

For の

第11巻、第3号

ランサムウェア レポート 2025

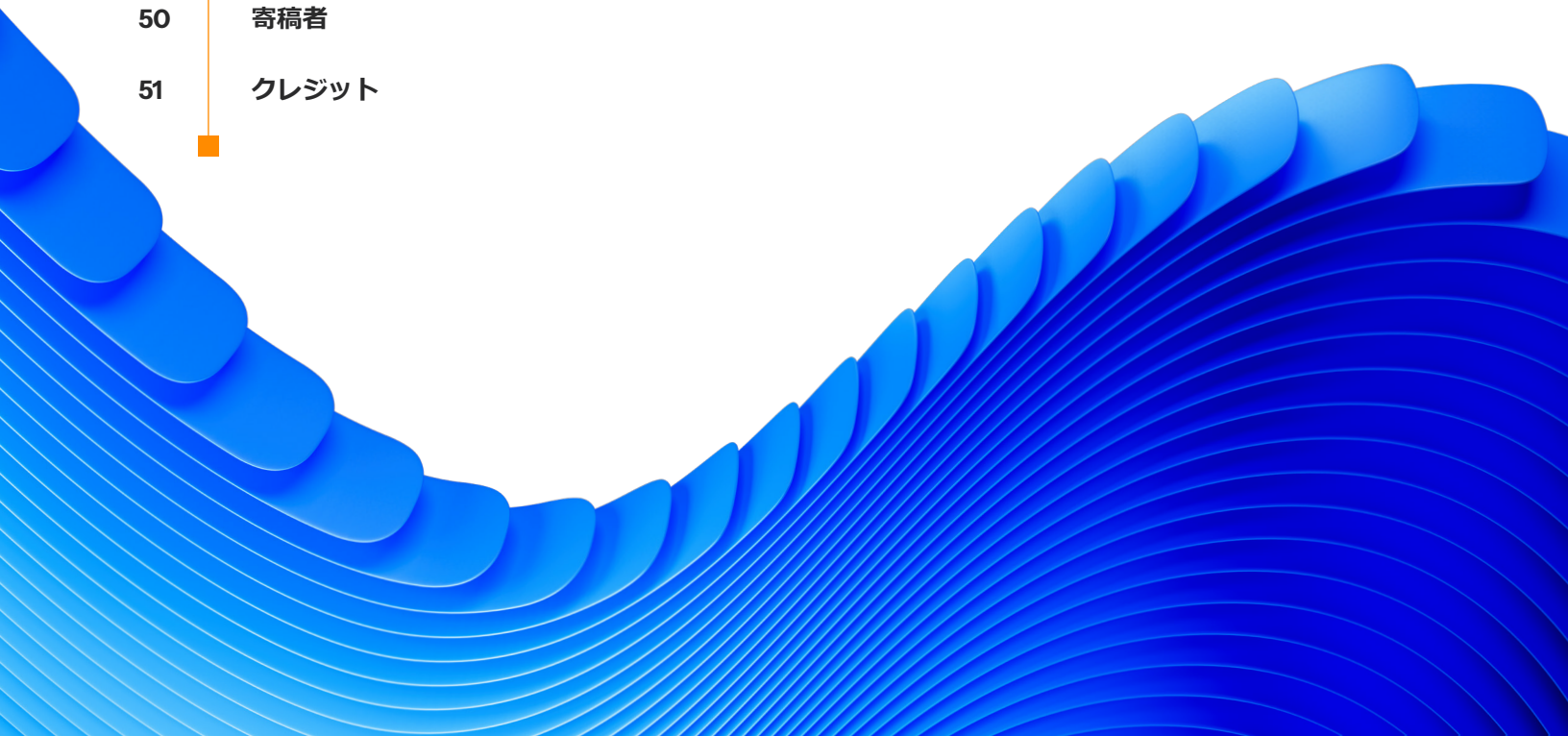
急変する脅威にさらされる中で回復力を構築



インターネットの現状／セキュリティ

目次

03	概要
05	本レポートの主な知見
06	攻撃パターンとお客様への影響の概要
07	脅迫戦術の進化
14	RaaS エコシステムの内幕
24	RaaS を伴うハクティビズム
27	セキュリティの注目点 ：TrickBot による悪性のおやつ（寄稿者：Or Zuckerman）
28	業界別の傾向
31	セキュリティの注目点 ：クリプトマイナー（寄稿者：Maor Dahan）
38	ランサムウェア攻撃が運用の継続性に与える影響
40	セキュリティの注目点 ：ランサムウェアと法律（寄稿者：James A. Casey）
43	世界中でランサムウェアに対する回復力を構築
47	緩和策
48	結論
49	調査手法
50	寄稿者
51	クレジット



概要

2025 年、ランサムウェア情勢は一層複雑性を増し、急激に変化しています。FunkSec や Black Basta などのグループは、それぞれ生成人工知能（生成 AI）や大規模言語モデル（LLM）を使用してランサムウェアコードを作成し、ソーシャルエンジニアリング攻撃を強化していると報告されています。攻撃者は多重脅迫手法を使用していますが（四重脅迫の場合さえあります）、攻撃者が好む手法は依然として二重脅迫です。法執行機関による大規模なテイクダウンにもかかわらず、脅威アクターは強い回復力を示しています。つまり、グループの再編成、リブランド、新しいグループの形成などにより、支配的なグループの解散によって生じた空白は迅速に埋められています。

攻撃者は AI と LLM をどのように利用しているか

攻撃者は **AI と LLM を迅速に統合**し、運用の規模拡大、高度化、効率性の向上を進めています。FunkSec などのランサムウェアグループは、生成 AI を使用して悪性コードを生成し、新しいランサムウェアバリエーションを作成し、チャットボットを展開して被害者と交渉します。また、攻撃者は **AI を使用して信憑性のあるフィッシングメールを作成**し、企業の従業員になりすます音声フィッシング（「ヴィッシング」）攻撃を行います。持続的標的型攻撃を行うグループも、限られた規模で **生成 AI** を使用し始めています。**Forest Blizzard（別名 Fancy Bear）** と **Emerald Sleet** は、フィッシングキャンペーンで LLM を活用して、公式文書の模倣や、脆弱性調査を実施していると言われています。また、WormGPT、DarkGPT、FraudGPT などの新しいツールは、サイバー犯罪者が攻撃の規模と有効性の両方を向上させるために役立っています。

分散型サービス妨害攻撃を多重脅迫に追加

従来の暗号化に加えて、攻撃者は複合的に圧力をかける高度な多重脅迫手法も展開しています。攻撃者は、同時暗号化、データ窃盗、分散型サービス妨害（DDoS）の脅威を巧みに利用して、組織に対する影響力を強めています。一部のランサムウェアグループは、利益を最大化するために、盗んだ重要資産や機密性の高い企業データを、ダーク Web 市場の最高入札者にオークションで売ります。

サイバー犯罪とハクティビズムの境界があいまいに

ランサムウェアグループの大半は主に金銭的な脅迫を追求していますが、厄介なことに、利益重視のサイバー犯罪と思想的な動機のあるハクティビズムの間にあった従来の境界が消滅しつつあります。Ransomware as a Service (RaaS) は、開発者、アフィリエイト、ゼロデイ市場、攻撃のオーケストレーションの鍵となるイニシャル・アクセス・ブローカーで構成される広範な犯罪エコシステムによって成り立っています。この広範な犯罪エコシステムはサービス産業へと発展し、犯罪グループは自組織のブランド構築やマネーロンダリングなどの機能に特化するようになっていきます。ハクティビストとしての動機のある RaaS グループは、思想的目的または政治的目的を前進させるために、支払われた身代金をキャンペーンの資金として使用します。さらに、Head Mare、Twelve、NullBulge などのハクティビストは、標的の国々で大きな混乱を引き起こすランサムウェア戦略を採用しており、これによって脅威の状況がさらに複雑化しています。

ランサムウェアとの戦いにパートナーが参戦

ゼロトラスト・アーキテクチャやその他のセキュリティ制御を導入することで、組織のサイバーレジリエンスを高め、ランサムウェアの被害をプロアクティブに緩和することが可能になります。しかし、さらなる支援も必要であり、着実に提供され始めています。防御者の官民のパートナーや法執行機関が脅威インテリジェンスとベストプラクティスを共有し、変化をもたらしています。[FBI が提供した復号キー](#)により、2022 年以降、被害者は 8 億米ドル以上の支払いを回避することができました。また、政府は[組織による脅威アクターへの支払い](#)を禁止することを目的とした法律の制定を進めています。身代金を支払ってもデータが戻ってくるとは限らないため、このような政策は組織にとって有益です。最後に、サイバー保険会社は、組織がセキュリティプログラムを強化することを奨励し、身代金支払額を減らすための交渉スキルを提供しています。

Akamai のソーتریダーシップと調査

Akamai のセキュリティリサーチは、攻撃者グループが使用する新たな手法を分析することにより、サイバー犯罪エコシステムを白日の下にさらすことに取り組んでいます。この「インターネットの現状 (SOTI)」レポートでは、次の 2 つの主要な脅威に焦点を当てています。



TrickBot マルウェア (Ryuk、Conti、Diavol などのランサムウェアグループが利用しています)



クリプトマイナー (Akamai の研究者は、クリプトマイナーをランサムウェア情勢の重要な交点の 1 つとして認識しています。なぜなら、クリプトマイナーの目標と戦略はランサムウェアグループのものと類似しているからです)

さらに、脅威に関する知識の豊富な Akamai のエキスパートは、セキュリティリーダーや防御者が組織の回復力を強化し、堅牢な保護を展開し、さらには現在ますます高度化しているランサムウェアの脅威にプロアクティブに対抗できるように、戦略的で実用的な知見を提供します。

本レポートの主要な知見



ランサムウェアの脅迫戦術は進化しています。**最も新しい戦術は四重脅迫**ですが、現在のところ最も一般的な戦術は、二重脅迫です。また、ランサムウェアグループは、被害者に圧力をかける、あるいはコンプライアンスを武器に使うなど、利益を生み出すための新たな方法を模索し続けています。



ランサムウェアグループが使用する TrickBot マルウェアファミリーに関連するマルウェアにより、**7億2,400万米ドル以上の暗号資産（仮想通貨）が脅し取られました**。Akamai Hunt Team は最近、5つの顧客資産上でスケジュールされた4つの悪性タスクにこのマルウェアが関連していることを発見しました。



FunkSec のようなグループが示しているように、**生成 AI と LLM を使用することで**、技術的な専門知識があまりない個人でも高度なキャンペーンを開始できるようになり、**ランサムウェア攻撃の頻度が高まり、規模も拡大しています**。



RaaS プラットフォームを活用して影響力を高めているハイブリッド・ランサムウェア・ハクティビスト・グループ（CyberVolk、Stormous、KillSec、Dragon RaaS、DragonForce など）の出現は、ランサムウェアの情勢が大きく変化し、**政治的動機や思想的動機が金銭目的の犯罪と絡み合うようになっていることを示しています**。



ハクティビストグループである Head Mare、Twelve、NullBulge は、政治的混乱を引き起こすために LockBit ランサムウェア（流出したビルダーまたは公開されているビルダーから構築）を頻繁に使用します。NullBulge は特に、**AI やオンラインゲームツールで動作するオンラインコミュニティやプラットフォームを標的にしています**。



クリプトマイナーには特有の危険がありますが、その目的や実践する戦略は前述のランサムウェアグループと類似しています。注目すべきは、**Akamai が分析したクリプトマイニング攻撃の約 50% が非営利団体や教育機関を標的としていたことです**。その理由は、これらの組織が多くの計算リソースを所有していることと、他の業界よりもセキュリティが弱いことであると考えられます。

攻撃パターンとお客様への影響の概要

Akamai の調査で、懸念すべき傾向が明らかになりました。複数のランサムウェアグループが同時に同じ組織を標的にすることが増えているため、それらの組織でリスクが高まっています。さらに、Akamai の調査では、2024 年にランサムウェアの標的となった全世界の顧客の数は大きく変動しており、顕著な山と谷があることが明らかになりました（図 1）。これらの変動は、主要なランサムウェアグループ内およびグループ間の不安定さを示唆しているとも考えられます。ランサムウェアグループは、法執行を回避し、検知されずに存在し続けるために、小規模な組織に分裂したり、リブランディングしたりすることがよくあります。

脅威グループ別の顧客数

2024 年 1 月 1 日～2024 年 12 月 31 日

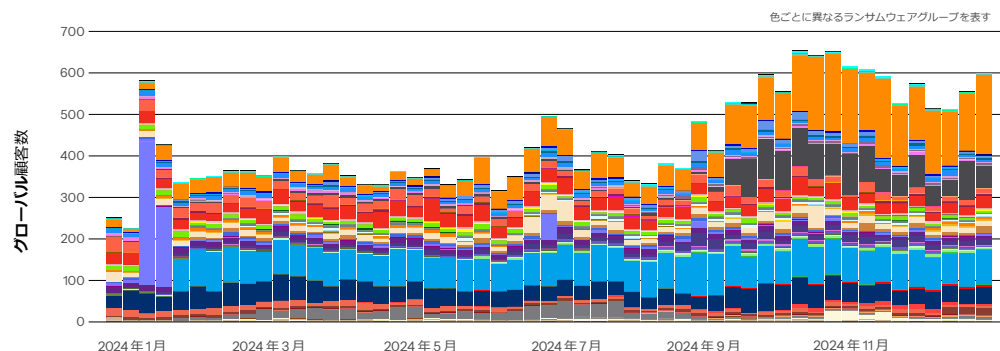


図 1: ランサムウェア攻撃の標的となった全世界の顧客数

地域別に調査したランサムウェアの活動と傾向（図 2）は、図 1 の世界的なパターンに類似しています。

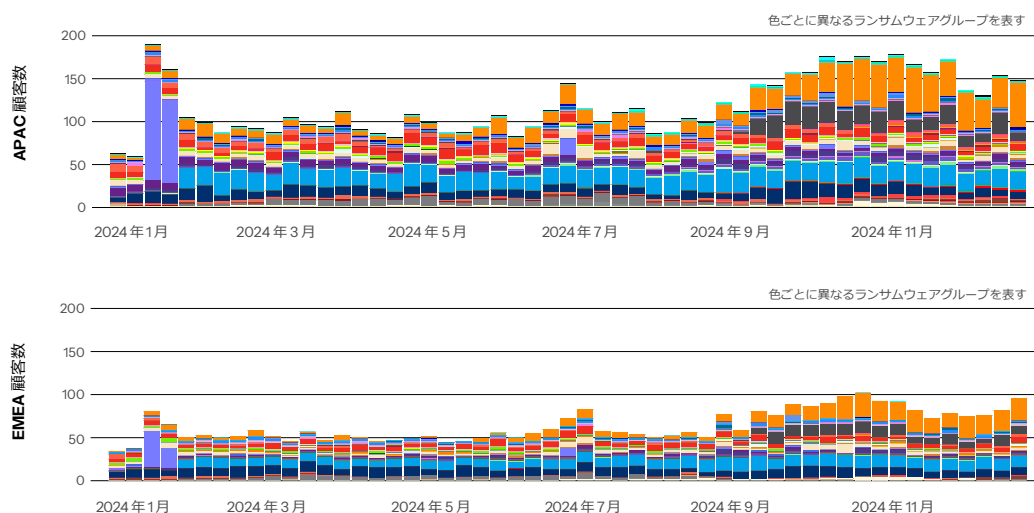


図 2: ランサムウェア攻撃の標的となったアジア太平洋（APAC）
地域と欧州・中東・アフリカ（EMEA）地域の顧客数

Verizon の「2025 年度データ漏えい／侵害調査報告書」によると、2024 年にランサムウェアは 37% 増加し、世界のデータ漏えいの 44% を占め、アジア太平洋地域では 51% を占めています。欧州・中東・アフリカ（EMEA）では、ランサムウェア攻撃を受けた企業の割合は 2024 年に 27% に増えました。ラテンアメリカ（LATAM）では、29% の企業が 2024 年に攻撃を受けたと報告しており、中小企業を標的とする攻撃が増加しています。

