



2025年版 ThreatLabz ランサムウェア レポート

目次

本書の要旨	3	2025～2026年に警戒すべきランサムウェア ファミリートップ5	24
主な調査結果	4	#1 Dark Angels	24
ランサムウェアの状況：主な傾向と標的	6	#2 Clop/CIOp	25
ランサムウェア攻撃は過去最多を記録	6	#3 DragonForce	26
データの持ち出しは92.7%増	7	#4 Akira	26
主な標的国と地域別の概況	11	#5 Interlock	27
2024～2025年に最も活発だったランサムウェア グループ	14	ThreatLabzによるランサムウェア メモのアーカイブ	28
新たに確認されたランサムウェア グループ	15	2026年の予測	29
ランサムウェア キャンペーンに悪用される主な脆弱性	16	ランサムウェアを阻止するZscalerのゼロトラスト+AI	31
ランサムウェアの総括：注目のニュース	17	ランサムウェア対策チェックリスト	33
ChatGPTを犯罪活動に悪用するBlack Basta	17	調査方法	35
ランサムウェア攻撃者からのなりすまし電話：多段階攻撃の実態	18	ThreatLabzについて	35
LockBitのデータベース漏洩：ダークWebの侵害から明らかになったRaaSの裏側	20	Zscalerについて	35
医療業界を襲う脅威：大規模なデータ窃取の増加	22		
ランサムウェア対策の新たな流れ：サイバーセキュリティの最前線	23		

本書の 要旨

ランサムウェアは長年にわたって存在する脅威であるものの、攻撃者の活動は絶えず変化しています。現代のキャンペーンはより標的を絞って展開され、自動化および効率化されています。生成AIの使用拡大もこの変化の一因となっており、フィッシングコンテンツの作成やマルウェア開発まで、あらゆる側面が強化され、加速しています。そして、この進化がランサムウェア攻撃の著しい増加と影響拡大につながっています。

2024年4月から2025年4月にかけて、Zscalerクラウドでは過去最高となる1,080万件以上のランサムウェア攻撃の試みがブロックされました。前年比で145.9%の増加となり、追跡開始以来最も多い件数を記録しました。同時に、ランサムウェアリークサイトに掲載された組織の数は70.1%増加し、広い範囲で脅迫による攻撃へのシフトが起こっていることが浮き彫りになりました。現代のキャンペーンは高い頻度で大規模に展開され、ターゲットに対し最大限の優位性を確立する設計になっており、多くの場合、暗号化を必要としません。暗号化を完全に放棄し、純粋なデータの窃取のみに走るランサムウェア攻撃者が増えており、この変化を反映するように、過去1年間に持ち出されたデータ量は92.7%の増加となっています。

エンドゲーム作戦のような解体活動が展開され注目を集めるなか、ランサムウェアグループの活動に減速の気配は見られません。むしろ、こうした活動が新たな手口を生む原動力になっている可能性があります。このレポートの分析期間中には、34の新たなランサムウェアファミリーが出現しました。一方、DragonForce、Akira、Clopなどの確立されたグループが上位を占め、成熟したランサムウェア活動の回復力を示す形となりました。

2025年版 Zscaler ThreatLabzランサムウェア レポートでは、これらの動向や調査結果について詳しく分析しながら、最も標的にされた業界と地域、警戒すべきランサムウェアファミリー、攻撃手法の進化、防御者向けの実用的なガイダンスを紹介していきます。なお、ThreatLabzでは、ランサムウェア攻撃からの回復を支援するカスタムツールの構築、大規模なマルウェアやランサムウェアのエコシステムの解明と解体を目指す世界的な取り組みの支援など、世界中の組織を保護するため積極的な役割を果たしています。脅威の追跡結果とあわせて、ぜひご確認ください。



主な 調査結果

ランサムウェア攻撃の試みは、前年比で**145.9%増加**し、過去3年間で最も大幅な増加を記録しました。

10の主要ランサムウェア ファミリーによる**データの持ち出しは前年比92.7%増加となる238.5テラバイト(TB)**に達し、広い範囲にわたってデータの窃取が主要な脅迫戦術にシフトしていることを示唆しています。

データ リーク サイトの分析によると、**公開された脅迫事例は70.1%増加**しており、暗号化のみよりも信用失墜や規制上のリスクが絡んだ方が圧力が高まるケースが多いことを示しています。

最も標的となった業界は製造、テクノロジー、医療で、石油/ガス業界を狙った攻撃は935.3%増加しました。



世界最大の標的国は引き続き米国で、全体の50.8%を占めています。米国に次いで多かったのはカナダ、英国、ドイツ、インドでした。

ランサムウェアの脅威アクターは生成AIで攻撃を強化しており、フィッシング コンテンツの迅速な作成、悪意のあるコードの記述、データ抽出の自動化などに悪用しています。

最も活発なランサムウェア ファミリーはRansomHub (833件)、Akira (520件)、Clop (488件)で、これらが大きな割合を占めています。

ビッシング(ボイス フィッシング)を取り入れたランサムウェア攻撃が増加しており、攻撃者は音声を使用することで信頼性を高め、効果的に初期アクセスを取得しています。

ThreatLabzは分析期間中に34の新しいランサムウェア ファミリーを特定し、調査開始以降、追跡対象となったランサムウェア ファミリーの合計は425となりました。

ランサムウェアの活動は増加しているものの、法執行機関が主導する活動はZscaler ThreatLabzのような業界の専門家の支援の下で大きな成果を上げており、エンドゲーム作戦では主要なランサムウェアのインフラ解体に成功しています。

ランサムウェアの状況：

主な傾向と標的

ニュースになるような侵害事例は、ランサムウェアが世界規模で展開されていることを示していますが、最も有益なインサイトは、脅威アクターが用いる標的の選定パターンや戦略上の行動をキャンペーン全体にわたって分析することで得られます。

このセクションでは、ニュースになるような侵害事例だけにとどまらず、ランサムウェアが最も大きな影響を与えている業界や地域、攻撃を主導しているランサムウェアファミリーについて詳しく見ていきます。また、過去1年間に出現した新しいグループについても取り上げます。

ランサムウェア攻撃は過去最多を記録

ランサムウェアの活動が着実に増加していることはもはや驚くべきことではありませんが、最新のデータは攻撃の劇的な増加を示しています。Zscalerクラウドでブロックされたランサムウェア攻撃の試みは前年比で145.9%増加し、2021年の6倍に増加しています。このデータは、量的な増加を反映しているだけでなく、影響の大きい環境を標的とした、より迅速で計画的なキャンペーンへのシフトが起こっていることも示唆しています。

セキュリティ部門にとって、ランサムウェアの戦術は概ね馴染み深いものかもしれませんが、最近のキャンペーンの拡散規模、精度、運用効率の向上は進化を示しています。生成AIの台頭を一因として、ランサムウェア攻撃はサイバー犯罪のビジネスモデルとしてより洗練されたスケーラブルなものへと加速的に進化しています。

10,887,030

2024年4月～2025年4月

+145.9%

4,426,966

2023年4月～2024年4月

3,756,858

2023

2,727,114

2022

1,502,175

2021

図1： Zscalerが1年間でブロックしたランサムウェア攻撃

データの持ち出しは 92.7%増

過去1年間で、ランサムウェア攻撃におけるデータの窃取は、補助的な行動から主要なイベントへと変化しており、暗号化だけを最終目的としないケースが増えています。脅威アクターは、圧力を強め、身代金を支払わなかった場合の被害者のリスクを高めるために、大量のデータを盗み出しています。

最近のデータの持ち出しの増加はこの傾向を反映しています。ThreatLabzの分析によると、盗まれたデータの合計は10の主要なランサムウェアグループ全体で前年より増えています。持ち出されたデータの合計は、123.8 TB (2023年4月～2024年3月)から92.7%増加し、238.5 TB (2024年4月～2025年3月)となりました。なお、2023～2024年の期間には単一の侵害で100 TBのデータが盗まれた事例が存在しますが、これはデータセット全体の中で最大の規模であり、年間の合計に大きな歪みが生じるため除外しています。この外れ値を除去することで、データ窃取のより広範な傾向をいっそう正確に把握できます。

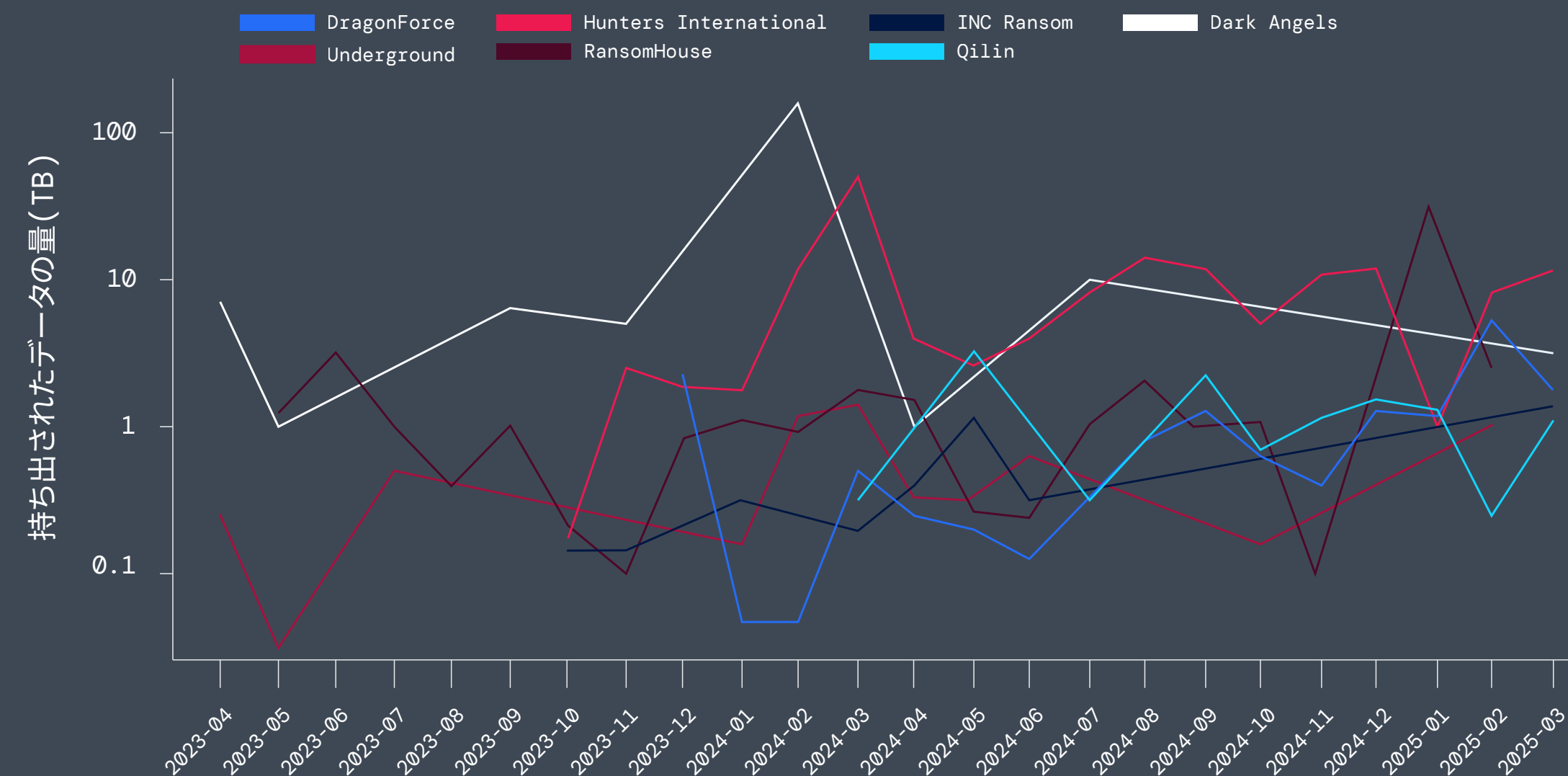


図2: 主なランサムウェアグループによるデータの持ち出し

- **Hunters International:**盗んだデータの合計は、前年の37.7 TBから224.3%増の122.1 TBとなっています。被害を受けた組織1件あたりのデータ流出量の中央値も、前年の約300 GBから19.6%増加し、359 GBとなりました。次のセクション(「データ脅迫のみへの移行」)では、このグループがファイルを暗号化するアプローチから完全に移行した経緯について見ていきます。
- **DragonForce:**持ち出したデータの合計量は前年の4.2 TBから382.6%増の20.3 TBとなり、最も高い増加率を見せました。中央値はほぼ横ばい(微減)でしたが、合計量が増加していることから、このグループがより多くの組織を侵害していることがうかがえます。
- **Dark Angels:**被害組織1件あたりの影響の中央値は2.15 TBから132.6%増の5 TBとなり、最も高くなりました。全体の件数は減少しているものの、大規模で高価値な標的への攻撃に注力し続けていることがわかります。
- **RansomHub:**2024年4月から2025年3月までに持ち出したデータの合計は前年比86.2%増となる22.4 TBに達しました。被害を受けた組織1件あたりのデータ流出量の中央値は、前年の50 GBから118 GBに増加し、2倍以上となりました。
- **RansomHouse:**盗んだデータの合計は前年の17.2 TBから83.1%増の31.6 TBとなりました。被害を受けた組織1件あたりのデータ流出量の中央値も425 GBから500 GBに増加しました。

データ脅迫のみへの移行

2024年版 Zscaler ThreatLabzランサムウェア レポートでは、同年初めにFBI主導の作戦でランサムウェア グループ「Hive」のインフラが押収された後、このグループが2023年10月に「Hunters International」にリブランドした経緯を調査しました。Hunters Internationalは出現以来、非常に活発に活動しており、暗号化よりもデータの窃取に重点を置いています。活動開始以来、このグループが盗んだデータ量は約160 TBに上ります。Hunters Internationalの被害を受けた組織1件あたりのデータ流出量の平均値は698 GB、中央値は317 GBでした。図3は、結成以来このグループによって盗まれた1か月あたりのデータ量の推移を示しています。

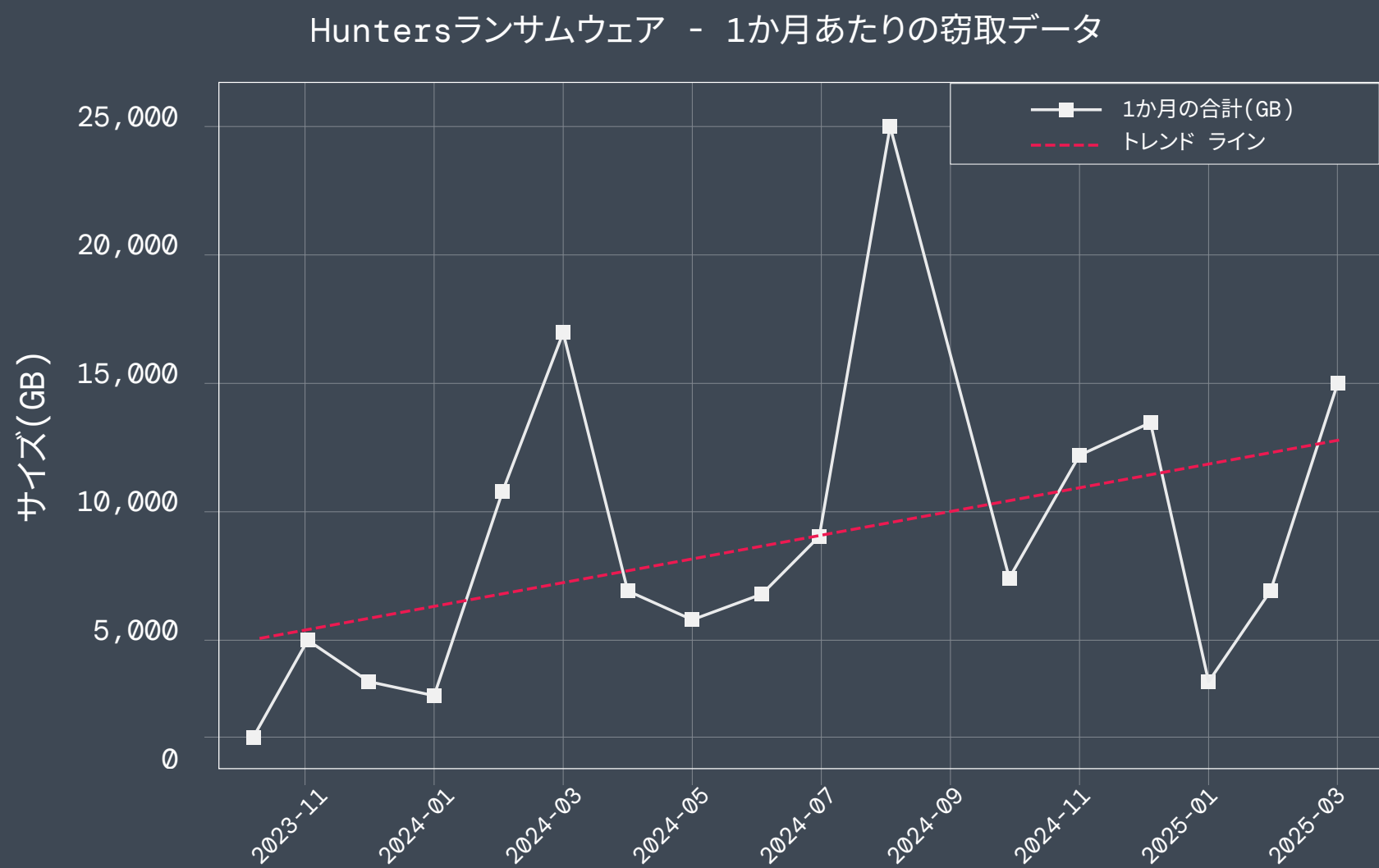


図3: Hunters Internationalによる1か月あたりのデータ窃取の量(GB)

