これは彼らが協力体制をとっている可能性があることを示唆しています。

主な調査結果

攻撃者の活動

- ランサムウエアブログやデータリークサイトのオペレーターの中でもトッププレイヤーとして活動しているのは、**Conti**、**LockBit**、**Pysa**、**Avaddon**、**REvil**（Sodinokibi）です。一方、新参プレイヤーの中では**Alphv**、**Hive**、**AvosLocker** が重大な脅威となっています。

- 我々は、目覚ましい進化を遂げ、数多くの成功を収めたランサムウエアグループのひとつである**LockBit**の活動について、サイバー犯罪フォーラムで詳細な調査を行いました。

ランサムウエアにダメージをもたらしたアフィリエイトやフォーラム

- ランサムウエアグループの内部情報がリークされるという事件が複数件発生しましたが、これはランサムウエア・アズ・ア・サービス（RaaS）がランサムウエア攻撃に関与するサイバー犯罪者たちに益をもたらす一方で、彼らのオペレーションを「内部脅威」のリスクにさらしうるものであるという事実を表しています。

- 2021年第2四半期にはサイバー犯罪フォーラムで「ランサムウエア禁止令」が出されましたが、これはランサムウエアプログラムのアフィリエイト募集能力や、ランサムウエアグループのサイバー犯罪マーケット参加状況に影響を及ぼすことはありませんでした。むしろこの「禁止令」が、新たなフォーラムRAMP誕生の追い風となりました。

主な調査結果

ランサムウエア攻撃者と初期アクセス・ブローカー

- RaaSエコノミーでは、初期アクセス・ブローカーの提供する「商品」が重要な役割を果たしています。2021年には、約300人の初期アクセス・ブローカーが1,300件を超える初期アクセス商品を売りに出しました。

- 初期アクセス・ブローカーは不正アクセス先企業の名称を公開しませんが、KELAでは彼らの被害者となった企業を150社以上特定することができました。

- 少なくとも5つのランサムウエアオペレーション（**LockBit**や**Avaddon**、**DarkSide**、**Conti**、**BlackByte**）で、初期アクセス・ブローカーから購入したネットワークアクセスが使用されていました。これらのオペレーションのほとんどは、ロシア語話者のアクターによって運営されています。

- ネットワークアクセスが売り出された時点から攻撃にいたるまでの流れを様々な事例で観察した結果、企業がランサムウエア攻撃を受け、ランサムウエアオペレーターのブログでその名前が公開されるまでの平均期間は1カ月となりました。攻撃者が初期アクセスを購入したことから始まった可能性が高いと思われるランサムウエア攻撃5件について、本レポート内で解説します。

- ランサムウエアアクターは、ネットワークアクセス「商品」をフォーラムで探すにとどまらず、そういった商品について非公開のメッセージ経由で連絡し、販売してくれるよう初期アクセス・ブローカーに依頼する声明も発表しています。彼らは、米国に拠点を置く収益6,000万米ドルの企業（教育、政府、非営利業界を除く）を理想の被害者として定義しています。彼らは、この定義に合致する企業へのアクセスであれば最大100万米ドルを支払う用意があるとしています。

被害者学

攻撃件数の増加

2021 年は、ランサムエアの活動件数が著しく増加しており、メディアの報道やランサムウエアグループにとっての公開インフラ（主にランサムウエアブログやランサムウエア交渉用ポータルなど）を確認しただけでもこの結論に達することができます。2021 年に公開インフラで確認された被害者の数は 2,860 件となっており、これは 2020 年の 1,460 件と比較して約 2 倍の数字となっています。またランサムウエアグループの活動は、被害者のデータを流出するだけにはとどまっていません。2021 年には、一部のランサムウエアグループが被害者のデータを他のサイバー犯罪者に販売したり、ランサムウエアグループ **Conti** や **Lorenz** が不正アクセスしたネットワークのアクセスを販売している状況が確認されました。

KELA はランサムウエアブログを監視していますが、ランサムウエアキャンペーンを展開しているわけではないと思われる他のグループが運営するポータルについても監視しています。それらのポータルはランサムウエアブログと似ていますが、我々はランサムウエアブログと区別して「データリークサイト」と呼んでいます。なお、データリークサイトを運営しているグループもデータを窃取しますが、その後は身代金を要求するケース（例：Karakurt）もあれば、窃取したデータを販売したり（Marketo）、単にデータをリークするといったケースもあります。

我々が 2021 年に監視していたランサムウエアブログとデータリークサイトの数は 60 を超えますが、そのうち 65%が 2021 年中に開設されたものです。これらブログやサイトをソースを利用することで、多数のランサムウエア攻撃に関する情報を垣間見ることができますが、実際に発生しているインシデントの件数は、これらのソースで確認できるものよりも大幅に高い数字となっています。また不正アクセスを受けた多くの企業が、身代金を支払ってランサムウエアブログでその名を公表される事態を回避していますが、その一方でランサムウエア交渉用ポータルでは確認できない被害企業も存在します。また、すべてのランサムウエア

グループが独自のブログや交渉用ポータルを運営しているわけではなく、別の手段を使って被害者と連絡を取り、公の場では被害者を脅迫しないランサムウエアグループも存在します。それでも、ランサムウエアブログやポータル、データリークサイトで確認された被害者は、我々が最も活発に活動を展開している攻撃者や、標的となっている企業のパターンを読み取るにあたって十分な数にのぼりました。

トップターゲット

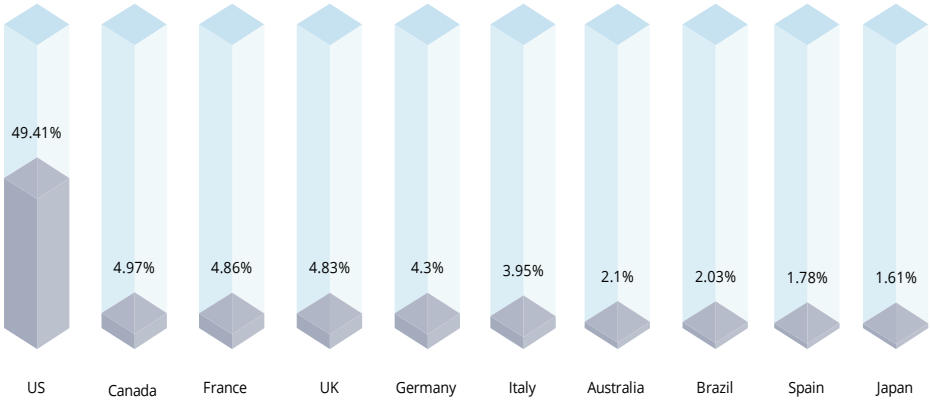
ランサムウエアの標的にされた米国企業は数多く存在しており、その結果、米国が最も標的にされた国となっています。ランサムウエアアクターは、大規模な収益が見込めると同時に、身代金の支払いに対応したサイバー保険を導入している先進国の企業を攻撃しようと狙っています。また彼らは、身代金が支払われる可能性を見極めるために、特定の国々や業界に注目しています。以前我々は **LockBit** のインタビュー内容を翻訳しましたが、その中で同グループの代表者は自分たちの標的について次のように述べていました。*「米国や欧州では、この分野の保険（KELA 訳：ランサムウエア攻撃に対する保険）がより多く展開されており、また世界で最も裕福な企業の大多数がこれらの地域に集中している」*[1]。つまり、最も標的とされている国の上位リストと、米州や欧州地域内でも上位にある先進国市場（米国、カナダ、フランス、英国、ドイツ）には相関性があるということです[2]。

ランサムウエアの被害者となった業界のプロファイルを見てみると、2021 年にランサムウエアの攻撃者が不正アクセスした企業の業界は、主に製造・工業製品、専門サービス、テクノロジー、土木建築、消費財・小売となっています。

[1] https://ke-la.com/lockbit-2-0-interview-with-russian-osint/
[2]本調査の地理情報は、ISO 3166 の基準（https://www.iso.org/iso-3166-country-codes.html ）に準拠しています。

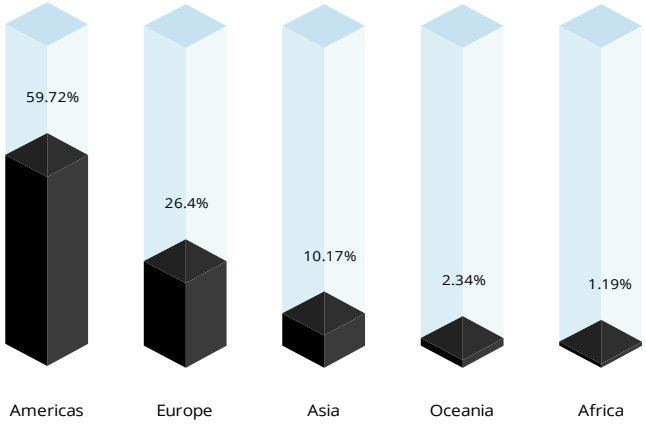
Top countries of ransomware victims

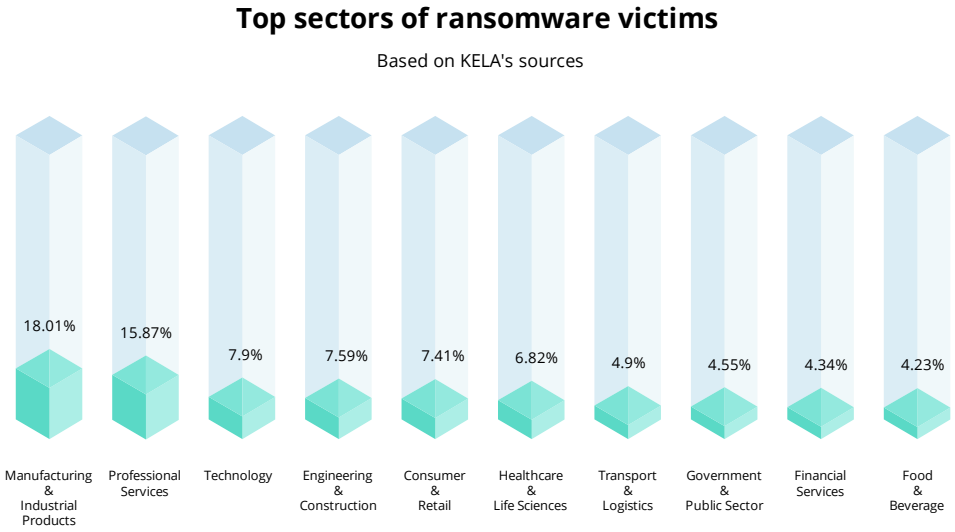
Based on KELA's sources



Regions of ransomware victims

Based on KELA's sources





二重恐喝の被害者たち

攻撃を 1 回受けただけでも十分な災難であるといえますが、我々が観察した結果、2021 年には約 40 社が不正アクセスを 2 回受けており（それぞれ別々のグループによる別々の犯行）、実質的な「二重恐喝」の被害者となっています。その他にも 17 社を超える企業が 2020 年に 1 回目の不正アクセスを受け、2021 年に 2 回目の不正アクセスを受けていたことが判明しました。

一部の企業は、1 カ月という短期間の間に異なる 2 つのランサムウエアグループから攻撃を受けており、それぞれのグループによってリークされた情報も異なっていたとされています。これに該当する事例例と一カ月 Party Rental 社のインシデントが挙げられます。2021 年 2 月 20 日、同社から窃取された約 170 GB 相当のデータが **Avaddon** のブログで公開されました。さらにその後の 2021 年 2 月 24 日、今度は **Conti** が Party Rental 社に不正アクセスしたと主張して、同社から窃取した 226 GB 相当のデータを公開しました。

また別の事例として、Amey 社のインシデントが挙げられます。2020 年 12 月 26 日、Amey

社から窃取された 143 GB のデータダウンロード用リンクが、**Mount Locker** のサイトで公開されました。そしてその後の 2021 年 1 月 13 日、今度は **Clop** が同社に不正アクセスしたと主張して、同社のデータ 470 GB 相当を公開しました。

我々は、これら事件の背後に最もあり得るであろうと思われる原因を、以下に絞り込みました。

- 別々のグループが同じ企業を攻撃しようと試み、その際に同じ侵入経路（脆弱性やネットワークのアクセスなど）が使用された。
- 同じ企業に別々の初期侵入ベクトル（フィッシングメールやソーシャルエンジニアリング攻撃など）が存在しており、別々のグループが別々に攻撃を行った。その結果、1 社に対する 2 つの攻撃が偶然発生した。
- 2 つのグループが何らかの協力体制をとり、その結果が別々の形で公表された。その例として、2021 年に Trend Micro 社の研究者が発見して「フランチャイズ方式」と名付けた、新たな協働モデルが挙げられます。同社が確認した事例では、**Mount Locker** が自らのランサムウエアを、**Astro Team** と **Xing Team** に彼らのブランドとして使用させていました[3]。そしてこういった協力体制をとりながらも、Astro Team と Xing Team はそれぞれ独自のブログを運営していました。なお、Astro Team が自らのブログを立ち上げた際には 11 件の被害者が掲載されており、そのうち 5 件については、Mount Locker がブログで公表した被害者のものと窃取された文書のサイズが一致していました。この 5 件の被害者は先に Astro Team のブログで公開されており、後に Mount Locker のブログで公開された時には、「提携」商品であることを示す印が付けられていました。

Conti や **Egregor**、**Nefilim**、その他一部のランサムウエアグループについては、彼らからの攻撃を受けた後に、別のグループからも不正アクセスを受けた被害者の数が、いずれも 4 件を超えていました。例えば **Conti** の被害者のうち 6 件は、Conti から最初の攻撃を受けた

[3] https://www.trendmicro.com/fr_fr/research/21/j/ransomware-operators-found-using-new-franchise-business-model.html

後に別のランサムウエアグループからも攻撃を受けており、11 件は別のランサムウエアグループから攻撃を受けた後に、Conti から 2 回目のランサムウエア攻撃を受けていました。Conti は、2021 年に最も活発に攻撃を展開していたグループであり（「攻撃者の活動」の章をご参照ください）、論理的に考えると同グループがこれら二重恐喝の事例に関与していた理由は、そもそも彼らの被害者となった企業の数が多かったことにあるといえます。また我々はこれらのインシデントを調査する中で、ランサムウエアブログとデータリークサイトの間に興味深いつながりを発見しました。

ランサムウエアとデータリークサイトのつながり

我々は、14 件の被害者がランサムウエアブログと、データリークサイト（**Quantum**、**Marketo**、**Snatch**）の両方で公開されていることを発見しました。そしてここから、データリークサイトのオペレーターはランサムウエアグループのライバルではなく、実は協力者であるのかという疑問が浮かび上がりました（Snatch というリークサイト名は、2018 年 12 月以降に存在が確認されたランサムウエア「Snatch」を連想させますが、両者の間に関連があるという証拠は確認されていません）。

彼らが協力体制をとっている場合は、ランサムウエアグループが窃取したデータを、データリークサイトを運営しているアクターらと条件付きで共有している可能性があるということを意味します。ランサムウエアオペレーターにとっては、データリークサイトでデータが販売されれば追加の利益を手にすることができる、または単純に現在の被害者（もしくは将来の被害者）に対し、さらなる恐怖感を与えることができるといったメリットが考えられます。またその一方で、協力体制とは別に、ランサムウエアグループと上述のデータリークサイトを運営するアクターが偶然同じ初期アクセスを使用している、または別々の初期アクセスを使って偶然同じ企業を攻撃しているという可能性も考えられます。その他、ランサムウエアグループが公開した全情報をデータリークサイトのオペレーターがダウンロードして、自ら

が利益を得る糧として利用しているという可能性も考えられます[4]。

Quantum

Quantum は、ランサムウエアグループと同じ被害者を公開しているデータリークサイトのひとつであり、その活動は 2021 年 10 月から始まりました。同サイトが最初に掲載したのは、掲載日の半年前に **Dopple Paymer** が攻撃した企業のデータでした。そして 2 件目に掲載されたのは、その数日前に **Xing Team** が攻撃した企業のデータでした。この時 Quantum で公開されたデータのサイズは、Xing Team が公開した窃取データのサイズと一致していましたが、これに加えて、Xing Team のブログでこのファイルダウンロード用リンクをクリックすると、Quantum のページへと移動したのです。これは、両グループのアクターがひとつの攻撃の後に協力体制をとったことを意味しています。なお、この 2 件のインシデント以降、Quantum は独自の被害者のものと思われるデータを公開し始めました。

Marketo

Marketo では 70 件を超える被害者のデータが公開されましたが、そのうち 9 件は先にランサムウエアブログに掲載されていました。その一例として、Align Technology 社の事例が挙げられます。2021 年 9 月 1 日、ランサムウエアグループ **Karma Leaks** が、Align Technology 社を攻撃したと主張しました（リークされたファイルの正確なサイズについては記載されていませんでした）。その後の 2021 年 10 月 2 日、今度は **Conti** が自らのブログで同社のデータ 164 GB（Conti が保有していた同社の全データ）を公開しました。そして 2021 年 10 月 25 日には、Marketo が同社のデータ 145 GB を公開しました。つまり、Align Technology 社は「三重恐喝」の犠牲者となったのです。