こうしたリスクを緩和するために、企業はサイバーレジリエンス（回復力）の強化を優先的に行う必要があります。これには、攻撃を阻止し、脅威アクターがネットワーク内で横方向に移動して機微な情報を侵害できないようにするためのセグメンテーションの実装が含まれます。

脅迫戦術の進化

ランサムウェア脅迫戦術は、単一脅迫（従来のすべてのランサムウェアオペレーションの本質）から、二重脅迫（2019 年の Maze ランサムウェアグループなど）、三重脅迫（2021 年の ALPHV / BlackCat など）、四重脅迫（2024 年の CL0P など）へ進化しました（図 3）。

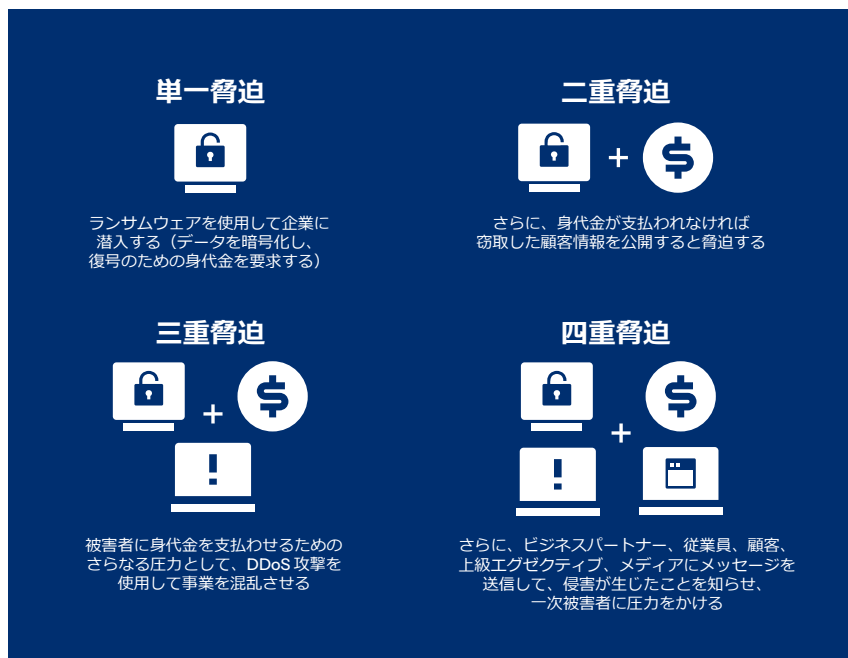


図 3：ランサムウェア脅迫戦術

このような進化した戦術は、ランサムウェアグループにとって有効であることが実証され、その結果として平均身代金支払額の上昇につながりました。三重脅迫や四重脅迫の頻度が増していますが、最も一般的な戦術は依然として二重脅迫であるようです（図 4）。また、二重脅迫戦術や四重脅迫戦術を使用しているランサムウェアグループの新しいトレンドは、**政府の規制を武器として利用**することです。

ランサムウェア	二重脅迫	三重脅迫	四重脅迫
Abyss Locker	⚠		
Black Basta	⚠		
FunkSec	⚠		
HellCat	⚠		
Interlock	⚠		
Lynx	⚠		
Morpheus	⚠		
Nnice	⚠		
RansomHub	⚠		
XELERA	⚠		
Akira	⚠	⚠	
Medusa	⚠	⚠	
ALPHV/BlackCat	⚠	⚠	⚠
CL0P	⚠	⚠	⚠
LockBit 3.0	⚠	⚠	⚠

図 4 : Akamai の研究者たちが、ランサムウェアグループがさまざまな脅迫戦術を使用していることを確認

史上最も有名なランサムウェアグループである ALPHV / BlackCat、CL0P、LockBit の 3 つのグループはすべて、四重脅迫を行いました。また、2025 年 2 月には、CL0P がわずか数週間で 385 件の攻撃を実行したと主張し、1 つのグループに起因する月間攻撃件数の**新記録**を打ち立てました。昨年 ALPHV / BlackCat と LockBit が活動停止したことを考慮すると、CL0P は 3 つのグループの中で最も安定しています。その一方、LockBit は復活した後に分裂し、コードが他のグループに広く再利用されている上に、最近では**ハッキング**を受けました。

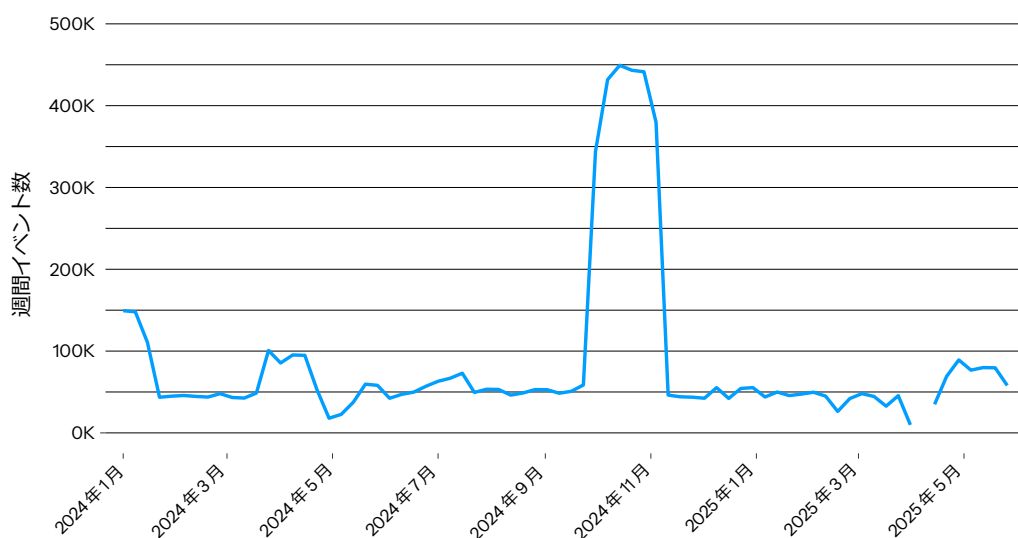
しかし、ここ数か月の間で、ランサムウェア情勢は大きく変化し、新しいグループや新興グループが大きな脅威となっています。ALPHV / BlackCat、CL0P、LockBit と同様に、これらの新興グループの多くは、暗黙のうちに（二重脅迫など）または明確に（ALPHV / BlackCat と同様）、戦術的アプローチの一環として**コンプライアンス規制を武器化**しています。いずれにしても、組織はそうした戦術への警戒を怠らず、ランサムウェア攻撃に関する特定の規制に留意し、これを遵守する必要があります。

諸地域内の注視すべきグループ

北米以外の地域で最も活動的なグループとして、2024 年に [FBI の Internet Crime Complaint Center（インターネット犯罪苦情センター、IC3）に報告された上位のバリエーション](#) である、Akira、LockBit、RansomHub、Play があげられ、これらのグループが全世界で支配的立場にあることが浮き彫りになっています。例えば、2024 年から 2025 年前半に、Akamai の研究者は、さまざまな混乱があったにもかかわらず、LockBit が APAC（2024 年 10 月に急増）と EMEA において持続的な脅威であることを確認しました（図 5）。

APAC のランサムウェアイベント：LockBit

2024 年 1 月 1 日～2025 年 5 月 31 日



EMEA のランサムウェアイベント：LockBit

2024 年 1 月 1 日～2025 年 5 月 31 日

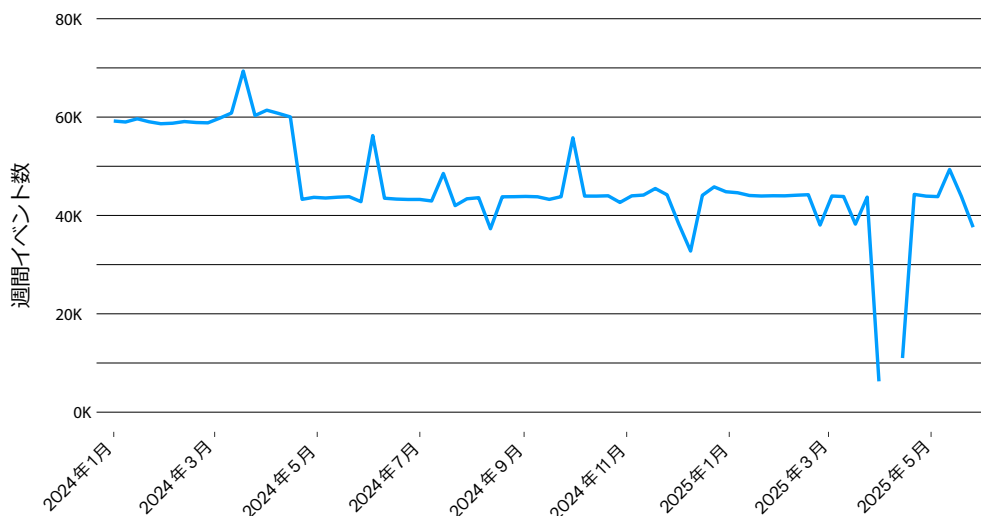


図 5：LockBit は、2024 年 1 月から 2025 年 5 月にかけて、
APAC と EMEA で依然として脅威となっている

（注：2025 年 4 月の減少している箇所は正確な描画ではありません。この時期にデータ収集上の問題がありました。）

⚠ APAC の活動的なグループ

APAC では、LockBit、ALPHV / BlackCat、CL0P などの有名なグローバルランサムウェア組織が活発であり、Royal / BlackSuit、RansomHub、Akira、Abyss Locker、Play などの新興グループも活発です。

Abyss Locker は [Australian Nursing Home Foundation](#)（オーストラリア介護施設財団）から 1.5 テラバイトのデータを流出させました。また、[シンガポールを拠点とする法律事務所](#)が、Akira グループによる高度なランサムウェア攻撃で約 190 万米ドルを支払ったと報告されています。

地域的な活動をしている他の脅威アクターも、APAC 地域全体に影響を与えています。Termite（Babuk のアフィリエイト）と Anubis は、過去 1 年間に APAC 地域で積極的に攻撃を行っています。[重要なインシデント](#)として、2025 年前半に Termite がオーストラリアの体外受精クリニックに対してランサムウェア攻撃を行ったことや、Anubis がオーストラリアの複数の病院から機微な患者記録を窃取して公開したことなどがあげられます。

⚠ EMEA の活動的なグループ

EMEA で最も活動的なのは、LockBit、RansomHub、Medusa、Akira などのグループです。2025 年 1 月には、Medusa が英国政府機関から[盗んだ文書をリークサイトに掲載](#)しました。Akira は、EMEA 地域全体の組織に影響を与える[データ漏えい](#)のリストを公開しました。これらのグループが行ったその他の具体的なインシデントとして、[ドイツの製造業者](#)に対する攻撃、[イタリア](#)での一連の攻撃、スペインのエネルギープラントの[産業用制御システム](#)に対する攻撃などが報告されています。

[英国の小売企業](#)に対する相次ぐ攻撃は、RansomHub のアフィリエイトとして知られている Scattered Spider と、[RansomHub のインフラを引き継いでいる](#)と主張する DragonForce の両方に起因しています。また、当局によるさまざまなテイクダウンやライバルグループによる攻撃にもかかわらず、LockBit と Black Basta は[適応力](#)と[変化する戦略](#)を駆使して運営を継続しています。

⚠ LATAM の活動的なグループ

LATAM では、RansomHub、FunkSec、Akira が最近最も[活動的なランサムウェアグループ](#)となっています。ある月に LATAM において脅迫によるデータ開示の件数が最も多かったのは Akira で、ブラジルで 6 件、アルゼンチンで 2 件、コロンビアで 2 件でした。また、2024 年に発生した [LATAM の航空会社](#)に対する顕著な攻撃の裏にも Akira がいました。RansomHub の活動には、メキシコの[政府機関](#)に対する攻撃もありました。また、Medusa も影響力を持っており、ブラジルの[金融ソリューションプロバイダー](#)を侵害しました。

規制違反の暴露：流行中の脅威

近年強まりつつある傾向として、ランサムウェアグループが、企業が規制に違反していることを暴露するという脅威がみられました。この戦術は、ブランドの評判低下のリスクを高め、攻撃によって生じる潜在的なコストを増大させます（規制当局からの罰金や法的費用が追加されます）。しかし、このようなコンプライアンスの武器化はまったく新しい手法というわけではありません。例えば、2019 年 12 月、REvil は、企業が身代金の支払いを拒否した場合、漏えいしたデータの開示によって厳しい規制上の罰金を科される可能性があり、その金額は身代金要求額の 10 倍以上になるかもしれないとロシアのハッカー掲示板に投稿しました*。また、2023 年末頃、ALPHV / BlackCat ランサムウェアグループは、デジタル融資ソリューションプロバイダーに対する正式な告発状を米国証券取引委員会（SEC）に提出し、同社が必要な期間内にサイバーセキュリティ侵害を開示しなかったと主張しました。

Anubis ランサムウェアグループ（2024 年後半に活動開始）は、ヘルスケアプライバシー侵害などの規制違反を明らかにして、公に（ソーシャルプラットフォーム X、リークサイト、直接コミュニケーションなどを通じて）組織を貶めることが多く、コンプライアンスリスクの高い業界（ヘルスケアやエンジニアリングなど）に注力しています。また、RansomHub（2024 年 2 月に最初に検知）のランサムウェア攻撃は注目度が高く、急速な成長を遂げていることもあって、大きな脅威となっています。同グループは、アフィリエイトに対して、規制上の罰則（一般データ保護規則（GDPR）、個人情報保護法（PIPL）、個人データ保護法（PDPL）など）の脅威を活用して被害者への圧力を高めることを明示的に促しています。WereWolves というランサムウェアグループ（2023 年 5 月に登場）は、他の攻撃的な戦術（二重脅迫、LockBit 3.0 の使用、被害者との公開コミュニケーション）に加えて、コンプライアンスの武器化も行っています。