2025年5月、World Leaksというブランド名で新たなグループが登場し、データの窃取のみに焦点を当てた、ランサムウェアを展開しない攻撃が実行されました。World Leaksのサイトは、見た目もプログラムもHunters Internationalに類似しており(図4参照)、背後に同一の組織が存在する可能性が高いと考えられます。

World Leaksは2025年5月に攻撃活動を開始して以来、25 TB以上のデータを盗み出しています。盗まれたデータ量に関する統計値はHunters Internationalと非常に近似しており、被害を受けた組織1件あたりのデータ流出量の平均値は769 GB、中央値は452 GBです。

なお、Hunters Internationalは2025年7月3日にリーク サイト上のメッセージを通じて閉鎖を発表しました。活動を終了し、無料の復号ツールを提供すると主張しています(図5)。

ファイルの暗号化からデータの窃取への転換は前例のないことはありません。BianLianやClonなどの他のグループも、ランサムウェアからデータ脅迫へと方向転換しています。この傾向については、このレポート後半でさらに詳しく解説します。

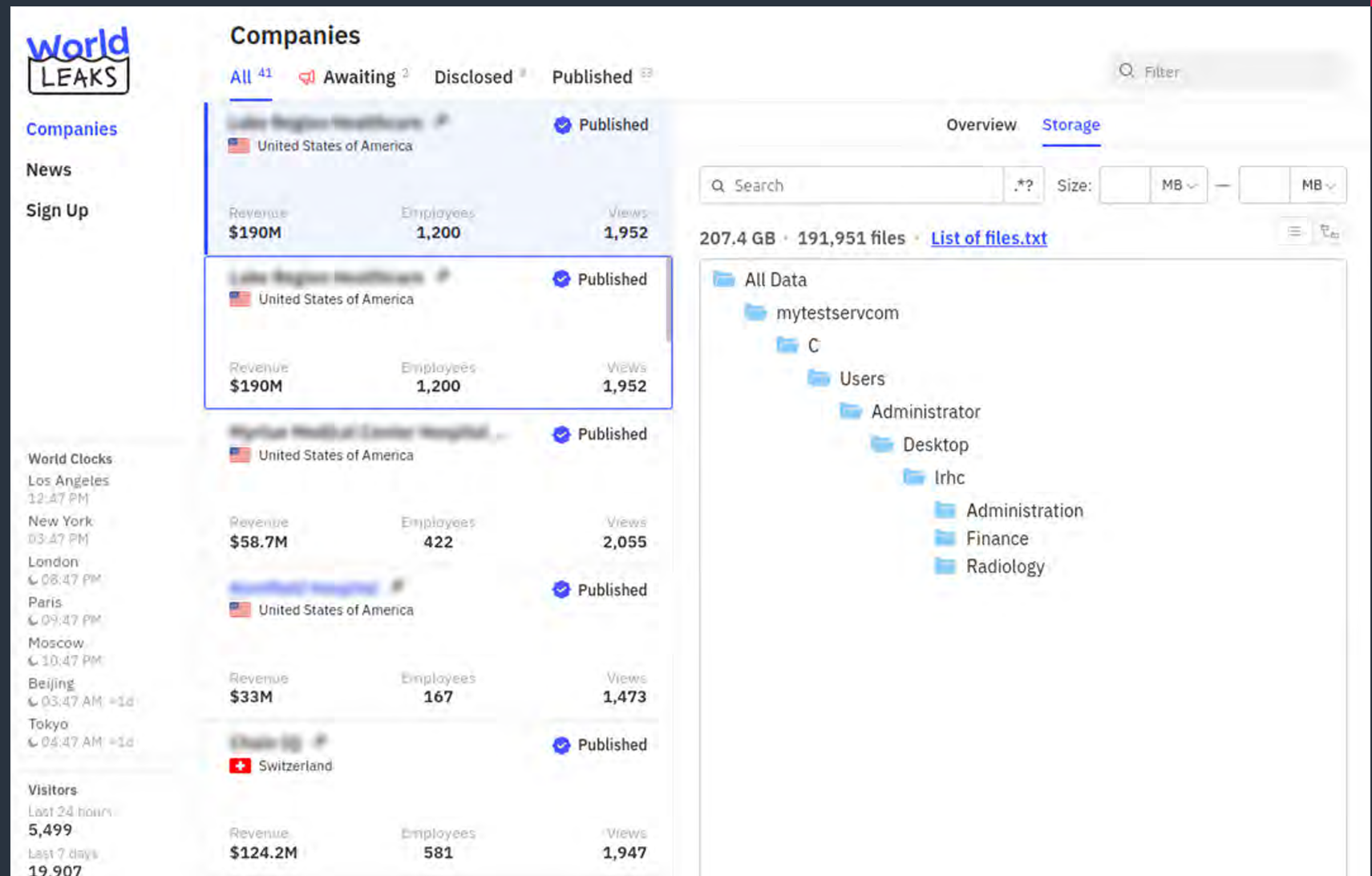


図4: ランサムウェア グループ「World Leaks」のWebサイト

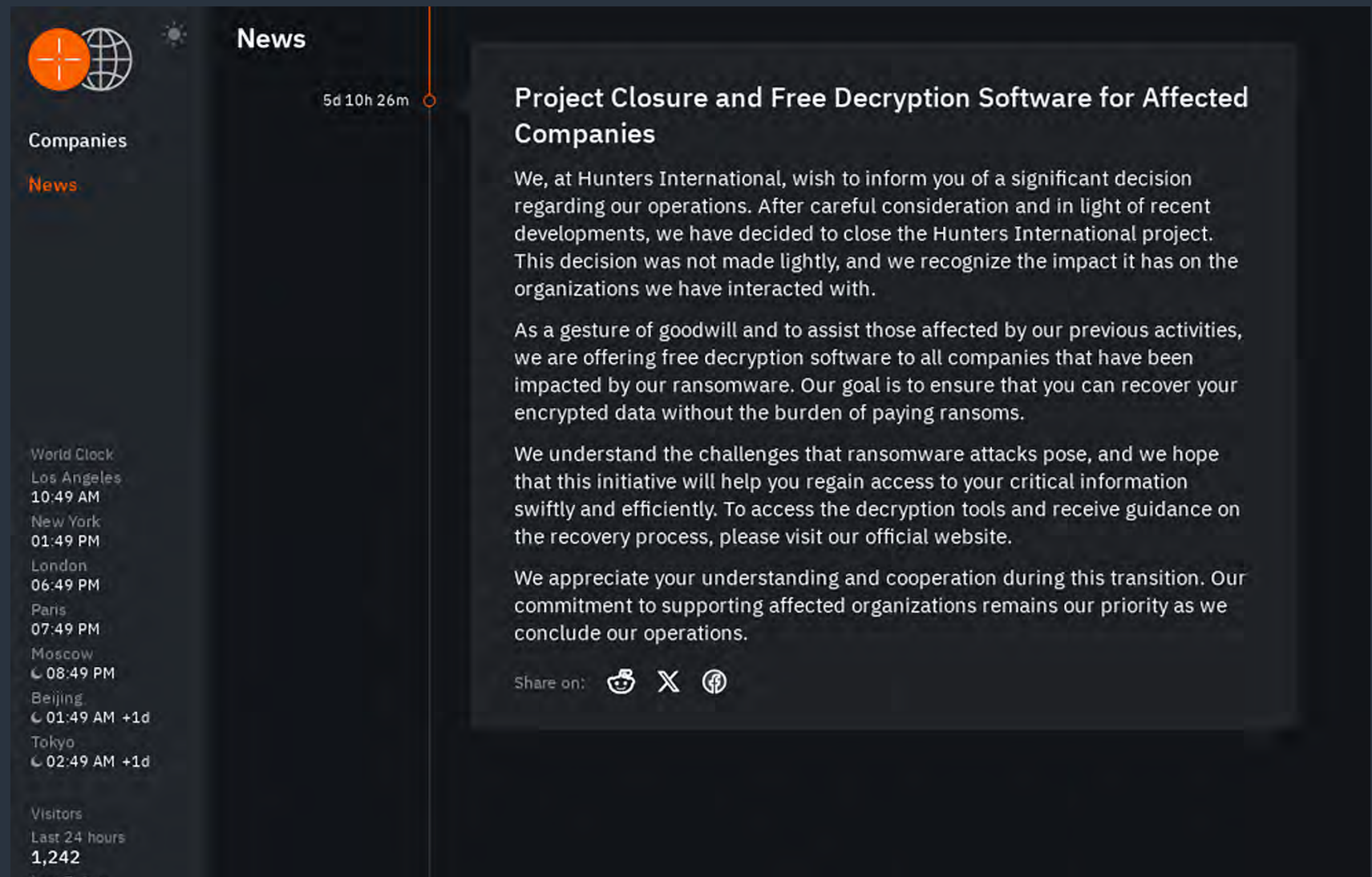


図5: Hunters Internationalの活動停止に関する声明

最も多くの攻撃を受けている業界

攻撃者は、身代金の支払い圧力が最も高くなる業界を優先的に狙い続けています。業務中断の可能性、盗まれたデータの機密性とそれに伴う信用失墜の可能性、規制上のリスクなどが高い業界が標的となっています。

図6は、リーク サイトのデータに基づき、ランサムウェア インシデントの件数を業界別に示したものです。脅威アクターによるデータの持ち出しと脅迫が確認された攻撃についての概況がうかがえます。製造、テクノロジー、医療は依然として最も頻繁に標的とされる業界であり、脅迫や優位性の利用に好都合な高リスクの環境であることがわかります。

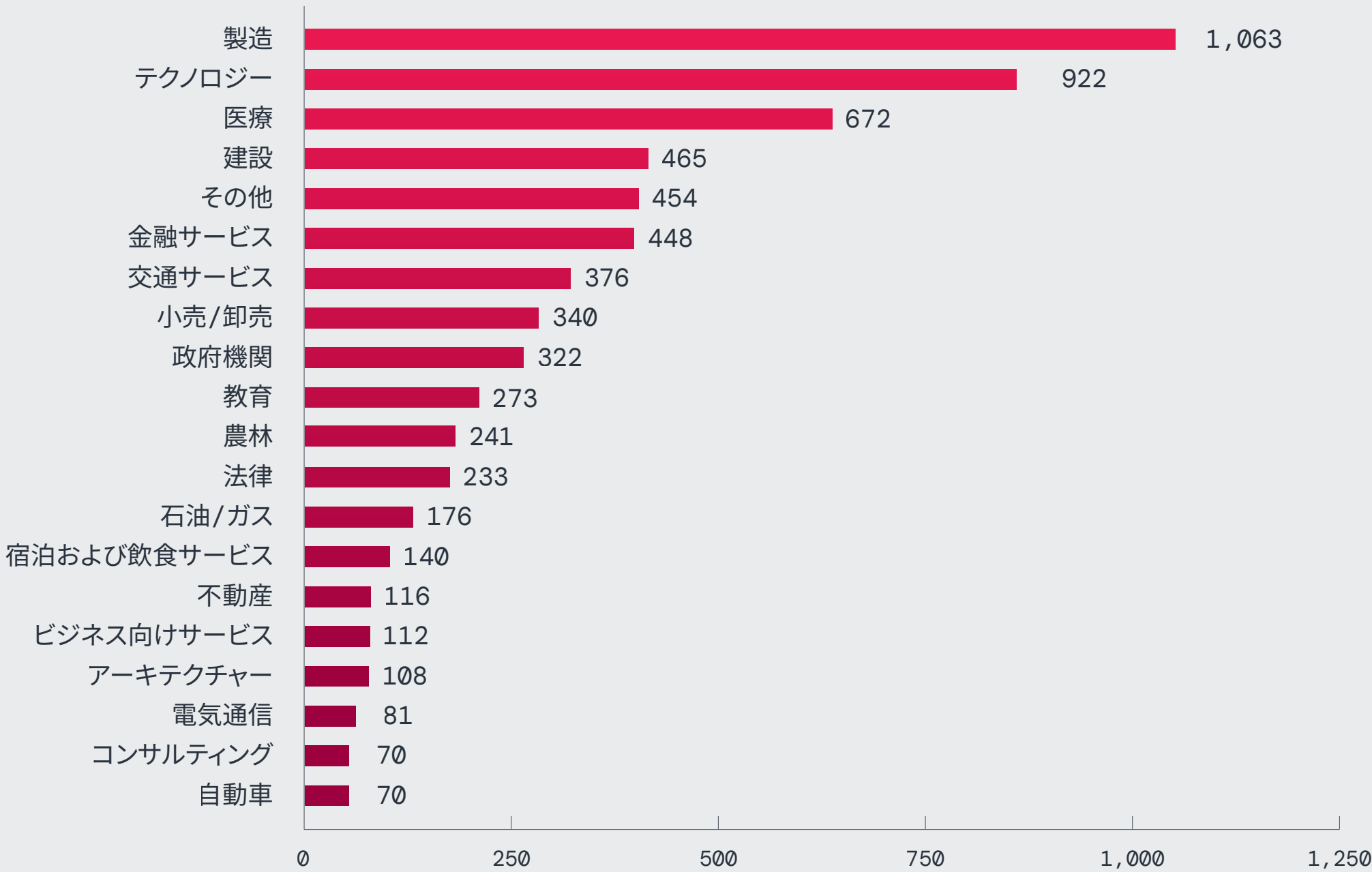


図6: データ リーク サイトに掲載された被害組織を基にしたランサムウェア攻撃の業界別件数 (上位20の業界)

前年比の傾向

図7は、ランサムウェア攻撃の前年比増加率を業界別に示したものです。

石油/ガス業界を標的とするランサムウェア攻撃は前年比で900%以上増加しました。掘削装置からパイプラインに至るまでの自動化の進展によって攻撃対象領域が拡大したことや、古いセキュリティ慣行が採用されていることが原因と考えられます。サイバーセキュリティ インフラストラクチャー セキュリティ庁(CISA)は2025年、「高度でない」脅威アクターさえもが石油/ガスの事業に不可欠な産業用制御システム(ICS)やSCADAテクノロジーの脆弱性を悪用していると警告しました。¹

ランサムウェア攻撃は農業分野でも677.4%増加しています。スマート トラクターやIoT対応センサーが利用されるなど、農業においてもデジタル化が進む一方で、セキュリティ対策は追いついていません。それでも、一定の進歩の兆候は見られ、農業システムがランサムウェアの主な標的になっているという認識も生まれ始めています。農業機械の大手メーカーであるJohn Deereは、2025年にハッカソンを主催し、学生たちにスマートトラクターの脆弱性を明らかにしてもらう取り組みを行いました。²

医療業界は依然として最も頻繁かつ絶え間なく狙われる業界の一つであり、攻撃は前年比115.4%と着実に増加しています。HIPAA Journal³によると、ミシガン州立大学、イェール大学、ジョンズ ホプキンス大学の研究者らは、ランサムウェアが医療データ侵害の主な原因の1つになっていることを発見しました。このリスクは現実のものとなり、複数の大手医療機関がランサムウェア グループ「Interlock」(**2025～2026年に警戒すべきランサムウェア ファミリー トップ5**に掲載)の攻撃を受けています。詳細は「**医療業界を襲う脅威:大規模なデータ窃取が新たなトレンドに**」のセクションをご覧ください。

¹ CISA、**Unsophisticated Cyber Actor(s) Targeting Operational Technology**、2025年5月6日。

² Axios、**John Deere invites students to hack tractors**、2025年6月24日。

³ The HIPAA Journal、**Study Explores Extent of Hacking and Ransomware Attacks in Healthcare**、2025年5月16日。