Align Technology 社の場合、Marketo はランサムウエア攻撃の直後に被害者のデータを公開

[4]特定のデータセットを分析することでさらなる洞察を得ることが可能となりますが、大半のデータリークサイトは、ランサムウエアグループが被害者を公開した数カ月後に二重恐喝の被害者を公開しており、データリークサイトに情報が掲載された時点では、ランサムウエアブログやブログ内のデータを分析に利用することができませんでした。また、一部のランサムウエアグループは脅迫行為を行ったにもかかわらず、窃取したデータを一部しか公開していませんでした。

しましたが、平均して同サイトではランサムウエアブログで被害者が公開されてから約 220 日後に二重恐喝の被害者を公開しています。従って、Marketo とランサムウエアグループが協力している可能性と単なる偶然という可能性のどちらもありえますが、Marketo を運営するアクターが、ランサムウエアグループの活動から企業に何らかの攻撃ベクトルが存在することを察知して、同じ企業に不正アクセスを試みているという複合的な説も考えられます。

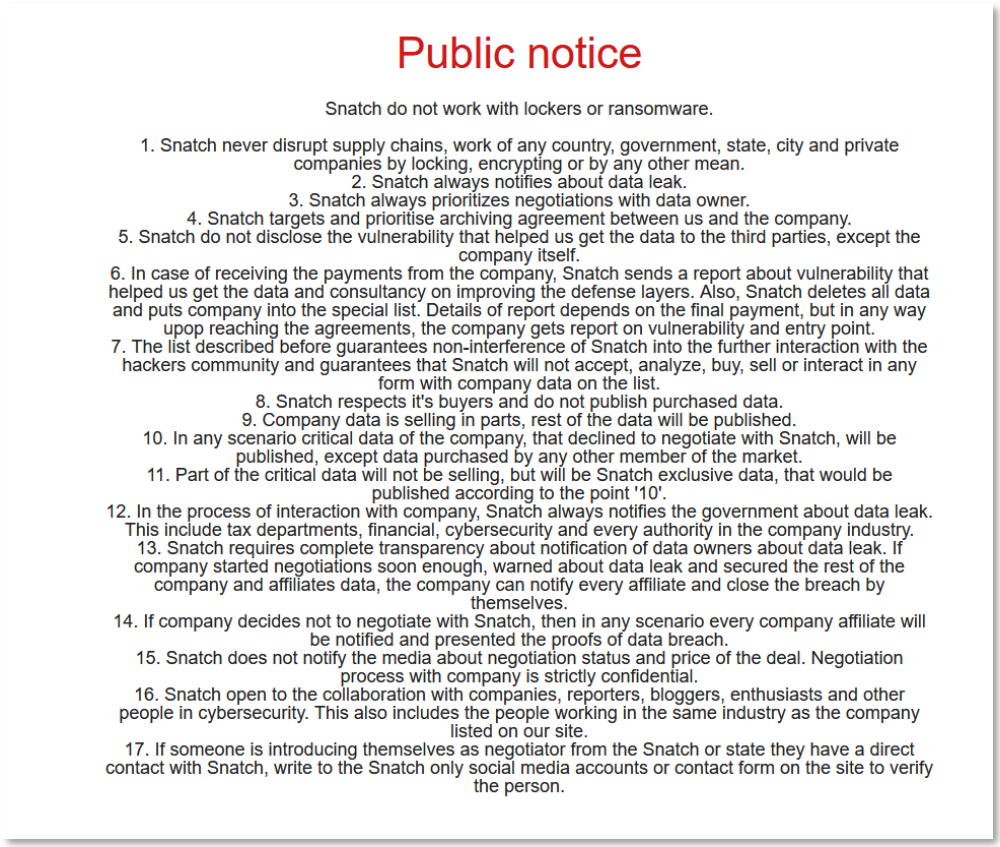
Snatch

Snatch の被害者については、約 30 件のうち 6 件が他のランサムウエアグループと共有されているものと思われます。そのうちのひとつである InTown Suites 社は、2021 年 12 月 22 日、同社から窃取されたデータの 1TB 分が Snatch に掲載されました。しかしそこから日付をさかのぼる 2021 年 5 月 6 日の時点で、**Astro Team** が InTown Suites 社に不正アクセスしたと主張し、同社から窃取したデータ 2TB を公開していました。平均して Snatch では、ランサムウエアブログで被害者のデータが公開されてから約 175 日後に、二重恐喝の被害者のデータを公開しています。

Marketo と Snatch については、いずれもランサムウエアグループとどのようにつながっているのかを特定することは困難ですが、両サイトを運営しているグループに類似点があるということは明らかとなっています。

Marketo と Snatch の間に想定される協力関係

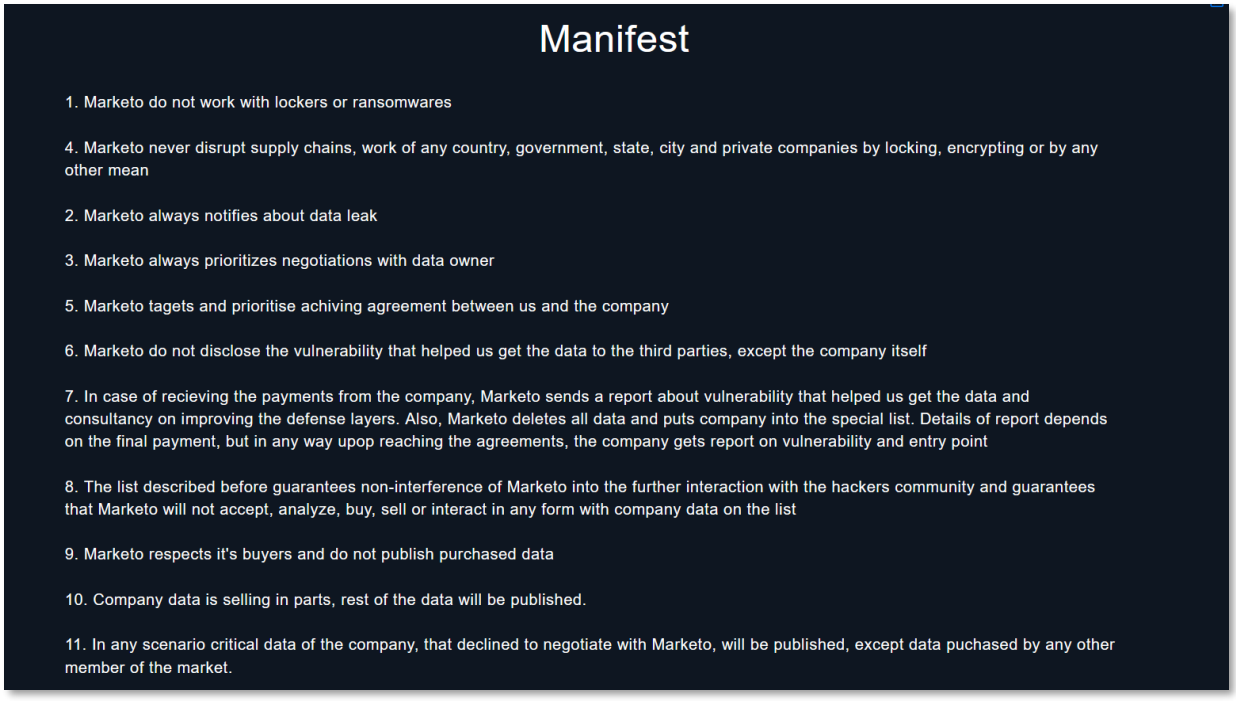
Marketo と Snatch を運営しているグループには、彼らの「ルール（Marketo では「マニフェスト」と呼ばれています）」をはじめ、いくつか共通している特徴があります。どちらのグループの「免責事項」もほぼ同じ言い回しで記載されており、また同じスペルミスがみられ、「ランサムウエアやロッカー」を使うグループとは連携していないと主張しています。また、どちらのグループも被害者に支払いを要求する代わりに、被害者を攻撃する際に使用した脆弱性を教えると述べていることや、第三者にデータを販売していることが共通点として挙げられます。



Public notice

Snatch do not work with lockers or ransomware.

1. Snatch never disrupt supply chains, work of any country, government, state, city and private companies by locking, encrypting or by any other mean.
2. Snatch always notifies about data leak.
3. Snatch always prioritizes negotiations with data owner.
4. Snatch targets and prioritise archiving agreement between us and the company.
5. Snatch do not disclose the vulnerability that helped us get the data to the third parties, except the company itself.
6. In case of receiving the payments from the company, Snatch sends a report about vulnerability that helped us get the data and consultancy on improving the defense layers. Also, Snatch deletes all data and puts company into the special list. Details of report depends on the final payment, but in any way upop reaching the agreements, the company gets report on vulnerability and entry point.
7. The list described before guarantees non-interference of Snatch into the further interaction with the hackers community and guarantees that Snatch will not accept, analyze, buy, sell or interact in any form with company data on the list.
8. Snatch respects it's buyers and do not publish purchased data.
9. Company data is selling in parts, rest of the data will be published.
10. In any scenario critical data of the company, that declined to negotiate with Snatch, will be published, except data purchased by any other member of the market.
11. Part of the critical data will not be selling, but will be Snatch exclusive data, that would be published according to the point '10'.
12. In the process of interaction with company, Snatch always notifies the government about data leak. This include tax departments, financial, cybersecurity and every authority in the company industry.
13. Snatch requires complete transparency about notification of data owners about data leak. If company started negotiations soon enough, warned about data leak and secured the rest of the company and affiliates data, the company can notify every affiliate and close the breach by themselves.
14. If company decides not to negotiate with Snatch, then in any scenario every company affiliate will be notified and presented the proofs of data breach.
15. Snatch does not notify the media about negotiation status and price of the deal. Negotiation process with company is strictly confidential.
16. Snatch open to the collaboration with companies, reporters, bloggers, enthusiasts and other people in cybersecurity. This also includes the people working in the same industry as the company listed on our site.
17. If someone is introducing themselves as negotiator from the Snatch or state they have a direct contact with Snatch, write to the Snatch only social media accounts or contact form on the site to verify the person.



Manifest

1. Marketo do not work with lockers or ransomwares

4. Marketo never disrupt supply chains, work of any country, government, state, city and private companies by locking, encrypting or by any other mean

2. Marketo always notifies about data leak

3. Marketo always prioritizes negotiations with data owner

5. Marketo tagets and prioritise achiving agreement between us and the company

6. Marketo do not disclose the vulnerability that helped us get the data to the third parties, except the company itself

7. In case of recieving the payments from the company, Marketo sends a report about vulnerability that helped us get the data and consultancy on improving the defense layers. Also, Marketo deletes all data and puts company into the special list. Details of report depends on the final payment, but in any way upop reaching the agreements, the company gets report on vulnerability and entry point

8. The list described before guarantees non-interference of Marketo into the further interaction with the hackers community and guarantees that Marketo will not accept, analyze, buy, sell or interact in any form with company data on the list

9. Marketo respects it's buyers and do not publish purchased data

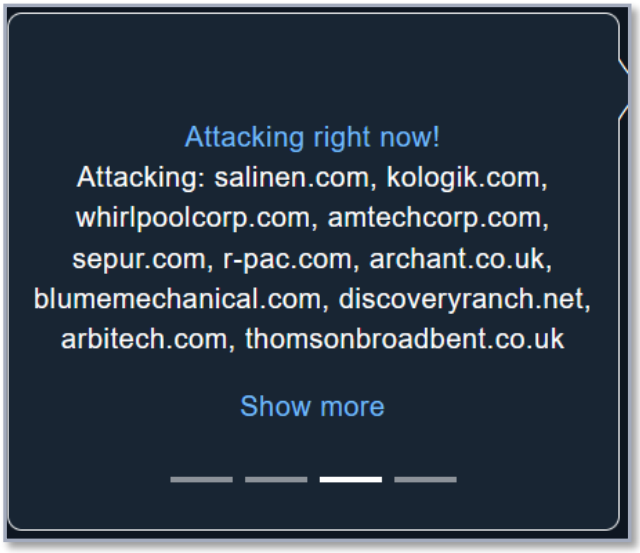
10. Company data is selling in parts, rest of the data will be published.

11. In any scenario critical data of the company, that declined to negotiate with Marketo, will be published, except data puchased by any other member of the market.

Snatch と Marketo がそれぞれ公言しているグループとしてのルール

（上図：Snatch　下図：Marketo）

さらに Marketo と Snatch には、共通する被害者（Lootah BCGas 社）も存在していました。Marketo は 2021 年 10 月 30 日、同社から窃取したデータ 406 GB 相当を売りに出しました。一方で Snatch は 2021 年 12 月 3 日、被害者は Lootah Group であるとしながらも Lootah BCGas に関連する証拠のみを公開しました。さらに Marketo では、彼らが「現在」攻撃していると主張しているドメインのリスト（ただし同サイトは 2021 年 10 月以降 2021 年末まで更新されませんでした）があり、そのうちの 2 件は後に Snatch が攻撃したと主張した被害者のドメインでした。



「現在」攻撃されている被害者（ソース：Marketo）

Marketo が「現在」攻撃している被害者のうち、Snatch と共有されていた 1 社

（ソース：Snatch）

Marketo は 2021 年 4 月に出現し、2021 年 10 月にその活動を停止しました。そしてその一方で、Snatch は 2021 年 11 月から活動を開始しました。つまり、Marketo と Snatch はひとつのグループがリブランドしたものである、または両グループの背後にいるアクターにつながりがあるという可能性が考えられます。しかしながら、Marketo は 2022 年 2 月に沈黙を破り、被害者 1 社を公表しています。そしてこの被害者も、Snatch がすでに不正アクセスしたと主張していた企業です[5]。2022 年 2 月の Marketo の活動が同サイトの完全復活を意味しているのか、それとも偶発的な活動であったのかは明らかではありませんが、この 2 グループの間に何らかのつながりがあるという構図に変わりはありません。

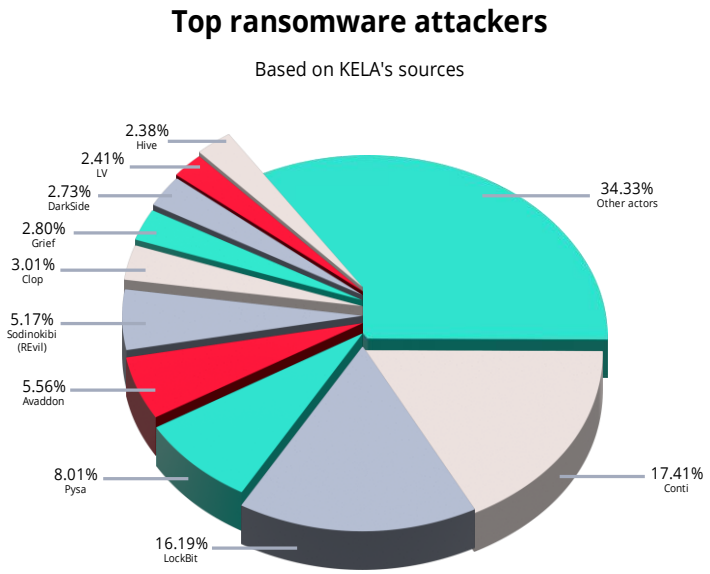
二重恐喝の被害者となった組織について調査を進めてゆくと、とりわけランサムウエアグループの活動が増加し、新たなグループも登場している現在の状況においては、1 度攻撃を受けた企業がその後は永遠に攻撃されないという保証はないことがわかります。これらのインシデントについて調査を行い、自らのネットワークを確実に保護して、さらなる攻撃を回避することが非常に重要であるといえるでしょう。

[5] 本レポートは 2021 年に確認された活動を報告対象としていますが、2022 年に発生したこの動向も本レポートに掲載するに値する情報であると判断して記載しております。

攻撃者の活動

2021 年にランサムウエアブログやデータリークサイトを運営していた攻撃者として、**Conti**、**LockBit**、**Pysa**、**Avaddon**、**REvil**（**Sodinokibi**）が挙げられます（最後の 2 グループは現在は存在しません）。これらオペレーションの大半は、ロシア語話者のアクターがランサムウエア・アズ・ア・サービス（RaaS）方式で運営しています。つまり彼らは、ランサムウエアオペレーションを実行するアフィリエイトやパートナーを募集しているということです。