これらの規制違反の脅威の影響は、世界中で感じられています。例えば、Anubis、RansomHub、WereWolves、ALPHV はコンプライアンスを武器化することによって被害者を明示的に脅迫しました（表 1）。

ランサムウェアグループ	標的となる地域	標的となる業界	規制違反の公表 （脅迫に利用される 法令／規制）	脅迫に利用される報告先
Anubis	グローバル （特に米国と欧州）	ヘルスケア、政府機関	HIPAA（米国）、 GDPR および 2018 年 データ保護法（英国）、 GDPR（EU）	米国保健福祉省（HHS）、 英国情報コミッショナー オフィス（ICO）、欧州 データ保護会議（EDPB）
RansomHub	グローバル （特に欧州、中国、 サウジアラビア）	IT と重要インフラに 集中しつつ、さまざま な業界に広く普及	GDPR（EU）、PIPL （中国）、PDPL （サウジアラビア）	EDPB、中国サイバースペ ース管理局（CAC）、サウジ・ データ AI 庁（SDAIA）
WereWolves	ロシア、欧州、 北米、アフリカ	IT、金融サービス、 ホスピタリティに 集中し、さまざまな 業界に広く普及	明確ではないが、次の 規制に基づいて脅迫される 可能性がある。GDPR （EU）、ePrivacy（EU）、 GLBA（米国）、SEC 規則 （米国）、連邦法 152-FZ （ロシア）、2012 年デー タ保護法（法令 843、 ガーナ）	明確ではないが、次の規制に 基づいて脅迫される可能性が ある。各国のデータ保護当局 （DPA）、SEC、ロシア連邦 通信・情報技術・マスコミ分 野監督庁、およびデータ保護 委員会
ALPHV（2024 年に 活動中止）	グローバル （特に米国）	ハイテク、ヘルスケア	SEC（米国）開示 規則、HIPAA（米国）	SEC および HHS（米国）

表 1：コンプライアンスを武器化しているランサムウェアグループ

* メッセージには、「GDPR。我々に身代金を支払わない場合、どうぞ、政府に 10 倍以上の罰金を支払ってください。」と記載されています。

表に記載しているのは、被害があった特定の規制違反の脅威のみです。これらのグループは、他の地域の他の規制も武器化する可能性があります。二重脅迫を行うだけで当局には接触しないとしても、被害者の規制違反を引き起こす可能性のある機微な情報を公開しています。そのため、公表される可能性のあるその他の規制違反（WereWolvesによって引き起こされたものなど）と関連規制当局を含めました。

サイバーセキュリティ規制は、企業のデジタル環境および運用環境のセキュリティ強化を促進し、業界全体でデータ保護、継続性、信頼性、コンプライアンスを強化する上で有益です。しかし、さまざまな業界や地域でサイバーセキュリティ規制が強化され続けているため、サイバー犯罪者が脅迫に利用できるコンプライアンス違反を発見し、身代金支払い要求に活用する機会が増大しています。

地域ごとの苦悩

脅威アクターは調査を行い、規制違反を公表するという脅威によって生じ得る損害が最も大きい地域に引き寄せられます。例えば、EMEA では、政府主導の規制機関が EU および英国内のコンプライアンスを推進し、報告の期限、施行、および罰金の一貫性を高めています。同様に、北米では、産業審議会または協会、連邦政府機関、州／省が積極的に規制を推進しており、通常厳格に施行されます。

対照的に、LATAM の急速なデジタルトランスフォーメーションと、増え続ける接続システムに見られる脆弱性は、ランサムウェア攻撃の標的として、この地域の魅力を高めています。しかし、同地域全体でサイバーセキュリティ規制とその施行に一貫性がないため、この種の脅迫の影響は抑えられています。APAC でも同様です。この地域には多種多様な新しいコンプライアンス要件があり、より厳格に施行されている地域もあれば、報告しなかった場合に生じる影響が一貫していない地域もあります。そのため、LATAM や APAC の一部の地域で、規制違反を公表すると脅迫するグループが影響を及ぼしているという証拠はまだ見られず、NIS2 などの新しい規制はまだ活用されていません。しかし、脅威アクターがどれほど迅速にフォーカスを移すことができるかは分かっているため、より広範なトレンドを追跡する価値があります。

Akamai の研究者は、ランサムウェアグループが使用する規制に関する脅威の戦術における進化を追跡し続けています。国際的な企業にとっては、地域ごとの報告要件に適切に対応し、セキュリティ能力が監査や危機管理措置をサポートする形で、コンプライアンス文書を提供できるようにすることは、複雑な課題です。それでも、この攻撃の矢を脅威アクターの矢筒から取り除くことが重要です。以下は、それぞれの地域で追跡すべき規制の重要箇所の一部を挙げたものです。

- **APAC :** 報告期限は、攻撃の影響度に応じて 12 ～ 72 時間です。一部の国（日本など）では、現在罰金は科されていません。シンガポールなど他の国では、**PDPA** に違反した場合、年間収益の 10% の罰金が科されることがあります。**インド**では、刑事罰が科される可能性もあります。
- **EMEA :** 速やかな報告と罰金の要件は、APAC の要件と似ています。例えば、**NIS2 の 24 時間の報告期限**に従わなかった場合、最大 1,000 万ユーロまたは会社のグローバル年間収益の 2% のいずれか大きい方の罰金が科される可能性があります。**GDPR** では、組織の報告期限が長い（72 時間以内）ですが、罰金は 2 倍になります。現在、**英国**と**欧州連合**の両方でランサムウェアに関するその他の報告要件が検討されています。
- **LATAM :** 規制は**国によって異なります**。ブラジルでは、**Lei Geral de Proteção de Dados Pessoais（個人情報保護法、LGPD）**に基づく厳格な方針が示されており、最初の報告は 72 時間以内に、補足情報は 20 日以内に提出する必要があります。報告しなかった場合の罰金は、1 回の違反につき年間収益の 2% になる可能性があります。
- **北米:** 24 時間以内に報告しなかった場合、**SEC の制裁金**は 1,000 万米ドルとなります。**Health Insurance Portability and Accountability Act of 1996（1996 年医療保険の携行性と責任に関する法律、HIPAA）への違反**を開示しなかった場合、刑事罰に加え、インシデントの重大度に応じて、インシデント 1 件あたり 100 米ドルから最大 150 万米ドルまでの罰金が科される可能性があります。**Cyber Incident Reporting for Critical Infrastructure Act（重要インフラに係るサイバーインシデント報告法、CIRCA）**が 2026 年に施行される見込みで、この法令ではランサムウェアの報告が義務付けられます。

RaaS エコシステムの内幕

RaaS はランサムウェアの運用に革命をもたらし、高度に専門的な攻撃から、より幅広い、サイバー犯罪者が利用できるスケーラブルなサブスクリプションベースのサービスへと変革しました。この重要な変化により、これまでランサムウェアの展開を妨げていた技術的な障壁がなくなり、サイバー犯罪者は最小限の技術的な専門知識で巧妙な攻撃を仕掛けられるようになりました。ランサムウェアが一般化すると、犯罪者グループ内の開発者は安定した収益を得られるようになります。また、技術的な知識の浅い脅威アクターが重大なデジタル脅迫キャンペーンに参加できるようになります。RaaS の普及により、攻撃の規模と頻度が大幅に増大し、組織ではこの脅威に対応するため、より回復力の高いセキュリティアーキテクチャの実装が強く求められるようになっていきます。

REvil、Ryuk、DarkSide などの RaaS プラットフォームは、2010 年代半ばに登場し、すぐに使用できるランサムウェアキットをアフィリエイトに提供して収益の一部を得るというコンセプトを先駆けて開発しました。金銭的利益を生み出すことだけでなく、このビジネスモデルが実際に及ぼす悪影響が、注目度の高いオペレーションにおいて明らかになりました。例えば、[Colonial Pipeline のインシデント](#) (DarkSide グループに起因) は、米国内の重要なサービスやインフラを混乱させると同時に、オペレーターにかなりの利益をもたらしました。

RaaS ビジネスモデルの主要なエンティティ

RaaS の急速な成長と成功は、アクセス性、運用効率、および正当なビジネスを反映した組織構造から生まれています。これらの犯罪企業では、役割を分担し、それぞれに専門的な役割を持たせることで、全体的な業務の最適化を図っています。図 6 は、RaaS エコシステムにおける主要プレイヤーとその役割を示したものです。



図 6 : RaaS チェーンを構成している重要なプレイヤー

ランサムウェア開発者

RaaSの開発者やオペレーターは、ランサムウェアソフトウェアの作成、更新、および保守を担当し、そのソフトウェアはその後、アフィリエイトに販売またはリースされます。さらに、強力なマルウェア（多くの場合、使いやすいインターフェースと24時間体制の顧客サポートを備えています）を設計し、サポートインフラを管理し、アフィリエイトのための安全な通信チャネルを確立します。このような高度なスキルを持つサイバー犯罪者は、検知を回避し、運用上の信頼性を確保するために、頻繁に新しい機能と能力を実装しています。

金銭的な取り決めは通常、利益共有モデルに従います。攻撃を実行するアフィリエイトの取り分が大きく、その幅は60 / 40から始まり、90 / 10といった有利な比率まであります。

アフィリエイト

アフィリエイトは、ダーク Web 市場を通じて開発者からランサムウェアを取得し、標的の特定、攻撃の展開、時には被害者組織との交渉も行います。このようなサイバー犯罪者は、月額料金を支払い、ランサムウェアソフトウェアをリースすることがあります。また、ライフタイムライセンスを取得することもあります。開発者とは異なり、アフィリエイトの方が一般的に技術的スキルは低く、運用上のミスや法執行機関に見つかるリスクが高くなります。

標的を選択するのはアフィリエイトですが、アフィリエイトが遵守する必要がある一連のルールを提供するのは開発者です。例えば、特定の国や業界に対して標的を制限するルールなどがあります。このような規則を破ることは、グループからの排除を意味する場合があります。また、場合によっては、開発者が**無料**で復号ツールを被害者に提供することもあります。いくつかのランサムウェアグループは一時、特に COVID-19 のパンデミック期間中に、ヘルスケア組織を標的にすることを避けました。**DragonForce** は、LockBit 3.0 と Conti コードを組み合わせたコードを使用しており、一部の種類のヘルスケア組織を標的としない道德規範に従っていると主張しています。

イニシャル・アクセス・ブローカー

標的の特定と偵察を促進するために、アフィリエイトは、標的に対する侵害とサイバー犯罪者（ランサムウェアオペレーターなど）へのネットワークアクセスの販売を専門とするイニシャル・アクセス・ブローカー（IAB）を参加させることがよくあります。

IAB には、攻撃自体を開始せずに足掛かりを得ることにより RaaS の運用を合理化することができる特定のスキルがあります。これにより、法執行機関から注目を浴びるのを避けることができます。IAB は、リモート・デスクトップ・プロトコル（RDP）、VPN アクセス、電子メールアクセス、ファイル共有アクセスなど、さまざまなアクセスタイプを販売しています。RDP は販売されている最も一般的なアクセスタイプですが、VPN アクセスも徐々に普及しつつあります。これは、VPN が、企業ネットワークへのより隠蔽性が高く、かつ直接的なアクセスを提供するためかもしれません。

アクセスの価格は、標的となる組織の収益によって異なり、より価値の高い環境では価格が高くなります。2024年には、**アクセスリストの86%**が3,000米ドル以下に価格設定されました。

RaaS エコシステムの主要プレーヤー

以下のプロフィールでは、2024 年から 2025 年前半に活動していた最も顕著な RaaS グループのいくつかについて説明し、それらの革新的な戦術を明らかにします。各グループは、手法の重大度と、この文書の作成時点での企業への影響に基づいてまとめられています。それらのグループのイノベーションは、セキュリティ防御担当者や法執行機関からのプレッシャーが高まっているにもかかわらず、RaaS がどのように進化し続けているか、オペレーターやアフィリエイトがどのように適応し続けているかを示しています。

RansomHub

[RansomHub](#) は、2024 年初頭に初めて観測され、Windows、VMware ESXi、SFTP サーバーを標的とするマルチ OS ランサムウェアとして注目を集めました。このグループは二重脅迫を使用しており、ヘルスケア業界、教育業界、公共部門の 200 以上の組織に影響を与えました。

今年の初めには Akamai の顧客の環境における RansomHub のアクティビティが大幅に増加し、70 万件近くのイベントが記録された期間や、それ以上の件数が記録された期間がありました（図 7）。

全世界のランサムウェアイベント：RansomHub

2024 年 9 月 1 日～ 2025 年 5 月 31 日

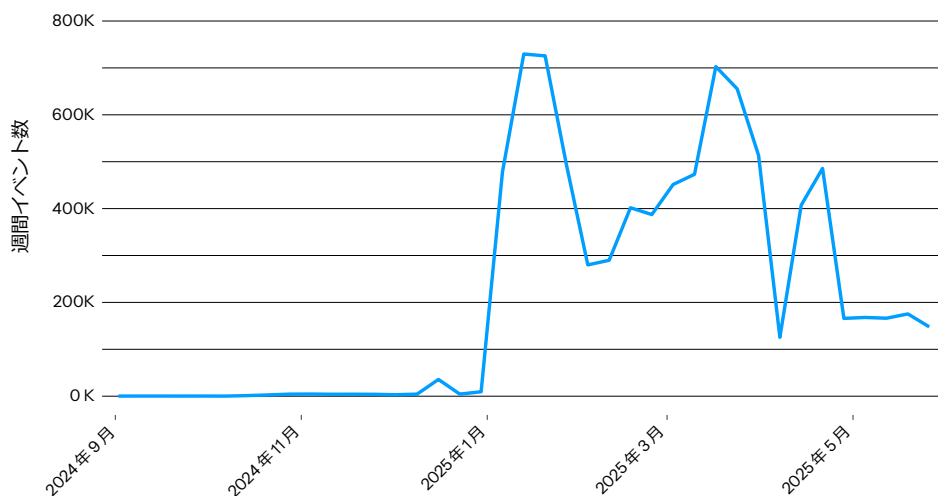


図 7：Akamai の顧客の間で観察されたトラフィックの増加により、2025 年 1 月以降に RansomHub の広まりが拡大していることが明らかとなっている

RansomHub は、EDRKillShifter などの[回避ツール](#)を使用してエンドポイント保護を無効にし、[CVE-2024-1709](#) などの脆弱性を悪用することで広まっています。ほとんどのグループと同様に、RansomHub は二重脅迫戦術を使用しており、データを暗号化して、被害者が身代金を支払わなければ窃取した情報をリークすると脅迫します。また、脅迫メカニズムの一環として、RansomHub は、規制上の罰則を回避するために身代金を支払うよう組織に圧力をかけるために、被害者を GDPR 当局などの規制機関に報告するようリークサイト上のアフィリエイトに指示しています。さらに、オペレーターはカスタマイズされたツールとサポートをアフィリエイトに提供し、アフィリエイトが別個のステップとして機密情報を窃取できるようにしています。場合によっては、以前に侵害を受けた組織をアフィリエイトが再び標的にし、窃取したデータを利用してさらに金銭的利益を得ることもあります。