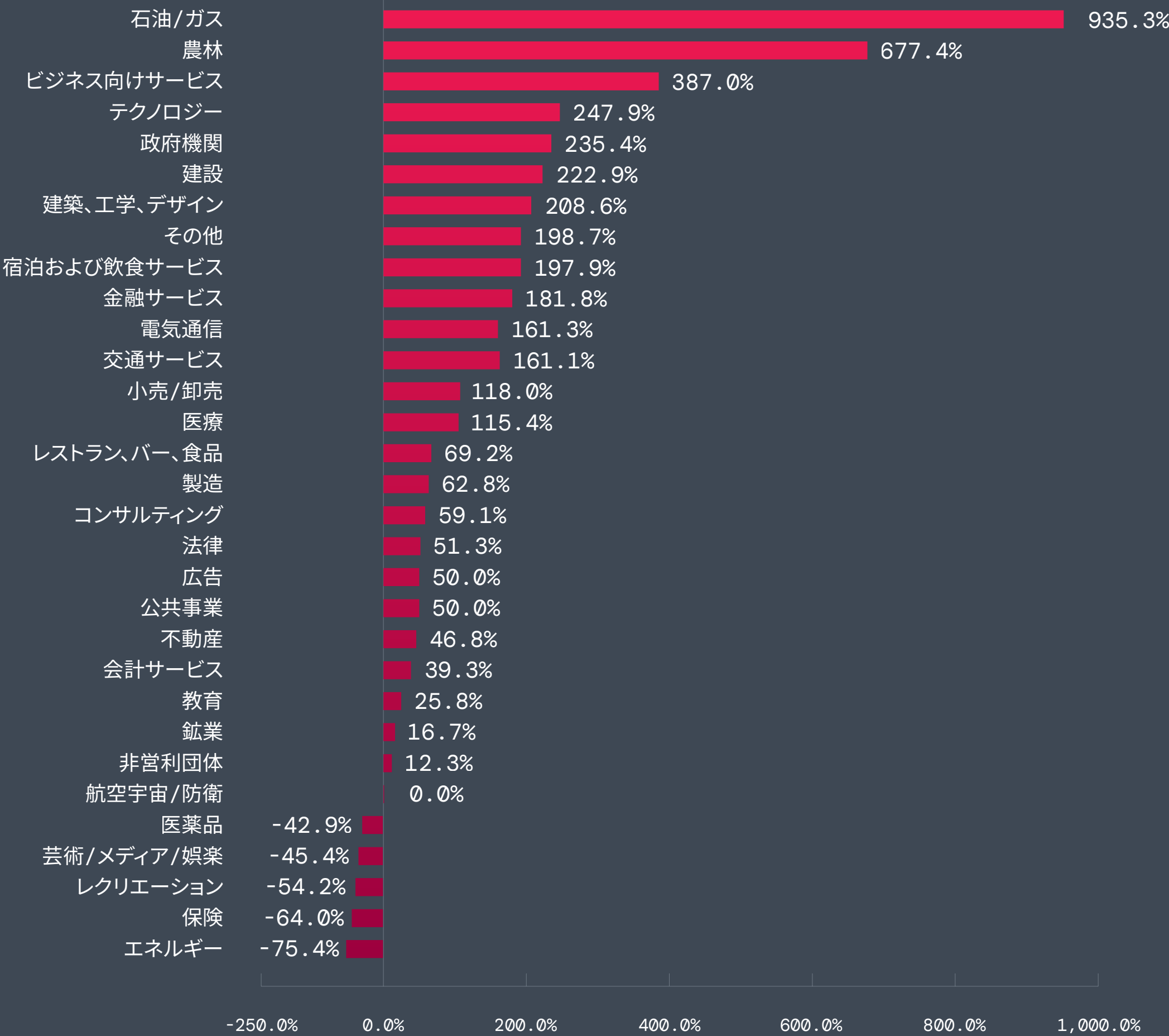


図7: 各業界のランサムウェア攻撃の前年比増加率
(ベースラインが低い場合、増加率が過大な値になるため、昨年のデータセットで報告された攻撃が10件未満の業界は除外)

主な標的国と地域別の概況

リーク サイトのデータによると、ランサムウェア攻撃には明らかな地理的集中が見られます。圧倒的に多いのは米国の組織を標的とした攻撃(50.8%)で、カナダ(5.2%)や英国(4.6%)などを大きく上回っています。これは、脅威アクターが引き続きデジタル化が進んだ高価値の経済圏を優先していることを反映しています。図8は、標的となった上位15か国を、データ リーク サイトで記録されたランサムウェア攻撃の割合と共に示したものです。

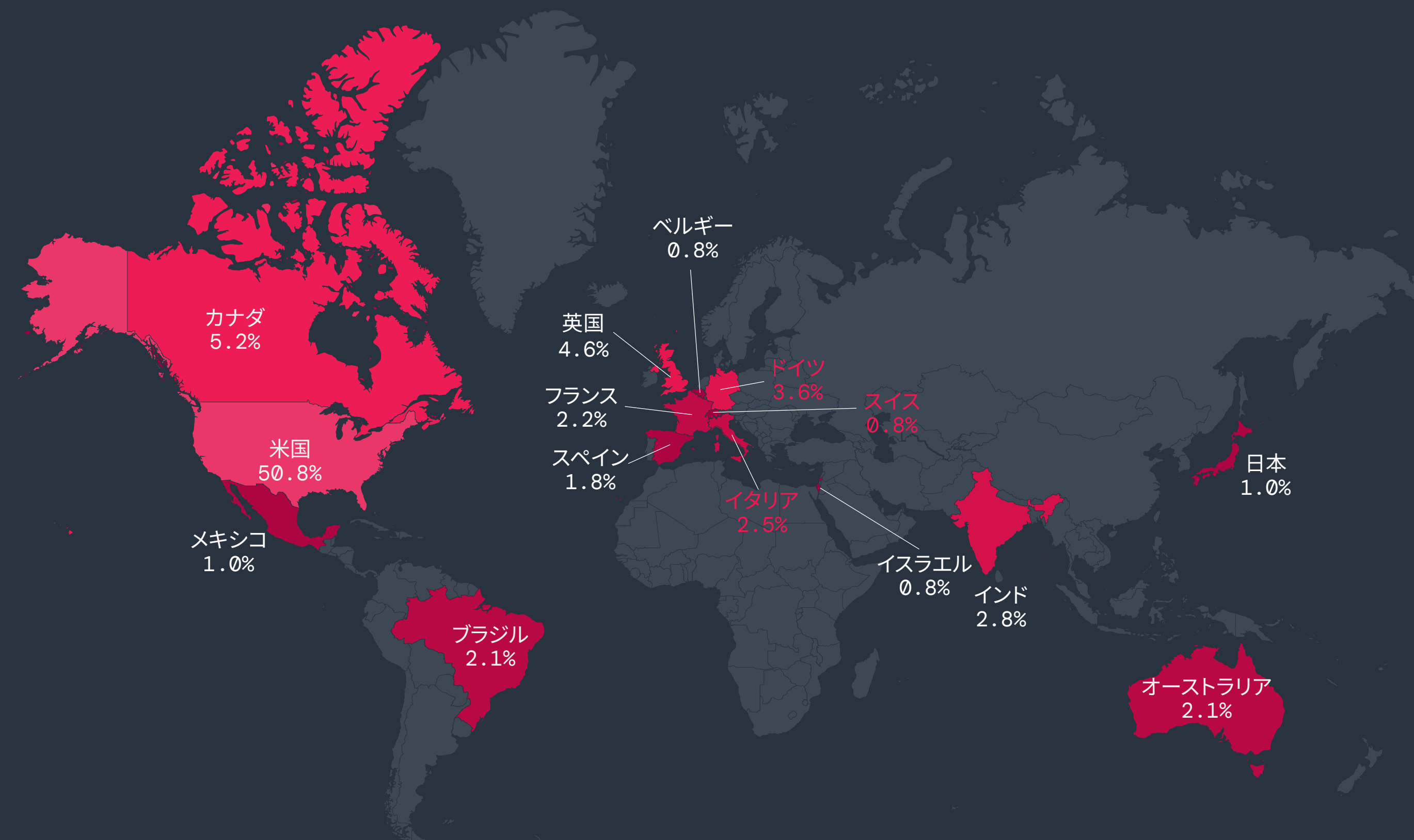


図8: ランサムウェア攻撃の標的上位15か国とその割合

前年比の傾向

ランサムウェアの影響は地域によって大きく異なります。どこで攻撃が加速しているかを把握することで、脅威アクターが今後標的とする可能性の高い地域を予測し、その地域に固有のデータに基づく防御戦略を立てることができます。

上位15か国：米国で大幅な増加

ランサムウェア攻撃は世界中で急増しており、上位15か国における増加率は2桁または3桁となっています(図9参照)。米国の攻撃は前年比2倍以上の3,671件となり、上位15か国に入るその他の国々の合計を上回りました。カナダの増加率は194.5%となり、脅威アクターが北米全土に拡大し、脆弱な業界が狙われていることがわかります。カナダ サイバーセキュリティ センターの「National Cyber Threat Assessment 2025–2026」では、ランサムウェアが同国の重要インフラに対する最大のサイバー犯罪脅威とされており、医療、産業、公共部門の組織への攻撃が激化していることが指摘されています。⁴

⁴ Canadian Centre for Cyber Security, [National Cyber Threat Assessment 2025–2026](#), 2025年7月14日アクセス。

国	ランサムウェア攻撃 (2024年版 レポート)	ランサムウェア攻撃 (2025年版 レポート)	増加率
米国	1,821	3,671	101.6%
カナダ	128	377	194.5%
英国	216	333	54.2%
ドイツ	149	260	74.5%
インド	60	199	231.7%
イタリア	118	181	53.4%
フランス	119	159	33.6%
オーストラリア	73	152	108.2%
ブラジル	57	149	161.4%
スペイン	62	134	116.1%
日本	42	75	78.6%
メキシコ	57	74	29.8%
スイス	43	60	39.5%
ベルギー	34	59	73.5%
イスラエル	11	59	436.4%

図9：ランサムウェア攻撃の前年との比較(国別)

EMEA:欧州とその他の地域における攻撃の激化

図10に示すように、欧州、中東、アフリカ(EMEA)地域では、広範囲でランサムウェア活動が増加しています。スペイン(+116.1%)やドイツ(+74.5%)などの主要経済国のほか、ベルギー(+73.5%)などの小規模市場でも前年比で顕著な増加が見られました。イスラエルの増加率は436.4%で、ベースラインとなる攻撃件数は少ないものの、相対的な急増が見られます。これは、地政学的緊張の高まりと国家が関連するランサムウェア攻撃の増加が反映されたものと考えられます。

国	ランサムウェア攻撃 (2024年版 レポート)	ランサムウェア攻撃 (2025年版 レポート)	増加率
英国	216	333	54.2%
ドイツ	149	260	74.5%
イタリア	118	181	53.4%
フランス	119	159	33.6%
スペイン	62	134	116.1%
スイス	43	60	39.5%
ベルギー	34	59	73.5%
イスラエル	11	59	436.4%
アラブ首長国連邦	21	52	147.6%
オランダ	50	52	4%

図10： EMEA地域におけるランサムウェア攻撃の前年との比較(国別)

APAC:新興市場と確立された市場における爆発的な増加

アジア太平洋(APAC)地域の前年比増加率は、世界全体で最も高いものとなりました。急速なデジタルトランスフォーメーションが進む一方でサイバー成熟度にはばらつきがあることを背景に、攻撃者はこの地域全体にわたってその活動範囲を拡大しています(図11)。シンガポール(+237.5%)や台湾(+147.1%)のようなテクノロジーと物流の拠点から、中国(+186.7%)やインド(+231.7%)などの大規模経済圏まで、その影響はAPAC全体に及んでいます。

国	ランサムウェア攻撃 (2024年版 レポート)	ランサムウェア攻撃 (2025年版 レポート)	増加率
インド	60	199	231.7%
オーストラリア	73	153	109.6%
日本	42	75	78.6%
シンガポール共和国	16	54	237.5%
インドネシア	23	43	86.9%
中国	15	43	186.7%
台湾	17	42	147.1%
タイ	25	32	28%
マレーシア	20	27	35%
香港	7	23	228.6%

図11： APAC地域におけるランサムウェア攻撃の前年との比較(国別)



2024～2025年に 最も活発だった ランサムウェア グループ

引き続き、いくつかの非常に活発なグループがランサムウェアのエコシステムを支配しています。中でもRansomHubは群を抜いており、公になっている被害組織は833件で最多となっています。過去1年間に報告された活動に基づく、このグループは最も活発なランサムウェアグループとして位置付けられます。ただし、興味深いことにこのグループは2025年4月に活動を中止し、姿を消しています。

AkiraとClopはいずれも昨年から順位を上げています。Akiraの被害組織は520件に上り、多数のアフィリエイトやイニシャル アクセス ブローカーを通じて着実に影響範囲を拡大しています。Clopは、サプライチェーン攻撃に特化していることで知られ、その被害組織は488人とAkiraに僅差で続いています。多くの組織が使用するサードパーティー ソフトウェアを標的とすることで影響を最大化する戦略が特徴です。

図12は、過去1年で最も多くの被害が報告されているランサムウェア グループを示したものです。

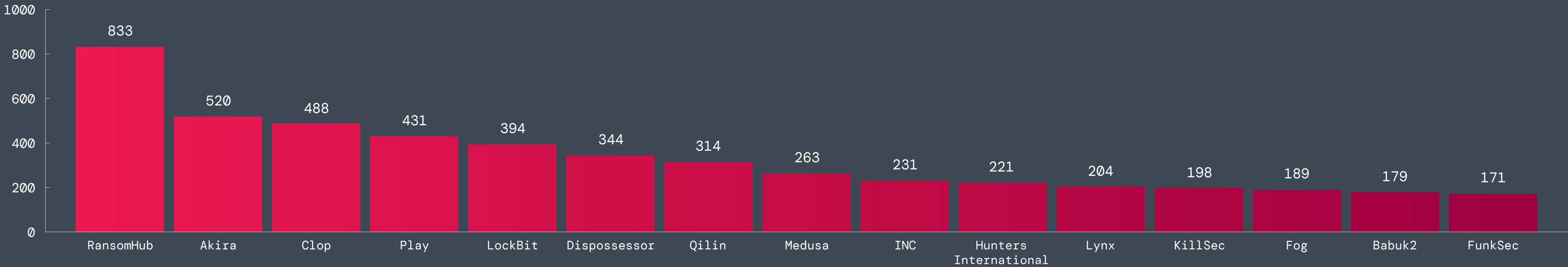


図12: データ リーク サイトで報告されたランサムウェア攻撃の件数



新たに確認されたランサムウェア グループ

ランサムウェアをめぐる状況は常に変化しており、従来のグループの一部が姿を消す一方で、新たなグループも登場しています。制裁を回避するために戦略的なリブランドが行われている場合もあれば、他のグループが残した空白を埋める形で新たなグループが生まれている場合もあります。いずれにせよ、姿を消したランサムウェア グループの関係者は、確立された攻撃手法を利用しながら定期的に活動内容を切り替えています。図13のタイムラインは、2024年4月から2025年4月の間に活動を開始し、リーク サイトでデータを公開し始めたランサムウェア グループを示しています。

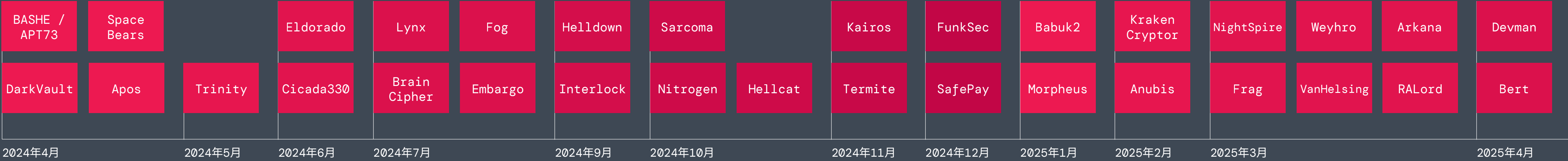


図13: データ リーク サイトを保有する新しいランサムウェア グループ



ランサムウェア キャンペーンに悪用される主な脆弱性

ランサムウェア グループは、組織の重要なテクノロジーの脆弱性を悪用し、影響の大きい攻撃を実行するようになっています。こうした脆弱性を悪用することで、ラテラルムーブメント、機密情報の窃取、ネットワーク環境全体でのランサムウェアの拡散を可能にする直接的な経路が得られます。脆弱性のほとんどはインターネットに接続されたアプリケーションに存在し、基本的なスキャン技術で検出できるため、簡単に悪用される恐れがあります。主な標的には、VPN、バックアップ システム、ハイパーバイザー、リモート アクセス ツール、ファイル転送アプリケーションなど、組織全体にわたって利用され、運用に不可欠なテクノロジーが含まれます。

VPN

仮想プライベート ネットワーク(VPN)の脆弱性を悪用することで、攻撃者は組織の内部ネットワークに直接アクセスできます。これにより、偵察活動やラテラルムーブメント、重要なシステムの侵害とデータの窃取、ランサムウェアの展開が可能になります。

このような脆弱性の例としては、**CVE-2024-55591** (FortiProxy SSL-VPN) や**CVE-2024-40766** (SonicWall SSL-VPN) などがあります。

バックアップ ソリューション

バックアップおよび複製テクノロジーは、ランサムウェア攻撃者にとって重要な攻撃ベクトルとなっています。これらのシステムの脆弱性を突くと、ファイルの暗号化前にバックアップ ソリューションを無効化し、情報を直接盗み出すことが可能です。

ランサムウェアの脅威アクターによって悪用されている脆弱性の例には、**CVE-2023-27532** (Veeam Backup & Replication)があります。

仮想化ソフトウェア

VMware ESXiなどのハイパーバイザーはワークロードを集中させるため、ランサムウェアにとって非常に価値の高い標的となります。ESXiに対するエクスプロイトによって、仮想化環境全体が侵害される可能性があります。

たとえば、**CVE-2024-37085**を悪用すると、攻撃者はESX Adminsグループを操作してサーバーを制御できるようになります。また、ここ数年、ランサムウェアグループはESXi環境内のファイルの暗号化に特化したカスタム ランサムウェアビルドの開発を推進しています。

リモート アクセス ツール

リモートの監視と管理(RMM)ツールは、組織のIT環境においてエンドポイントやインフラを管理するうえで不可欠な存在です。しかし、特に基盤となるソフトウェアに脆弱性がある場合、ランサムウェア グループの標的となることも少なくありません。

このような脆弱性の例としては**CVE-2024-57726**、**CVE-2024-57727**、**CVE-2024-57728** (SimpleHelp RMM)があり、脅威アクターはこれらを悪用することで組織の環境にアクセスすることが可能です。

ファイル転送アプリケーション:

多くの企業は、社内システム間、外部のパートナー、ベンダー、顧客間でファイルを効率的に共有するためにファイル転送アプリケーションを使用しています。しかし、インターネットに公開されると、基盤となるアプリケーションに存在する脆弱性が悪用され、組織のデータにアクセスされる可能性があります。こうしたアプリケーション群は、ランサムウェア グループ「Clon」の主要な標的となっています(このレポートで後述)。