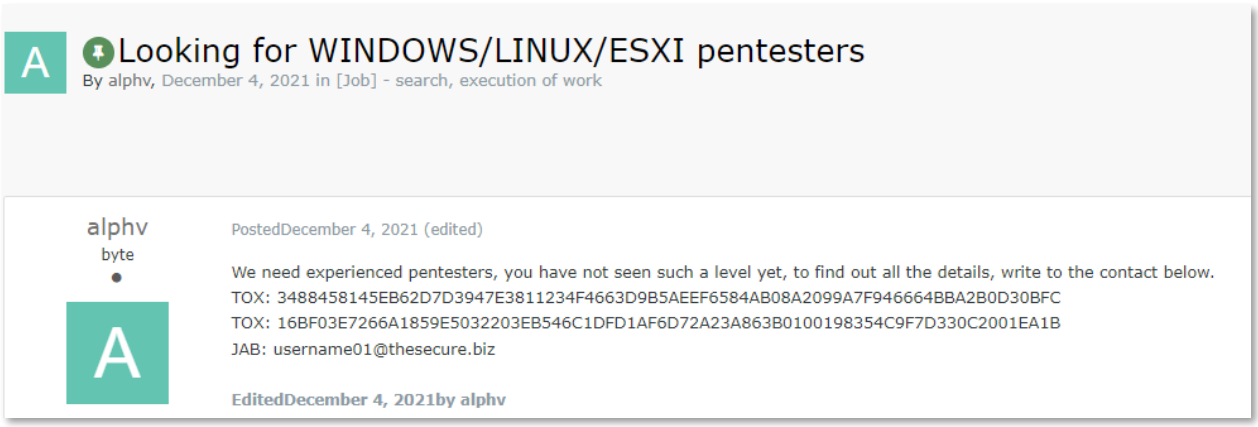
その一方で 2021 年には、実入りの良い業界のメンバーになろうと願う新たなグループが多数登場しました。その中でも **Hive**、**AvosLocker**、**Vice Society**、**Alphv** など一部のグループは現在も活動していますが、**BlackMatter** をはじめとする他のグループはすぐに活動を終了しました。また、**Avaddon** や **Egregor**、**DarkSide**、**REvil** など高い位置付けにあったランサムウエアグループも、法執行機関の作戦をはじめとする様々な理由によって姿を消しました。



新たに登場したプレイヤー

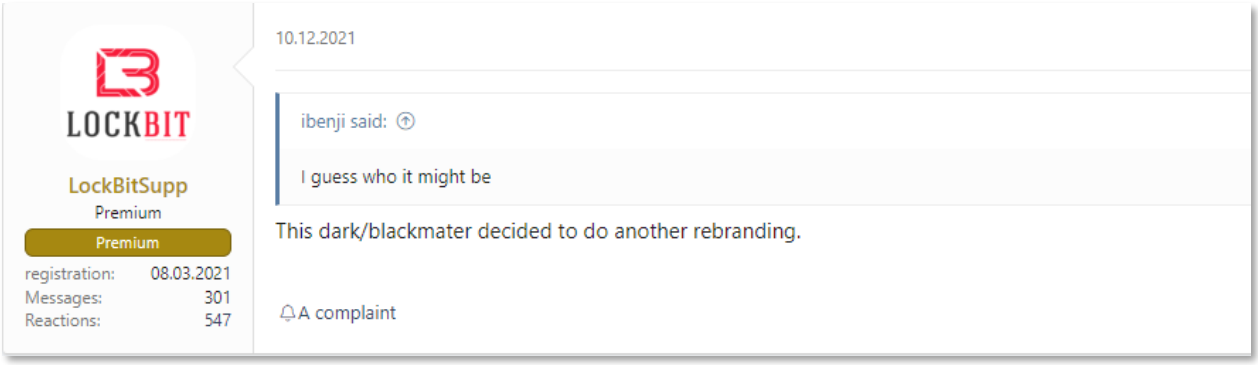
新たなプレイヤーの中でも非常に有望なグループのひとつは、2021 年 12 月にランサムウエア業界に参入した **Alphv** です。同グループのランサムウエアは Rust で記述されておりマルウエアとしては一般的ではありませんが、その高い性能とメモリの安全性で人気が高まっています[6]。Alphv は、自らの RaaS プログラムをサイバー犯罪フォーラム RAMP で宣伝しており、彼らのアフィリエイトも RAMP で活動しています。また他のサイバー犯罪フォーラムでも自らのプロファイルを掲載して、ペンテスター（当初は侵入テスト要員を指す略語として使用されていましたが、現在はネットワークに不正アクセスする十分なスキルを有するすべてのハッカーを表す言葉として使用されています）を募集しています。

Alphv は、活動を開始した最初の月に約 20 の被害者（大半は米国、カナダ、欧州の組織）をブログで公開しました。なお 2021 年 12 月には、**LockBit** の代表者が XSS フォーラムにて、Alphv はランサムウエアグループ **DarkSide** と **BlackMatter** のリブランドであると発言していました。しかし、Alphv が DarkSide や BlackMatter のオペレーションに参加していたアフィリエイトの一部を採用しただけという可能性も考えられます。



Alphv の代表者がペンテスターを募集している投稿（ソース：Exploit）

[6] https://www.bleepingcomputer.com/news/security/alphv-blackcat-this-years-most-sophisticated-ransomware/

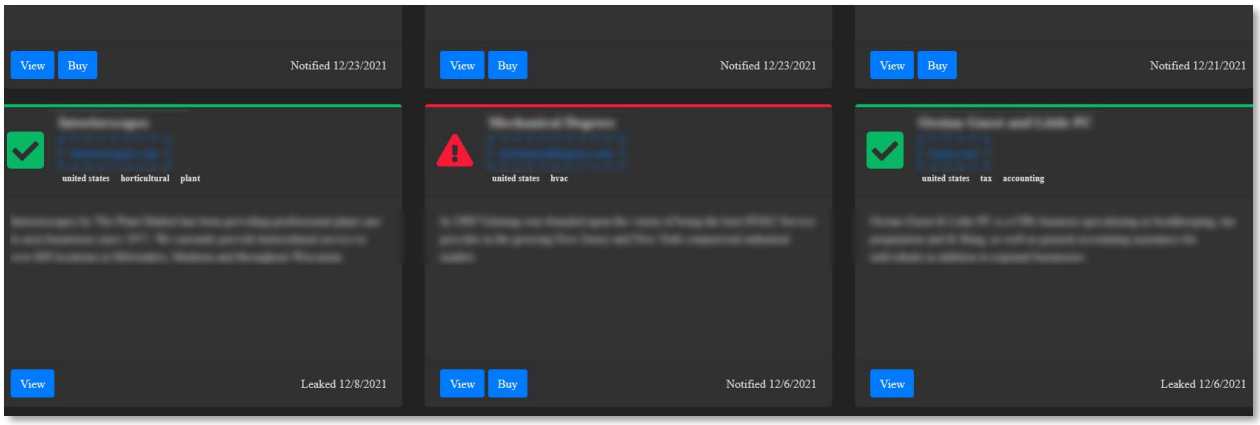


Alphv に関する LockBit の反応（ソース：XSS）

その他に注目すべきランサムウエアグループとして、2021 年 6 月に活動を開始した **Hive** が挙げられます。その後の 8 月には、米連邦捜査局（FBI）が Hive に関する警告を発表しており、この警告は同グループが重大なリスクをもたらす存在であることを裏付けています[7]。Hive が関与した大規模な攻撃のひとつは、2021 年 11 月に行われた MediaMarkt 社への攻撃です。報道にもあるとおり、Hive は 2 億 4,000 万米ドルという巨額の身代金の支払いを要求し、同社がオランダやドイツをはじめ欧州に展開している小売店は一時業務停止に追い込まれました[8]。Hive は現在も活動しており、昨年同グループのブログに掲載された被害者の数は 60 を超えています。

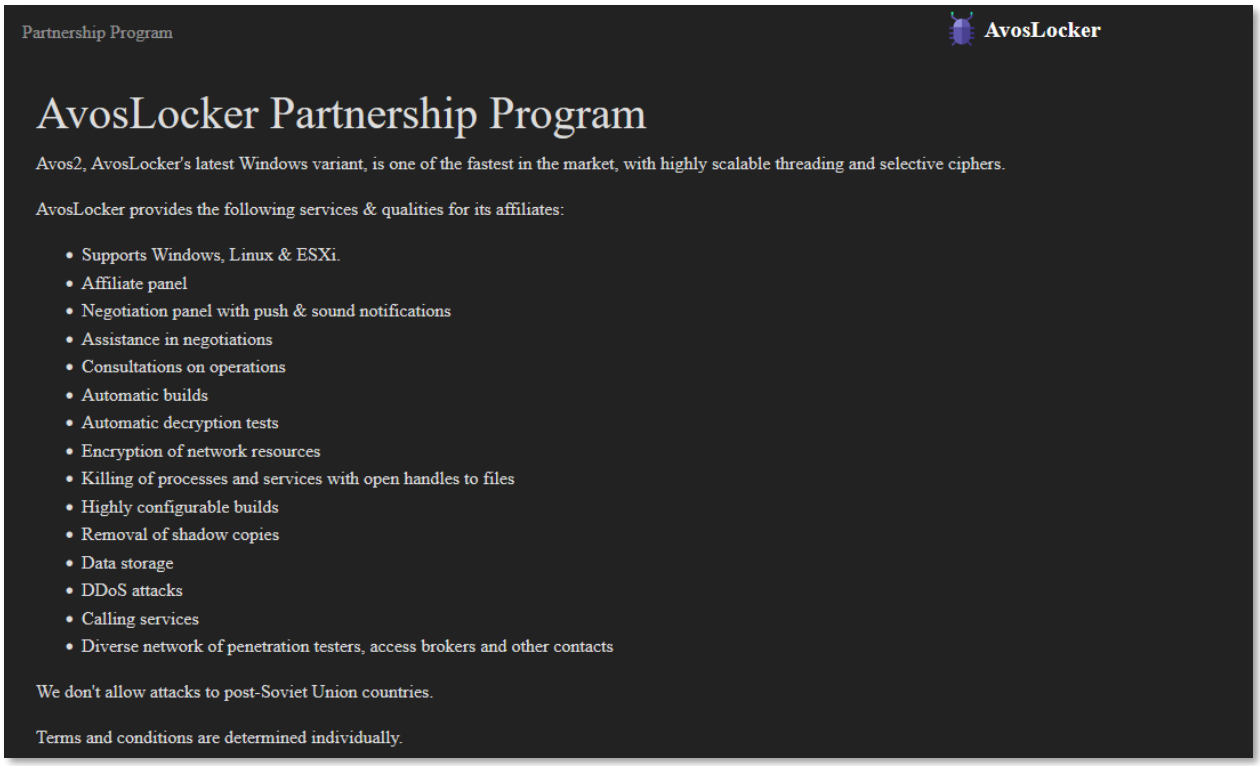
AvosLocker は、2021 年 7 月にはじめてその存在が確認されたランサムウエアグループであり、当初はランサムウエアグループ **DoppelPaymer** のリークサイトに似たデザインのサイトを運営していました。しかし 2021 年 9 月中旬、同グループは身代金の支払いを拒否した企業のデータをオークション形式で販売する新機能を追加し再編成したサイトを新たに立ち上げました。また同グループは 2021 年 11 月、Windows と Linux を標的とするランサムウエアもリリースしています（Windows 版ランサムウエア「Avos2」、Linux 版ランサムウエア「Avoslinux」）。

[7] https://www.ic3.gov/Media/News/2021/210825.pdf
[8] https://www.bleepingcomputer.com/news/security/mediamarkt-hit-by-hive-ransomware-initial-240-million-ransom/



AvosLocker のリーク用ブログ（ソース：AvosLocker）

AvosLocker は、XSS や Exploit、RAMP などのフォーラムでアフィリエイトを積極的に募集すると同時に、自らのブログでもパートナーシッププログラム専用のページを開設しました。その一方で同グループは、フォーラムでネットワークアクセスを購入することにも関心を示していました。その一例を挙げてみると、2021 年 12 月 AvosLocker は、米国とカナダに拠点を置き 5,000 万米ドル超の収益を有する企業のアクセスを購入することに意欲を示しており、身代金の一部を分け前として支払うつもりであると発言していました（「理想的なランサムウエア被害者」の章を参照）。AvosLocker は現在も活動を続けており、昨年は 55 件を超える被害者を自らのブログで公開しています。



AvosLocker のRaaS プログラム（ソース：Avos）

有名グループの消滅

世間の注目を集める攻撃が複数件発生したことを受け、ランサムウエアグループに対する法執行機関の圧力が高まりました。その結果、優勢であったアクターのものも含めて 14 のランサムウエアブログが 2021 年に活動を停止しており、うち 6 つについては法執行機関から注目が高まったことがその活動停止の理由と関連しています。また数グループについてはブランドを再編したり、所属するアフィリエイトが別のグループへ移動した可能性が高いと考えられます。

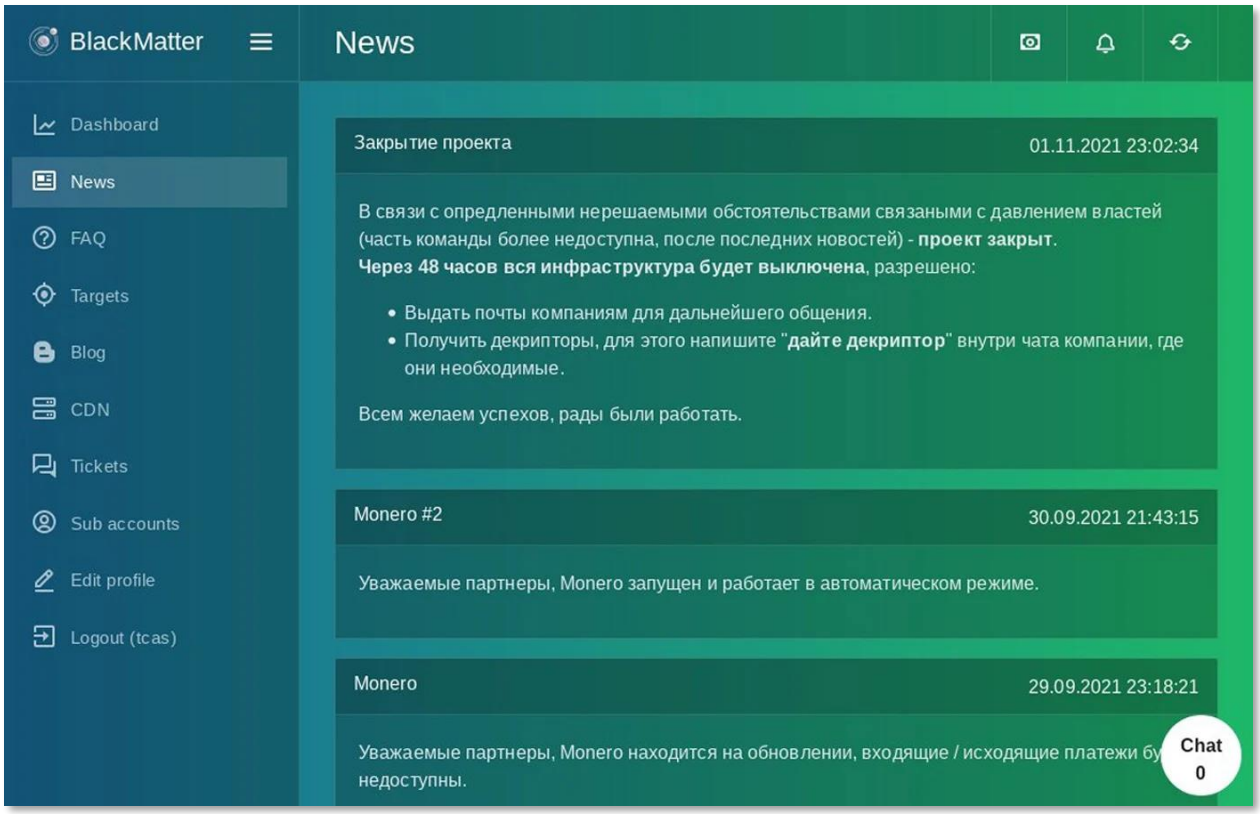
大きな注目を集めたインシデントのひとつに、2021 年 5 月に発生した **DarkSide** による Colonial Pipeline 社への攻撃が挙げられます。この事件によって DarkSide に対する米国当局の関心が高まり、同月に同グループのサーバーが押収され、さらにはアフィリエイトへの支

払い用に使用していたアカウントから暗号資産が引き出される事態となり、その結果 DarkSide は活動を停止することを発表しました[9]。その後の 2021 年 6 月、米国司法省が DarkSide に支払われた身代金のうち 230 万米ドル相当の暗号資産を差し押さえたことが明らかとなりました[10]。米国国務省は DarkSide の逮捕につながる情報に対して 1,000 万ドルの報奨金を提供すると発表しており、同グループは現在も引き続き当局のトップターゲットとなっています[11]。

2021 年 7 月には、ランサムウエアグループ **BlackMatter** が出現し、米国やカナダ、オーストラリア、英国で 1 億米ドル超の収益を有する大企業を攻撃するために、初期アクセス・ブローカーとペンテスターを募集していることをフォーラム Exploit と XSS で発表しました。また同グループは自らのブログを立ち上げ、その中で医療機関や重要インフラ、石油及びガス、防衛、非営利団体、政府機関などの業界を攻撃しないことを公言していました。BlackMatter のブログのデザインは、DarkSide のリークサイトと非常に類似しており、両グループのランサムウエアのコードにも類似性がみられました（ただし全く同じコードではありませんでした）[12]。これらの事実から、DarkSide の主要メンバーか元アフィリエイトがランサムウエアグループ BlackMatter を立ち上げた可能性が考えられます（前述の LockBit の発言を参照）。

そして DarkSide と同様に BlackMatter も 2021 年 11 月、法執行機関の圧力を受けてオペレーションを終了するとの声明を自らの RaaS ポータルで発表しました。この当局からの圧力とは、ランサムウエアオペレーションを停止させることを目的として、米国とロシアの法執行機関が連携して行っている先般の活動を指しているものと考えられます[13]。