[RansomHub の構造とビジネスモデル](#)、特に 90 / 10 の身代金分配率を含む優遇条件は、経験豊富な脅威アクターとサイバー犯罪初心者の両方を惹きつけています。2025 年 4 月 1 日、RansomHub の[インフラはオフラインとなり](#)、アフィリエイトのいくつかは DragonForce や Qilin などのグループに移行しました。

CLOP

CLOP は、ファイル転送システムのゼロデイ脆弱性を体系的に悪用することに秀でています。これには、ファイル転送アプライアンス ([CVE-2021-27101](#)、[CVE-2021-27102](#)、[CVE-2021-27103](#)、[CVE-2021-27104](#))、GoAnywhere MFT ([CVE-2023-0669](#)) および PaperCut ([CVE-2023-27350](#)、[CVE-2023-27351](#)) を標的にした攻撃などがあります。特に、CLOP は MOVEit Transfer を悪用し ([CVE-2023-34362](#))、2,500 台以上の脆弱なサーバーを侵害しました。[同グループ](#)は最近、クラウド・サービス・プロバイダーからデータを抜き取ってリークしたことと、Cleo が管理するファイル転送製品のゼロデイ脆弱性を悪用してリモートコード実行を可能にしたことを明かしました。

CLOP は独特の戦略を採用しています。それは、ゼロデイ脆弱性の発見と同時期に綿密にキャンペーンを計画し、その合間には活動を休止することです。このアプローチにより、同グループは、攻撃の急増時を除き、全体的な被害者数を比較的少なく抑えながら、高価値の標的を効果的に侵害することができます。さらに、三重脅迫メカニズムを使用しています。場合によっては、顧客に連絡を取って、その顧客の情報を公開すると脅し、影響を受ける組織に身代金を支払うようさらに圧力をかける、[四重脅迫](#)戦術を使用します。

FunkSec

RaaS グループ FunkSec は、生成 AI と LLM によってランサムウェアのオペレーションがどのように変化しているかを示す良い例です。二重脅迫モデルを使用する FunkSec は、2024 年後半に登場し、ランサムウェアコードの開発、チャットと通信のサポートの強化、新しいバージョンの迅速な生成に AI ツールを活用して、瞬く間に注目を集めました。まだ開発中の最新バージョンには、オークションの最高入札者に窃取データを売ること、被害者の個人的なネットワークや家族を標的にすること、標的への圧力を強めるために DDoS 攻撃を実行することなど、多重脅迫スキームが含まれる可能性があります。研究者の間では、[FunkSec の AI への大きな依存](#)は、技術的専門知識が不足していることが原因であると考えられています。

FunkSec は、オークションプラットフォーム FunkBID を導入して、従来のリークサイトから移行しました。これにより、窃取データを売却して利益を最大化できるようになりました。同グループの Rust ベースのランサムウェアは、過去に他のグループによって侵害された組織を標的にすることがよくあります。過去の侵害で盗まれたデータを使用するため、攻撃を行ったという主張の正当性を検証することが困難になります。FunkSec のアクティビティは本物の脅威なのか、認知度を高めるために騒いでいるだけなのか、多くの研究者が疑問視しています。

同グループは、FSociety などの他のランサムウェア脅威アクターと戦略的な提携関係を結び、犯罪ネットワークを拡大しています。一部のレポートは、FunkSec のアクティビティをアルジェリアまでたどり、金銭的動機に加えてハクティビストとしての動機も考えられると指摘しています。FunkSec は経験不足であるにもかかわらず、デジタル脅迫において AI を革新的に利用しており、ランサムウェア情勢における新たなトレンドのきっかけとなる可能性があります。

LockBit 3.0

2024 年 2 月に法執行機関の国際共同捜査（Operation Cronos）が行われて注目を集めるまでは、LockBit が脅威情勢を支配していました。Akamai の以前のランサムウェア SOTI レポートで、2021 年 10 月から 2023 年 5 月までは LockBit の被害組織が全体の大部分を占めていたことがわかります。同グループが長期にわたって有力だったのは、その継続的なイノベーションのためです。同グループの主要なバージョンである LockBit 3.0 は、カスタマイズ可能なペイロードと、二重脅迫（場合によっては三重脅迫）戦術をアフィリエイトに提供します。LockBit 3.0 は、重要なインフラを標的とすることや、バグ・バウンティ・プログラムと脅迫ポータルを備えた高度なアフィリエイト構造を保持していることで知られています。このバグ・バウンティ・プログラムは、1,000 米ドルから 100 万米ドルの報酬でハッカーを誘惑してソフトウェアの欠陥に関する情報を送信させ、脅威の普及を促進しています。

LockBit の回復力の証明として、同グループはオペレーションの深刻な中断から数日後には、新しいデータ・リーク・サイトと共に復活しました。報告によると、Operation Cronos 後の数か月間、同グループのアクティビティは大幅に減少しましたが、LockBit には依然として紛れもない影響力があります（図 8）。

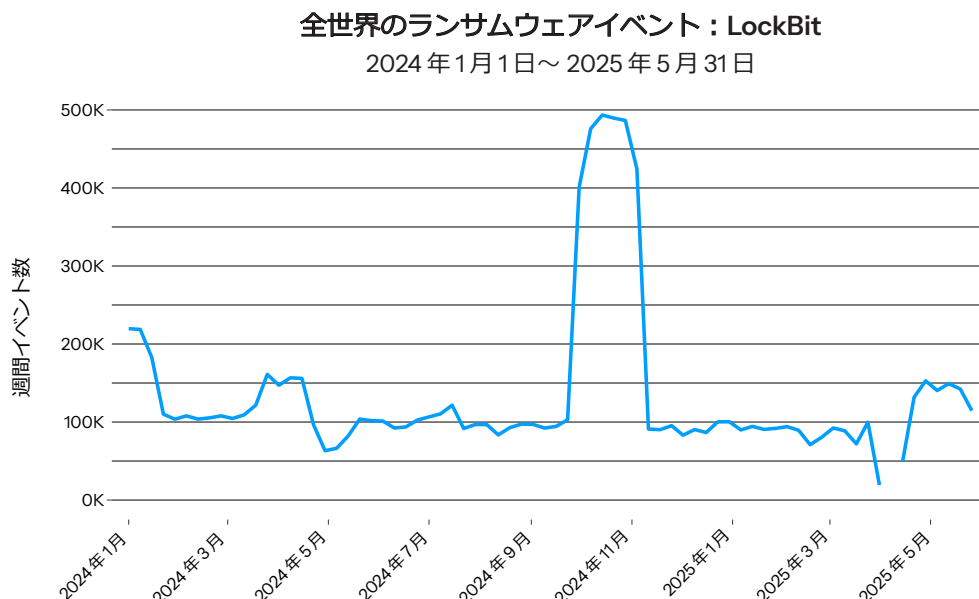


図 8：2024 年 10 月に Akamai の顧客の環境全体で LockBit のアクティビティが急増した。これは、データ・リーク・サイトで同グループが発表した被害者の増加と関連している

2025 年 5 月、LockBit は未知の攻撃者から大きな侵害を受け、2024 年 12 月から 2025 年 4 月までデータ漏えいが発生しました。これには、身代金オペレーションに使用されるビットコインのウォレットアドレスや、LockBit と被害者の交渉メッセージなどが含まれます。LockBit のダーク Web アフィリエイトパネルが書き換えられ、図 9 に示すメッセージが表示されました。このメッセージには、リークした MySQL データベースダンプをダウンロードするためのリンクが含まれています。

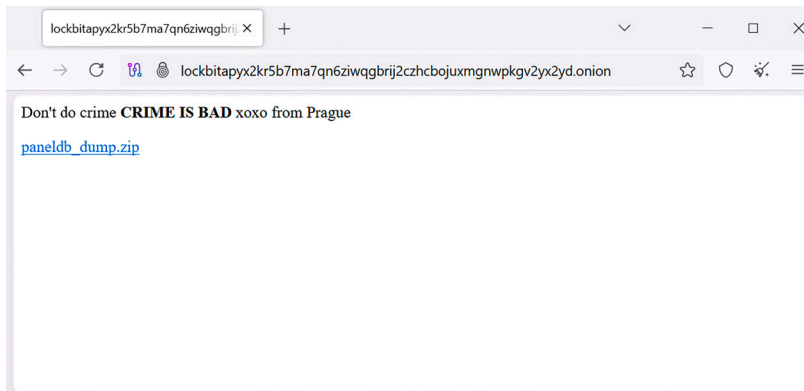


図 9 : LockBit のデータ・リーク・サイトは、2025 年 4 月に未知の攻撃者によって書き換えられた
(出典 : [Bleeping Computer](#))

Black Basta

Black Basta は二重脅迫のアプローチを採用しており、ヘルスケアプロバイダー、製造業者、金融機関を含む全世界の **500 以上の組織に対する攻撃** に関与しています。Akamai の顧客では、ある週の攻撃試行数が 120,000 件以上に達し、それがピークとなりました (図 10)。

全世界のランサムウェアイベント : Black Basta

2024 年 1 月 1 日 ~ 2025 年 5 月 31 日

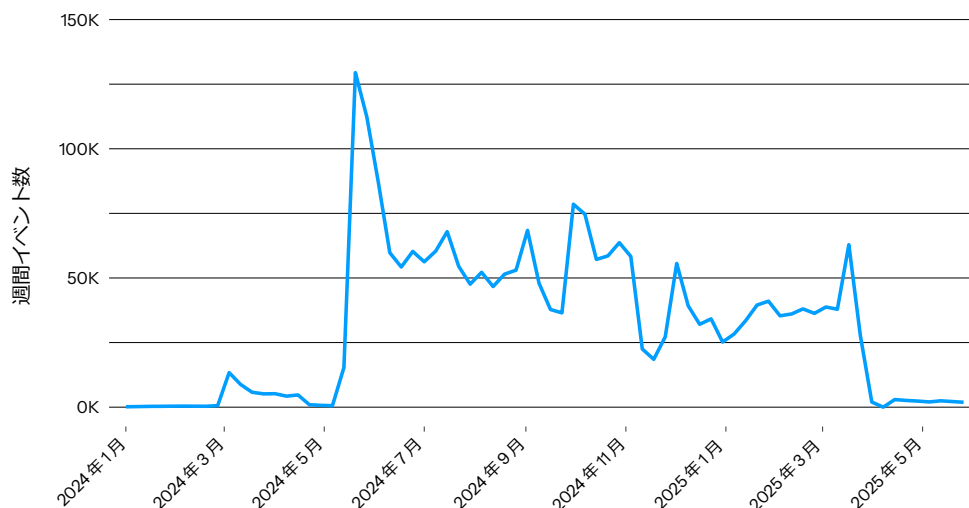


図 10 : Black Basta のランサムウェアアクティビティは、ある週に 120,000 件以上に達し、ピークとなった

同グループは、以前の Conti オペレーターと関連付けられており、ランサムウェアを展開する前にセキュリティソフトウェアを無効にし、機微な情報を窃取することで知られています。2025 年 2 月、同グループのチャット内容が流出し、オペレーションや戦術・手口・手順（TTP）に関する知見が明らかになりました。これには、グループ内で不和が発生していることなどが含まれ、防御者にセキュリティボスチャを強化するための貴重なインテリジェンスがもたらされました。

Black Basta は、Ivanti Connect Secure を標的とするゼロデイ脆弱性を 200,000 米ドルで購入する機会があったほか（実際に購入したかは不明）、VPN などのエッジデバイスを標的とするブルートフォースツール BRUTED を積極的に使用しています。

Medusa

Medusa ランサムウェアは、2021 年に登場して以来、ヘルスケア、教育、法律、技術、製造などの複数の業界に影響を与えています。Akamai の顧客のネットワークに対しても、2024 年 1 月から 2025 年 5 月まで継続的に攻撃を試行しています（図 11）。

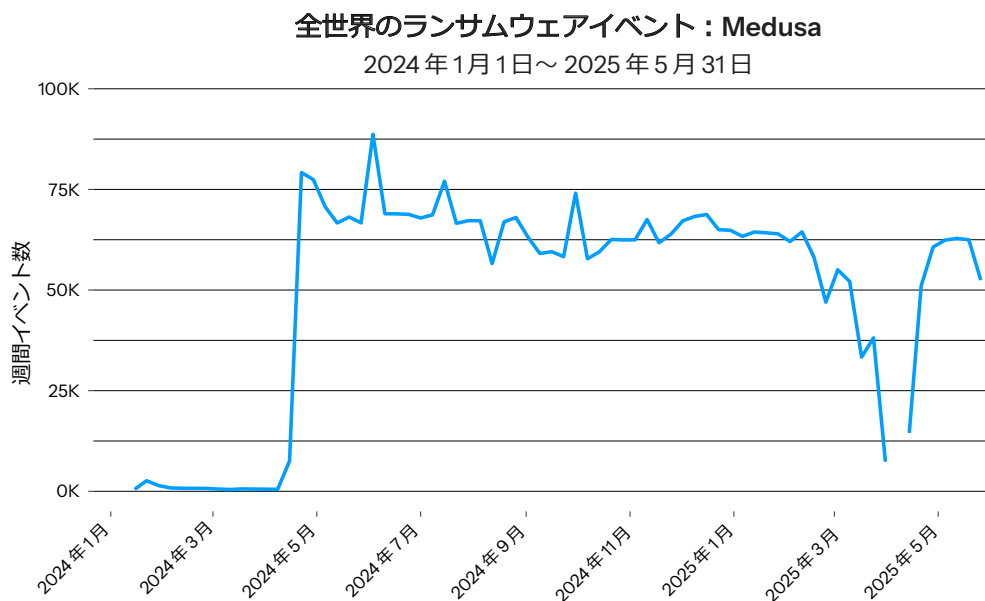


図 11：Medusa は、レポートの対象期間中、Akamai のお客様のネットワークに対する攻撃を継続的に試みている

Medusa は、開発者がすべての攻撃と交渉を処理する自己完結型のオペレーションとして発足し、RaaS ビジネスモデルに移行しました。標的を侵害するために、同グループはフィッシングキャンペーンを使用し、パッチが適用されていない脆弱性（CVE-2024-1709 や CVE-2023-48788 など）を悪用します。さらにプレッシャーをかけ、緊迫感をあおるために、データ・リーク・サイトにカウントダウンタイマーを表示します。

ALPHV / BlackCat

ALPHV（別名 BlackCat）は、三重脅迫スキームを採用している最も高度な RaaS グループの1つと見なされています。このランサムウェアは、2021年後半に初めて特定されました。Rust プログラミング言語で記述されていることで知られており、柔軟性と回避機能を備えています。このグループは、標的に潜伏して機会をうかがう手法を用いて、標的のネットワークに居座り続けます。また、セッションをハイジャックして認証情報を窃取するツールである [Evilginx 2](#) を使用し、2 要素認証などのセキュリティ制御をバイパスします。