このグループは、ファイル転送アプリケーションの複数のゼロデイ脆弱性(**CVE-2024-50623**と**CVE-2024-55956**)を悪用し、昨年だけでも数百の組織からデータを盗み出しています。

脆弱なシステムの補強

このような脆弱性を悪用したランサムウェア攻撃に対抗するために、防御者は多層型のセキュリティ アプローチを採用する必要があります。

- 優先的なパッチ適用:** エッジ向けサービス (ファイアウォール、VPN、バックアップ システム)の修正を迅速に実行します。
- セグメンテーションとゼロトラスト:** ユーザーとアプリ間のセグメンテーション、デバイス ポスチャー管理、厳格なアクセス制御の実施、特権アカウントの監視により、ラテラルムーブメントを阻止します。
- ゼロデイ攻撃を防御する高度な脅威対策:** インライン サンドボックスと分離テクノロジーを活用し、ゼロデイ攻撃を阻止します。TLSインスペクションを実行して悪意のあるペイロードをブロックし、情報漏洩防止(DLP)対策を適用してデータの持ち出しを阻止します。

これらのセキュリティ ギャップをプロアクティブに解消することで、ランサムウェア攻撃者が脆弱性を悪用する能力を低減し、組織のレジリエンスを大幅に強化できます。

ランサムウェアの総括： 注目のニュース

ChatGPTを犯罪活動に悪用する Black Basta

2025年2月、ランサムウェア グループ「**Black Basta**」内部のMatrixチャット サーバーから大量のメッセージがオンラインで流出し、研究者はこのグループの活動を直接観察できました。2023年9月から2024年9月にかけて、このチャットを通じてグループの内部構造、攻撃戦略、プロセスが明らかになりました。特に注目すべきは、Black BastaにおけるChatGPTの悪用方法が明らかになった点です。ChatGPTの普及を考えれば、悪用されていること自体は当然のことです。[2025年版 ThreatLabz AIセキュリティ レポート](#)によると、ChatGPTはAI関連トランザクションの約45%を占め、AI市場を席巻しています。

ChatGPTはAI市場において広く人気を集め、圧倒的な存在感を持つことから、ThreatLabzでは、Black Bastaにおける日常的な活動にChatGPTがどのように取り入れられているかについて重点的な分析を行いました。

調査結果から、ChatGPTは以下のような形で悪用されていることが明らかになりました。

- **コードの書き換え**: チャット ログには、ChatGPTを使用したPythonのスクリプトの書き換えについて明確に言及されています。
- **AIへの依存**: Black Bastaでは、インターネットのリソースに加え部分的にChatGPTを利用しているという言及があり、ChatGPTが幅広いワークフローに取り入れられていることが示唆されています。さらに、チャット ログでは、メンバー同士がChatGPTでの問題解決を促し合っている様子が見られました。
- **制限のないAIモデルへの関心**: WormGPTに関する議論に反映されているように、ChatGPTに組み込まれた法律や倫理規則による制約を受けない機能を提供する無検閲のAIツールを探そうとする動きが出ています。

ロシア語

щас попизжу с chat gpt

日本語

これからChatGPTと
会話をします

メッセージが意味すること

Black Bastaのメンバーが
技術的タスクの遂行に
ChatGPTを活用している

чату gpt задайте вопрос

он поможет вам

ChatGPTに
聞いてください

助けてくれると思います

Black BastaはChatGPTを
問題解決ツールとして使用し
グループ内の他のメンバーにも
使用を促している

что они подразумевают под
тем что все что ты писал надо
переписать на питон ?

надо тз и какие функции, а я
скажу возможно это или нет

попробуй переписать чатом
gpt

「同じ内容をすべて
Pythonで書き直す
必要がある」とは
どういう意味ですか？

要件や必要な機能は
ありますか？
それを教えてもらえれば
可能かどうか
お伝えします

ChatGPTで
書き直してみてください

Black BastaはPythonでの
スクリプトの書き直しに
ChatGPTを活用しており
時間の節約やPythonの
コーディング スキルの不足を
補っている可能性がある

на половину инет, на
половину chatgpt

半分はインターネットで
もう半分はChatGPTの
回答に基づいています

Black Bastaのメンバーは、
重要な情報源として
ChatGPTとインターネットを
組み合わせて活用している

бля найти бы доступ в
WormGPT

без цензуры chatGPT который

WormGPTへのアクセス
方法がわかりません

無検閲のChatGPTは...

Black BastaはChatGPTのみに
とどまらずWormGPTなどの
倫理的制約の少ないツールに
関心を持っているほか
ChatGPTはすでに広範に使用し、
その制約についてもよく理解している

ランサムウェア攻撃者からの なりすまし電話：多段階攻撃の実態

イニシャル アクセス ブローカーが初期の感染経路として大規模なスパム キャンペーンを用いる傾向は薄れつつあります。それに代わって、過去2年間は図14に示す手法を使用して、より標的を絞った攻撃が効果的に展開されています。

これらの攻撃の背後にいる脅威アクターは、まずZoomInfoなどのサイトで偵察活動を行い、標的組織の従業員の連絡先情報を購入します。LinkedInなどのサイトを通じて追加の従業員情報を入手することで、IT部門の従業員など、なりすましの対象とすべき人物を正確に特定できます。一般に、特権アクセスを持つ特定の従業員(通常は人事、給与、財務部門)が攻撃の標的となります。

脅威アクターはターゲットの連絡先情報を入手すると、「スパム ボミング」攻撃を開始し、相手の受信トレイをスパム メールで埋め尽くします。次に(先に入手した情報をもとに)その従業員に電話をかけ、IT部門の別の従業員になりすまします。これは、ビッシング(ボイス フィッシング)の典型的な例です。発信者は、なりすまし対象のIT部門の従業員に一致するように選ばれます(同性かつ同一言語の母語話者)。脅威アクターは、組織のIT部門の担当者を名乗り、「スパム フィルターの更新」をサポートするために連絡していると伝え、Microsoft Teams、Quick Assist、Team Viewer、AnyDeskなどのRMMツールを介したリモート アクセスを要求します。この要求に応じた場合、脅威アクターはスパム フィルターが「更新された」という十分な信憑性を与えながら、いくつかの操作を実行してターゲットのシステムにバックドアをインストールします。図15は、この手法を用いるランサムウェア イニシャル アクセス ブローカーが運営する実際のWebサイトのものです。

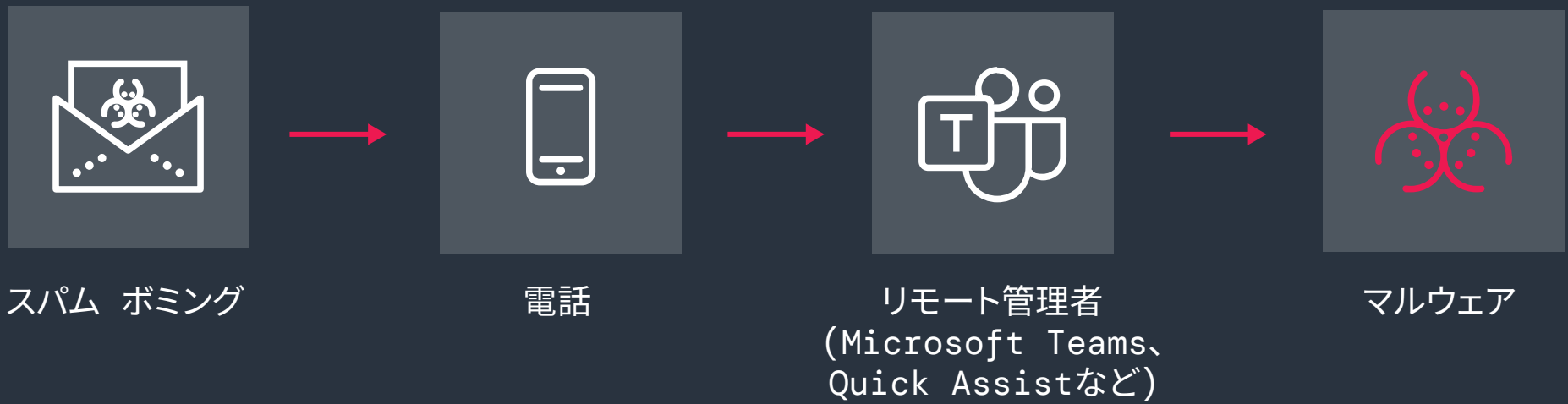


図14：多段階のランサムウェア攻撃の手法

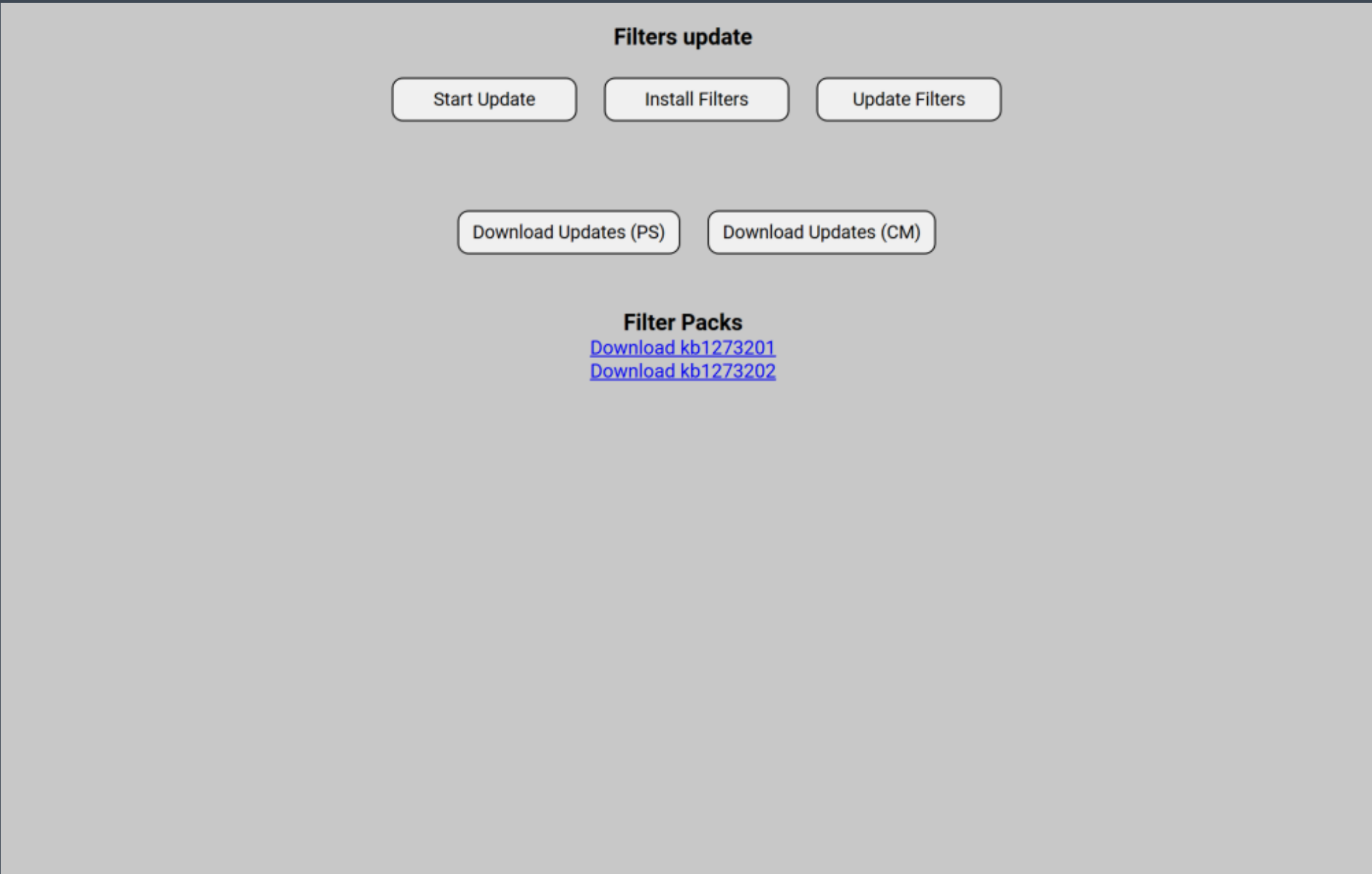


図15：ランサムウェア イニシャル アクセス ブローカーが運営する偽のフィルター更新用サイト

こうしたWebサイトの多くは、AzureまたはAmazon Web Servicesでホストされており、一見シンプルですが、ウイルス対策やマルウェア サンドボックスを回避するためにさまざまな技術を組み込むことができます。例えば以下が挙げられます。

- Filter Packsのリンクは、実際には複数の部分から成る(kbxxxxxxxxxのように2つの部分に分割されている) ZIPアーカイブであり、パスフレーズで暗号化されています。
- [Download Updates]をクリックすると、クリップボードにPowerShellまたはWindowsシェ ル コマンドがコピーされ、実行されます。このコマンドは、脅威アクターにZIPアーカイブのパスフレーズの入力を要求し、さらにマルウェア ペイロードのコマンドと制御情報を用いてレジストリー値を設定します。したがって、この事前の初期化手順を踏まない限り、マルウェアの実行ファイル自体はサンドボックス環境で適切に動作しません。
- ZIPアーカイブが復号、解凍された後、正規の実行ファイル(Microsoft OneDriveなど)が利用され、DLLサイドローディングによって悪意のあるペイロードが復号、展開されます。