[9] https://krebsonsecurity.com/2021/05/darkside-ransomware-gang-quits-after-servers-bitcoin-stash-seized/
[10] https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside
[11] https://www.state.gov/darkside-ransomware-as-a-service-raas/
[12] https://news.sophos.com/en-us/2021/08/09/blackmatter-ransomware-emerges-from-the-shadow-of-darkside/
[13] https://www.politico.com/news/2021/06/16/putin-biden-cybersecurity-494875



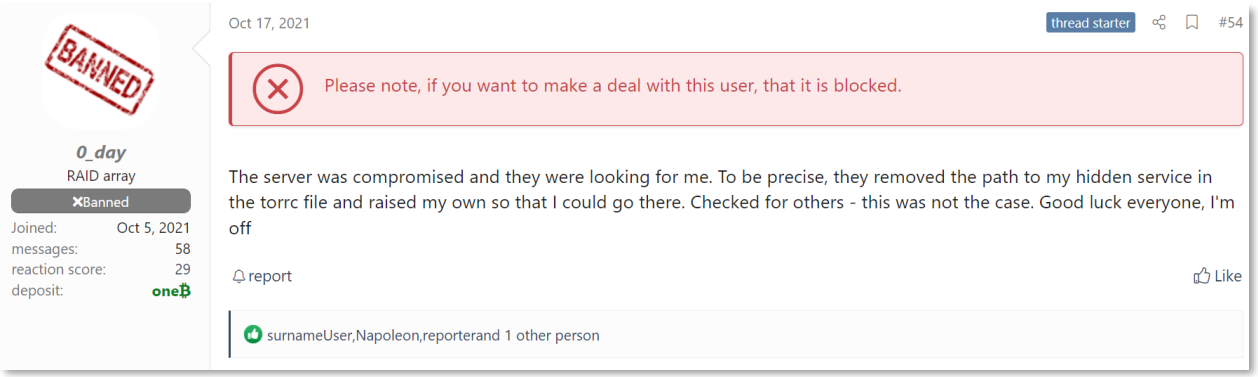
BlackMatter がアフィリエイト用サイトに掲載した活動停止の告知
（ソース：Bleeping Computer）

また 2021 年には、悪名高いグループ **REvil** が世間の注目を集める攻撃 2 件を実行した後にオフラインとなりました。2021 年 5 月、REvil は食肉大手企業 JBS 社に不正アクセスし、その結果同社の米国及びオーストラリアにおける業務が一時停止を余儀なくされました[14]。JBS 社は、身代金として 1,100 万米ドルを支払ったことを認めています[15]。2 件目の攻撃は 2021 年 7 月に行われ、IT 管理ソフトウエア企業 Kaseya 社が攻撃を受けました。この攻撃では 17 カ国で被害組織が確認され、少なくとも 1,000 の組織が影響を受ける事態となりました[16]。この攻撃の後 REvil は自ら姿を消し、同グループのサイトもオフラインになりました。

しかし 2021 年 9 月、今度は REvil（後に 0_neday に変更）と名乗るユーザーが、REvil の前

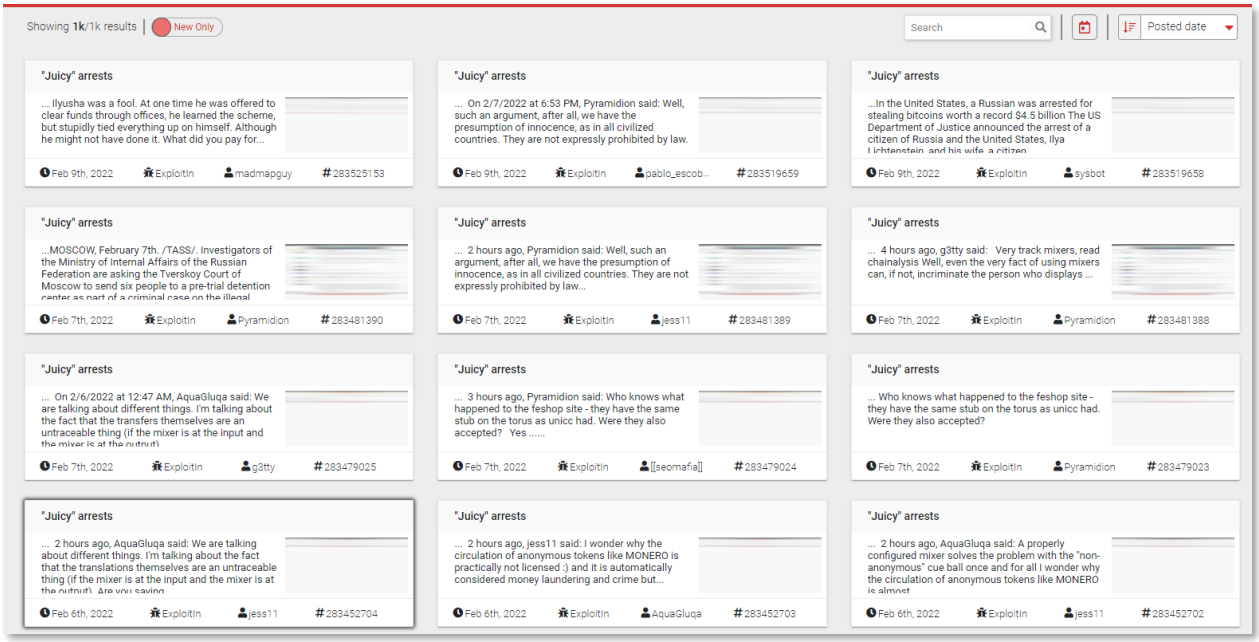
[14] https://www.zdnet.com/article/ransomware-meat-firm-jbs-says-it-paid-out-11m-after-attack/
[15] https://jbsfoodsgroup.com/articles/jbs-usa-cyberattack-media-statement-june-9
[16] Checkpoint, CYBER ATTACK TRENDS Mid Year Report 2021

代表者 UNKN（Unknown）の代わりとしてフォーラムに登場しました。このアクターはフォーラム Exploit で、サイバー犯罪グループとしての REvil は法執行機関を恐れて消滅したと述べました。そして 2021 年 10 月、法執行機関や当局が連携した取り組み（この取り組みについて公式な発表は行われていません）により、REvil のオペレーションは停止に追い込まれ、彼らのサイトもオフラインになりました[17]。2022 年 1 月には、ロシア連邦保安庁（FSB）がサイバー犯罪グループ REvil のメンバー14 名を逮捕しました[18]。この事態を受けてアンダーグラウンドでは多数の反応が沸き起こっており、ダークウェブ内で確認された会話や投稿には、逮捕されたのがランクの低いアフィリエイトだけであったことが示唆されていました[19]。従って、REvil を背後で操っていた主要なアクターたちは今も自由の身であるのか、そして同グループが 2022 年に新たなオペレーションとしてリブランドするのかは定かではありません。



REvil の声明（ソース：XSS）

[17]https://www.reuters.com/technology/exclusive-governments-turn-tables-ransomware-gang-revil-by-pushing-it-offline-2021-10-21/
[18] https://therecord.media/fsb-raids-revil-ransomware-gang-members/
[19]https://www.bleepingcomputer.com/news/security/russia-charges-8-suspected-revil-ransomware-gang-members/



REvil のアフィリエイト逮捕に対する反応（ソース：KELA のプラットフォーム）

2021 年に姿を消したもうひとつの重要なプレイヤーとして、ランサムウエアグループ **Egregor** が挙げられます。**Egregor** は、二重恐喝の先駆者であった Maze が 2020 年 11 月にその引退を発表する直前に登場しました。Maze が活動を終了した後に同グループのアフィリエイトが Egregor に移動した結果、2021 年は Egregor の認知度が大きく向上しました[20]。Egregor は世間の注目を集めた攻撃にも複数件関与しており、その活動期間においては、多数の国々と業界にまたがる 215 の被害者が公開されました。しかし 2021 年 2 月、米国、フランス、ウクライナの当局による合同捜査により Egregor のメンバーが逮捕され、同グループのコマンド&コントロールサーバーとデータリークサイトが閉鎖されました[21]。

その他にも姿を消した有名なランサムウエアグループのひとつとして、**Avaddon** が挙げられます。同グループは 2019 年に登場しましたが、2021 年 6 月に復号キーをリリースして[22]

[20] https://blog.malwarebytes.com/ransomware/2020/12/threat-profile-egregor-ransomware-is-making-a-name-for-itself/
[21] https://www.zdnet.com/article/egregor-ransomware-operators-arrested-in-ukraine/
[22] https://www.bleepingcomputer.com/news/security/avaddon-ransomware-shuts-down-and-releases-decryption-keys/

オペレーションを停止しました。

新たなグループが出現し、古い主要なプレイヤーが活動を終了してゆく中で、目覚ましい進化を遂げたと思われれるオペレーションもありました。LockBit は 2021 年に最も成果を上げたランサムウエアグループのひとつであり、我々はダークウェブにおける同グループの存在とランサムウエア活動について徹底的な調査を行いました。

ランサムウエアグループ「LockBit」の進化

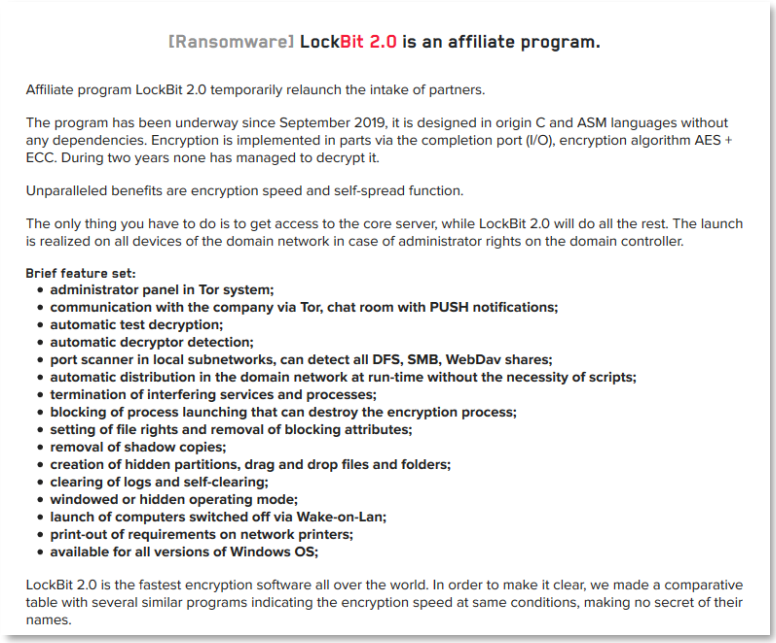
LockBit は、2019 年にその活動を開始しました。活動当初、同グループは自らのブログを持っておらず、被害者の名称はランサムウエアグループ Maze のブログ内で「provided by LockBit（LockBit より提供）とのシグネチャーの下に掲載されていました。そしてその一方で、アフィリエイトの募集をはじめとする様々な活動で利用していたフォーラムでは、独立したグループとしてのプロファイルを保有していました。2020 年になると LockBit は自らのブログを立ち上げましたが、その当時の同グループのオペレーションは、それほど活発ではなかったものと思われます。

LockBit 2.0

2021 年のはじめ、LockBit は今後のランサムウエアオペレーションに向けた環境を確立しました。同グループは、被害者の名前とデータを公開するブログの他、新興のアフィリエイトプログラムも立ち上げており、中程度ではあるものの成長しつつある脅威として見なされ、2021 年第 1 四半期には最もよく使用されるランサムウエア亜種の 3 位となりました[23]。LockBit の代表者は、2021 年 3 月以降 LockBitSupp とのハンドル名を使い、フォーラム XSS や Exploit で活動しています。また同グループは、2021 年 6 月に立ち上げられたランサムウエアの新バージョン LockBit 2.0 のリリースを宣伝する場、そして新たなアフィリエイトを集める場としてこれらのフォーラムを利用していました。

[23] https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound

LockBit 2.0 へのアップデート以降、同グループは自らのランサムウエアの機能について高い自信を持っているものと思われ、2021 年 8 月のインタビューでも次のように述べています。「*LockBit は他の RaaS とは異なっており、まず非常に複雑なソフトウエアである（...）。このような武器を備えたアフィリエイトプログラムは、地球上を見渡しても他にはないんだ*[24]」。また同グループは自らのブログの中で、LockBit 2.0 と他のランサムウエアグループのソフトウエアを比較して、LockBit 2.0 は世界最高速度の暗号化ソフトウエアであると主張していました。



[Ransomware] LockBit 2.0 is an affiliate program.

Affiliate program LockBit 2.0 temporarily relaunch the intake of partners.

The program has been underway since September 2019, it is designed in origin C and ASM languages without any dependencies. Encryption is implemented in parts via the completion port (I/O), encryption algorithm AES + ECC. During two years none has managed to decrypt it.

Unparalleled benefits are encryption speed and self-spread function.

The only thing you have to do is to get access to the core server, while LockBit 2.0 will do all the rest. The launch is realized on all devices of the domain network in case of administrator rights on the domain controller.

Brief feature set:

- **administrator panel in Tor system;**
- **communication with the company via Tor, chat room with PUSH notifications;**
- **automatic test decryption;**
- **automatic decryptor detection;**
- **port scanner in local subnetworks, can detect all DFS, SMB, WebDav shares;**
- **automatic distribution in the domain network at run-time without the necessity of scripts;**
- **termination of interfering services and processes;**
- **blocking of process launching that can destroy the encryption process;**
- **setting of file rights and removal of blocking attributes;**
- **removal of shadow copies;**
- **creation of hidden partitions, drag and drop files and folders;**
- **clearing of logs and self-clearing;**
- **windowed or hidden operating mode;**
- **launch of computers switched off via Wake-on-Lan;**
- **print-out of requirements on network printers;**
- **available for all versions of Windows OS;**

LockBit 2.0 is the fastest encryption software all over the world. In order to make it clear, we made a comparative table with several similar programs indicating the encryption speed at same conditions, making no secret of their names.

アフィリエイトプログラム LockBit 2.0 についての説明（ソース：LockBit のブログ）

[24] Russian OSINT による LockBit 2.0 とのインタビューを KELA にて書き起こし翻訳しました。（https://ke-la.com/lockbit-2-0-interview-with-russian-osint/）

Encryption speed comparative table for some ransomware - 02.08.2021

PC for testing: Windows Server 2016 x64 \ 8 core Xeon E5-2680@2.40GHz \ 16 GB RAM \ SSD

Name of the ransomware	Date of a sample	Speed in megabytes per second	Time spent for encryption of 100 GB	Time spent for encryption of 10 TB	Self spread	Size sample in KB	The number of the encrypted files (All file in a system 287472)
LOCKBIT 2.0	5 Jun, 2021	373 MB/s	4M 28S	7H 26M 40S	Yes	855 KB	109964
LOCKBIT	14 Feb, 2021	266 MB/s	6M 16S	10H 26M 40S	Yes	146 KB	110029
Cuba	8 Mar, 2020	185 MB/s	9M	15H	No	1130 KB	110468
BlackMatter	2 Aug, 2021	185 MB/s	9M	15H	No	67 KB	111018
Babuk	20 Apr, 2021	166 MB/s	10M	16H 40M	Yes	79 KB	109969
Sodinokibi	4 Jul, 2019	151 MB/s	11M	18H 20M	No	253 KB	95490
Ragnar	11 Feb, 2020	151 MB/s	11M	18H 20M	No	40 KB	110651
NetWalker	19 Oct, 2020	151 MB/s	11M	18H 20M	No	902 KB	109892
MAKOP	27 Oct, 2020	138 MB/s	12M	20H	No	115 KB	111002
RansomEXX	14 Dec,2020	138 MB/s	12M	20H	No	156 KB	109700
Pysa	8 Apr, 2021	128 MB/s	13M	21H 40M	No	500 KB	108430
Avaddon	9 Jun, 2020	119 MB/s	14M	23H 20M	No	1054 KB	109952
Thanos	23 Mar, 2021	119 MB/s	14M	23H 20M	No	91 KB	81081
Ranzy	20 Dec, 2020	111 MB/s	15M	1D 1H	No	138 KB	109918
PwndLocker	4 Mar, 2020	104 MB/s	16M	1D 2H 40M	No	17 KB	109842
Sekhmet	30 Mar, 2020	104 MB/s	16M	1D 2H 40M	No	364 KB	random extension
Sun Crypt	26 Jan, 2021	104MB/s	16M	1D 2H 40M	No	1422 KB	random extension
REvil	8 Apr, 2021	98 MB/s	17M	1D 4H 20M	No	121 KB	109789
Conti	22 Dec, 2020	98 MB/s	17M	1D 4H 20M	Yes	186 KB	110220
Hive	17 Jul, 2021	92 MB/s	18M	1D 6H	No	808 KB	81797
Ryuk	21 Mar, 2021	92 MB/s	18M	1D 6H	Yes	274 KB	110784
Zeppelin	8 Mar, 2021	92 MB/s	18M	1D 6H	No	813 KB	109963
DarkSide	1 May, 2021	83 MB/s	20M	1D 9H 20M	No	30 KB	100549
DarkSide	16 Jan, 2021	79 MB/s	21M	1D 11H	No	59 KB	100171
Nephilim	31 Aug, 2020	76 MB/s	22M	1D 12H 40M	No	3061 KB	110404
DearCry	13 Mar, 2021	64 MB/s	26M	1D 19H 20M	No	1292 KB	104547
MountLocker	20 Nov, 2020	64 MB/s	26M	1D 19H 20M	Yes	200 KB	110367
Nemty	3 Mar, 2021	57 MB/s	29M	2D 0H 20M	No	124 KB	110012
MedusaLocker	24 Apr, 2020	53 MB/s	31M	2D 3H 40M	Yes	661 KB	109615
Phoenix	29 Mar, 2021	52 MB/s	32M	2D 5H 20M	No	1930 KB	110026
Hades	29 Mar, 2021	47 MB/s	35M	2D 10H 20M	No	1909 KB	110026
DarkSide	18 Dec, 2020	45 MB/s	37M	2D 13H 40M	No	17 KB	114741
Babuk	4 Jan, 2021	45 MB/s	37M	2D 13H 40M	Yes	31 KB	110760
REvil	7 Apr, 2021	37 MB/s	45M	3D 3H	No	121 KB	109790
BlackKingdom	23 Mar, 2021	32 MB/s	52M	3D 14H 40M	No	12460 KB	random extension
Avos	18 Jul, 2021	29 MB/s	59M	4D 2H	No	402 KB	79486