ALPHV は、2023 年に [Reddit](#) を標的とした際に、主に機密情報を窃取し、従来の暗号化戦術から脱却しました。FBI は 2023 年 12 月に [同グループのデータ・リーク・サイトを押収](#)し、オペレーションを妨害しました。しかし、ALPHV はすぐに立ち直り、2024 年 2 月に Change Healthcare に対する注目度の高い攻撃を実行しました。この大きな注目を集めたサイバー攻撃を行った後、同グループのアクティビティは減少し（図 12）、「消失」しました（図 13）。[研究者の推測](#)によると、同グループのアフィリエイトは RansomHub としてリブランドしたか、RansomHub に移行しました。

全世界のランサムウェアイベント：ALPHV / BlackCat

2024 年 1 月 1 日～2025 年 5 月 31 日

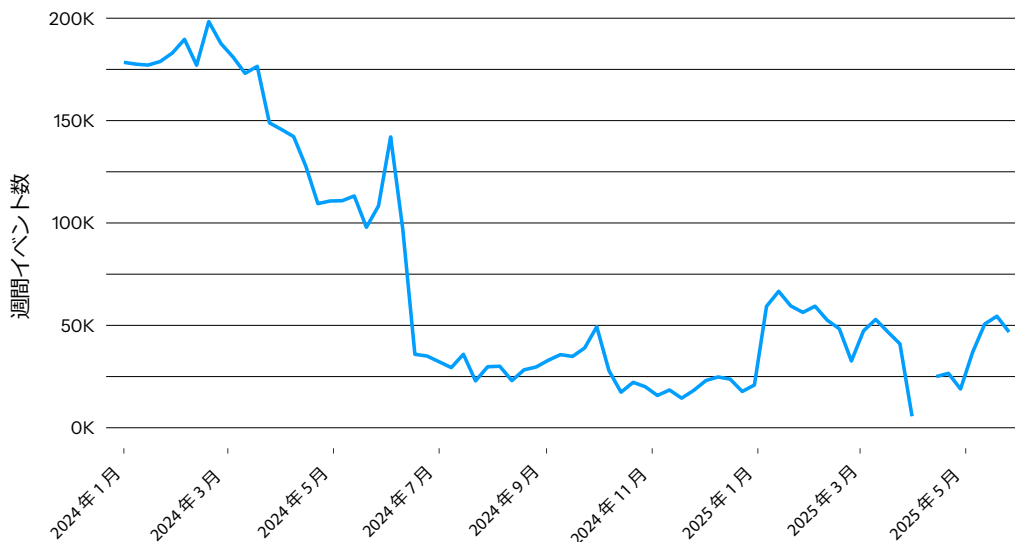


図 12：ALPHV / BlackCat のアクティビティは、2024 年 2 月の大きな注目を集めたサイバー攻撃の後、着実に減少した

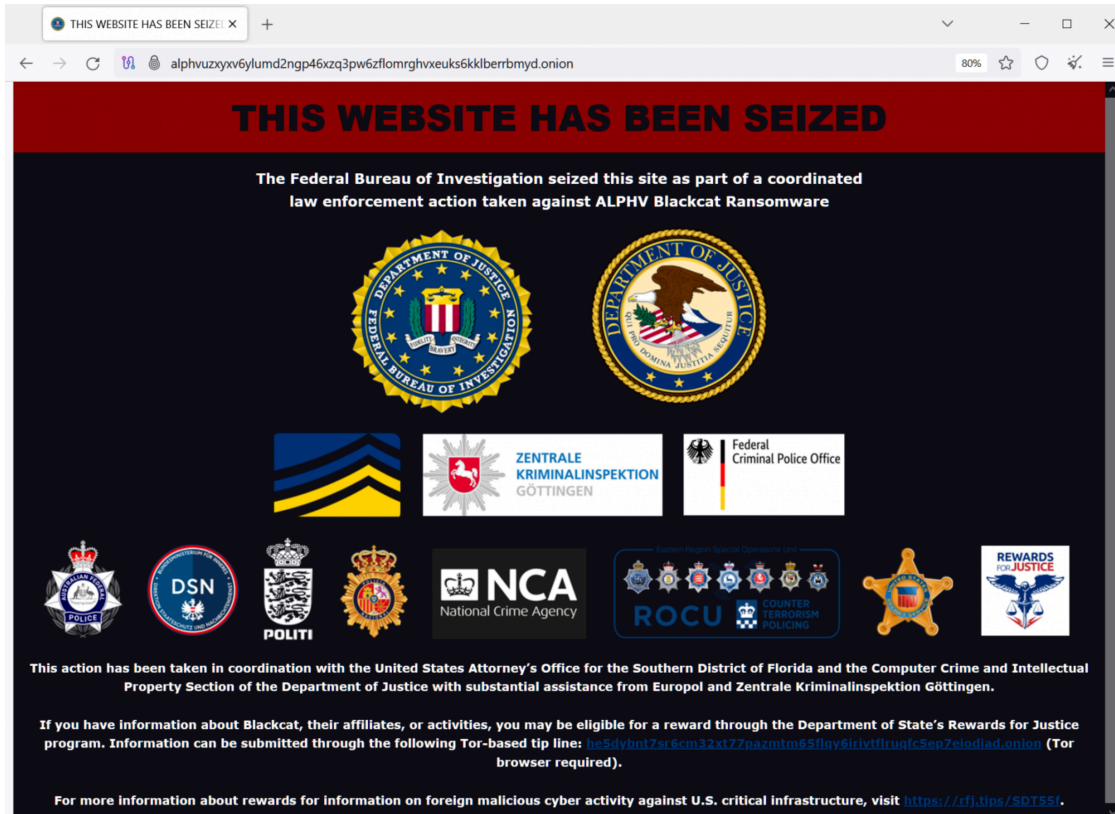


図 13 : 崩壊したふりをするために、ALPHV は FBI がデータ・リーク・サイトを押収したことを示す偽のバナーを使用した (出典 : [Bleeping Computer](#))

Akira

Akira は 2023 年初めに発足し、製造、教育、行政などの業界で急速に被害者を生み出しました。このグループは、データの暗号化、リークするという脅迫、場合によっては電話を介した直接的な圧力や、セキュリティが確保されていない Web カメラなどの内部デバイスの不正利用を含む、二重脅迫と三重脅迫の両方の手法を使用します。Akira は VPN の脆弱性を利用してアクセスし、PowerShell や SoftPerfect などのツールを使用して標的に潜伏し、機会をうかがうことが多いです。

Interlock

Interlock は、2024 年後半に初めて観測された新興のランサムウェアオペレーションです。二重脅迫モデルを使用し、Worldwide Secrets Blog と呼ばれるリークサイトを保持しています。被害者は、フィッシングや、ブラウザーの更新に見せかけた悪性インストーラーを通じて、侵害を受けることがよくあります。同グループは、ラテラルムーブメント（横方向の移動）や回避に AnyDesk や PowerShell などのツールを使用しており、最近登場したばかりにもかかわらず、技術力が高いと考えられています。

RaaS への対抗

2024 年と 2025 年の RaaS の継続的な成功は、サイバー犯罪のオペレーションが高度に進化し続けていることを示しています。脅威アクターがゼロデイ脆弱性を活用するようになっていたため、組織には潜在的な損害を最小限に抑えるゼロトラスト・ソリューションが必要です。

また、不正アクセスを防止するために、特にデフォルトまたは再利用の認証情報を使用する VPN のセキュリティを確保する必要があります。Akamai の「[Defenders' Guide](#)」では、VPN 認証に専用のアイデンティティを使用することや、サービスアカウント権限を制限することなど、セキュリティ担当者が VPN のセキュリティを強化するための、ベストプラクティスをご紹介します。

企業は、サイバーセキュリティ防御機能を継続的に革新し、更新して、Web アプリケーションファイアウォール（WAF）保護を API や生成 AI などの新しいインフラに拡張する必要があります。さらに、ランサムウェアの影響を最小限に抑えるためには、アクティブな攻撃が環境全体を移動するのを防ぐ保護（セグメンテーションなど）をエッジの背後に導入することが重要です。

RaaS を伴うハクティビズム

犯罪的な RaaS ビジネスモデルでは、さまざまな理由で提携関係が形成されています。ハクティビスト（政治的または社会的な目的を推進する悪性の意図のあるハッカー）との提携により、RaaS プロバイダーは、特に法執行機関に監視されている場合や政府による措置に直面している可能性がある場合に、**ハクティビストの動機**や政治的理由を拝借または拠り所にして注目を集めるほか、正当性を高める、金銭的動機を覆い隠すといったことが可能になります。また、このようなアプローチにより、RaaS グループを単独で犯罪企業として扱うための当局の取り組みも複雑化しています。

このセクションでは、RaaS を提供していてハクティビストとも見なされるランサムウェアグループ（ハクティビスト／ランサムウェアハイブリッドと呼びます）を時系列順に取り上げます。また、ランサムウェアをツールとして使用しているハクティビストグループについても詳しく説明します。

ハクティビスト／ランサムウェアハイブリッド

Stormous

Stormous は、2021 年半ばにオペレーションを開始したハクティビスト／ランサムウェア・ハイブリッド・グループであり、政治的動機と金銭的動機の両方があります。GhostLocker などのツールを使用して、共同のランサムウェアキャンペーンを開始するために、他のサイバー犯罪組織（最も顕著なのは GhostSec）と提携することで知られています。多くの場合、コミュニケーションや身代金要求にアラビア語を使用します。メンバーには、ロシアや中東諸国の個人が含まれると考えられます。同グループは、Coca-Cola や Mattel などの大手企業に対する攻撃を行っており、複数の国にわたる政府機関や民間企業を標的としています。Stormous は、ロシアに敵対的と見なされる国や西側の利益に沿う国を標的にすることが知られています。これには、米国、ウクライナ、インド、フランス、スペイン、ベトナムなどが含まれます。

DragonForce

DragonForce として知られるハイブリッド脅威アクターは、マレーシアを拠点とする地政学的なランサムウェアグループで、2023 年半ばから後半に出現しました。同グループは、複数の業界や国で注目度の高い破壊的な攻撃を行ったことで知られるようになり、現在最も活発に活動しているランサムウェアグループの 1 つと考えられています。DragonForce は特にイスラエルとインドを標的としています。また、英国の政府機関、公共交通機関、法律事務所、医療機関、大手小売企業、および米国、サウジアラビア、オーストラリアなどの組織も標的になっています。

KillSec

2023 年 10 月に発足した [KillSec ランサムウェア](#) は、親ロシアの政治的な報復を主な動機としてオペレーションを実施しており、サイバー攻撃がロシアの地政学的利益と合致していることがよくあります。主な標的はヘルスケア業界であり、金融機関と行政機関がそれに続きます。KillSec は、インドやその他のアジア諸国（バングラデシュなど）を標的にすることに特に関心を示していますが、米国を含む他の国への攻撃も行っています。

CyberVolk

[CyberVolk](#) は、2024 年 6 月に政治的な意図を持ったハクティビストグループとして誕生し、ロシアやインドの敵対者に対する報復としてランサムウェアを使用し始めました。同グループは、主に重要インフラ、政府機関、科学機関を標的としており、他のハクティビストや親ロシアのグループ（NoName057(16)、Moroccan Dragons、LAPSUS\$ など）と協力しています。スペインは、特に NoName57(16) のメンバーが逮捕された後、主要な標的として際立っています。また、CyberVolk のオペレーションは、NATO 加盟国を広く標的としています。

Dragon RaaS

名前に「ドラゴン」が含まれるもう一つのハクティビスト／ランサムウェア・ハイブリッド・グループである [Dragon RaaS](#) は、2024 年 7 月に Stormous グループの分派として登場しました。親ロシアのハクティビストサークルと関係があり、ランサムウェアの展開と脅迫を中核的な活動としています。Dragon RaaS は、主に米国、イスラエル、英国、フランス、ドイツなどの、セキュリティの脆弱な小規模組織に重点を置いています。

表 2 は、これらのグループの詳細をまとめたものです。

RaaS ハクティビスト			
グループ	出現	オリジン	標的となった地域
Stormous	2021 年中頃に活動開始	ロシア、中東	米国、ウクライナ、インド、フランス、スペイン、ベトナム
DragonForce	2023 年の中頃から年末に出現	マレーシア	インド、イスラエル、英国、米国、サウジアラビア、オーストラリア
KillSec	2023 年 10 月に活動開始	東欧 および／またはロシア	インド、バングラデシュ、アジア全体、米国
CyberVolk	ハクティビストとして発足し、2024 年 6 月にランサムウェアの使用を開始	ロシア、インド	スペイン、NATO 加盟国
Dragon RaaS	2024 年 7 月に出現	ロシア	米国、イスラエル、英国、フランス、ドイツ

表 2 : RaaS を使用しているハクティビスト／ランサムウェア・ハイブリッド・グループの例

ランサムウェアをツールとして使用しているハクティビストグループ

これまでハイブリッドと位置付けられていたグループは、RaaS プラットフォームを活用して金銭的利益を追求するだけでなく、**思想的意図や政治的意図を推進**しているため、ハクティビストとも見なされるランサムウェアグループです。しかし、ランサムウェアをツールとして使用しているにもかかわらず、従来の意味でランサムウェアグループとはみなされていない、有名なハクティビストグループがいくつか存在します。

例えば、ハクティビストグループである Head Mare、Twelve、NullBulge はすべて、ランサムウェアをハクティビストツールキットに組み込みました。しかし、これらのグループの目的は金銭的利益を得ることではなく、主に政治的混乱を引き起こすための手段としてランサムウェアが使用されています。また、各グループは、一般的な RaaS アフィリエイトと同様に RaaS 協定の対価を支払うのではなく、リークされたビルダーや公開されているビルダーから構築された LockBit ランサムウェアを使用します。

Head Mare は主にロシアやベラルーシの組織を標的としますが、**Twelve** は主にロシアの組織を標的とします。また、**NullBulge** は特定の地理的地域ではなく、AI ツールやゲームツールが開発、配信、使用されるオンラインコミュニティやプラットフォームに結び付いています（表 3）。

ランサムウェアを使用するハクティビストグループ			
グループ	出現	オリジン	標的となった地域
Head Mare	2023	ロシア・ウクライナ戦争における反ロシアハクティビズムに同調	ロシアとベラルーシ
Twelve	2023 年 4 月から活動	親ウクライナ志向のグループから派生した可能性が高い	ロシア
NullBulge	2024 年春	不明	特に集中している地域はないが、AI コミュニティやゲーミングコミュニティを標的としている。米国やインドが影響を受けている

表 3：ランサムウェアをツールとして使用しているハクティビストグループの例

セキュリティの注目点

TrickBot による悪性のおやつ (寄稿者: Or Zuckerman)