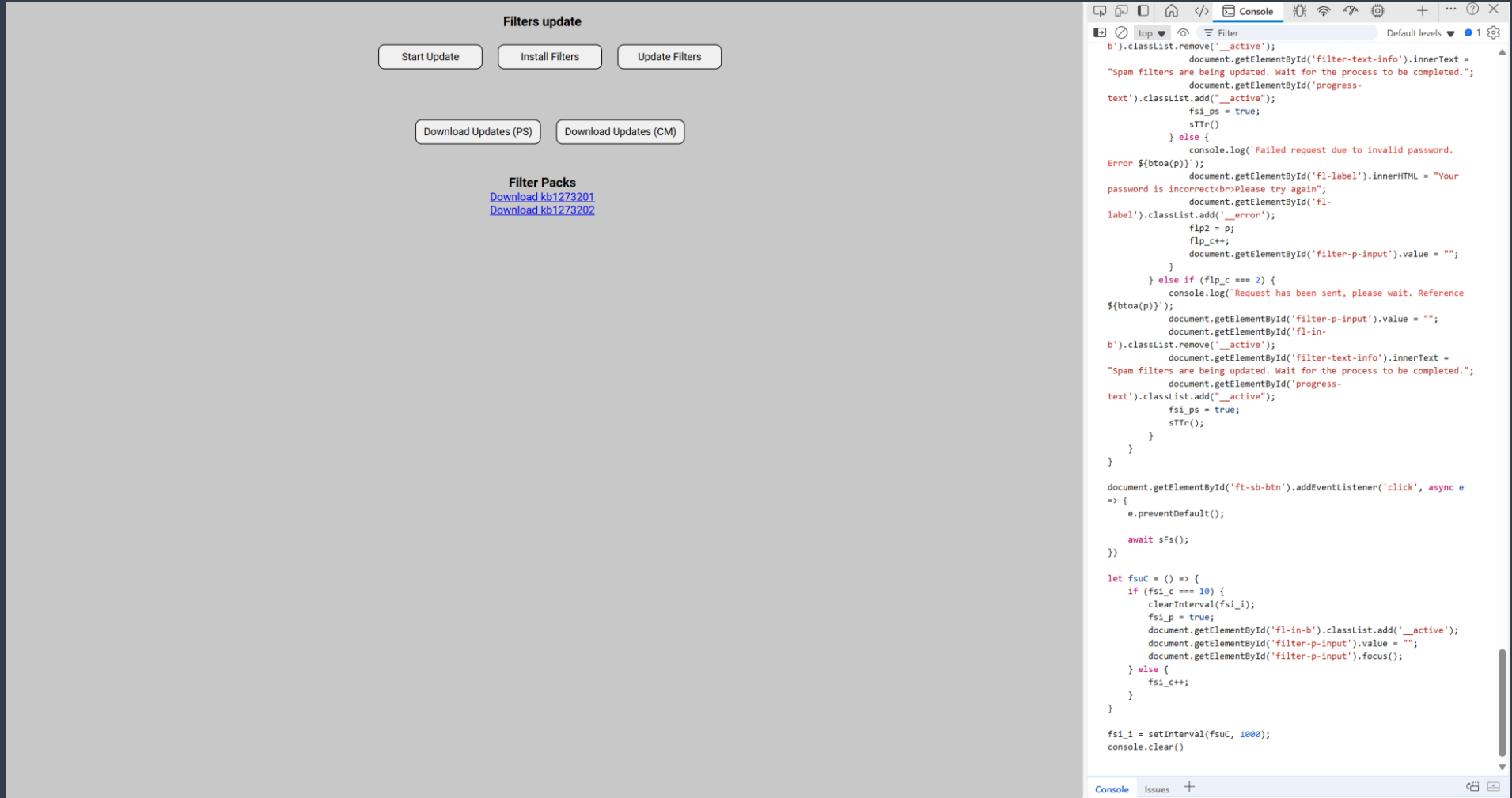


図16: ターゲットのエンドポイント上でのコンソールへのアクセス

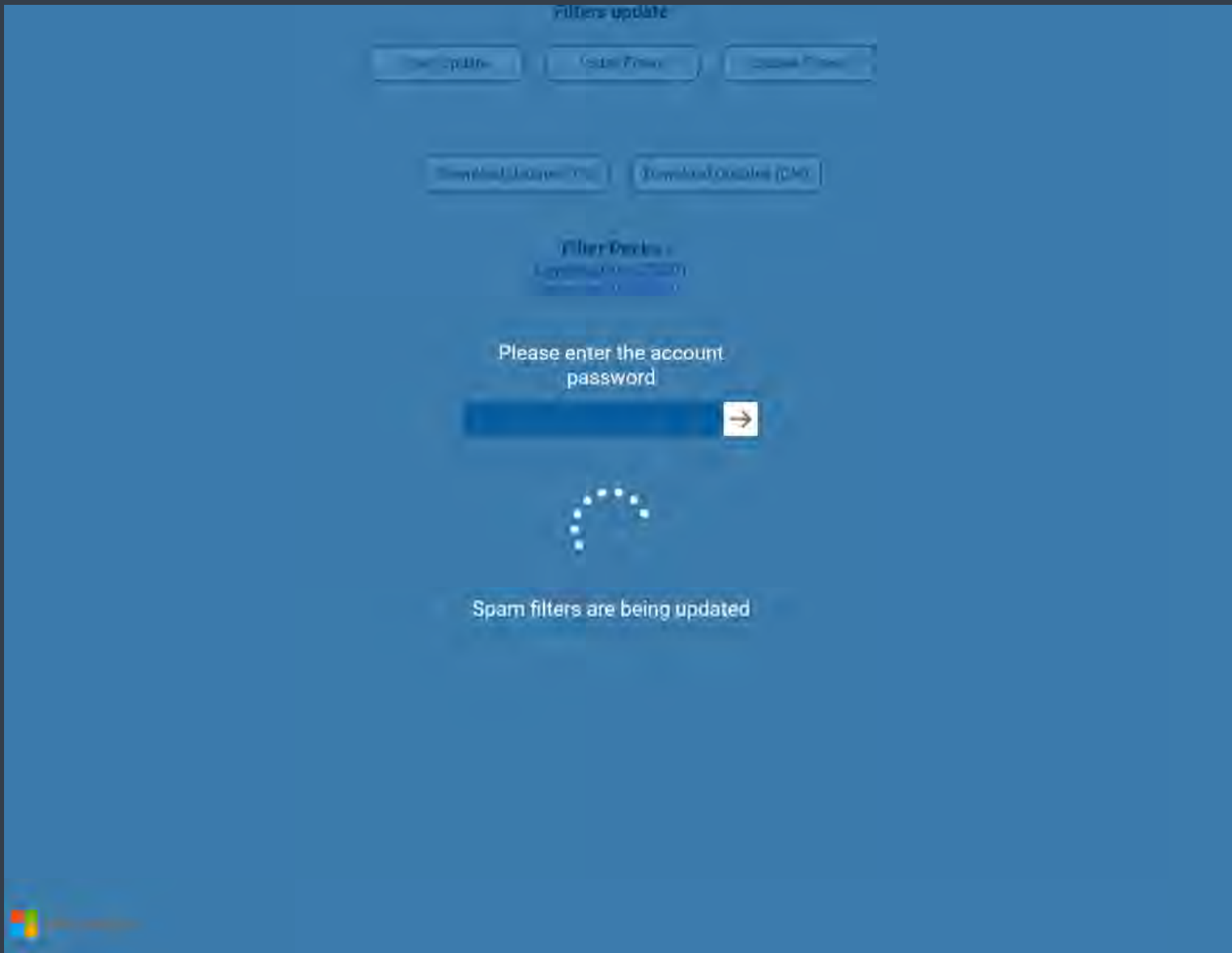


図17: 悪意のあるパスワード入力フィールド

上部の3つのボタンは、ターゲットのMicrosoft 365 のパスワードを盗むためのものです。クリックすると、ターゲットのクリップボードにJavaScriptコンテンツがコピーされます。そして、脅威アクターはWebブラウザの開発者ツールを開いてコンソールにアクセスします(図16)。

次に、クリップボードのJavaScriptコンテンツがコンソールに貼り付けられて実行され、パスワードの入力を促すオーバーレイが表示されます(図17)。

ターゲットのアカウントのパスワードが盗まれ、マルウェアのバックドアがインストールされると、脅威アクターは組織内でのラテラルムーブメントを通じて情報の窃取とランサムウェアの展開を試みます。この新しいタイプの標的型ランサムウェア攻撃は成功率が高く、多くのターゲットがだまされ、被害を受けています。

LockBitの データベース漏洩： ダークWebの侵害から 明らかになったRaaSの裏側

2025年5月、LockBitのアフィリエイト パネルと管理パネルが改ざんされ、グループのデータベースをダウンロードするためのリンクが追加されました(図18)。

漏洩したMySQLデータベースによって、ThreatLabzなどの研究者は、LockBitの内部運営を詳細に把握できました。なお、このグループのリーダーは、2024年2月に実施された国際的な法執行機関による大規模な活動(クロノス作戦)によって起訴されていますが、データベースはその後に得られたものです。LockBitは解体後も**わずか数日で活動を再開**し、新たなリーク サイトから攻撃を展開していました。漏洩したデータベースからは、2024年12月18日から2025年4月29日までの**LockBit 4.0リリース前後**の活動状況が確認でき、75組のアフィリエイトのコードネーム、身代金に関する4,423件のチャット メッセージ、約60,000件のビットコイン ウォレット アドレスが明らかになりました。75組のアフィリエイトのうち54組は、LockBitランサムウェア ビルドを作成し、156の組織にわたる246人を標的に攻撃を展開していました。なお、各アフェリエイトには特定の信頼レベルが割り当てられていました(図19)。

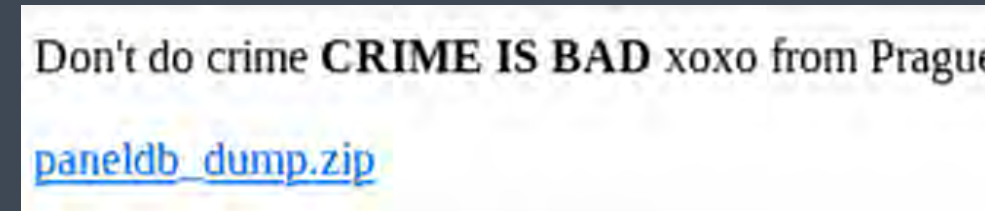


図18:改ざんされたLockBitの管理パネル

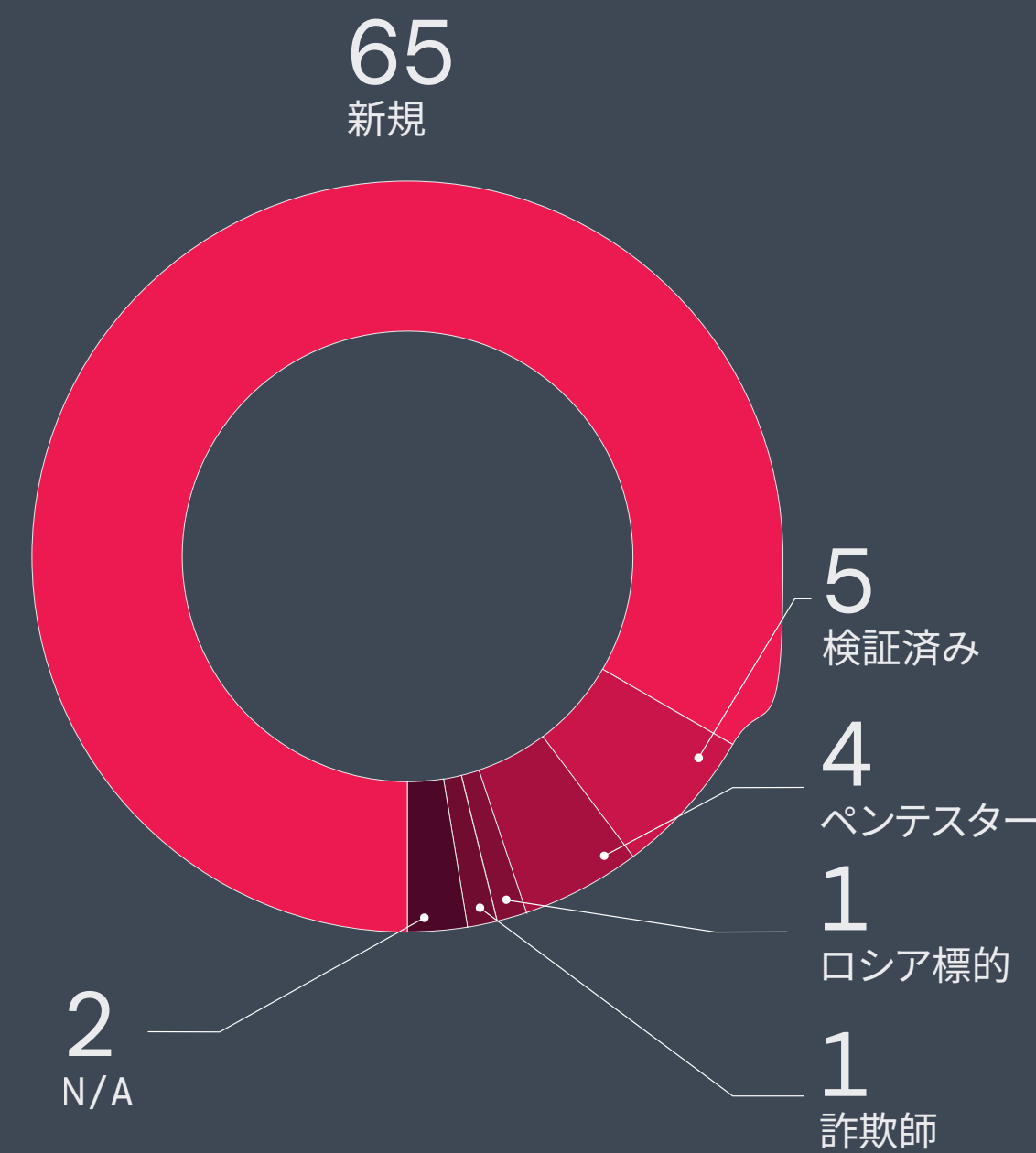


図19:「信頼レベル」別のLockBitのアフィリエイト数

休止状態のアフィリエイトも35組存在し、現在活動していないか、活動を停止させられていると考えられています。興味深いことに、BaleyBeachというコードネームを使用していたあるアフィリエイトは、ライバルであるRansomHub (後述)の閉鎖後にLockBitに乗り換えています。以下は、このアフィリエイトがターゲットに送信したチャット メッセージです。

我々はRansomHubのアフィリエイトでしたが、RansomHubが閉鎖されたため、こちらに移転しました。したがって、取引中だった企業(貴社を含む)には、データの漏洩を防ぐチャンスが残されています

図20は、LockBitのビルド生成数で上位のアフィリエイトを示しています。

管理ユーザーと「matrix777」は、信頼レベルが割り当てられておらず、同じTOX IDで登録されていたため、同一人物である可能性が高いと考えられます。

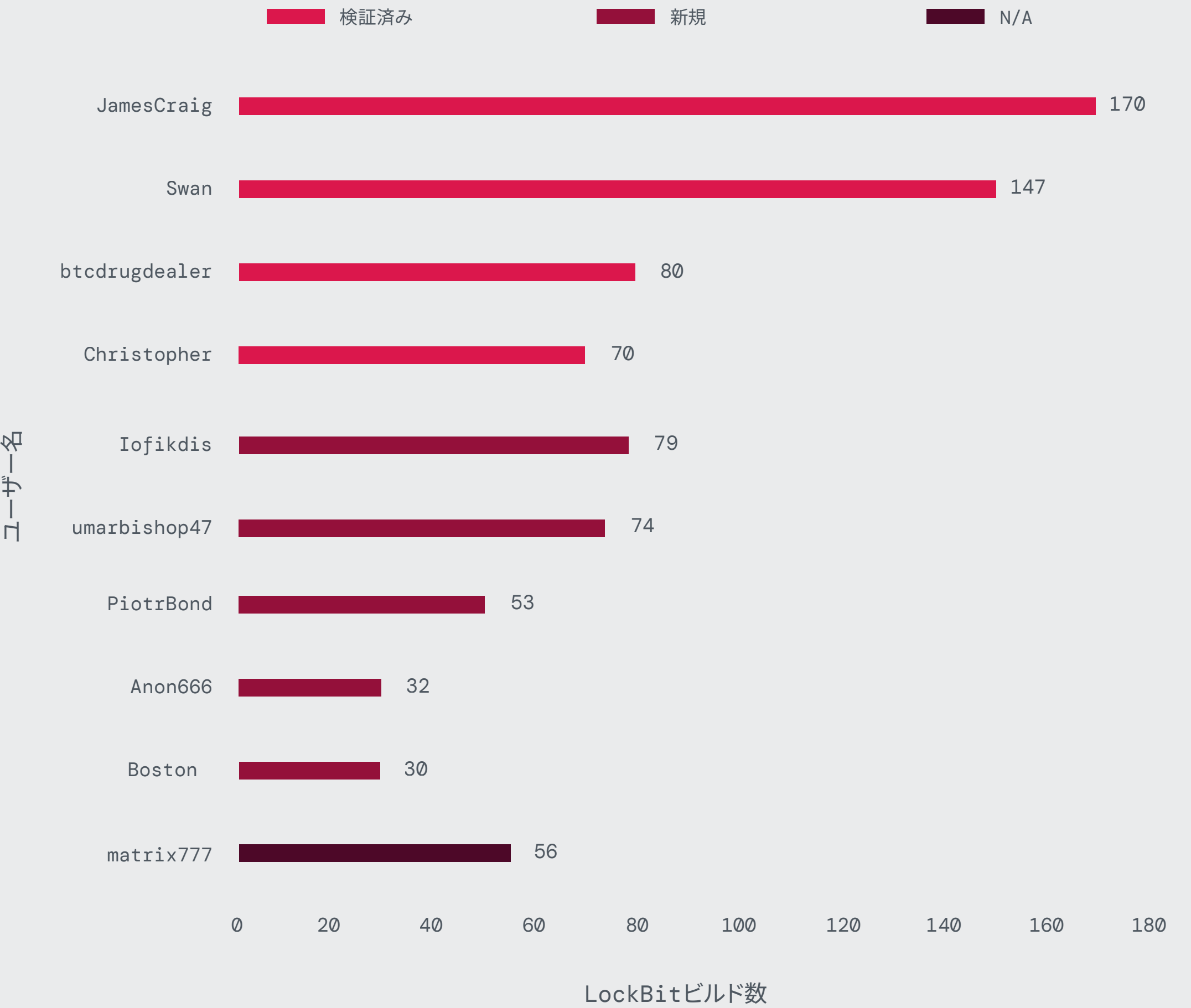


図20: アフィリエイトごとLockBitのビルド数

身代金を要求するチャットに含まれていたターゲットは全体で208件で、うち20件が身代金を支払っていました。この約6か月間で身代金を受け取ったLockBitのアフェリエイトはわずか10組でした(図21)。

あるケース*では、ターゲットがLockBitのアフェリエイト「Swan」に対し200万ドルを支払うことに同意していたものの、チャット ログは支払い情報が提供される直前で終了していました。しかし、実際には、LockBitグループが管理するデータベース内の別のビットコイン ウォレットを通じて支払いが行われ、同グループがこの被害者からの支払いに対して20%のコミッションを受け取っていたと推測されます。10万ドル以上を稼いだアフィリエイトは2組(SwanとChristopher)だけでした。LockBitのすべてのアフィリエイトを合わると、獲得した身代金の総額は2,334,615ドル(コミッションを差し引くと1,867,692ドル)となりました。LockBitグループはその20%となる約466,923ドルを受け取っています。この金額は決して少ないものではありませんが、数百万ドルの支払いを頻繁に受け取っている多くの主要なランサムウェア グループと比較すれば、はるかに小さな金額です。漏洩したLockBitのデータベースの内容からは、2024年2月の混乱によってこのグループが著しく弱体化したことがうかがえます。

ユーザー名	おおまかな身代金受取額(米ドル)	身代金を支払った被害組織の数	被害組織とのチャットの件数
Swan	\$2,021,000ドル*	2*	17
Christopher	231,015ドル	8	44
umarbishop47	40,000ドル	1	10
PiotrBond	\$13,000ドル	2	16
ArrynBaird	\$10,000	1	5
Iofikdis	6,000ドル	1	12
RiccardoBond	4,400ドル	1	4
Brown	3,600ドル	1	5
JamesCraig	3,600ドル	2	17
btcdrugdealer	2,000ドル	1	6

図21: LockBitのアフェリエイトが受け取った身代金

医療業界を襲う脅威： 大規模なデータ窃取の増加

医療業界におけるランサムウェアは、まず情報を盗んでから混乱を引き起こす新たな手口と共に進化しています。最新の脅威アクターは、優位な立場を作るための主な手段としてデータの窃取を優先しています。医療機関は保護対象医療情報(PHI)の膨大なりポジトリを保有しているため、圧力を最大化しようとするランサムウェア攻撃者にとって格好の標的となっています。医療においては患者の信頼が非常に重要であるため、侵害が公になればダウンタイムと同等の損害が発生する可能性があります。

世界的に、医療業界におけるランサムウェア攻撃は前年比で大幅に増加しています。これらの攻撃は多くの場合、大量のデータの窃取と暗号化を組み合わせたもので、医療機関は業務上の混乱、経済的損失、信用失墜といった損害を受けています。2024年には、米国保健福祉省公民権局(OCR)が、500人以上の個人が関与する725件の侵害と、約2億7,500万件の医療記録の漏洩を報告しています。⁵