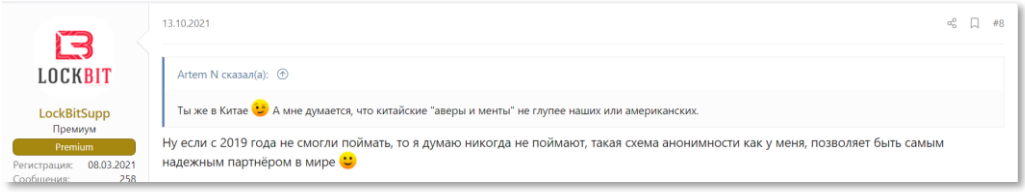
暗号化速度の比較表（ソース：LockBit のブログ）

研究者たちが、LockBit 2.0 の特定の機能について一部確認しており、その報告によると LockBit 2.0 は「ワームのような機能」を使ってネットワーク内に伝播することができ、手動操作不要で自己拡散します[25]。そして実行された後は、ローカルのサブネットワークを検索して水平移動を行います。同グループは、高速暗号化プロセスを補完するためにデータ抽出プロセスをスピードアップするべく、このランサムウエアの他に独自のデータ流出ツール StealBit も開発していました[26]。

LockBit はこのランサムウエアの機能に加え、自らの RaaS モデルが革新的であり、アフィリエイトの安全と匿名性を優先したものであると主張しています。このトピックに関する議論の中で LockBit は次のように回答しています。「2019 年以降、当局が[我々のアフィリエイトを（KELA による追加訳）]捕まえられていない場合は、今後も捕まえられることはないと

[25] https://www.kaspersky.com/resource-center/threats/lockbit-ransomware
[26] https://www.trendmicro.com/en_us/research/21/h/lockbit-resurfaces-with-version-2-0-ransomware-detections-in-chi.html

思う。我々のアフィリエイトプログラムの匿名性スキームが、我々を世界で最も信頼できるパートナーたるものにしている」。



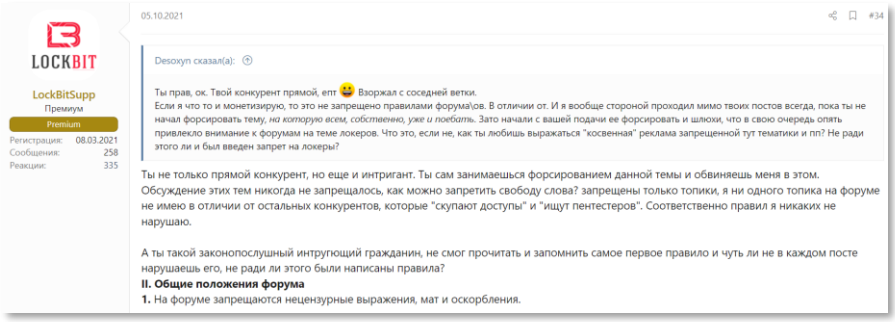
自らの RaaS モデルについて述べる LockBit のコメント（ソース：XSS）

同グループのビジネスモデルにおいて、他のランサムウエアオペレーターとの間にみられるもうひとつの違いは、彼らが受け取った身代金の配分方法です。LockBit はインタビューの中で、被害者が支払った身代金はまずアフィリエイトのウォレットに送金され、アフィリエイトがその身代金のうち 20%を LockBit に送る仕組みとなっていると説明しており、一方でほとんどのランサムウエアプログラムはこの反対の方式を採用していると語っています[27]。

ダークウェブでの活動

2021 年 10 月、LockBit の代表者は、そのランサムウエア活動を理由にフォーラム Exploit を出入り禁止となりましたが、フォーラム XSS には引き続き参加することができました。LockBit の代表者は Exploit で出入り禁止となったことについて、フォーラムでネットワークアクセスを購入し、新たなアフィリエイトを募集している同業者たちと比べて、自分たちは「何もルールを破っていない」と反論しました。

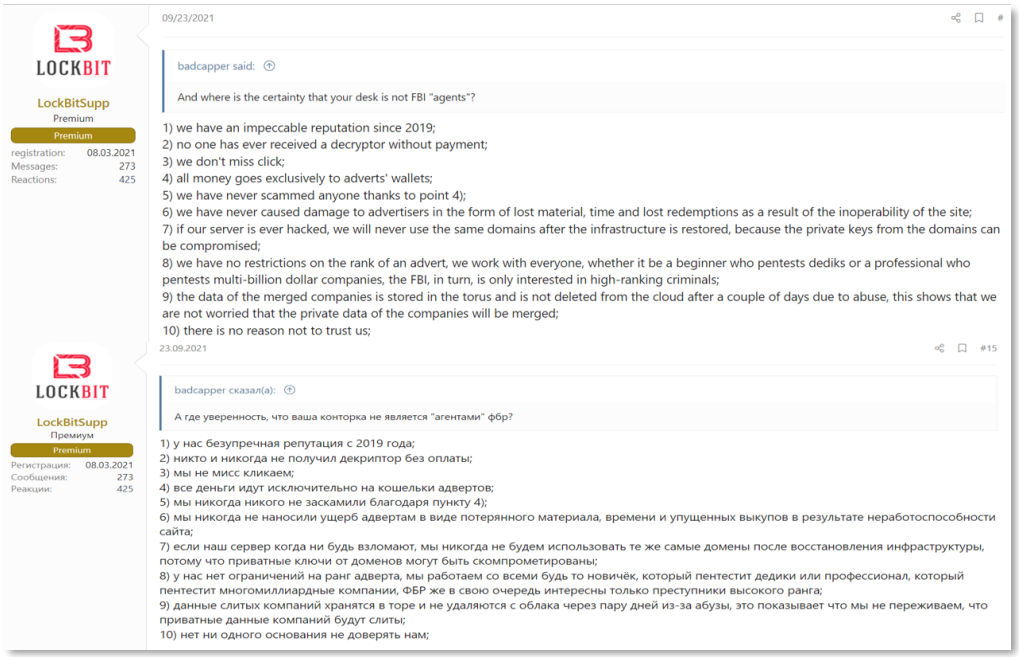
[27] https://ke-la.com/lockbit-2-0-interview-with-russian-osint/



Exploit での禁止令に対する LockBit の反応（ソース：XSS）

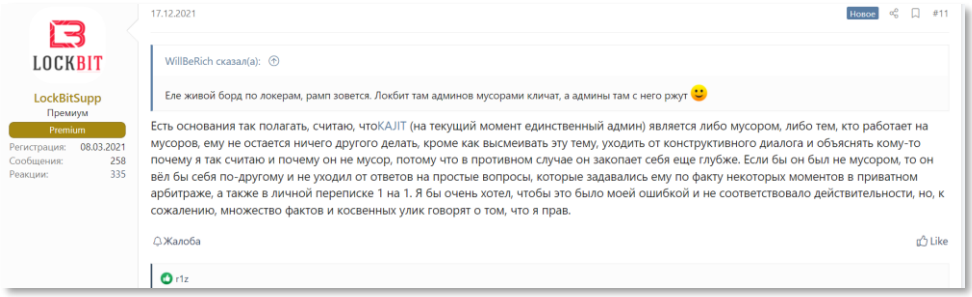
2021 年 9 月には、XSS における LockBit の活動件数が増加しました。LockBit の代表は数件のディスカッションに参加して、同グループの評判と活動を非難する投稿に対し返答していました。

例えば REvil のアフィリエイト数人が逮捕された件について、LockBit は現在 REvil のアフィリエイトプログラムを管理しているとされるコーダーを調べ、その人物が FBI の潜入捜査官ではないことを証明するよう提案しました。しかしあるユーザーはこの提案に対し、FBI の捜査官が LockBit グループを運営している可能性もあるぞと返信していました。



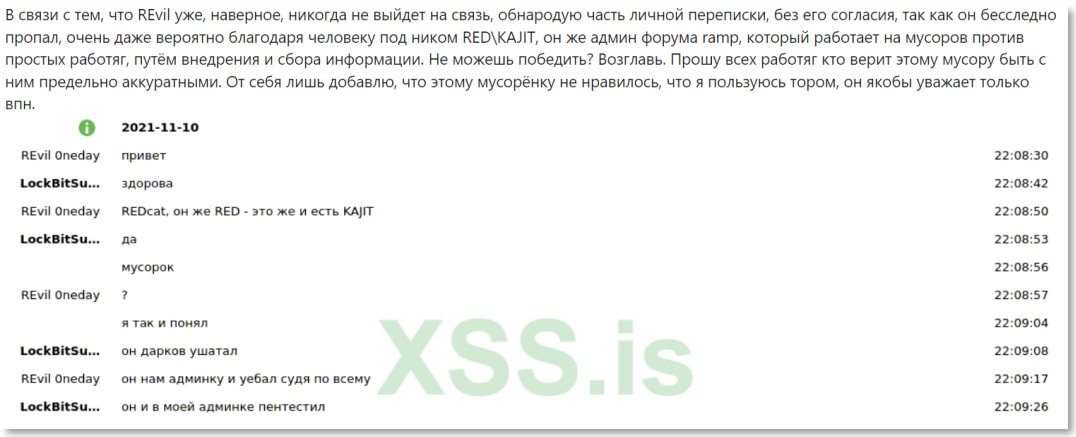
非難に対する LockBit の回答（ソース：XSS）

我々が、過去数カ月間にわたって LockBit の代表者のコメントを観察したところ、彼は「ウオッチャー」がいたるところにいると発言しており、またフォーラム RAMP とその管理者 KAJIT に対しては、KAJIT が法執行機関と関係している可能性があることを示唆する申し立てを行っていました。



KAJIT に対する LockBit の主張（ソース：XSS）

そして 2022 年 1 月にランサムウエアグループ REvil のメンバーが逮捕された後、LockBit は自らが REvil の某メンバーと 2021 年 11 月初旬より交わしていた会話の内容を、XSS で公開しました。その内容は、KAJIT が REvil に関する情報を集めており、同グループのテイクダウンに関与している可能性があることを証明するものでした。また LockBit は、KAJIT と vx-underground（匿名のセキュリティ研究グループ）の間で交わされた会話を公開し、KAJIT がランサムウエアオペレーション BlackMatter の管理パネルのスクリーンショットをリークしていたことを証明しました。LockBit の取り組みが功を奏し、KAJIT は XSS や Exploit で出入り禁止となり、RAMP の運営から脱退しました。



LockBit と REvil の会話（ソース：XSS）

パートナー

また我々は、複数の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・ブローカーの活動を分析しました。そしてその結果、彼らが販売したアクセスが LockBit がブログに掲載した被害者のものと一致しているケースを数件発見しました。

2021 年 9 月 20 日、我々は脅威アクターorange cake がイスラエルに拠点を置く移民コンサルティング企業へのアクセス（VPN 経由）を売りに出したことを確認しました（同社ではランサムウエア攻撃についてさらなる情報を公開していません）。そしてその翌日には、同社のアクセスが 200 米ドルで脅威アクターchakalaka に売り渡されていました。chakalaka については、ネットワークアクセスの販売と買取の両方を手掛けていること、またハッシュを復号化してくれる人材を探していたことがこれまでに確認されています。そして 2021 年 10 月 25 日、LockBit のブログで同社の名前が公開されました（「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」の章で解説されている事例をご参照ください）。この被害企業のネットワークアクセスが売り出されてから LockBit のアフィリエイトが攻撃を実行するまでの期間は、約 1 カ月でした。

LockBit は初期アクセス・ブローカーからアクセス情報を入手することに加え、フォーラム外にもパートナーシップ関係を広げようと試みていました。2021 年 8 月、LockBit の被害者のファイルが暗号化された後、デスクトップの壁紙に同グループからのオファーが表示されました。LockBit は、RDP や VPN、電子メールの資格情報を提供してくれる、または悪意ある電子メールをオフィスのコンピューターで開封してくれる「インサイダー」に数百万ドルを支払うと約束していました。このオファーは、ランサムウエアに感染した被害企業の従業員ではなく、恐らくはこのインシデントに対応する外部の IT コンサルタントを対象としていたものと思われます[28]。

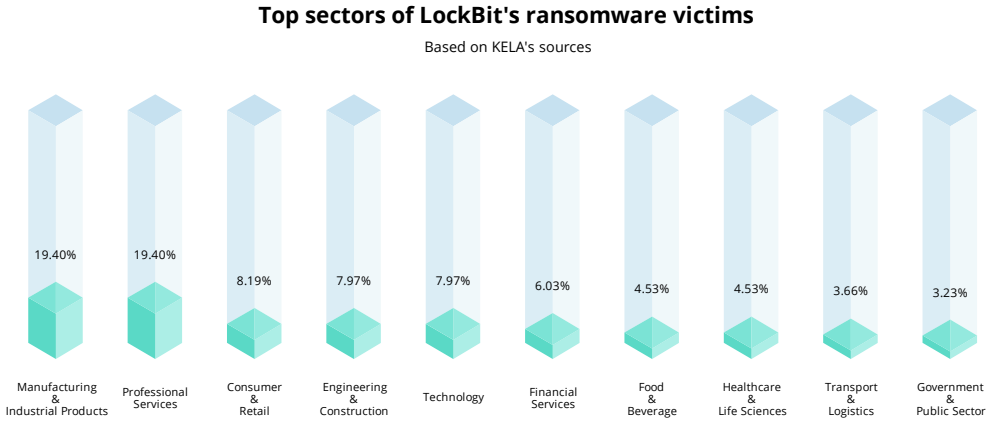
[28] https://www.bleepingcomputer.com/news/security/lockbit-ransomware-recruiting-insiders-to-breach-corporate-networks/

LockBit のインサイダー募集メッセージ（ソース：BleepingComputer）

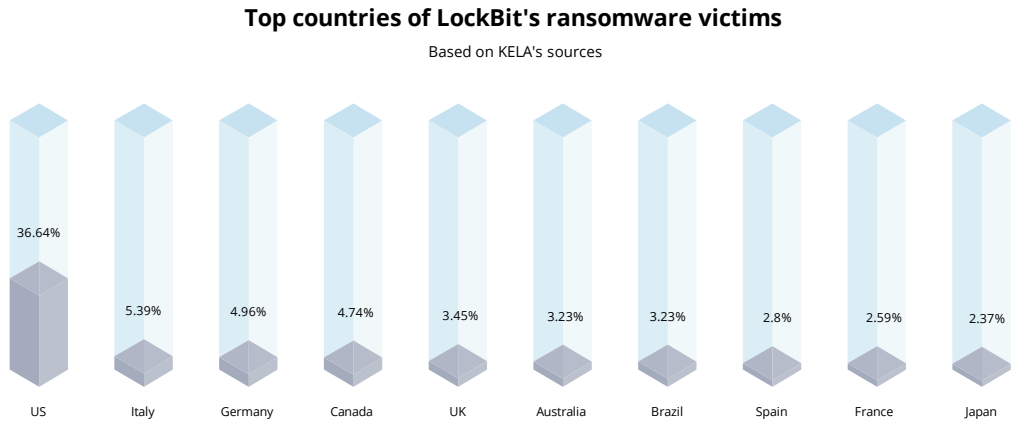
2021 年の被害者

我々は、2021 年の間に LockBit が 450 件以上の被害者をブログで公開したことを確認しました。2021 年前半においては、同グループがブログに掲載した被害者の数はゼロですが、2021 年 7 月には、アフィリエイトプログラム LockBit 2.0 の公開と同時に、公の場で繰り広げられるランサムウエアの活動が大幅に増加しました。

LockBit のブログに基づくと、最も影響を受けた業界は、製造・工業製品、専門サービスであり、その次に消費財・小売、テクノロジー、土木建築が続きました。



また 2021 年に LockBit の攻撃を最も多く受けた国は米国であり、その後にイタリア、カナダ、ドイツが続きました。既出のセクションでもお伝えしたとおり、LockBit はこれらの国々には最も理想的な標的がいると断言していました。