Wizard Spider (別名 TrickBot) は、ヘルスケアシステムを含む重要インフラを標的としている金銭的動機を持ったサイバー犯罪グループです。TrickBot という悪性のツールをランサムウェアグループに提供しているロシアのインテリジェンスサービスともつながりがあります。Wizard Spider の一部であり TrickBot を使用するランサムウェアグループとして、Diavol や、RaaS オペレーターの Ryuk と Conti があげられます。これらのグループは、世界で最も重大なランサムウェア攻撃をいくつか引き起こしています。

2016 年に生まれた TrickBot は、高度なモジュール式のバンキング型トロイの木馬として登場しました。現在では、さまざまなサイバー犯罪アクティビティ（ランサムウェアなど）をサポートできる、非常に汎用性の高いマルウェアプラットフォームへと発展しました。TrickBot に関連するマルウェアによって脅し取られた金額は、暗号資産（仮想通貨）で 7 億 2,400 万米ドル以上にのぼります。また、TrickBot は、被害者のネットワークへの初期アクセスを提供し、認証情報を盗み、侵害された環境内でのラテラルムーブメント（横方向の移動）を可能にします。2025 年 5 月、TrickBot のインフラが [Operation Endgame 2.0](#) の一環で Europol と Eurojust によって破壊され、オペレーターは強力な法的措置に直面しています。しかし、TrickBot はこれまでに過去の障害からの回復力を示しているため、引き続き警戒が必要です。

Wizard Spider の TTP

顧客をサポートする Akamai Hunt Team は最近、5 つの顧客資産に、「WindowsUpdate」という名前で偽装された、TrickBot マルウェアファミリーに関連する 4 つの悪性スケジュールタスクがあるのを発見しました。これらのタスクは、「C:\ProgramData」ディレクトリにあるペイロードを実行するように設定されていました。このフォルダ内で発見された TrickBot マルウェアファミリーのファイルには、悪性の DLL ファイル、Windows Registry 内で DLL を COM オブジェクトとして登録するために使用される BAT スクリプト、インタラクティブ SQL シェルを模倣した実行可能ファイルが含まれていました。これは、攻撃者がハンズオンキーボード・アクティビティを行ったことを示唆している可能性があります。影響を受けた顧客には通知があり、ランサムウェアがリリースされる前に対策を実施することができました。

Akamai Hunt Team は通常、顧客と協力し、DLL ファイルと BAT ファイルの両方によって API ハンマリングなどの一般的な回避手法がいつ行われたのかを把握できるようにします。これには、実行を遅延し、検知メカニズムをバイパスするための、反復的で無害な API 呼び出しが含まれます。このような手法（API ハンマリング、「WindowsUpdate」として偽装されたスケジュールタスクを使用した TrickBot マルウェア、ハンズオンキーボード・アクティビティなど）は、Wizard Spider とそのランサムウェアオペレーター（Diavol、Ryuk、Conti）が使用する幅広い TTP の典型例です。これらのグループは、ステルス性、持続性、および（多くの場合、初期アクセスベクトルとして）TrickBot マルウェアを一貫して活用し、リーチの最大化と検知の回避を図ります。

業界別の傾向

金融サービス *

Financial Services Information Sharing and Analysis Center (FS-ISAC) の [Navigating Cyber 2025 : Annual Threat Review and Predictions](#) レポートによれば、金融サービス業界が直面する最も深刻かつ偏在的な脅威の一つがランサムウェアです。しかし、ランサムウェアオペレーターが 2024 年に過去最高額の身代金を要求した一方で、FS-ISAC の情報共有プラットフォームでは、ランサムウェアインシデントの報告件数が大幅に減少しました。

この傾向は、アジアを除き、リークサイトのデータに表れています（表 4）。[eCrime Threat and Risk Intelligence Services](#) によって収集されたデータによると、アジアはランサムウェア攻撃が特に集中している地域でした。実際、ランサムウェアオペレーターによる主張件数を見ると、インドの金融機関に対する攻撃は米国企業よりはるかに少ないものの、英国やカナダの企業より多くなっています。

ランサムウェア・リーク・サイトにおける主張件数の国別内訳	
米国	151
インド	17
英国	16
カナダ	11
ベルギー	7

表 4 : 影響を受けた金融サービス組織の 2024 年国別内訳
(出典 : [eCrime Threat and Risk Intelligence Services](#))

ランサムウェアオペレーターは日和見主義的な傾向がありますが、専門家によると、ますます高度化しています。

FS-ISAC では、攻撃者が生成 AI を悪用して金融サービス企業への攻撃を自動化およびカスタマイズし、イニシャルアクセスを産業規模のサービスとして販売すると予測しています。このようなアプローチは、すでに危険な脅威環境にさらされている金融サービス業界のリスクを増幅させます。また、タイムリーな脅威インテリジェンスと予防への投資は、サイバー防御と回復力にとってますます重要になっています。

* このセクションの情報は、FS-ISAC によって提供されています。

コマース

ランサムウェアグループは、常にコマース業界（特に小売企業や e コマース企業）を標的にしています。2025 年初頭、CLOP ランサムウェアグループは、Cleo が管理するファイル転送ソリューションの [2 つのゼロデイ脆弱性](#)（[CVE-2024-50623](#) および [CVE-2024-55956](#)）を悪用しました。小売企業は注文管理などの重要な機能をこれらのプラットフォームに依存しており、攻撃者はそれを予期しないエントリポイントとして活用しました。この戦術により、CLOP は 2025 年 2 月だけで複数の業界の [335 の組織](#)を侵害することができました。

さらに、Scattered Spider（別名 UNC3944）は、さまざまなランサムウェアバリエーションを使用して英国の小売企業に対して[攻撃を開始](#)し、現在は米国の小売組織を標的にしていると報告されています。コマース業界は、絶え間ないアップタイムと貴重なデータを必要とするため、攻撃者にとって特に魅力的な標的となっています。迅速なデジタル化とサードパーティ統合への依存度の増加により、セキュリティギャップがさらに拡大します。

ヘルスケア

ヘルスケア組織は貴重なデータを保有しているため標的とされ、盗まれた患者記録は個人情報の窃取や詐欺などの二次的な攻撃に利用されます。攻撃が原因で生じるダウンタイムにより患者の治療が脅かされ、[平均身代金支払額](#)は 86 万米ドル、[1日あたりのダウンタイム損失額](#)は 190 万米ドルに達しています。SOTI レポート「[ヘルスケアに関する詳細な調査：アプリケーションと API に特化した攻撃](#)」において、Akamai はこの業界で Web アプリケーションと API への依存が強まることによってどのようにランサムウェアに対する脆弱性が高まるのかを分析しました。

特に地方の病院では、レガシーシステム、Internet of Medical Things デバイス、限られたサイバーセキュリティリソースが原因でアタックサーフェスが拡大しています。規制が厳しいということは、侵害されれば深刻な結果がもたらされるということであり、これによりヘルスケア業界は主要な標的となっています。

公共部門

公共部門は、地方自治体、州政府、連邦政府、および公共サービスを提供する政府管理機関で構成されており、貴重なデータを収集できる利益の出やすい標的となっています。攻撃が成功すると、サービスの中断やデータの損失がもたらされ、復旧コストも高くなります。米国だけでも、政府を標的としたランサムウェア攻撃が[大幅に増加](#)し、2018 年から 2024 年 12 月の間のダウンタイムコストは 10 億 9,000 万米ドルに達しました。ランサムウェア攻撃は、2024 年に 230 万件の記録に影響を与えました。これは、2023 年の約 3 倍の件数です。最新の [Verizon の「2025 年度データ漏えい／侵害調査報告書」](#)では、この傾向が確認され、米国連邦政府と州政府、EMEA 議会に対する標的型攻撃が指摘されています。

身代金支払いの禁止などの法的措置が実施されているにもかかわらず、攻撃は弱まることなく続いており、フロリダ州は 2024 年にランサムウェアによる最も深刻な[政府データ漏えい](#)の被害を受けました。この傾向はグローバルに拡大しています。2024 年には Fog ランサムウェアが[ブラジルの省庁](#)を標的としました。また、[インドネシアの国立データセンター](#)が LockBit 3.0 の被害を受け、200 以上の行政機関の重要なサービスが停止し、800 万米ドルの身代金が要求されました。

製造業

2025 年第 1 四半期には、**400 社以上の製造会社**がランサムウェアの被害を受け、製造業全体がその四半期の最大の標的となりました。これは、運用技術や産業用制御システムに対する**攻撃の急増**と合致しています。製造企業は、15,000 社のカーディーラーを混乱させた **BlackSuit 攻撃**で見られるように、レガシーシステム、接続デバイス、複雑なサプライチェーンが原因で脆弱になっています。この業界でランサムウェアの被害を受けることは、運用、財務、評判の低下につながります。2024 年には**平均復旧コスト**が 170 万米ドルに上昇しました。これにより、この業界は身代金を支払う可能性が高いとみなされ、サイバー犯罪者がますます標的とする動機となりました。

教育

教育機関は**前例のないランサムウェア攻撃**に直面しており、平均的な身代金要求額は 608,000 米ドル、最高で 150 万米ドルに達するものもあります。大きな注目を集めたインシデントとして、**PowerSchool**（北米でクラウドベースの教育ソフトウェアを提供しているプロバイダー）や**米国シカゴ公立学校**が侵害され、学生の機微な情報が公開されたことがあげられます。本書の作成時点で、米国シカゴ公立学校への攻撃を行った**罪をハッカーが認めました**。

学校は、リソースが限られていること、セキュリティが弱いこと、サイバー意識が不足していることなどの理由で脆弱です。**インシデント報告の遅延**により、リスクがさらに高まり、迅速で透明性の高いコミュニケーションの必要性が強まっています。教育機関に対してランサムウェア攻撃が成功すると、多くの場合、大幅なデータの損失、運用の中断、**教育の遅延**、場合によっては**永久的な閉鎖**につながることもあります。

業界別の傾向の概要

すべての業界がランサムウェア攻撃のリスクにさらされていますが、攻撃の影響度は、組織の準備レベルと、そのような攻撃に耐えて回復する能力に大きく左右されます。堅牢なサイバーセキュリティ対策や専門のセキュリティ担当者がいない組織では、データの損失が大きく、運用の中断が長引くことが多くなります。極端な場合には、運用の完全停止を余儀なくされることもあります。

デジタルトランスフォーメーションを進める業界は、意図せずセキュリティギャップを生み出して、アタックサーフェスを拡大しています。これは、サイバー犯罪者が悪用するエントリポイントが増えるため、包括的なセキュリティ戦略が不可欠になることを意味します。特に懸念されるのは、攻撃者がサードパーティベンダーやサプライチェーンパートナーを標的として、より優れた防御を備えた組織にアクセスする傾向があることです。こうした増大するリスクに対処するためには、組織はマイクロセグメンテーションなどの高度な戦略を実装して違反を阻止し、ラテラルムーブメント（横方向の移動）を防止する必要があります。これにより、最終的にランサムウェアへの暴露を軽減できます。

セキュリティの注目点

クリプトマイナー（寄稿者：Maor Dahan）

クリプトマイナーはランサムウェアと同様に、主に匿名の暗号資産（仮想通貨）取引を通じて金銭的な利益を求めます。ランサムウェアオペレーションには通常、複雑なネットワーク侵入や、被害者を直接脅迫してすぐに身代金を支払うよう促すことが伴いますが、クリプトマイナーは密かに活動し、サイバー犯罪者にとっては安定的に低リスクで収益を生み出します。

クリプトマイナーとランサムウェアは、攻撃者の金銭的動機から生まれる明らかな脅威です。クリプトマイナーは主に組織のコンピューティングリソースを利用して利益を生み出しますが、ランサムウェアは機微な情報の暗号化や窃盗などによって身代金を脅し取ります。どちらのタイプのマルウェアも暗号資産（仮想通貨）の匿名性を活用しています。ランサムウェアグループはそれを利用して身代金の支払いを促し、クリプトマイナーはそれを利用して採掘作業から直接利益を得ます。

どちらのタイプの攻撃者も、フィッシングキャンペーンや脆弱性の悪用など、同様の戦術を使用して、最終的なペイロードを展開する前に初期アクセスを取得する可能性があります。ただし、これらの脅威の間で検知戦略は大きく異なります。悪性のクリプトマイニングは、長期間潜伏して利益を最大化します。一方、ランサムウェアは、初めは密かに活動しますが、最終的には目的を達成した後に被害者に警告して支払いを要求します。このセキュリティの注目点では、クリプトマイナーとそれが組織に及ぼすリスクについて詳しく見ていきます。

クリプトマイナーとは

クリプトマイナー（クリプトジャッカー）は、暗号資産（仮想通貨）のマイニングによって利益を得るために被害者のリソースを悪用するマルウェアの一種です。攻撃者が通常の支払い方法として暗号資産を使用するのは異なり、クリプトマイナーは暗号資産の基礎的基盤であるブロックチェーンマイニング作業を利用して、金銭的利益を生み出します。

暗号通貨はもともと、国境を越えた分散型の送金方法として、従来の銀行システムから切り離して設計されました。ビットコインの登場以来、他の多くの暗号資産や暗号ベースのトークンが作成されています。どのトークンも、他のトークンと区別するテーマや機能セットに基づいています。

攻撃者は匿名性を確保しながら利益を得ようとするため、暗号資産は利益の出やすい選択肢であり、脅威アクターは法執行機関に特定されるリスクを最小限に抑えながら暗号資産ファンドを使用できます。身元を特定されずに金銭的利益を得る最も直接的な方法は、プライバシー重視の暗号資産をマイニングすることです。これにより、攻撃者は被害者に自分をさらけ出すことなく即座に利益を得ることができます。

攻撃者の動機

脅威アクターは、主に利益とプライバシーの2つの理由でクリプトマイナーを取り入れています。

利益目的

国家の支援を受けている脅威アクターやハクティビストを除き、ほとんどのサイバー犯罪者は金銭目的です。クリプトマイナーは、攻撃者によるネットワークの支配を資本に変換する段階（[ランサムウェア](#)による脅迫や機微な情報の販売など）を追加することなく、簡単かつ直接的に侵害を収益化する方法です。そのため、クリプトマイニングマルウェアは脅威アクターにとって魅力的な資金創出ツールです。

その他にも、攻撃者は暗号資産（仮想通貨）の価値やマイニング・シェア・レートなどを考慮します。例えば、攻撃者が1年間に生み出す利益が1米セント（0.1米ドル）である場合、それは逮捕されるリスクに見合いません。したがって、攻撃者の目標の1つは労力と利益のバランスを取ることです。それを知っていれば、攻撃者がマイニングする可能性のあるコインを絞り込むことができます。

Akamai は調査中に、少なくとも 2018 年 6 月以降に活動していて、毎年平均 300 XMR の収益を上げることに成功した攻撃者を特定しました。現在の Monero の価格(1 XMR 150 米ドル)で収益を計算すると、約 45,000 米ドルになります。これは、従業員のいない米国の小規模企業の 2024 年の[平均収益額](#)よりわずかに少ないです。