医療業界におけるランサムウェア攻撃で重要になるのは、単に混乱を引き起こすことではありません。重要なのは、いかにして優位性を生み出すかであり、その起点となるのがデータです。数百万件もの記録を盗み出して公開することで、ランサムウェア攻撃者は標的となる医療機関への圧力をさらに強めることができます。複数のランサムウェア ファミリーから得られた最近のデータは、ある重要な傾向を示しています。データ窃取の規模が急速に拡大しているのです。この進化を牽引するグループの1つがInterlockです。このグループの詳細については、「[2025～2026年に注目すべきランサムウェア ファミリー トップ5](#)」のセクションで取り上げます。

⁵ The HIPAA Journal, [2024 Healthcare Data Breach Report](#), 2025年1月30日。



ランサムウェア対策の 新たな流れ:サイバー セキュリティの最前線

昨年はランサムウェア攻撃の大幅な増加が見られた一方で、ランサムウェア対策の成功事例も報告されています。世界中の法執行機関と民間の研究者との連携は、ランサムウェア攻撃の重要要素を解体し、被害組織の回復を支援するうえで効果的であることが証明されています。

たとえば、2025年前半、ThreatLabzはRansomHubに身代金を支払うことなくファイルを復号する抜け道を発見しました。この発見に基づき、ThreatLabzは、RansomHubのランサムウェア攻撃を受けた組織を支援する専用ポータルとしてDecryptHubを開発しました(図22)。

ThreatLabzのDecryptHubポータルにより、数十の被害組織がファイルを復元し、数百万ドルの身代金の支払いを回避できました。

RansomHubは、2025年4月に閉鎖されるまで最も規模が大きく活発なランサムウェア グループの1つでした。このグループのアフェリエイトの多くは、過去に、消滅したランサムウェア「BlackCat」の運用に関与していました。BlackCatと同様、RansomHubはプログラミング言語「Rust」を使用して、以下のようなさまざまなアーキテクチャー向けにランサムウェアを開発し、クロスコンパイルしていました。

- Windows (x86, x64, ARM, ARM64)
- FreeBSD (x64)
- Linux (x86, x64, ARM, ARM64, ARMv5, ARMv5-64, ARMv6, ARMv6-64, ARMv7, ARMv7-64)
- ESXi (x64)

過去1年間で注目すべきその他の成果としては、**エンドゲーム作戦**が挙げられます。この作戦は、法執行機関による大規模な活動であり、Zscalerを含む業界パートナーと連携して実行されました(図23)。

エンドゲーム作戦は、サイバー犯罪組織、およびランサムウェア攻撃の温床となるマルウェア エコシステムの解体を目指す世界的な取り組みです。この取り組みの成果として、直近では、強力なモジュール型マルウェア ファミリーである **DanaBot** が解体されています。DonaBotの運営グループは、さまざまなランサムウェア グループと連携してMalware as a Service (MaaS) プラットフォームを運営していました。**SmokeLoader**、IcedID、SystemBC、Pikabot、Bumblebeeといった広く知られたマルウェア ファミリーを対象とした2024年のエンドゲーム作戦での成果が今回の結果につながっています。

Zscaler ThreatLabzは過去2年間にわたりエンドゲーム作戦を支援し、マルウェア キャンペーンの特定、犯罪インフラの解体、サイバー犯罪者の摘発に必要なリソースとインテリジェンスを提供してきました。また、ThreatLabzは **GitHub** を通じて、感染の検知と修復に使用できる無料ツールも公開しており、ランサムウェア対策における連携の重要性を示しています。

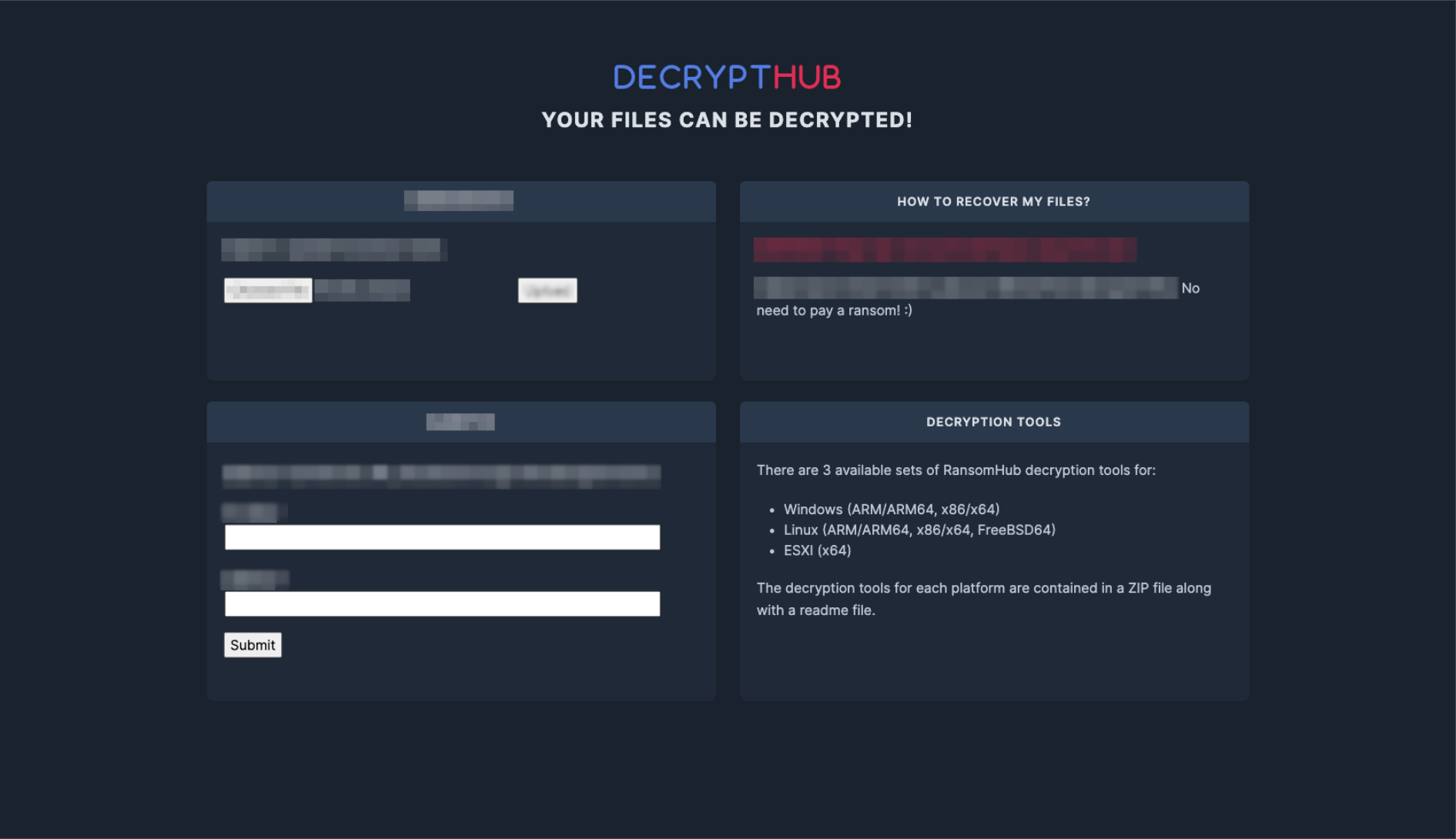


図22: 被害者向けポータル「DecryptHub」

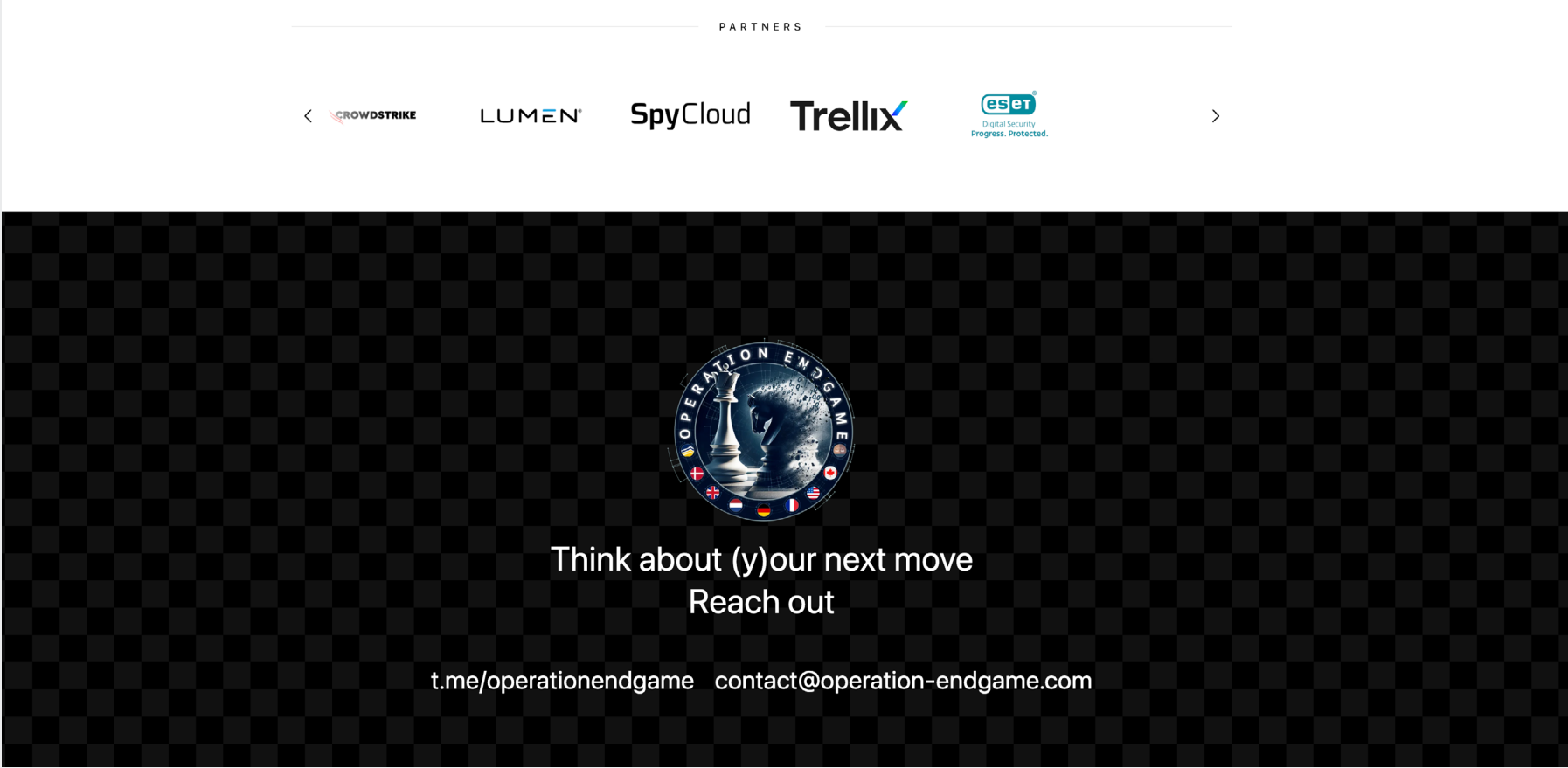


図23: エンドゲーム作戦の連絡先案内ページ

2025～2026年に警戒すべき ランサムウェア ファミリー トップ5

#1 Dark Angels

2022年4月から活動しているランサムウェア グループ「Dark Angels」が運営するランサムウェア ファミリーは、ランサムウェア史上有数の成果を収めています。2024年にThreatLabzが明らかにしたとおり、このグループは、史上最高額となる7,500万ドルの身代金を獲得しており、非常に収益性の高い攻撃を展開していることで知られています。このグループは、さまざまな点で他のグループとは一線を画しています。Dark Angelsは、攻撃をサードパーティーのアフェリエイト(つまり、イニシャル アクセス ブローカー)にアウトソーシングせず、大規模な組織に注力し、限られた数の攻撃のみを実行しています。また、平均で9.6 TB、中央値で2.35 TBという膨大な量のデータを持ち出したうえで、ランサムウェアを展開して組織のデータを暗号化するかどうかを選択します。Dark Angelsは、ランサムウェアで組織を弱体化させることやニュースで取り上げられることを避け、目立たずに活動しようとしています。

Dark Angelsは、盗んだデータをDunghill LeakというWebサイトとTelegramチャネルに投稿していますが、いずれの投稿先でもDark Angelsについては触れられていません。(攻撃元の特定を防ぐために)攻撃から距離を置くことがその狙いの一つと見られます。

Dark Angelsは、フィッシング メール、CVE-2023-22069などの脆弱性を含む公開されたアプリケーションなど、さまざまな手口で組織のネットワークに侵入します。そして、侵害したネットワークをスキャンし、Microsoft Active Directory環境を悪用します。主な標的は、組織のドメイン コントローラーへのラテラルムーブメントとアクセスを容易にするドメイン管理者権限を持つユーザーです。

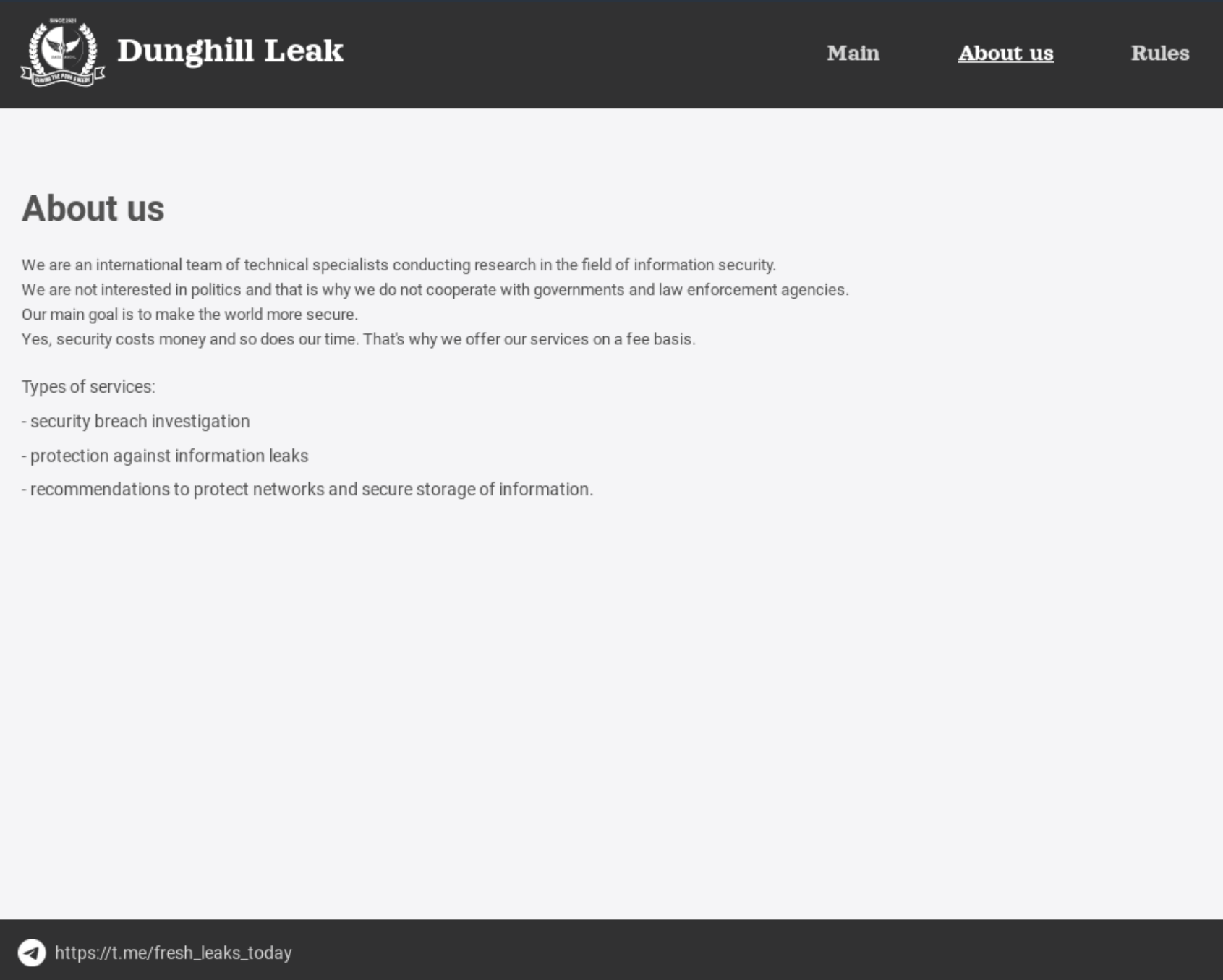


図24: Dark Angelsのリーク サイト「Dunghill」

興味深いことに、Dark Angelsは独自のランサムウェアを開発していません。代わりに、Babuk、Read the Manual (RTM) Locker、RagnarLockerの亜種など、サードパーティーのランサムウェア ファミリーのカスタム ビルドを利用して、Windows、Linux、ARM、ESXi上のファイルを標的に暗号化を行います。