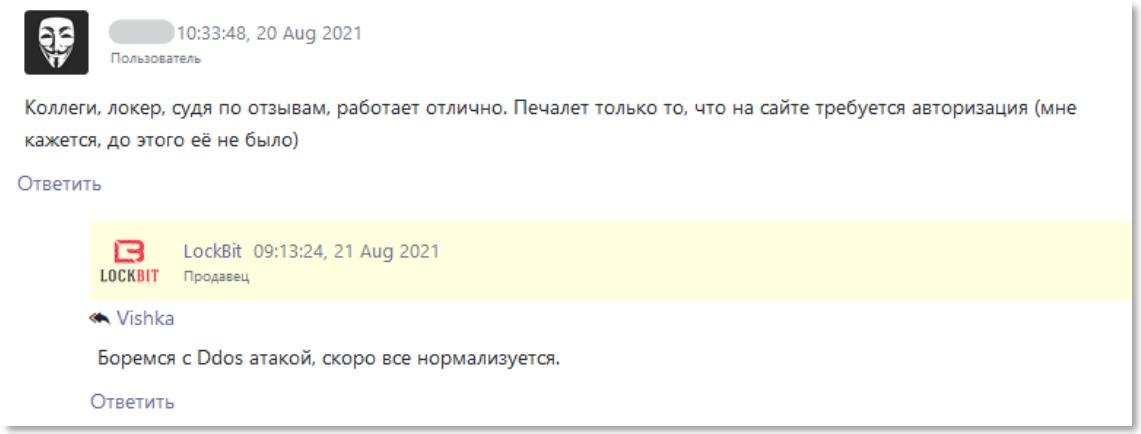


DDoS 攻撃

2021 年、LockBit は自らのブログが一連の DDoS 攻撃を受けていると主張していました。2021 年 8 月 18 日に我々が LockBit のブログにアクセスしたところ、ログイン「承認」用のポップアップが表示されるようになっており、その後の 8 月 20 日には LockBit の代表者が、「我々は今 DDoS 攻撃と戦っている。事態はすぐに正常に戻る」とフォーラム RAMP で発言していました。

そしてこれら一連の DDoS 攻撃を受けた結果、9 月初旬、LockBit は将来同様の事態が発生することを避けるべくミラーサイトを導入しました。

ミラーサイトを導入した LockBit のブログ



「DDoS 攻撃と戦っている」ため、ブログに認証ページが表示されるようにしたと告げる LockBit の投稿

ランサムウエアにダメージをもたらしたアフィリエイトとフォーラム

内部情報の流出

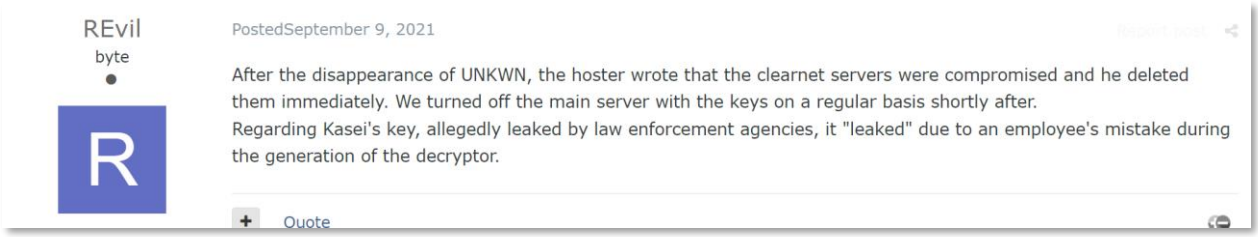
2021 年は、ランサムウエア・アズ・ア・サービス（RaaS）の人気が特に高まりましたが、RaaS はランサムウエアに関与するサイバー犯罪者たちにとって有益である一方で、彼らのオペレーションをリスクにさらす可能性もはらんでいます。ランサムウエアグループの内部情報がリークされた様々な事例でも確認されたとおり、ランサムウエアのサプライチェーンに関与するアクターの数が増えるにともない、内部の脅威の数も増加します。

2021 年 6 月、何者の仕業であったのかは明らかになっていませんが、**Babuk** のビルダーが VirusTotal にアップロードされました[29]。さらに 2021 年 9 月には事態をさらに複雑にするかのように、Babuk の開発者の一人であると自称するアクターが、Windows、ESXI、NAS 機器用ソースコードを XSS でリークしました。そしてこのリークにより、新たなランサムウエアグループが増加しました。報道によると、2021 年後半に登場したランサムウエアグループ **Rook** は、自らのマルウエアに Babuk のソースコードを使用していました[30]。そして 2021 年末にはその設計と暗号化面で Rook とわずかに異なる新バージョンのランサムウエア **Nightsky** が登場しました[31]。

[29] https://www.virustotal.com/gui/file/82e560a078cd7bb4472d5af832a04c4bc8f1001bac97b1574efe9863d3f66550/detection
[30] https://www.sentinelone.com/labs/new-rook-ransomware-feeds-off-the-code-of-babuk/
[31] https://twitter.com/vinopaljiri/status/1480059715392622597

Babuk のソースコードが XSS にリークされた投稿（ソース：XSS）

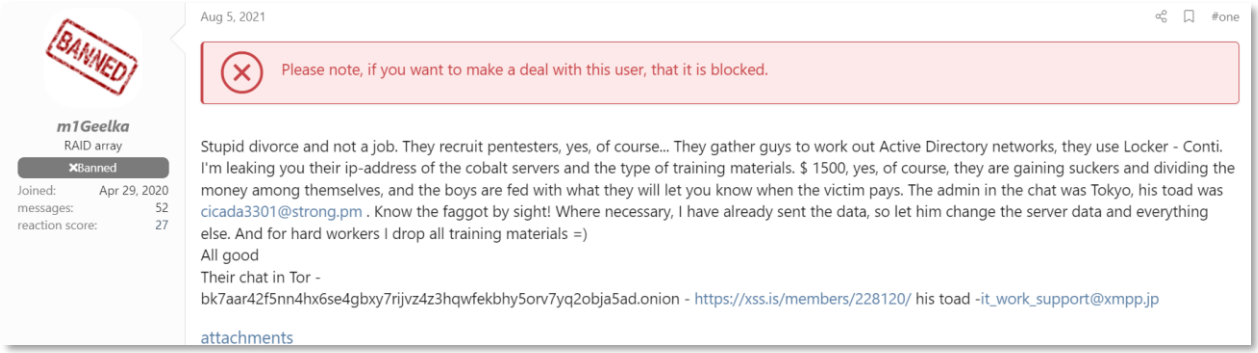
2021 年 7 月、Kaseya 社は **REvil** の攻撃でデータを暗号化されてしまったクライアント用の復号キーを、突如手に入れることができました。ユーザーREvil（別名 0_neday）はフォーラム Exploit にて、この事態は人為的ミス（コーダーの一人が間違えてクリックし、身代金を支払った被害者用に、個別の復号キーではなくユニバーサル復号キーを生成した）によって発生したと語っていました。



REvil の代表者が、Kaseya 社に復号キーが送られたのは人為ミスであると認めている投稿（ソース：Exploit）

2021 年 8 月には、**Conti** の「マニュアル」が脅威アクターm1Geelka によってフォーラム XSS にリークされるという事態が発生しました。m1Geelka は、Conti のオペレーターがアフィリエイトに毎月 1,500 米ドルを支払うと約束していたにもかかわらず、速やかに支払い

を実行しなかったことに失望していました。我々がこのマニュアルを入手して確認したところ、その中には被害者に関する情報の見つけ方からネットワークを暗号化してデータを窃取する方法にいたるまで、どのようにしてランサムウエア攻撃を成功させるかをアフィリエイトに教示する内容が記載されていました。



Conti のマニュアルを XSS でリークしている投稿（ソース：XSS）

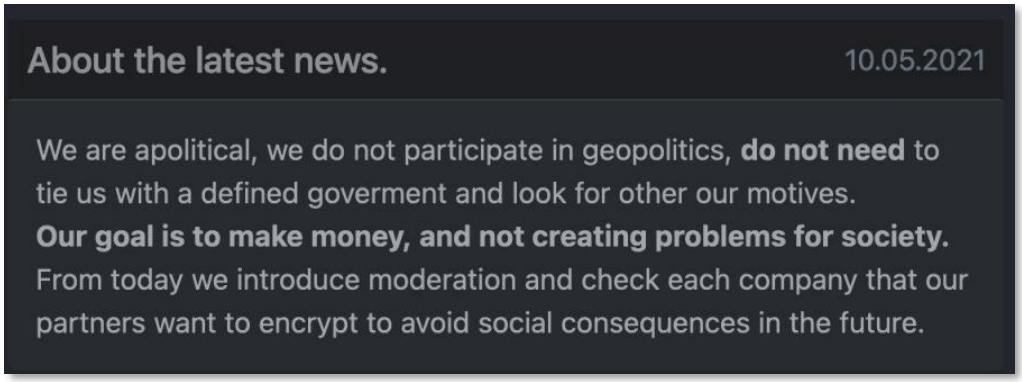
全般的にこういったリーク事件は、主にアフィリエイトがその原因となっており、RaaS モデルに伴うリスクの一部をより明確にしています。企業はその規模が拡大するにつれ、「人的要因」に対してより脆弱になりますが、我々は、そういった企業を攻撃する側であるランサムウエアのオペレーションにも同じことがあてはまると予想しています。

フォーラムに出されたランサムウエア禁止令

2021 年春、ロシア語話者の集うサイバー犯罪フォーラム XSS と Exploit の管理者が大胆な措置を講じました。「ランサムウエア禁止令」を出したのです。2021 年 5 月 7 日に Colonial Pipeline 社がランサムウエア攻撃を受け、業務と IT システムの停止を余儀なくされるという事態が発生しており、この禁止令はその余波によるものでした[32]。Colonial Pipeline 社に対する攻撃により、米国東海岸の燃料供給の約半分が遮断され、南東部ではガソリン不足が発生しました。**DarkSide** はこの攻撃に対する犯行声明を出しており、この事実については米

[32] https://www.colpipe.com/news/press-releases/media-statement-colonial-pipeline-system-disruption

連邦捜査局にも確認されています[33]。そして 2021 年 5 月 19 日、Colonial Pipeline 社は 440 万米ドルもの身代金を支払って復号キーを手に入れたことを公表しました[34]。



Colonial Pipeline 社に対する攻撃の 3 日後に出された DarkSide の声明――攻撃がアフィリエイトの犯行であったことを示唆している（ソース：DarkSide〔KELA アーカイブ内〕）

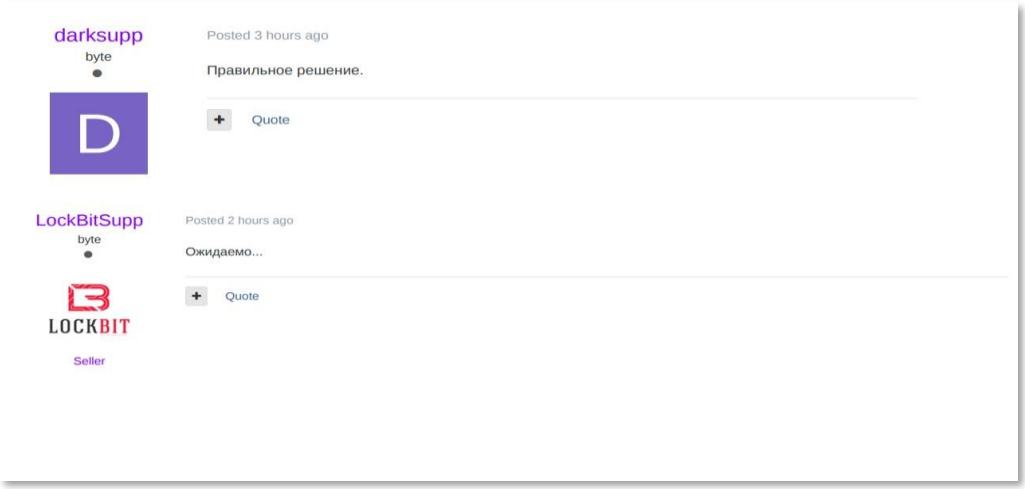
2021 年 5 月 14 日、DarkSide は米国からの「圧力」により活動を終了すると発表しました。この声明が出されたのは、国々がランサムウエア攻撃に対して行動を起こさなければならないとの声明を米国のバイデン大統領が発表した翌日のことです[35]。DarkSide は、自らのブログや支払用サーバーをはじめ、外部に公開されているインフラにアクセスできなくなったと述べていました[36]。

REvil の代表者は事後対応として、XSS と Exploit で自らのアフィリエイトに対する新たなルールを導入しました。このルールは、医療及び教育業界、政府機関への攻撃禁止し、またネットワークを暗号化する前には各被害組織について RaaS 管理者の承認を得るよう要求するものでした。一方 XSS と Exploit の管理者は、その後それぞれのフォーラムがランサムウエア活動と距離を置くことを決定しました。彼らの説明によると、ランサムウエア攻撃に

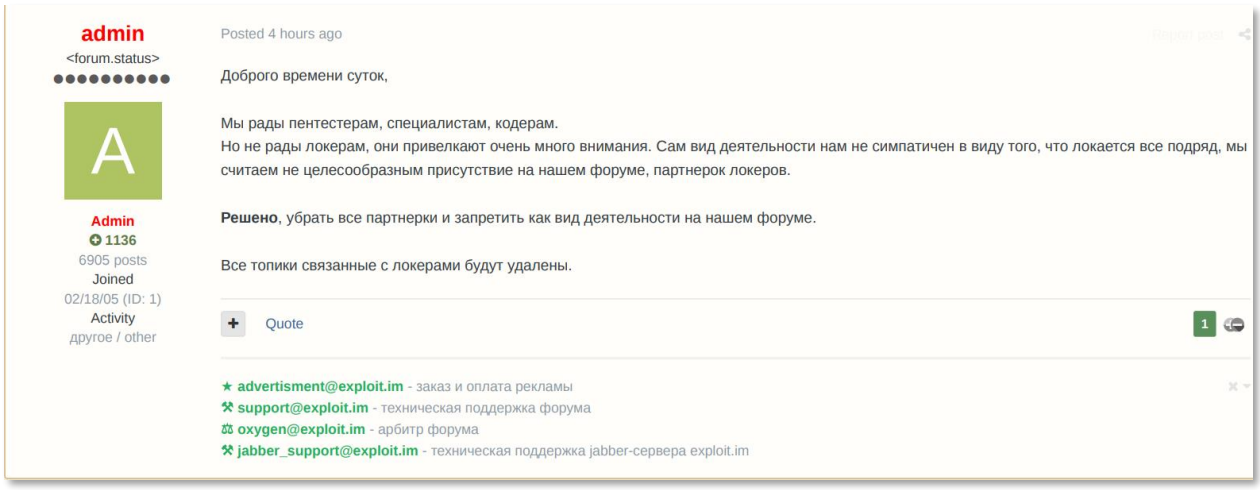
[33] https://www.fbi.gov/news/pressrel/press-releases/fbi-statement-on-compromise-of-colonial-pipeline-networks
[34] https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636
[35] https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/05/13/remarks-by-president-biden-on-the-colonial-pipeline-incident/
[36] https://www.nytimes.com/2021/05/14/business/darkside-pipeline-hack.html

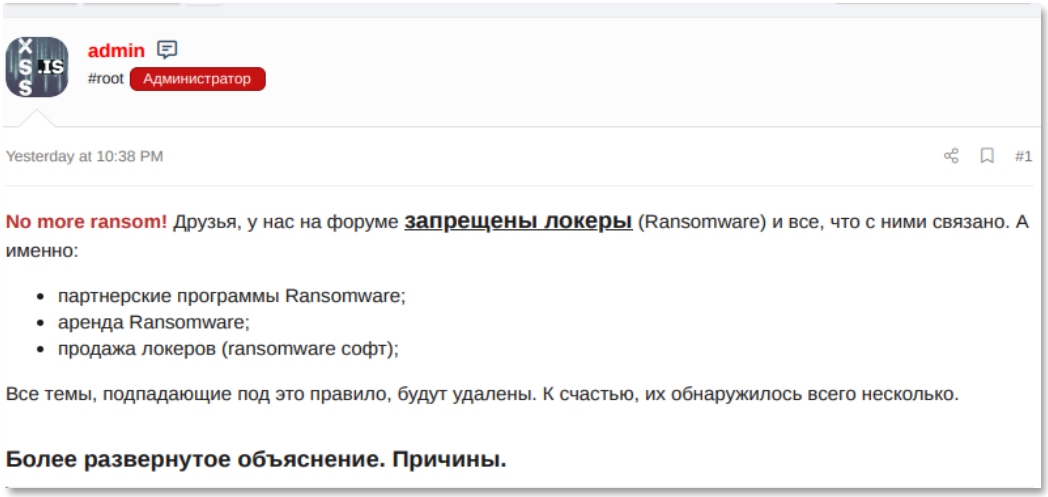
よって特に法執行機関やセキュリティ研究者からの余計な注目がフォーラムに集まっており、ランサムウエアを禁止したほうがユーザーとフォーラム両方にとって安全であるとのことでした。またサイバー犯罪フォーラムのユーザーたちも、ランサムウエアグループはすでにニュースなどの報道で十分な宣伝活動が行えており、他のサイバー犯罪者たちとの関係も確立できているのだから、彼らがこのランサムウエア禁止令で被害を被ることはないであろうという考えに同意していました。