プライバシーを重視

プライバシーはほとんどの暗号資産に本来備わっています。暗号資産は暗号化アルゴリズムを使用しており、対応する公開鍵とペアになった秘密鍵を使用してプライバシーと所有権を保護します。公開鍵は、ウォレットアドレスとして機能します。この暗号資産固有の機能と、取引額、送信者アドレス、受信者アドレスを隠すように設計された追加のプライバシーアルゴリズムを活用することで、攻撃者はアクティビティをほぼ完全に隠蔽することができます。

前述のとおり、攻撃者はボットネットを特定の暗号資産のマイニングにシフトする際に、いくつかのトレードオフを考慮します。そのトレードオフの1つが、攻撃者のプライバシーと利益です。なぜなら、プライバシー性は低いが高収益性の高いコインが存在する可能性があるからです。コインのプライバシーは、次の3つの側面でそのコインが提供できる匿名性によって測定されます。

1. ネットワークとの通信（Tor や I2P などのプライバシー・ネットワーク・プロトコルに依存するコインがある）
2. 追跡の防止や口座残高の秘匿のための、トランザクション情報（ウォレットアドレスや金額）の保護
3. プライバシーをサポートする取引プラットフォームでの暗号資産の取り扱い

たとえば、ビットコインにはトランザクションのプライバシーがないため、ユーザーは監視に対して脆弱であり、匿名性が損なわれるリスクが高まります。この制約により、攻撃者が悪用できる暗号資産の範囲は制限されます。そして、採算の取れるプライバシー重視のコインが利用できる限り、攻撃者の意欲は衰えません。

しかし、プライバシーコインが不採算になった場合や、ブルーフ・オブ・ステークへの移行など、マイニングプロセスが変更されたことにより、攻撃者がリソースを大量に消費する方法で簡単に利益を生み出せなくなった場合、この意欲は低下する可能性があります。

意欲のある攻撃者はそのようなクリプトマイナーキャンペーンを実行する方法を検討しなければならず、その検討のためにはマイニングプロセスの基礎を理解することが不可欠です。

世界に対するクリプトマイナーの影響

ビデオゲーム会社が顧客のマシンをビットコインのマイニングに利用したとされる 2013 年以降、クリプトマイナーは世界に影響を及ぼしてきました。それから 10 年以上が経ち、脅威は巨大な規模にまで拡大し、クリプトマイナーは現在、世界的なサイバー犯罪の重要な要素となっています。

数年の間に、クリプトマイナーの数多くのケーススタディが公開されてきました。例えば、2017 年の WannaMine ボットネット、Redis を標的とした Migo キャンペーン、2024 年初めのクラウド固有のスクリプトやブラウザー・マイニング・スクリプトのバリエーションなどです。近年、Akamai は Panchan や NoaBot など、いくつかのクリプトマイニングボットネットを発見しました。



攻撃ボリューム

時が経つにつれて、クリプトマイナーに注目する攻撃者が増えました。図 14 は、2023 年に悪性のグローバルなクリプトマイニングアクティビティが大幅に増加したことを示しており、この傾向は 2024 年も続きました。爆発的に増加しているにもかかわらず、クリプトマイナーのふるまいに大きな変化はありませんでした。2024 年の典型的なクリプトマイナーは、非常に人目を引く非標的型攻撃であり、クラウドリソースや家庭のコンピューターに感染し、プライバシー重視のコインをマイニングするという点で、10 年前のクリプトマイナーによく似ていました。

全世界におけるクリプトジャッキングの件数

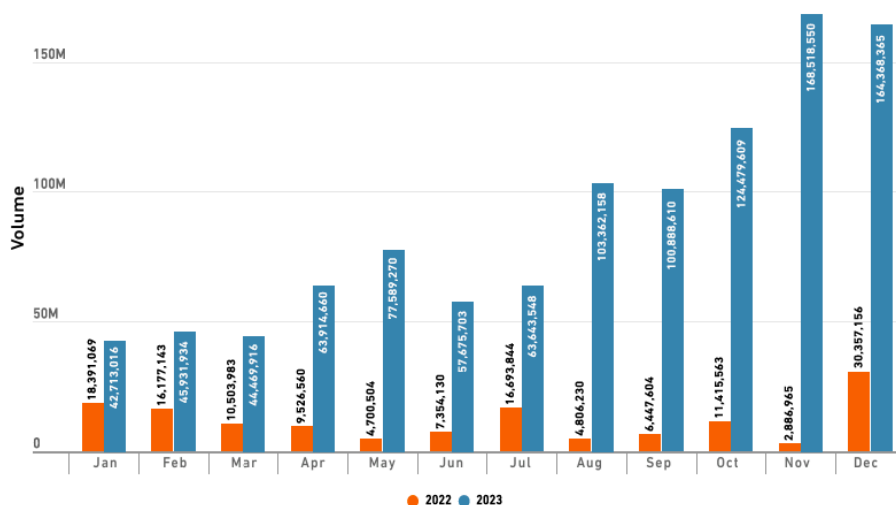


図 14 : 検知されたクリプトマイナー攻撃の件数（出典 : [SonicWALL](#)）

クリプトマイナーの産業およびセクター分布

クリプトマイナーは、さまざまな産業やセクターに影響を与えます（図 15）。

2024 年のセクター別攻撃

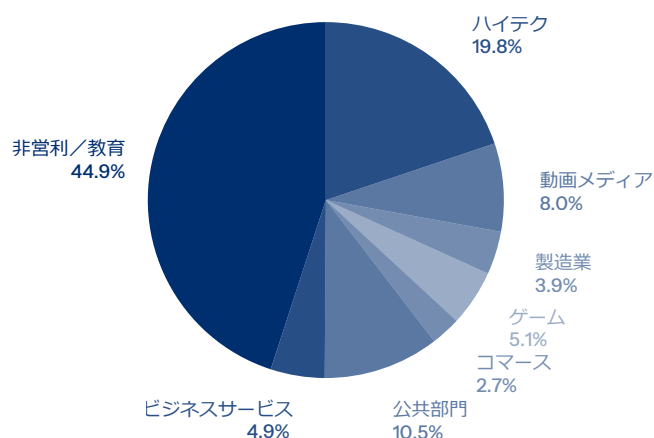


図 15 : 2024 年に観測された攻撃のセクター分布

高等教育機関は、最も標的とされているセクターの1つでした。その理由はおそらく、膨大な計算リソースがあり、多くの場合そのリソースに人間が介在していないからです。

大規模なテクノロジー企業の中でも、クリプトマイナーはクラウドやホスティングサービスなどの業界を優先的にターゲットとしています。これらのターゲットは、攻撃者に大きな機会をもたらします。なぜなら、攻撃者は広範な計算リソースにアクセスできると同時に、被害者の環境内の副産物（検知につながる可能性のある大きなノイズ、熱、電力消費など）を排除できるからです。

このタイプの攻撃は、被害者に経済的に破壊的な損害をもたらします。[Sysdig](#) によると、2022 年の時点で、クリプトマイナーの利益1米ドルにつき、被害者の損害額は約 53 米ドルでした（図 16）。

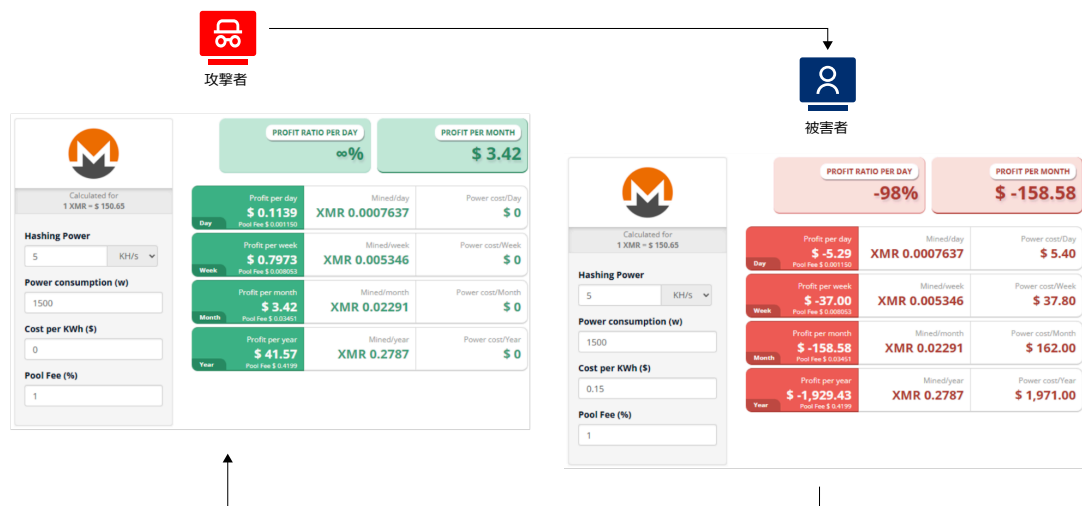


図 16：攻撃者の利益と被害者の損失の比較

生成 AI はクリプトマイナーに新たなアタックサーフェスをもたらす

Akamai は、昨今の生成 AI の台頭がクリプトマイナーの情勢に大きく影響すると予測しています。AI の計算はグラフィックス・プロセッシング・ユニット（GPU）に大きく依存しているため、このコンポーネントは組織のネットワークやサーバーによく使われるようになっています。多くのマイニングアルゴリズムも GPU 向けに設計されているため、AI 業界の基盤となるコンピューティングインフラはクリプトマイナーオペレーターにとって非常に魅力的です。

モデルインタラクションやトレーニングプロセス、またはその両方を通じて AI インフラを直接的にターゲットとするキャンペーンを目的にすることは、おそらく時間の問題です。

クリプトマイニング攻撃に最適な暗号資産

攻撃者はビットコインだけでなく、独自の機能を備えた暗号資産を多数利用しています。コインを選択する際には、サイバー犯罪者は以下のいくつかの重要な要素を考慮します。

- ・ クロスプラットフォームの互換性：コインは、さまざまなアーキテクチャ（x86、AMD64、ARM など）でマイニングできる必要があります。
- ・ ハードウェアの柔軟性：標準デバイスでマイニングできる必要があります。GPU のような特殊なハードウェアを必要とすべきではありません。
- ・ プライバシー機能：違法行為を隠蔽できるよう、追跡不可能なトランザクションをサポートしている暗号資産である必要があります。
- ・ 収益性：コインは高水準で持続可能な収益を生み出すものでなければなりません。

これらの基準が満たされていれば、攻撃者は検知リスクを最小限に抑えながら、最大限の成果を得ることができます。

クリプトマイナーのリスクの緩和

Akamai のセキュリティスタックを活用することで、組織はアタックサーフェスの複数の層にまたがり、クリプトマイナーの感染リスクを緩和できます。

Akamai Guardicore Segmentation を使用してラテラルムーブメントを防止

多くのクリプトマイナーは、ワームのようなふるまいを示します。つまり、ホストを侵害した後、ネットワークを横方向に移動して、できるだけ多くの他のシステムに感染しようとしています。このラテラルムーブメント（横方向の移動）は通常、スプレー攻撃によって脆弱な認証情報を試すか、内部サブネット全体で既知の（n デイ）脆弱性を悪用することによって実行されます。

[Akamai Guardicore Segmentation](#) を使用して厳密なマイクロセグメンテーションポリシーを実装することで、防御者はこのリスクを大幅に軽減できます。不要な内部通信を制限することで、防御者は大部分のラテラルムーブメントの試行を効果的にブロックし、感染が拡散する前に阻止できます。

Akamai Secure Internet Access Enterprise を使用して、マイニング関連の接続をブロック

クリプトマイニングの設定の多くは、既知のマイニングプール（つまり、異なるマイニングオペレーション中にマイニングネットワークのすべてのノードが使用する DNS アドレス）との直接通信に依存しています。

通常、ほとんどの企業環境でクリプトマイニングの正当なユースケースがないため、これらのドメインへの接続を特定してブロックすることは、マイニングマルウェアを破壊するうえで非常に効果的な方法です。[Akamai Secure Internet Access Enterprise](#) は、既知のマイニング・プール・アドレスへのアクセスをデフォルトでブロックすることで、この脅威から保護します。

Akamai Hunt を使用して、悪性のクリプトマイナーをプロアクティブに特定

ファイルハッシュや既知の DNS アドレスなど、セキュリティ侵害の静的インジケータを用いても、すべてのクリプトマイニングマルウェアを確実に検知できるわけではありません。Akamai Hunt は、未知のサンプルや回避可能なサンプルを特定するために、一連のプロアクティブなふるまいベースの検知技術を採用しています。

これらの手法は、一般にクリプトマイナーと関連のある異常なふるまいを特定することに焦点を当てています。例としては、[疑わしい通信パターン](#)、異常なプロセス実行、および永続性メカニズムなどがあります。このような異常が検知されると、関連するプロセスがさらに分析され、悪性のアクティビティが確認されます。

注目すべき点のまとめ

サイバー犯罪オペレーションにおける暗号資産（仮想通貨）の使用は、身代金収集に限られたことではありません。クリプトマイナーマルウェアは、利益を生み出す主要な手段として、暗号資産（仮想通貨）の基本的な側面であるマイニングプロセスを悪用します。クリプトマイニングは効果的で、シンプルで、非常に気付かれづらく、あまり高度でない脅威アクターにも侵入を収益化する絶好の機会をもたらします。

ランサムウェア攻撃が運用の継続性に与える影響

ランサムウェアは、即座の身代金支払い以外にも、企業経営に重大な脅威をもたらします。真の財務的および運用上の影響には、ダウンタイムの長期化、生産性および収益の損失、インシデント後の広範囲な復旧および緩和作業が含まれます。このような影響は、組織のサイバーセキュリティポスチャ、インシデント対応能力、セキュリティ管理によっては、数週間から数か月続く可能性があります。

報告によると、ランサムウェアインシデント後の平均ダウンタイムは21日です。これは、評判への悪影響、顧客の信頼の悪化、恒久的な閉鎖などの深刻な結果を招く可能性があり、特にヘルスケアや製造といった重要な業界においては、患者の安全リスクやサプライチェーンの混乱などにつながります。

影響がもたらされるのは最初のターゲットに対する攻撃に限定されず、連鎖していく可能性があります。ランサムウェア攻撃者は、[社内に展開された商用ソフトウェア](#)や社外のサービスプロバイダーを含むサプライチェーンを標的とする場合があります。このようなサプライチェーンは、サイバーセキュリティの成熟度が低いため、「簡単なターゲット」と見なされることが多いです。例えば、[2025年4月](#)には、外部パートナーを積極的に標的としたことで、攻撃者は2つの大規模銀行の顧客データにアクセスできるようになりました。

身代金要求以外の潜在的なコスト

身代金の支払額は、ランサムウェア攻撃の総コストのわずか数分の1にすぎません。Cybersecurity Ventures は、2031年までに[ランサムウェアの被害額は年間2,760億米ドル](#)（または1分あたり525,000米ドル）に達すると予測しています。これは、2025年の年間570億米ドル（または1分あたり109,000米ドル）からさらに増加した金額となっています。さらに、長期的な影響として、顧客ロイヤルティの喪失やブランド評判の低下などが挙げられます。また、GDPRやHIPAAなどのデータ保護法に違反した場合には、規制上の制裁や罰則に直面する可能性があります。これにより、財務上および評判へのさらなる悪影響がもたらされます。