#2 Clop/C10p

Clop (別名C10p)は、2019年から活動しているランサムウェア グループです。Clopはファイルの暗号化から大きく方向転換し、代わりにゼロデイ脆弱性を悪用するサプライ チェーン攻撃によるデータ脅迫に特化しています。特に、一般的なWebベースのファイル転送アプリケーション プラットフォームの脆弱性を悪用し、一度に数百あるいは数千の組織の機密データにアクセスし、窃取しています。2020年12月に悪用された最初のファイル転送アプリケーションの1つは、Acellionの従来型ファイル転送アプリケーション(FTA)でした。従来のAcellion FTAには多数の脆弱性(CVE-2021-2710、CVE-2021-27102、CVE-2021-27103、CVE-2021-27104)が存在し、Clopはこれを悪用してカスタムWebシェルを展開し、数十の組織からデータを盗み出しました。また、2021年7月、ClopはServ-U Managed File TransferとServ-U Secure FTPアプリケーションのCVE-2021-35211を悪用して、複数の組織の内部ネットワークにアクセスし、データの持ち出しとファイルの暗号化を実行しています。

2023年初め、ClopはGoAnywhereのマネージド ファイル転送(MFT)アプリケーションを標的とした別のサプライ チェーン攻撃を実施しました。この攻撃は、認証されていないリモート コードの実行とデータの窃取を可能にする脆弱性CVE-2023-O669を悪用したものでした。Clopはこのゼロデイ脆弱性を悪用し、**100社以上から**データを盗み出しています。さらに、GoAnywhereのMFTインシデントのわずか数か月後にあたる2023年5月、ClopはMOVEit TransferアプリケーションにおけるSQLインジェクションのゼロデイ脆弱性(**CVE-2023-34362**)を悪用し、インターネットに接続されたインスタンスを持つ多数の組織からデータを窃取しました。これは史上最大規模のランサムウェア サプライ チェーン攻撃の1つであり、2,500社以上に影響を与え、**数百万人**の個人情報の漏洩につながりました。Clopはデータ リーク サイトでこの攻撃を公表しています(図25)。



図25: MOVEitの脆弱性(CVE-2023-34362)の悪用に関するClopの声明

Clopによる直近の大規模なサプライ チェーン攻撃は、2024年10月に発生しています。Cleoのファイル転送アプリケーションであるHarmony、VLTrader、LexiComに存在する2つの脆弱性(CVE-2024-50623、CVE-2024-55956)が悪用されました。これらの脆弱性は、未認証のユーザーが**任意のBashまたはPowerShellコマンドをインポートして実行**することを可能にするものでした。Clopは、これらの脆弱性を悪用して、またもインターネットに公開されたCleoのファイル転送アプリケーションを使用する組織からデータを窃取しました。Cleoのアプリケーションを狙ったこれらの攻撃の被害組織が受け取ったClopの身代金要求メッセージの例は、ThreatLabzによって記録されており、こちらからご覧いただけます。

Clopの攻撃の幅は大きく、一部の組織はこのグループによる侵害を複数受けています。実際、ThreatLabzは、ClopのMOVEit攻撃の被害組織の一つが過去に身代金として1万ドルを支払い、その後このグループのCleo攻撃の被害を受けていることを確認しています。



#3 DragonForce

DragonForceは2023年12月にRaaSグループとして出現しました。DragonForceのランサムウェアの初期バージョンは、漏洩したLockBitビルダーを使用していましたが、後に漏洩したContiのソースコードに基づく独自のランサムウェアが作成されています。2025年初頭には、サイバー犯罪フォーラムとそのニュースサイトで新たな「カルテル」ビジネスモデルを発表しました(図26)。

この新しいモデルにより、ランサムウェアのアフェリエイトは、DragonForceのインフラ、ツール、サービスを80/20%の利益分配スキームで独自の攻撃に使用できるようになります。このグループのアフェリエイトは30 TB以上のデータを盗み、各被害者のデータ流出量の平均値は約156 GB、中央値は72 GBでした。

DragonForceは、2025年4月に当時最も大規模かつ活発なランサムウェアグループの1つであったRansomHubと「合併」と発表するまで、それほど注目されていませんでした。RansomHubはこの主張を否定し、DragonForceのメンバーがRansomHubのインフラを混乱させ、Webサイトを改ざんしたと非難しました。この主張どおりの状況であったのか偶然は不明ですが、RansomHubは活動を停止し、このグループのアフェリエイトの多くはDragonForceに移行しました。なお、その中には、Scattered Spider (別名: The Com)も含まれています。Scattered Spiderは、IT部門を狙って多要素認証(MFA)を回避するさまざまなソーシャルエンジニアリング手法を用い、大規模な組織への攻撃を実行し、深刻な影響をもたらしています。2025年4月と5月に英国の複数の小売業者を標的としたDragonForce攻撃は、Scattered Spiderによるものと考えられています。

#4 Akira

Akiraは2023年4月に出現して以来、最も活発なランサムウェアグループの1つとしての地位を確立しました。Akiraの初期バージョンは、漏洩したContiのソースコードに基づいていました。その後、このグループはRustベースのランサムウェア「Megazord」を開発しました。しかし、Megazordも廃止され、現在ではC/C++ベースの亜種に移行しています。この亜種は、ESXiバージョン6と7、Windows x86とx64向けにコンパイルされています。また、最新の亜種では、RSA暗号化に以前のバージョンに見られたネイティブなWindows APIではなく、GNU Multiple Precision Arithmetic Library (GMP)が使用されています。なお、興味深いことに、**Black Basta**も過去(Crypto++ライブラリーへの移行前)にランサムウェアの非対称暗号化に同じGMPライブラリーを使用していました。

Akiraのアフェリエイトは、大量のデータを盗むのではなく、引き続きファイルの暗号化に重点を置いています。一般に、Akiraのアフェリエイトが持ち出す平均的なデータ量は、個々の被害組織からテラバイト単位以上のデータを盗む他の多くのランサムウェアグループに比べ少なくなっています。実際、Akiraのデータリークサイト(図27)によると、データ窃取量の平均値と中央値はそれぞれ44.87 GBと14.33 GBとなっています。最大のデータ窃取は約370 GBで、多くの主要なランサムウェアファミリーよりもはるかに小さいものでした。しかし、データの窃取を重視していないにもかかわらず、Akiraは多数の被害を出しており、流出したデータの合計は13 TBを超えています。

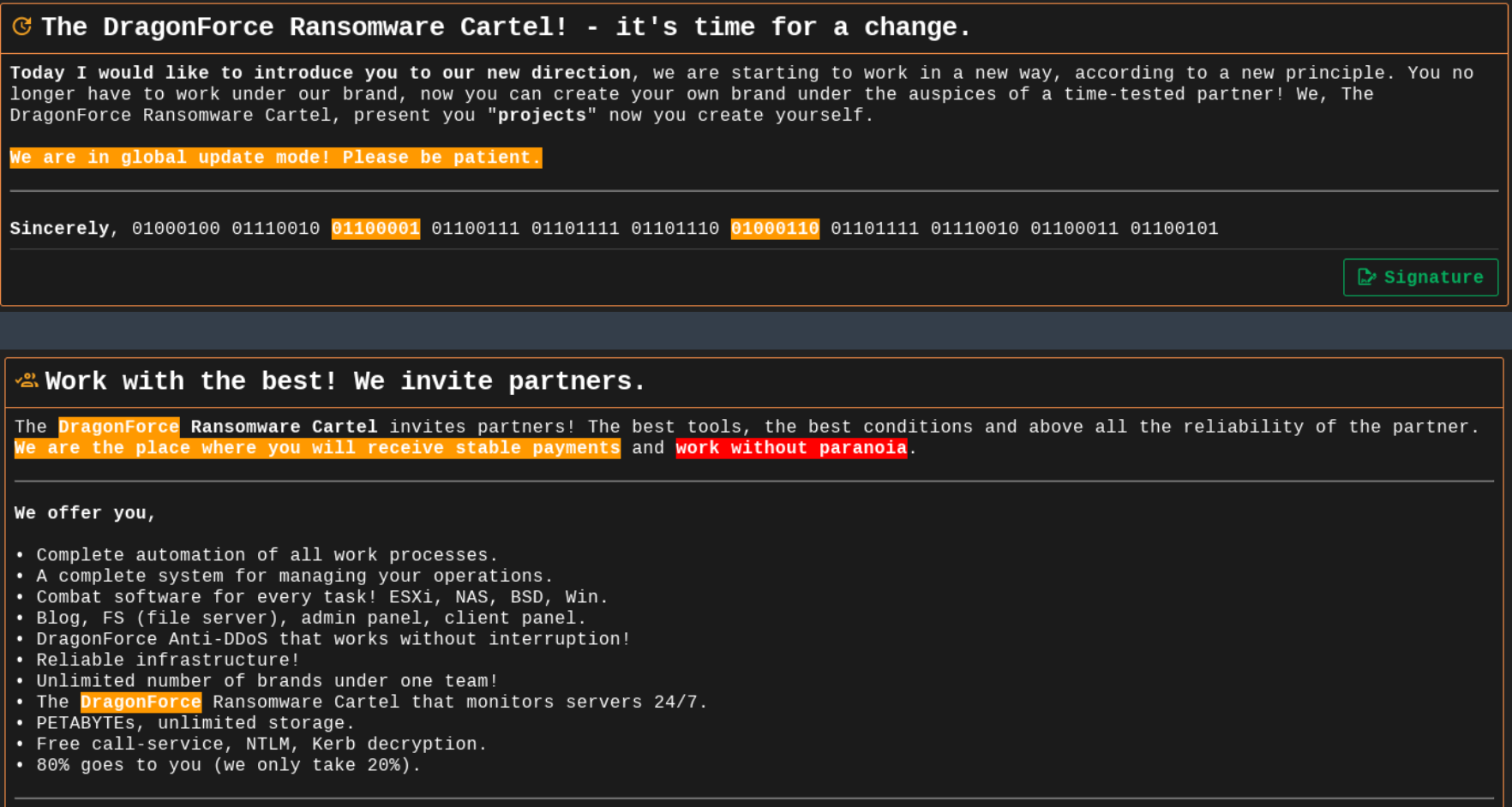


図26: DragonForceの「カルテル」に関する声明



図27: Akiraのデータリークサイト

#5 Interlock

Interlockは比較的新しいランサムウェアグループで、少なくとも2024年9月から攻撃活動を開始し、約50の組織に被害を与えています。Interlockの攻撃は、医療、教育、金融、政府機関、製造など、さまざまな業界に及びます。特に医療業界と教育業界はInterlockの攻撃によって大きな被害を受けています。その背景として、このグループがGDPR、HIPAA、CCPA、NYDFS、GLBAといったコンプライアンス フレームワークを深く理解していることが考えられます。Interlockはこれらの規制を悪用して、標的となる組織に身代金を支払わせようとします。実際、Interlockの**身代金の要求メッセージ**には、違反に対する罰金が明記されています。

Interlockは、Windows、Linux、FreeBSD向けのランサムウェアの亜種を開発しています。このランサムウェアは、全般的には注目に値するものではありませんが、FreeBSD専用のビルドが作成されることは比較的まれです。大規模な組織の多くは重要なサーバー インフラを実行するためにFreeBSDを使用しているため、こうしたインフラは当然Interlockの標的となり、今後も狙われる可能性があります。

Dark Angelsと同様、Interlockは組織から大量のデータを盗みます。ある事例では、被害組織1件から11 TBを超えるデータを盗み出しています。医療業界のある組織は、5 TB以上のデータを盗まれ、250万ドル以上の身代金を支払っています。このグループが盗み出したデータの合計は、過去9か月だけで73.5 TB超に上ります。被害組織1件あたりのデータ流出量は平均で1.6 TB、中央値で約700 GBとなりました。

Interlockのデータ リーク サイトの「About Us」のセクション(図28)では、被害組織に対するこのグループの姿勢が強調されています。Interlockは自らのランサムウェア攻撃について、根本原因は被害者側の「無謀さ」や「怠慢」にあると主張しています。

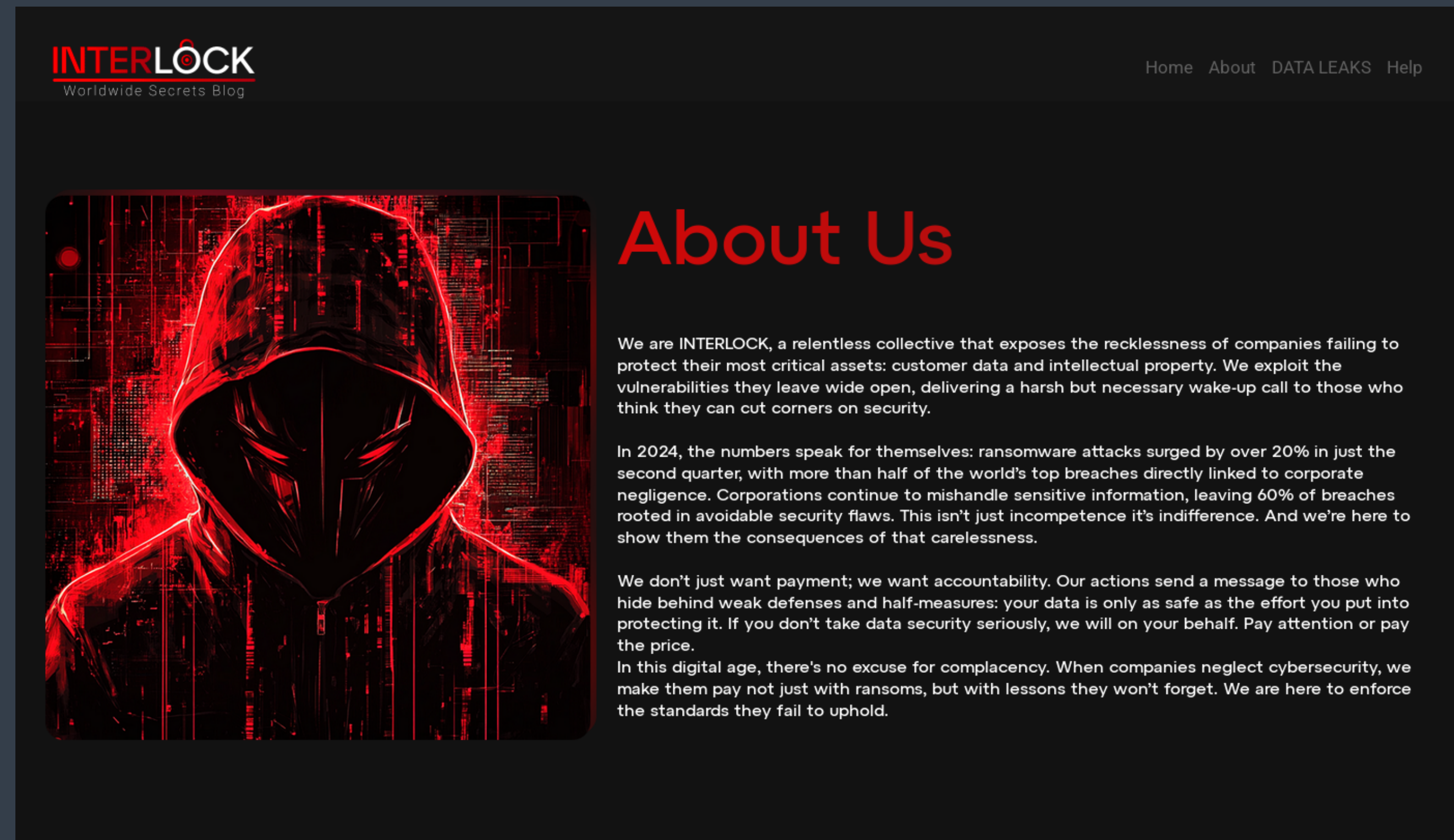


図28: Interlockのグループ概要ページ

ThreatLabzによる ランサムウェア メモの アーカイブ

Zscaler ThreatLabzは、[GitHubの公開リポジトリ](#)を作成しています。本レポート執筆時点で、過去1年に新たに追加されたランサムウェア メモは73件となりました。このリポジトリには計1,018件のランサムウェア メモが含まれ、データ リーク サイトや交渉戦術などがアーカイブされています。ランサムウェア グループを経時的に追跡したり、リブランドしたランサムウェア グループをスタイル分析によって関連付ける際に有用な資料となります。



2026年の 予測

1. ランサムウェア グループは、生成AIを武器化してスケーラブルな多段階の脅迫キャンペーンを展開する

生成AIは、ランサムウェア攻撃の中核的なインフラとしてますます重要になります。Black Bastaグループから漏洩したコミュニケーションの内容から、ランサムウェアの脅威アクターがすでにChatGPTなどのツールを悪用してフィッシングコンテンツや偽の文書の生成、マルウェアのデバッグや書き換え、ディープフェイクコンテンツの作成を行っていることが明らかになりました。今後のランサムウェア攻撃ではこのモデルが拡大し、盗んだ機密データをLLMで分析し、要約するなど、さまざまな手法に発展していくことが予想されます。また、組織がAIのトレーニング目的で収集するデータの量が増えるなか、こうしたデータはランサムウェア グループにとって格好の標的となるでしょう。

2. ランサムウェア グループは、引き続き多段階のソーシャル エンジニアリング攻撃を実行する

ランサムウェア攻撃者は、不特定多数を対象としたスパム キャンペーンを捨てて標的型攻撃を強化し、非常に正確なソーシャル エンジニアリングにシフトしていきます。攻撃者は、LinkedInやZoomInfoなどのプラットフォームを悪用して、特権アクセスを持つ従業員を特定し、その相手に大量のスパムを送信します。そのうえで、IT担当者を装った電話をかけ、侵入の糸口を作ります。