なおこの禁止令は、実際にはランサムウエアアフィリエイトの募集とランサムウエアの販売・レンタルに関する活動のみをフォーラムで禁止するものでした。その結果、ランサムウエアアフィリエイトは、「ランサムウエア」という言葉さえ使わなければ、他の参加者と同様に引き続き XSS と Exploit でランサムウエア関連以外の活動に参加することができました。



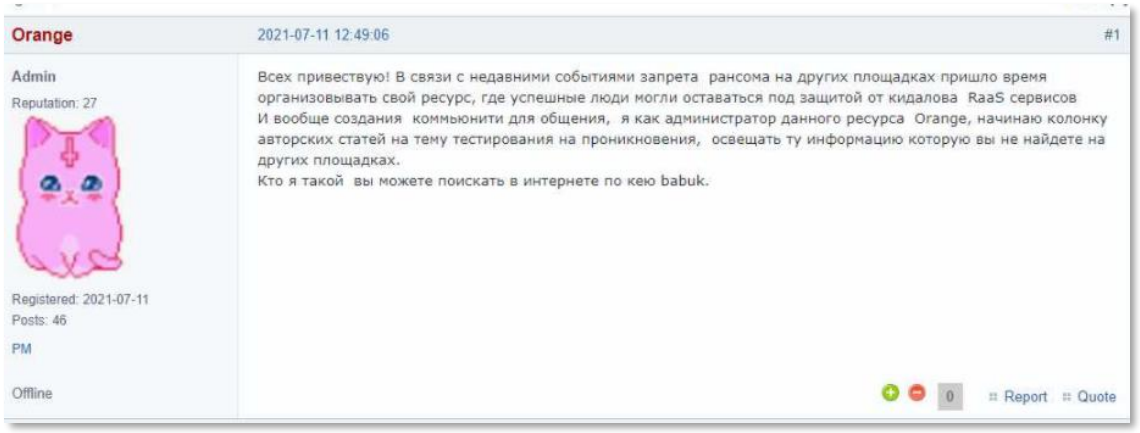
「正しい決断だ」、「予想していたよ」――ランサムウエア禁止令に対する DarkSide と LockBit の反応（ソース：Exploit）



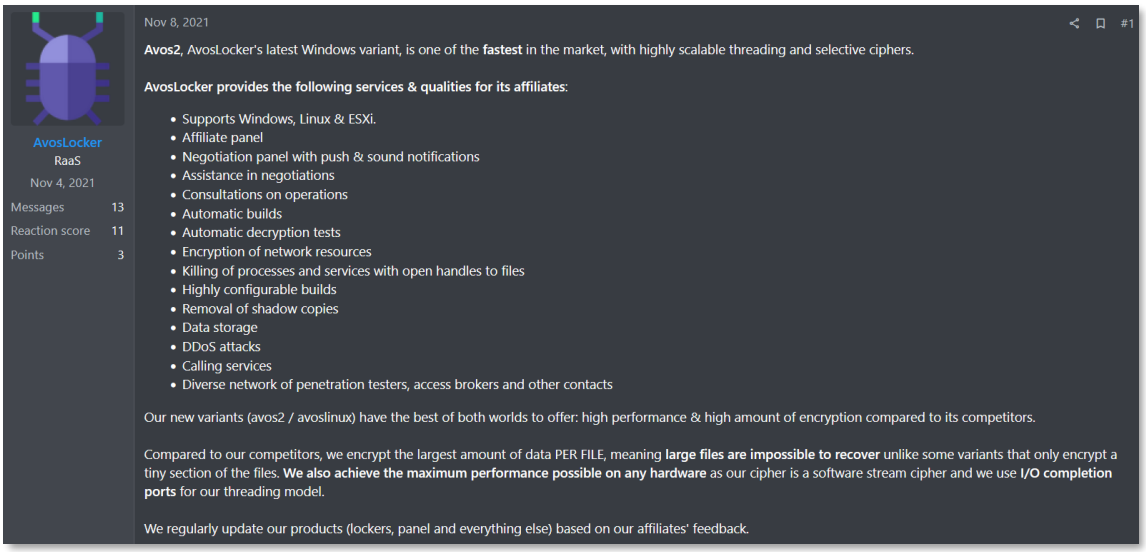


Exploit と XSS に出されたランサムウエア禁止令

こういった動きを受けて 2021 年 7 月、RaaS を歓迎するフォーラム RAMP が新たに誕生しました。RAMP ではランサムウエアアフィリエイトの募集も許可しており、ディスカッションや商品の取引にも「禁止」ルールに縛られずに参加することのできるプラットフォームでした。RAMP はその管理者が数回交代することはあったものの、依然ロシア語話者が集うその他のサイバー犯罪フォーラムの代わりとして活動を続けています。しかし我々が調査した結果、オペレーションをサポートするアフィリエイトを RAMP で募集していたのは数グループ（**Conti や AvosLocker**、**Alphv**）のみであることが確認されました。



フォーラム RAMP の管理者が掲載した最初の声明――このフォーラムの誕生とランサムウエア禁止令を関連付けている



RAMP に掲載されたランサムウエアグループ AvosLocker の投稿

我々は、2021 年第 2 四半期に出されたランサムウエア禁止令は、ランサムウエアプログラムがアフィリエイトを募集する点においても、アンダーグラウンドのサイバー犯罪社会で大きな役割を果たすという点においても、影響を及ぼしていないと判断しています。すでにランサムウエアオペレーションは最も収益性の高いサイバー犯罪「ビジネス」であるという評価を得ているため、大半のランサムウエアアクターは、特定のプラットフォームを使ってまでアフィリエイトを募集する必要はありません。

我々は、ランサムウエア関連のスレッドが禁止されたにもかかわらず、ランサムウエアアクターが現在も XSS や Exploit でネットワークのアクセスを購入し、ディスカッションに参加し、ランサムウエアオペレーションを最大化しようとマルウエアやツール、サービスなどを購入している状況を目撃しています。ランサムウエア攻撃者が構築したサプライチェーンは、サイバー犯罪のマーケットやフォーラムに著しく依存しており、その関係性については次のセクションで解説しているネットワークアクセスの売買を通じて解説してゆきます。

ランサムウエア攻撃者と初期アクセス・ブローカー

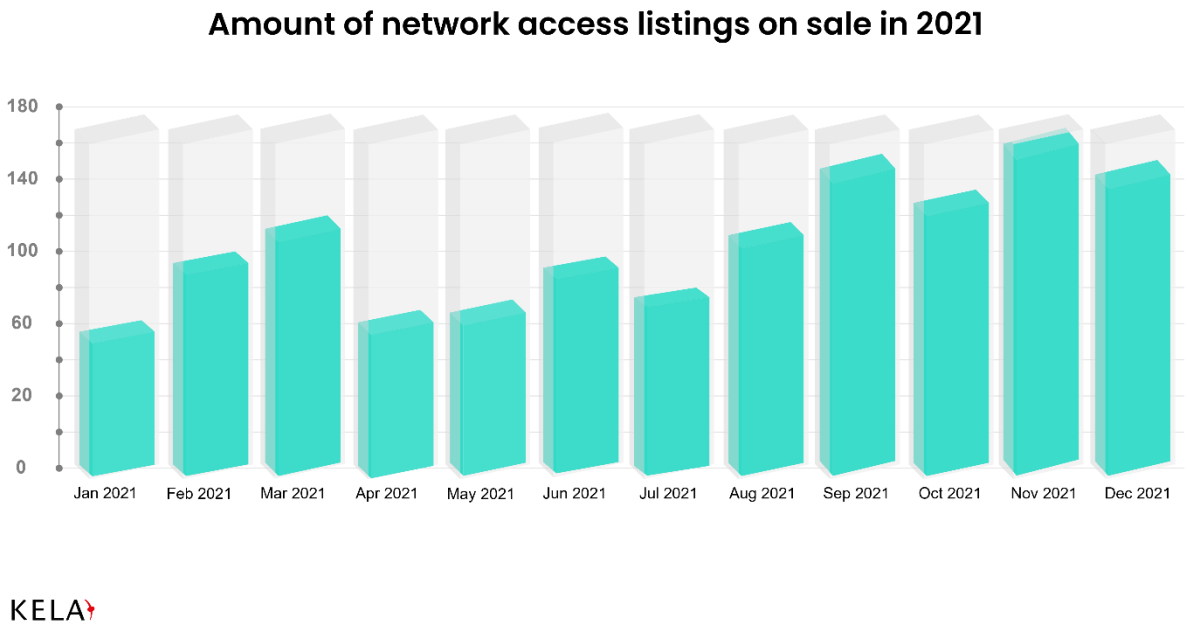
理想的なランサムウエア被害者

成功しているランサムウエア攻撃は、いずれも攻撃者が被害者に気付かれることなくネットワークへ侵入するところから始まっています。一部の攻撃者は、被害者のネットワークアクセスを秘密裡に入手していますが、サイバー犯罪フォーラムやマーケットで商品として販売されているアクセスを利用している攻撃者も存在します。

ランサムウエアアクターは、自分たちが理想とする被害者像に合致するネットワークアクセスを求めて、サイバー犯罪フォーラムの商品を積極的にチェックしています。そういった「商品」の一部は初期アクセス・ブローカーが販売しており、彼らはランサムウエア・アズ・ア・サービス（RaaS）エコノミーの中で重要な役割を果たしています。初期アクセス・ブローカーは、不正アクセス先の組織が所有するコンピューターへのリモートアクセス（ネットワークへの初期アクセス）を販売しており、彼らの活動がネットワークへの侵入を著しく容易にしていると同時に、無作為に行われる場当たり的なキャンペーンを標的型攻撃につなげる役割を果たしています。

2021 年には、約 300 人もの初期アクセス・ブローカーが 1,300 件を超えるネットワークアクセスを売りに出しました。我々の調査によると、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期間は平均 1 日から 3 日となっています。サイバー犯罪者は、500

米ドル（2021 年のネットワークアクセス価格の中央値。平均値は 4,600 米ドル）でネットワークアクセスを入手し、その後は好きなやり方で被害者にダメージを与えることが可能となります。そしてそういった事例のひとつとして、ランサムウエア攻撃が挙げられます。



2021 年に売り出されたネットワークアクセスの件数

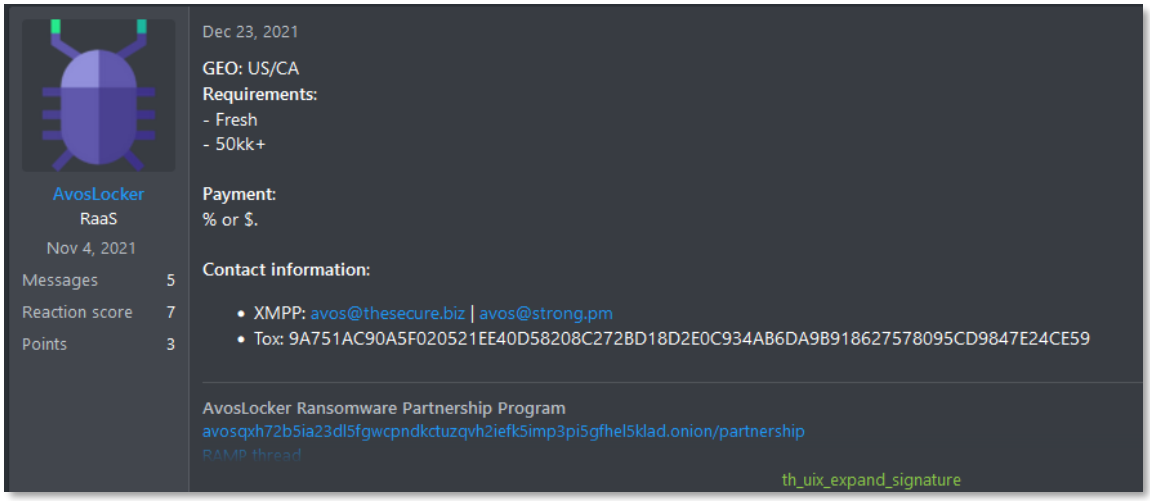
ランサムウエアアクターは、商品として売り出されているネットワークアクセスをフォーラムで探しており、初期アクセス・ブローカーに対しても、個人的（非公開）に自分たちに連絡を取ってネットワークアクセスを一定の条件で販売してくれるよう依頼する声明を発表しています。彼らは攻撃が成功した後で、一定の金額または利益の一部（最大で身代金の 10%）を料金として支払うというやり方を採用しています[37]。

我々は 2021 年 11 月から 12 月にかけて、アクターが RDP や VPN、その他ネットワークへ

[37] https://ke-la.com/ja/ransomware-gangs-are-starting-to-look-like-oceans-11/

のアクセスに利用可能なサービスに加え、オンラインショップの管理パネルやコンテンツ管理システム（CMS）、その他広範な種類のアクセスも購入する用意があると語っているスレッドのうち、アクティブであった 50 件超を観察しました。我々の調査の結果、これらのスレッドの最大 35%が、RaaS のサプライチェーンに関連するアクター（オペレーター、アフィリエイト、仲介者）によって作成されたものと思われます。

AvosLocker を例に挙げると、同グループは RAMP と Exploit で活動しており、ネットワークアクセスを購入する意思があることを表明していました。彼らは Exploit では「米国やカナダ、英国、オーストラリアに拠点を置き、1 億米ドル超の収益を持つ企業」へのアクセスを購入しようと狙いを定めており、一方 RAMP では要件を「収益 5,000 万米ドル超の米国またはカナダ企業」に絞り込んでおり、代金については特定の金額または身代金から一定の割合で支払うとの内容を両フォーラムに掲載していました。2021 年 9 月以降 AvosLocker は、ドメイン管理者権限が望ましいと主張するなど、スレッドの内容を定期的に更新しています。



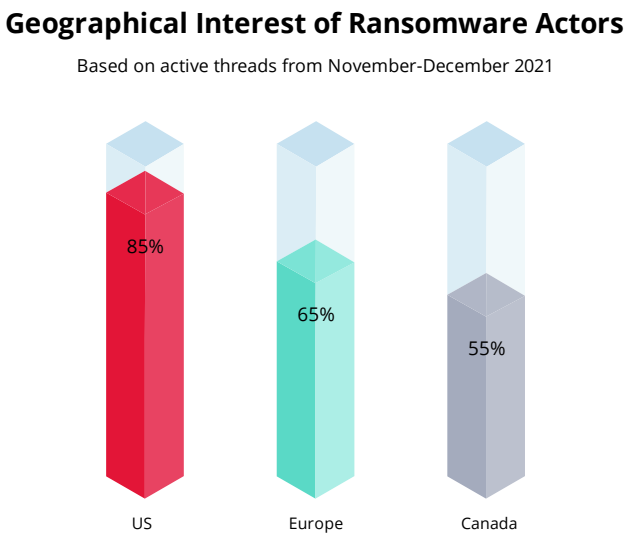
RAMP に掲載された AvosLocke の広告

脅威アクターは、初期アクセス・ブローカーから提供されるアクセスの持つ「可能性」をできるかぎり最大化するために、最高の収益、有望なロケーション、収益性の高い業界を探しています。我々は、ランサムウエアアクターが捜し求めている具体的な商品像を割り出すべく、過去数カ月にわたって彼らが定めていた要件の特徴を調査しました。

我々が 2021 年半ばに実施した同様の調査と比較したところ[38]、ランサムウエア攻撃者の求める条件は微妙に変化していることが判明しました。まず、理想とする被害者の地域を記載しているアクターの数が 30%増加していました。また人気のある地域についても、今回はカナダやオーストラリアと入れ替わって欧州が 2 位となりました（ただしほとんどのアクターが、希望する国をひとつに絞らず複数国挙げています）。

その他、アクターが考えているアクセスの最大予算額が増加していることも確認されました。2021 年 7 月に我々が行った調査では、脅威アクターは最大 10 万米ドルまで支払う用意がありましたが、2021 年 12 月には 2 名の脅威アクターが最大 100 万米ドルまで支払う場合もあると発言していました。また、ランサムウエア攻撃者の 35%は金額について言及しておらず、その代わりに身代金の一部を支払うとしていました。

[38] https://ke-la.com/ja/the-ideal-ransomware-victim-what-attackers-are-looking-for/



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 [39]

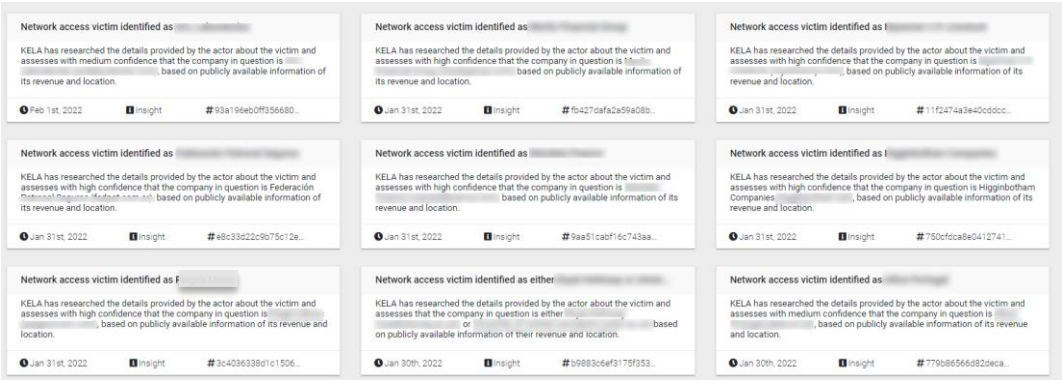
初期アクセス・ブローカーがネットワークアクセスを売り出す際、被害者の名前を明かすことはめったにありません。明かしてしまえば、セキュリティ研究者が侵入先となる企業に連絡を取り、不正アクセス経路を特定できるよう手助けし、無効にされる可能性があるからです。その代わりとして彼らは、以下の項目をはじめとする侵入先企業の特徴や性質を明記します。

- 収益
- 企業規模（従業員数）
- 業界
- その他の説明

[39] 2022 年 2 月 16 日に KELA のブログにて公開されている情報です: https://ke-la.com/ja/from-initial-access-to-ransomware-attack-5-real-cases-showing-the-path-from-start-to-end/

購入者となる脅威アクターらは、こういった情報を指標として活用することで被害者（侵入先企業）の価値を判断することができます。そしてありがたいことに、我々もこの指標を利用することで、中程度から高程度の信頼度で初期アクセス・ブローカーの被害者を 150 件以上特定することができました。

アクターcryzaa が、被害者の Zoominfo ページのリンクを投稿した某アクターにアドバイスしている投稿：「誰でも入手できる情報をフォーラムに投稿しても意味がない。それにフォーラムは監視されているんだぞ」（ソース：Exploit）

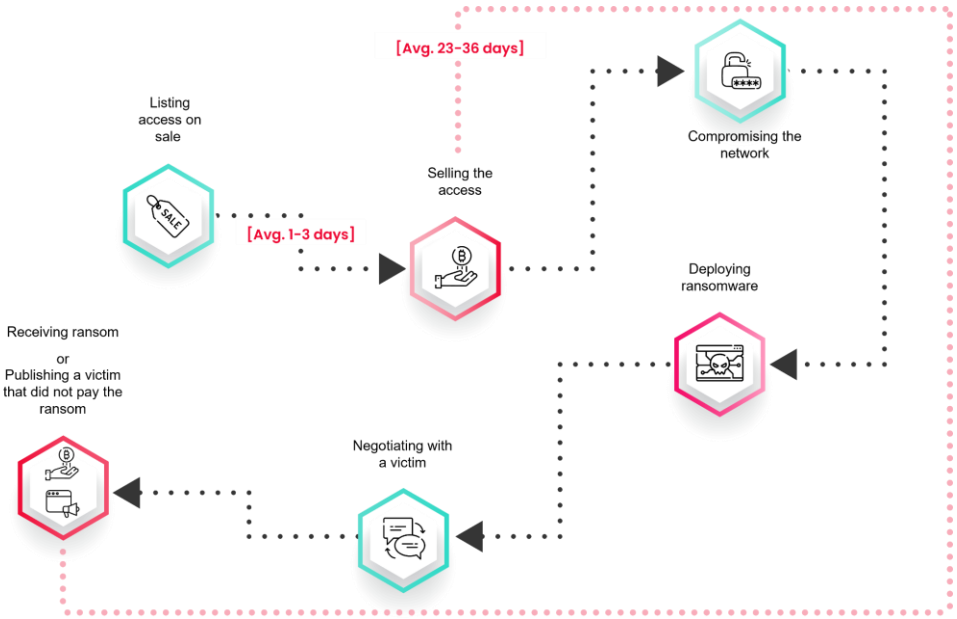


KELA が特定した被害者に関する最新のインテリジェンス

ネットワークアクセスの被害者とランサムウエア攻撃のマッピング

我々は、少なくとも5つのランサムウエアオペレーション（ほとんどは**LockBit**や**Avaddon**、**DarkSide**、**Conti**、**BlackByte** など、ロシア語話者グループが運営しているオペレーション）で、初期アクセス・ブローカーから購入したネットワークアクセスが使用されていることを突き止めました。我々はランサムウエアブログやデータリークサイトを日々監視していますが、売り出されるネットワークアクセスを並行して監視することで、初期アクセス・ブローカーとランサムウエアアクターの両方から不正アクセスされている企業を発見することが可能となります。また、両者から不正アクセスされている企業を発見した場合は、彼らが同じ被害者を標的としているのは単なる偶然の産物なのか、それとも各々の活動が一連の鎖となってランサムウエア攻撃という結果につながったのかを調査します。

また我々が、ネットワークアクセスが売り出された時点から攻撃にいたるまでの流れを様々な事例で観察した結果、企業がランサムウエア攻撃を受け、その後身代金交渉が失敗に終わり、ランサムウエアオペレーターのブログで企業名が公開されるまでの期間は 23 日から 36 日となりました。



ネットワークアクセスが売り出されてからランサムウエア攻撃に発展するまでの流れ

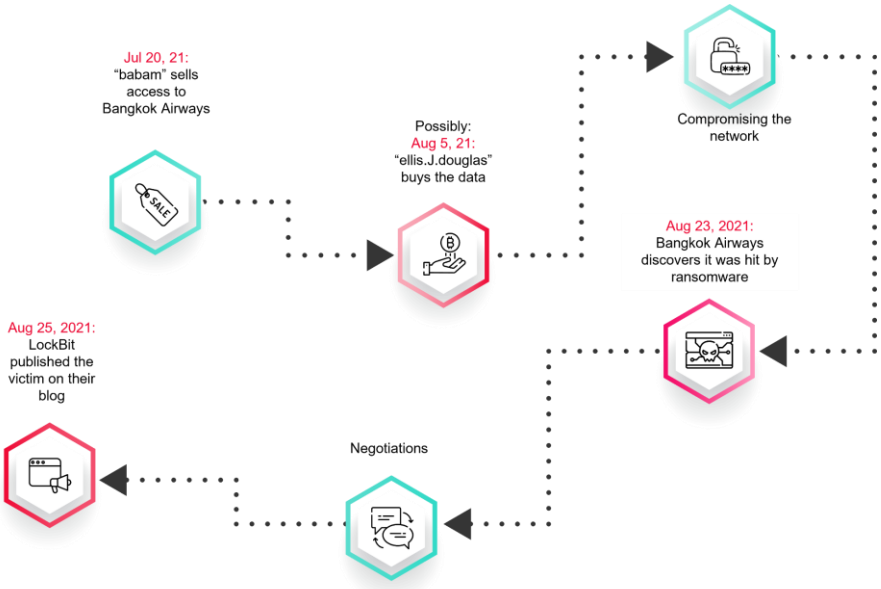
ここからは、実際の事例を数件取り上げて解説していきます（最後の 2 件の事例については、これまでに我々が公開した別のレポート「初期アクセス・ブローカーたちの間に生まれた 5 つのトレンド」でも取り上げています）。

Bangkok Airways 社への攻撃（LockBit）

2021 年 7 月 20 日、脅威アクターbabam が、タイの航空会社 Bangkok Airways 社のネットワークアクセス（Cisco 社の AnyConnect VPN 経由）を、開始価格 250 米ドル、即決価格 1,000 米ドルというオークション形式で売りに出しました。ただし、いつ誰がこのアクセスを購入したのかについては明らかとなっていません。その理由として、2021 年 8 月 5 日に脅威アクターellis.J.douglas がこのアクセスの即決価格を支払うと申し出たにもかかわらず、babam（アクセスの販売者）が公の場でこの取引を確定しなかった点が挙げられます。これは言い換えれば、ellis.J.douglas が即決価格を申し出るその前に、すでに babam が別の脅威アクターにこのアクセスを売却しており、そのために ellis.J.douglas との取引を確定できなかった可能性があることを示唆しています。その他に興味深い点として、同じ 8 月に ellis.J.douglas が、「アフィリエイトプログラムに参加して働き、分け前にあずかりたい」と述べていたことが挙げられます。ellis.J.douglas が言及しているこの働き方は、まさにランサムウエアオペレーションの在り方と共通する部分があります。なお、ellis.J.douglas は当初、初期アクセス・ブローカーとしてフォーラムで活動していましたが、後にアクセスを購入する側へと立場を転じました。

購入者が誰であったのかはさておき、Bangkok Airways 社へのアクセスが売り出されてから 1 カ月も経過していない 2021 年 8 月 23 日、同社はランサムウエア攻撃を受けていることに気が付きました[40]。そしてその 2 日後、Bangkok Airways 社の名がランサムウエアオペレーターLockBit のブログに掲載されました。Bangkok Airways 社は調査の詳細を公表していませんが、上述の一連の出来事を時系列で検討してみると、同社へのランサムウエア攻撃は babam から購入したアクセスを使って行われた可能性が高いと考えられます。

[40] https://www.bangkokair.com/press-release/view/clarifies-the-incident-of-a-cybersecurity-attack



ネットワークアクセスが売り出されてから Bangkok Airways 社への攻撃に発展するまでの流れ

アクター babam が Bangkok Airways 社のものと特定されたアクセスを売りに出した投稿

Bangkok Airways 社を攻撃したと主張する LockBit のメッセージ

米国の製造企業への攻撃（Conti）

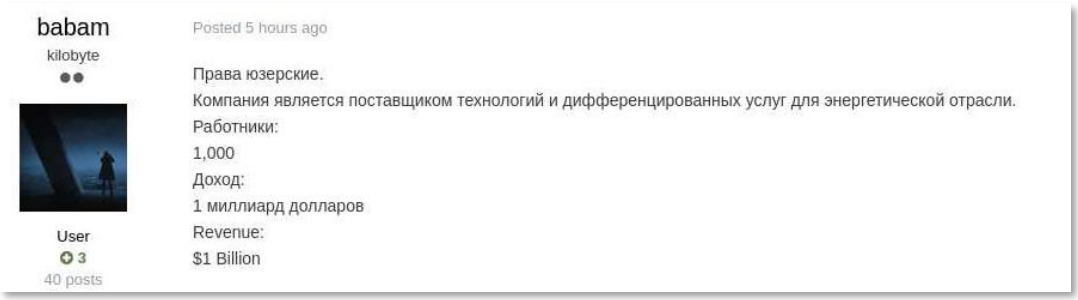
2021 年 9 月 30 日、脅威アクターbye47 が、米国に拠点を置く某製造企業へのアクセス（VPN 及び RDP 経由）を売りに出しました。しかしこのアクセスに興味を持つ者はいなかったため、bye47 は数段階に分けて価格を下げていきました。そして 2021 年 10 月 8 日、脅威アクターframework がこのアクセスを 800 米ドルで購入しました。framework は、これまで主にマルウエアやエクスプロイト、ツールを購入しており、その一方で framework 自身も販売者としてネットワークや窃取したアクセスを悪用するサービスを提供していました。

そして 2 週間と数日が経過した 2021 年 10 月 25 日、ランサムウエアオペレーターConti が、この製造企業の名を自らのブログで公開し、11 月には同社から窃取したデータを公開し始めました（しかし不思議なことに、Conti は同社から窃取した全ての情報までは公開しませんでした）。

Gyrodata 社への攻撃（DarkSide）

2021 年 1 月 16 日、前述の初期アクセス・ブローカーbabam が、Gyrodata 社のものと思われるネットワークアクセスを売りに出しました。その後の 2021 年 1 月 18 日には、babam がこのアクセスが売却済みとなったことを宣言し、2021 年 2 月 20 日には DarkSide のオペレーターが、同社に不正アクセスしたと主張する投稿を自らのブログに掲載しました。

Gyrodata 社がこのインシデントについて調査を行った結果、2021 年 1 月 16 日頃から 2021 年 2 月 22 日頃にかけて、権限のないアクターが同社内にある特定のシステムとその関連データに複数回アクセスしていたことが判明しました。この日付は我々の調査結果とも一致しています。



某アクターが Gyrodata 社のものと特定されたアクセスを売りに出した投稿

アラブ首長国連邦の鉄鋼製品企業への攻撃（Avaddon）

2021 年 3 月 8 日、我々は、脅威アクターthyjew がアラブ首長国連邦に拠点を置く某鉄鋼製品企業の初期アクセスを売り出したことを検知しました。そしてその 3 週間後となる 2021 年 3 月 31 日、ランサムウエアオペレーターAvaddon のブログに同社の名が掲載されました。

企業のネットワークアクセスが売り出されてからランサムウエア攻撃に利用されるまでのプロセスを考察すると、企業のネットワーク防御を担当される皆様がその事態に気付き、対応を取ることのできる時間は非常に限られています。脅威アクターが初期アクセスを購入してランサムウエア攻撃を実行するまでの期間は、通常 1 カ月未満です。また初期アクセスが売り出されてしまった場合、そのアクセスが買い取られてしまう前に自社ネットワークの侵害を把握するために残された時間は、わずか 1 日から 3 日です。我々は、ランサムウエア攻撃の増加と連動して、2022 年も引き続き初期アクセス・ブローカーの人気が高まるものと評価しています[41]。

[41] ネットワークアクセスはランサムウエア攻撃以外の悪意ある活動にも使用されており、様々なサイバー攻撃を事前に阻止するためには、販売されているアクセス商品を監視することが非常に重要であるという点にご留意ください。

結論

2021 年、ランサムウエアグループは様々なサイバー犯罪者を雇い、洗練された技術を採用し、拡大するサイバー犯罪のエコシステムを幅広く活用する「サイバー犯罪企業」へと進化しました。KELA は、ランサムウエアの脅威が 2022 年も増加し、その一方で法執行機関のオペレーションが強化されていることを受けて、ランサムウエア攻撃者が高度な TTP（戦術・技術・手順）を採用するであろうと予想しています。

企業においてネットワークの防御を担当される皆様がランサムウエアグループや類似の攻撃者に立ち向かうにあたっては、以下の 3 つの活動に投資することが求められます。

1. 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。サイバーセキュリティ・トレーニングについては、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です。

2. 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。

3. 主要な資産に的を絞って自動モニタリング・ソリューションで監視することにより、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が、アタックサーフェス（攻撃対象領域）を常に最小限に抑えることに大きく貢献し、最終的にはサイバー攻撃の阻止へとつながります。

KELA と KELA のサイバー犯罪脅威インテリジェンスプラットフォームについて

KELA は、あらゆる組織や企業を未知のサイバー脅威に対する不安から解放します。我々は、自動化された脅威インテリジェンステクノロジーと専門家の有する深い知識を融合して、それぞれのお客様にとって最適かつ実用的な脅威インテリジェンスをご提供しています。世界中のお客様から高い信頼を受けた KELA のソリューションが、アンダーグラウンドのサイバー犯罪社会を深淵まで調査し、皆様の業務を軽減するとともに的を絞った事前の防御を実現します。

業界トップクラスを誇る KELA のサイバー脅威インテリジェンスプラットフォームは、アクセスすることが最も困難とされるソースに潜入して、情報の収集、分析、監視を自動実行し、アンダーグラウンドのサイバー犯罪社会に出現した脅威をアラート通知するエンドツーエンドソリューションです。お客様の多様なニーズに合わせてご利用いただけるよう、それぞれの目的に特化した 3 種類の製品をご用意しております。

KELA の DARKBEAST は、ダークウェブを匿名で深堀調査・分析したり、高度な調査を行う目的でご利用いただけるソリューションです。我々は、長年をかけてダークウェブから収集した豊富なデータを独自のセキュアなデータレイクに保存しており、DARKBEAST をご利用のお客様にご自由にご利用いただいております。また、組織のネットワーク防御を担当される皆様が、サイバー攻撃のトレンドに関する知見を背景情報と併せてリアルタイムに入手し、サイバー攻撃者のプロファイルを調査・把握するための一助としてもご活用いただけます。KELA の監視・分析ツール RADARK では、それぞれのお客様の条件に合わせたリアルタイムなダークウェブ監視機能を実現するとともに、潜在的脅威の概要を明確に示し、脅威への対応策をカスタマイズしてご提案することで、お客様のインテリジェンス調査が次の段階へ発展するよう支援します。また、中小企業様や MSSP 様向けにご提供しているアタックサー

フェス・インテリジェンスソリューション INTELACT では、リアルタイムに送信される効率的なアラートと、背景情報を取り入れた実用的なインテリジェンスを併せてご提供することで、サイバー脅威の検知機能をさらに強化し、お客様が脅威に対処するとともにサイバーアタック・サーフェスを常時最小化できるようお手伝いします。

これらの製品を連携して活用することで、サイバー脅威の検知、無力化、分析を行う完全な脅威インテリジェンスプラットフォームとして機能する「お客様専用の SWAT チーム」としてご利用いただけます。KELA は、アンダーグラウンドに広がる混沌としたサイバー犯罪社会から重要な脅威を手動で検出するといった果てしない作業や、誤検知により大量発生するアラート疲れからお客様を解放し、自らの組織に関連する重要なサイバー脅威への対応のみに専念していただけるようご支援いたします。

DARKBEAST の 14 日間無料トライアルに今すぐお申込みください。