3. ランサムウェア攻撃者のソーシャル エンジニアリング戦術の進化に伴い、音声ベースの攻撃が増加する

ランサムウェア グループは、引き続き音声ベースの攻撃ベクトルを用い、ボイスフィッシング(ビッシング)やAIで生成した音声を通じて、標的となる組織にアクセスすることが予想されます。これらの戦術は、人間的な信頼や緊急性を悪用したものです。多くの場合、経営幹部やITスタッフになりすまして従業員を操作し、資格情報を開示させたり、内部システムへのアクセスを許可させたりします。生成AIツールが利用しやすくなるにつれ、ランサムウェアの脅威アクターは実質的にビッシングを自動化しており、多言語の音声クローニングや適応型の通話スクリプトなどの戦術で組織の従業員をあざむき、暗号化や脅迫の糸口を生み出しています。

4. 窃取されるデータ量はさらに増加し、データ脅迫は引き続き身代金を支払わせるための重要な手法となる

データの窃取はランサムウェア攻撃の主要な手法となりつつあり、この傾向は加速すると見られます。Clop、BianLian、Hunters Internationalなどのグループは、暗号化の手法を完全に廃止し、純粋な脅迫へのシフトを主導してきました。ThreatLabzは、これらのグループの一部が被害組織1件あたり平均数百ギガバイトを盗んでいることを確認しています。組織がバックアップと復旧機能を向上させるにつれ、脅威アクターは盗んだデータを武器にして、身代金を支払うよう圧力をかけるケースが増加すると予想されます。

5. 漏洩したランサムウェアのソース コードとビルダーが次世代の攻撃を生む

ランサムウェアのソース コードやビルダーの漏洩(意図的なものも含む)が発生し続けることで、少ない労力で大きな影響を与える新たな攻撃が出現することが予想されます。主要なランサムウェア グループからの漏洩により、すでにスピノフ作戦、リブランドされた亜種、模倣キャンペーンが活発化しています。新たなグループは、漏洩したコードベースを基にペイロードや配信手法を変更し、既存の検出シグネチャーを回避しています。

6. 法執行機関はランサムウェア グループを支援する存在にも取り締まり対象を広げる

国際的な法執行機関の活動はさらに大胆かつ標的を絞ったものとなり、ランサムウェア グループだけでなく、その攻撃を可能にするインフラやサービスの解体にも取り組むようになっていきます。エンドゲーム作戦では、マルウェア配信プラットフォームを大規模に解体できることが実証されました。

7. ランサムウェアのアフィリエイトは、引き続きグループ間を移動する

Ransomware as a Service (RaaS)モデルは、アフィリエイトに柔軟性を提供するとともに、脅威環境の変動性を高めます。アフィリエイトは、解体の圧力、支払い条件、ツール、評判に基づいて、グループを頻繁に切り替えます。この継続的な動きが、インフラの再利用、戦術の重複、運用中断時のスピーディーなリブランドにつながります。アフィリエイト モデルが低リスクで収益性を維持している限り、このパターンは継続するでしょう。

ランサムウェアを阻止する Zscalerの ゼロトラスト+AI

ランサムウェア攻撃が成功しやすい環境にはいくつかの特徴があります。セキュリティの断片化、限定的な可視性、暗黙の信頼です。しかし、多くの組織は依然として従来のセキュリティ ツール(次世代ファイアウォール、VPN、アンチマルウェアなどのポイント製品)を利用しています。こうしたツールは、最新の脅威に対処するために設計されたものではありません。

従来のアーキテクチャーは、軽減する以上に多くのリスクを生み出します。暗号化されたトラフィックによる死角、脅威に対する可視性のサイロ化、複雑で一貫性のないポリシー管理などにより、ランサムウェア対策に重大なギャップが残ります。さらに、このようなアーキテクチャーは広範かつ必要以上に寛容なアクセス モデルに依存し、内部リソースをリスクにさらします。攻撃者は、ひとたび足場を築くとシステム間を水平方向に移動できるようになるため、拡散、権限昇格、機密データへのアクセスを検出されることなく簡単に実行できます。

Zscaler Zero Trust Exchange™は、時代遅れになったネットワーク中心のモデルを、AIを活用したクラウド ネイティブのゼロトラスト アーキテクチャーでリプレースすることで、これらのリスクを排除します。スケーラブルな統合プラットフォームを提供することで、あらゆる場所のユーザー、デバイス、アプリケーションにわたってリスクを最小化し、ランサムウェア対策を簡素化します。

ZSCALERは、攻撃ライフ サイクルのあらゆる段階でランサムウェアを阻止します。

- **攻撃対象領域の最小化:** ユーザー、アプリケーション、デバイスをクラウド プロキシの背後に隠すことで、ランサムウェアの標的となり得る無防備なインフラを効果的に排除します。プロキシの背後に置くことで、インターネット上で発見できなくなるため、攻撃対象領域が大幅に縮小されます。パブリックIPアドレスを持たず、ネットワークに直接アクセスすることがなくなるため、内部リソースがランサムウェア攻撃者に発見、アクセスされることはありません。侵害予測テクノロジーは、AIを活用して攻撃シナリオのシミュレーションを行い、攻撃者が悪用する可能性のある経路を特定します。これにより、セキュリティ部門は攻撃が発生する前に対策を講じられるようになります。
- **最初の不正侵入の防止:** 完全なTLS/SSLインスペクション、インライン サンドボックス、分離により、悪意のあるコンテンツへのアクセスからユーザーを保護し、未知の脅威がネットワークに到達する前に検出します。これらの機能によって、不正侵入が発生するリスクを最小化したうえで、ランサムウェアの実行を未然に阻止できます。
- **ラテラルムーブメントの排除:** ユーザーとアプリケーション間(またはアプリ間)をネットワークを介さず直接接続することで、ラテラルムーブメントのリスクを排除します。また、AI活用型のセグメンテーションによって、ユーザー行動、デバイス ポスチャー、アプリのコンテキストに基づきアクセスを調整します。エンドポイントが不正侵入を受けた場合でも、ランサムウェアの脅威アクターはシステム間を移動して拡散できません。さらに、AIとアイデンティティ脅威の検知と対応(ITDR)で、異常なアクセス パターンを明らかにするほか、デセプション テクノロジーとデコイによってランサムウェアの脅威アクターを監視対象の罠に誘い込みます。
- **データ流出の阻止:** 脅迫を重視するランサムウェア キャンペーンに対抗するには、機密データの窃取を防ぐことが重要です。インラインDLP、CASB、トラフィック検査機能により、承認されたクラウド アプリ、シャドーIT、コマンド&コントロール(C2)インフラへの不正な転送をブロックします。

ZSCALERは、主に以下のようなAI活用型のツールおよび機能でランサムウェア対策を支援します。

- **侵害予測:** 生成AIと多次元予測モデルにより、潜在的な侵害シナリオを未然に防ぎます。
- **フィッシングとC2の検出:** Zscaler Secure Web Gatewayが備えるAIベースのインライン検出機能により、未知のフィッシング サイトやC2インフラを特定してブロックします。
- **インライン サンドボックス:** 高度なAIモデルを活用して、制御された環境で疑わしいファイルを分析することで、マルウェアやゼロデイ脅威を包括的に防止します。
- **Zero Trust Browser:** AIを活用して悪意のあるWebコンテンツを特定、分離し、データの漏洩やマルウェアの配信を防止します。
- **セグメンテーション:** 機械学習を活用することで、アプリ セグメントとポリシーに関する推奨事項を自動生成し、攻撃対象領域の最小化とラテラル ムーブメントの防止を図れます。
- **動的なリスクベースのポリシー:** AI活用型の振る舞い分析により、ユーザー、デバイス、アプリケーションのリスク状況を継続的に評価し、動的なセキュリティ ポリシーおよびアクセス ポリシーを施行します。
- **データ検出と分類:** エンドポイント、インライン トラフィック、クラウド アプリの機密データを瞬時にスキャンして分類するため、ランサムウェアが機密データを狙って暗号化することがより困難になります。
- **情報漏洩防止(DLP):** AIベースのコンテンツ検査とポリシーの施行によって、不正なデータ転送をブロックし、ランサムウェア攻撃者による機密データの窃取と脅迫を防ぎます。

ランサムウェアの戦術の進化に伴い、防御も進化させる必要があります。ZSCALER ZERO TRUST EXCHANGEは、攻撃対象領域の縮小、新たな回避型ランサムウェアのブロック、ラテラルムーブメントの防止、脅迫の試みとデータの持ち出しの阻止に不可欠な存在として組織を支援します。

ランサムウェア対策 チェックリスト

ランサムウェアを阻止するにはゼロトラストが必須ですが、効果的なランサムウェア対策はそれだけでは終わりません。従業員のトレーニング、安全なバックアップ、十分に準備された対応計画など、広範な運用面のレイヤーも重要です。

ここでは、ThreatLabzのエキスパートの知見に基づいて、ランサムウェアのリスクを軽減し、長期的なレジリエンスを構築するために今すぐ実行できる最も効果的な手順をチェックリストとしてまとめました。

データの定期的なバックアップ

- ☐ 暗号化された定期的なバックアップをオンラインとオフラインの両方で維持します。
- ☐ 復旧手順をこまめにテストし、ランサムウェアの戦術の進化に合わせてバックアップ戦略を調整します。

多要素認証(MFA)の適用

- ☐ 特に特権アクセスについては、すべてのユーザー アカウントにMFAを要求します。
- ☐ アイデンティティ保護と統合して、アカウントの乗っ取りを効果的に検出、ブロックします。

アプリケーションのセキュリティ強化

- ☐ 公開された状態のアプリケーションがないようにして、ランサムウェア攻撃者による脆弱性の悪用を防ぎます。
- ☐ ゼロトラスト アーキテクチャーを導入し、内部アプリをランサムウェアから保護します。

ソフトウェアやシステムの継続的なアップデートとパッチ適用

- ☐ 最新のセキュリティ パッチを速やかに適用し、既知の脆弱性を解消します。
- ☐ AIを活用した脅威インテリジェンスにより、実際のリスクに基づいてパッチ適用の優先順位を決定します。

組織のセキュリティ ポリシーの標準化

- ☐ MFA、ソフトウェア アップデート、アクセス制御など、すべてのユーザーが一貫したセキュリティ手順に従うようにします。
- ☐ セキュリティ サービス エッジ(SSE)アーキテクチャーを採用し、オンプレミスかリモートかを問わずユーザーを保護します。

最小特権アクセス制御の適用

- ☐ 最小特権ポリシーを導入し、各自の役割上のニーズに則した形でデータとシステムへのアクセスを厳密に制限します。
- ☐ AIを活用したソリューションを導入し、振る舞いを動的に分析し、それに応じて権限を調整します。





アイデンティティ保護の強化

- ITDRツールを使用して、アイデンティティの設定ミスを監視するほか、権限昇格とラテラルムーブメントに悪用されるActive Directoryの脆弱性を修復し、ステルス性の高いアイデンティティの脅威を検出します。

AI活用型のブラウザ分離の使用

- ユーザー セッションをWebから安全に分離し、ドライブバイ ダウンロード、フィッシング、資格情報の窃取を防ぎます。
- 疑わしいサイトには、隔離された読み取り専用環境でアクセスできるようにします。

デセプション テクノロジーの活用

- トラップ(ハニーポット、偽の資格情報など)を設置することで、キル チェーンの早い段階で攻撃者を検出するとともに、攻撃者を誤った方向に誘導し、攻撃を遅らせます。
- デセプション システムからのアラートを活用して、インシデント対応を迅速化します。

従業員の継続的なトレーニング

- フィッシング、ソーシャル エンジニアリング、偽のソフトウェア アップデートなどのランサムウェアの手法について、定期的なユーザー教育を行います。
- 実際の攻撃シナリオのシミュレーションを行い、従業員の備えを強化します。

すべてのトラフィック(特に暗号化されたもの)の検査

- 脅威の87%** は暗号化されたチャネルに潜んでいるため、暗号化の有無を問わずすべてのトラフィックを検査して、隠れた脅威を検出し、侵害を防止します。

AI活用型サンドボックスの導入

- AI/MLベースの振る舞い分析を活用して、過去に確認されたことのない回避型マルウェアを検出、ブロックします。
- 不審なファイルがエンドポイントに到達する前に検疫します。

CASBによるSaaSアクセスの制御

- クラウド アプリの使用状況を監視および管理し、ファイルのダウンロードやデータの持ち出しなどの悪意のある振る舞いを阻止します。
- データの共有とダウンロードに関するポリシーを施行します。

ランサムウェア対応計画の作成とテスト

- データ復旧、インシデント対応、通信プロトコルに関する手順を含めます。
- 定期的に机上演習を実施してレディネスを評価し、ギャップを埋めます。

ゼロトラスト ネットワーク アクセス(ZTNA)の導入

- 広範なネットワーク アクセスを、アイデンティティベースの詳細なセグメンテーション(ユーザーとアプリ間、アプリ間)でリplacesします。
- 最小特権アクセス制御でアクセスを仲介し、ラテラル ムーブメントを防ぎ、攻撃対象領域を削減します。

インラインDLPの導入

- インラインのDLP対策を展開し、データの持ち出しや機密ファイルの転送を防止します。
- Web、クラウド、メール チャネルにポリシーを適用します。

調査 方法

本レポートの調査には、複数のデータ ソースからランサムウェアの傾向を特定および追跡する包括的なプロセスが採用されています。ThreatLabzは、次のようなソースから2024年4月～2025年4月のデータを収集しました。

- **Zscalerのグローバル セキュリティ クラウド。**1日あたり500兆以上のシグナルを処理して合計90億件以上の脅威とポリシー違反をブロックするとともに、1日あたり25万件以上のセキュリティ アップデートをZscalerのお客様に提供しています。ThreatLabzは、ランサムウェア攻撃に関連する送信元IPアドレス、宛先IPアドレス、ファイルの種類などに関する情報を含むこれらのデータを分析して、ランサムウェアの活動を特定しました。
- **ランサムウェアのサンプルと攻撃データに関するThreatLabzチーム独自の分析。**ThreatLabzは、ランサムウェア ファミリーと脅威アクター、そして関連する攻撃テレメトリーを追跡しています。また、イニシャル アクセス ブローカーが使用するツールや、ランサムウェアそのもの(ファイル暗号化アルゴリズムを含む)を理解するために、徹底的なリバース エンジニアリングを実施しています。暗号に欠陥が存在し、それを利用して身代金を支払わずにファイルを復号できることを多くのケースで発見し、復号ツールを開発しました。これらのツールは、国際的な法執行機関に提供され、被害組織に無料で提供されています。ThreatLabzはまた、Zscalerクラウド内で脅威を自動的に検知し、阻止できる独自のマルウェア防御自動化プラットフォームも構築しています。
- **外部のインテリジェンス ソース。**可能な場合、独自のデータとオープン ソースの調査結果をまとめ、比較しました。

ThreatLabzについて

ThreatLabzは、Zscalerが誇る世界トップクラスのセキュリティ調査部門であり、Zscalerのプラットフォームを使用する世界中の組織が常に保護された状態にあることを保証する責任を担います。ThreatLabzのメンバーは、マルウェアの調査や振る舞い分析に加え、Zscalerのプラットフォームの高度な脅威対策を実現するための新しいプロトタイプ モジュールの研究開発も進めています。また、定期的に社内のセキュリティ監査を実施して、Zscalerの製品とインフラがセキュリティ コンプライアンス基準を満たしていることを確認します。ThreatLabzは、新たな脅威に関する詳細な分析を定期的にポータル (research.zscaler.com)で公開しています。

Zscaler ThreatLabzをフォローし、公開されている侵害の痕跡(IOC)やMITRE ATT&CKマッピングなど、最新のランサムウェアの脅威とその動向に関する情報を定期的に入手してください。これらの情報は、各担当者のトレーニング、セキュリティ態勢の改善、ランサムウェア攻撃の防止に役立てることができます。

ThreatLabzは、[IOC](#)、[ツール](#)(概念実証のランサムウェア復号ツールなど)、そしてすべての主要なランサムウェア グループから得た[ランサムウェア メモ](#)のアーカイブを含むGitHubリポジトリも管理しています。

X [@ThreatLabz](#)

ThreatLabz [セキュリティ リサーチ ブログ](#)

Zscalerについて

Zscaler (NASDAQ: ZS)は、より効率的で、俊敏性や回復性に優れたセキュアなデジタル トランスフォーメーションを加速しています。Zscaler Zero Trust Exchange™は、ユーザー、デバイス、アプリケーションをどこからでも安全に接続させることで、数多くのお客様をサイバー攻撃や情報漏洩から保護しています。世界160拠点以上のデータ センターに分散されたSASEベースのZero Trust Exchangeは、世界最大のインライン型クラウド セキュリティ プラットフォームです。詳細はこちら: www.zscaler.com/jp





Zero Trust Everywhere

Zscalerについて

Zscaler (NASDAQ: ZS)は、より効率的で、俊敏性や回復性に優れたセキュアなデジタルトランスフォーメーションを加速しています。Zscaler Zero Trust Exchange™プラットフォームは、ユーザー、デバイス、アプリケーションをどこからでも安全に接続させることで、数多くのお客様をサイバー攻撃や情報漏洩から保護しています。世界160拠点以上のデータセンターに分散されたSSEベースのZero Trust Exchange™は、世界最大のインライン型クラウド セキュリティ プラットフォームです。詳細は、zscaler.com/jpをご覧ください。Twitterで[@zscaler](https://twitter.com/zscaler)をフォローしてください。

© 2025 Zscaler, Inc. All rights reserved. Zscaler™およびzscaler.com/jp/legal/trademarksに記載されたその他の商標は、米国および/または各国のZscaler, Inc.における(i)登録商標またはサービス マーク、または(ii)商標またはサービス マークです。その他の商標はすべて、それぞれの所有者に帰属します。

+1 408.533.0288

Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134

zscaler.com/jp