ランサムウェアは、業務上重要な機能の一部または全体をシャットダウンさせ、業務を事実上停止させることがあります。攻撃者は、知的財産や顧客情報などの機微な情報を暗号化して窃取するために、ますます多重脅迫戦術を使用するようになっているため、依然として永続的なデータ損失のリスクが高いです。身代金を支払っても、企業がすべてのデータを回復できる保証はありません。

さらに、2024年に発生したランサムウェア攻撃からの[回復コスト](#)は大幅に増加しており、平均費用は2023年に報告された182万米ドルから、273万米ドルに増えています。この数字には、攻撃者が集めた身代金は含まれていません。

上がり続けるランサムウェア攻撃の頻度と影響度への対応

Cybersecurity Ventures のレポートによると、2031 年までに、消費者と企業は合わせて 1 日に 43,200 回のランサムウェア攻撃に直面する見込みです。これは、2 秒に 1 回の割合で攻撃が発生するということです。この脅威の影響を最小限に抑えるために、組織は次のことを行う必要があります。

- ・ 攻撃中および攻撃後にミッションクリティカルな機能を維持するための包括的な事業継続性計画を策定し、ダウンタイムと財務損失を削減する
- ・ 定期的なデータバックアップの実行
- ・ 攻撃が成功した場合に、環境内でのランサムウェアの拡散を制限するためにネットワークセグメンテーションを実装する
- ・ 迅速な対応による、攻撃の範囲と期間の大幅な短縮の確保

ネットワークと重要資産を保護する方法の詳細については、[緩和策](#)のセクションを参照してください。

ランサムウェアと法律 (寄稿者: James A. Casey)

ジェームズ・ボンド映画の悪役は、なぜ罪を犯すのかと聞かれて、「できるからさ、ボンド君」と答えることがよくあります。この短い対話は、ボンド映画の典型的な悪役が併せ持つ危険性と巧妙さを、よく表しています。この描写は、ランサムウェア犯罪者にも同様に当てはまります。犯罪者は、ランサムウェア攻撃が可能であり、効果的であるから実行するのです。ランサムウェアは、世界中の組織が直面する最も重大なサイバーセキュリティの脅威の一つとして浮上したため、各国政府はさまざまな法律、規制、プログラム、および意識向上キャンペーンを通じてこの増大する脅威に対処するために奮闘しています。

法律の現状

しかし、法的な取り組みの多くはランサムウェアに特化したものではなく、広範なサイバーセキュリティ法の適用にすぎません。ランサムウェアは確かに普及しており、有効ですが、犯罪者が武器とする単なるサイバー攻撃の1つにすぎません。ランサムウェアのインシデントには、他のサイバー攻撃と同じ法的原則が適用されます。また、サイバー衛生とセキュリティのベストプラクティスの多くがリスクの緩和に役立ちます。

例えば米国では、連邦捜査局 (FBI) や [サイバーセキュリティ・社会基盤安全保障庁 \(CISA\)](#) が、サイバー攻撃の防止と対応のためのフレームワークを提供しており、[Computer Fraud and Abuse Act \(コンピューター詐欺および濫用法, CFAA\)](#) は、ランサムウェアを含むサイバー攻撃を訴追するための基盤として機能し続けています。連邦および州のさまざまなサイバーインシデントの報告ルールはあらゆるサイバーイベントに適用されます。

欧州連合には、厳格な報告ガイドライン、重大な罰則、執行責任を定める [NIS2 指令](#) によって作成された強固な法的枠組みなど、さまざまなサイバー法があり、業界全体に適用されています。ランサムウェア攻撃には個人情報に関係しているため、多くの法域のプライバシー法が適用され、追加の要件と報告義務が生じます。

立法活動や規制活動に加えて、各国は脅威に対処するための協力的な取り決めに参加しています。例えば、[カウンターランサムウェア・イニシアティブ会合 \(ICRI\)](#) に加盟している全 50 か国が、「各中央政府に属する関連機関はランサムウェアの脅迫的要求に応じるべきではない」と主張する共同ポリシー声明を承認しました。さらに、[Oxford Statement on Ransomware Operations](#) では、ランサムウェアに国際法を適用する原則が定められています。これらの取り組みは、拘束力のある義務を生じさせるものではなく、民間部門には適用されませんが、ランサムウェアの脅威に対して、あらゆるレベルで大きな注目が集まっていることを示しています。

身代金支払いに関する制限

ランサムウェアには、具体的な法的取り組みによる対処が試みられている固有の問題があります。それは、脅迫です。ランサムウェア攻撃が成功すると、「身代金を支払うべきか」という疑問が生じます。この質問に対する答えは、ビジネスへの影響、身代金の規模と脅迫の性質（単一脅迫、二重脅迫、三重脅迫、または四重脅迫）、攻撃者のアイデンティティ（判明している場合）、身代金を支払うことによって実際にデータが解放される、または他の脅威が撤退する可能性など、さまざまな要因によって決まります。

これらの要因は企業が身代金を支払う動機になるかもしれませんが、ほとんどの政府は、被害者は支払うべきではないという立場をとっています。全面的な法的禁止は稀であり、ほとんどが政府／公共部門の機関や、いくつかの国の重要な産業部門に限られています。しかし、実質的にすべての国の政府が身代金を支払わないことを推奨しています。この立場をとる理由は明らかです。身代金が支払われなければ、この攻撃ベクトルの有効性が低下し、ハッカーグループにとって魅力的でなくなる可能性があるからです。さらに、身代金の支払いは、他の犯罪行為（金銭的動機と思想的動機の両方）の資金源となる可能性があります、すべての人のリスクが高まります。最後に、提示された身代金を支払ったり関連する脅迫的要求に応じたりしても、データの解放や関連する脅威（データの開示／販売、DDoS 攻撃、顧客への通知）の終結という結果になるとは限りません。

実際、身代金要求への対応を拒否した組織の数は、2022 年の 50% から 2024 年には 64% に増加しました。その結果、身代金要求は大幅に減少しました。これは、政府の介入、つまり、法執行機関によるインフラのテイクダウンと押収の成功によるものかもしれません。

身代金の支払いを思いとどまらせるための 3 種類の法的取り組み

政府が支払いを思いとどまらせるために用いる法的手段は、3 つの基本的なカテゴリーに分類されます。第 1 のカテゴリーは、制裁対象または制限対象の組織および国への支払いに関する法的制限と、犯罪企業への支払いに関するより一般的な制限です。これは、最もよく見られる種類の法的取り組みでもあります。米国や他の同盟国は、包括的制裁の対象国（北朝鮮、イラン、シリア、キューバなど）のランサムウェア攻撃者や、適用されるエンティティリスト（米国財務省外国資産管理局の特別指定国民リストなど）に含まれるランサムウェア攻撃者に身代金を支払うことを違法としています。実際、制裁法やマネーロンダリング防止法を有するほぼすべての国は、制裁対象の団体や犯罪組織への身代金の支払いを違法としています。これはランサムウェアに特有のものではありません。これらの法律は、テロリストグループ、組織犯罪者、国家が認可したサイバー攻撃者など、制裁対象者との取引に適用されます。

第2の法的取り組みのカテゴリーは、報告義務に焦点を当てたものです。サイバーインシデントの報告は、世界中の法域で広く行われており、一般的にランサムウェア攻撃に適用されます。しかし、身代金の支払いに関しては、より具体的な義務が制定され始めています。例えば、2025年5月30日より施行された [Australian Cyber Security Act](#)（オーストラリアサイバーセキュリティ法）では、身代金の支払いに関する報告が義務付けられるようになりました。英国では、公共部門の機関や重要インフラによる支払いについて、[報告義務の導入を検討](#)しています。また、米国では、[CIRCSIA](#) により、対象組織は身代金を支払ったことを24時間以内に報告することが求められるようになります（規則は最終決定待ち）。今後は、このようなランサムウェア固有の要件が増えると予想されます。

第3のカテゴリーは、特定の禁止法です。[英国のサイバーセキュリティ法案](#)は、公共部門や重要インフラ組織による支払いを禁止する可能性があります。より包括的な他の禁止措置や、金融やヘルスケアなどの重要インフラセクターを含む重要な産業のセクター別禁止措置の実施が予想されます。

今後の展望

地域的な違いはあるものの、ランサムウェアの規制やサイバーのベストプラクティスには、多くの共通要素があります。

- ・ インシデント報告：ほとんどの法域では、ランサムウェアを含む重大なサイバーインシデントを迅速に報告することが義務付けられています。
- ・ リスク管理：政府は、組織が適切なサイバーセキュリティ対策を確実に実施するための要件に引き続き焦点を当てています。
- ・ サプライチェーンのセキュリティ：サードパーティとの関係とサプライチェーン全体のセキュリティ確保にますます重点が置かれるようになっています。
- ・ 経営幹部の説明責任：サイバーセキュリティに対する管理責任の増大傾向が見られます。

ランサムウェア固有の規制、ガイドライン、および要件は、脅威の高度化に伴って進化し続ける可能性があります。

- ・ 人工知能を使用した新たなランサムウェアの戦術が登場することで、規制の更新が促されます。
- ・ 新たな法規制と法執行の取り組みは、RaaSモデルに焦点を置くようになります。
- ・ 罰則の増加と被害者支援メカニズムはグローバルに検討されています。
- ・ 国際的な協力は、国境を越えた脅威に引き続き対抗します。

ランサムウェアは世界中の組織に大きな脅威をもたらし続けているため、コンプライアンスを維持し、サイバーセキュリティポスチャを強化するために、進化を続けるこれらの国際的な規制と執行措置について、常に把握しておくことが不可欠です。

世界中でランサムウェアに対する回復力を構築

サイバー保険と多層セキュリティは、サイバーレジリエンスを構築するために相互に連携した構成要素です。これは、ランサムウェア攻撃の場合に特に当てはまります。この攻撃の目的は、ネットワークをできるだけ暗号化することです。ランサムウェア攻撃が発生した場合、攻撃による金銭的影響（ダウンタイム、修復、法的費用や規制上の罰金の可能性）に身代金の支払いが含まれる場合があります。

2022 年以降、FBI の IC3 はランサムウェアの被害者に何千もの復号キーを提供し、[8 億米ドル以上の支払いの回避](#)に貢献しています。ただし、復号キーは常に使用できるわけではないため、組織は回復力を構築するために独自の戦略を必要としています。

身代金の支払いとサイバー保険に関する意思決定をサポート

インシデントが発生する前に、組織はランサムウェアの支払いに関するポリシーを定めておくべきです。身代金を支払ってもすべてが回復するとは限りませんが、影響を受けたシステムの大部分を回復できる可能性があります。

また、暗号資産（仮想通貨）の支払いにも対応する必要があります。組織を廃業に追い込む意思と手段を持つ組織的な犯罪者と交渉するのは、大きなプレッシャーを伴う状況であるため、組織はサイバー犯罪者との交渉を専門とする第三者機関と提携しておく必要があります。経験豊富な交渉人は金銭的損害を最小限に抑え、会社の業務再開を支援することを目指しますが、被害者は当初の要求の [50 ~ 80%](#) を支払うことを想定しておく必要があります。

S&P Global Ratings は、2026 年末までに年間の[サイバー保険料](#)が約 230 億米ドルに達すると予測しており、2023 年末の推定 140 億米ドルから年間あたり 15% から 20% の増加が見込まれています。現在、北米がサイバー保険の総保険料の約 51%、EMEA が約 38%、APAC が 9%、LATAM が 3% を占めています。APAC および LATAM では、サイバー保険市場が米国や欧州よりも小規模で成熟度が低いことから、最も高い成長率が予測されています。

2024 年は、他の種類のインシデントよりも[ランサムウェア攻撃に対する保険請求が高く](#)、保険請求の約 21% を占めました。ただし、過去 2 年間で平均的な請求の規模と頻度は減少しています。ランサムウェアの被害を受けた保険契約者の約 44% は、「妥当かつ必要と判断した場合」に身代金を支払う決断をしました。それらのケースにおいて、保険会社は身代金支払額を交渉し、平均で 60% 減額させています。

[ランサムウェア保険の事例](#)で最もよく見られるランサムウェアグループは Akira で、イベントの 13.4% を占めており、Play (6.2%)、Medusa (5.7%)、RansomHub (4.6%) がそれに続きました。Black Basta は平均身代金要求額が 400 万米ドルで最も高いですが、請求件数の割合はわずか 3% でした。

信頼は双方向的なものではない

興味深い力学として、サイバー保険が犯罪者を助長する場合があります。なぜなら、犯罪者グループは、データの復号キーを得るために保険で補償される金額を要求する可能性があるからです。一方、保険会社の交渉人や保険会社が認可する交渉人の関与により、暗号化キーが機能する可能性が高まり、完全な回復が保証される可能性も高くなります。

これはビジネス上の取引であり、サイバー犯罪者は自分に餌を与える手に噛みつこうとはしません。ルールに従うこともありません。信頼は双方向的なものではないのです。サイバー犯罪者は、要求が満たされていても、LockBit の場合と同様に、盗んだデータを削除しない可能性があります。また、データが暗号化された場合、**35% の企業**は身代金を支払っても復号キーを得られないか、キーが機能しません。機能するキーを使用できたとしても、復旧プロセスは非常に困難であり、専門的な知識が必要です。さらに、同じまたは関連する脅威アクターによって再び標的にされるリスクも残っています。

多くの場合、身代金を支払わないことに決めた組織は、事業継続性／災害復旧危機管理計画に頼ります。このアプローチには数日から数週間かかることがあり、回復を促進するために行われた投資の種類や、計画のテストや更新の頻度によって異なります。

地域のセキュリティプログラムを強化

ランサムウェア攻撃の増加、AI 主導型攻撃の高度化、および増加する法律により、サイバー保険会社は、サイバーセキュリティ機能の料金を引き上げ、監査を強化することを余儀なくされました。これにより、企業が最善の等級を得られるようにするためのコンプライアンス意識が高まりました。保険プランの根拠となるセキュリティ管理が実施されておらず、ランサムウェアの実行を許した場合、補償が失効する可能性があります。

免責事項や制限事項により、補償が失効することもあります。地域紛争を支援しているハクティビストによって企業が攻撃された場合、その攻撃は国家による攻撃と見なされ、戦争行為の特例により補償されない可能性があります。最後に、企業は保険契約を確実に理解する必要があります。場合によっては、保険会社に通知される前に行われたすべての措置が補償されないこともあります。

多くの企業は、復号キーのコストの補償を含め、大規模なサイバーイベントのリスクを緩和するために保険に依存していますが、セキュリティプログラムを除外して保険に頼っている企業はありません。実際、多くの保険会社は、一連の基本的な制御を展開している企業のみを保険の対象とします。企業がより多くのセキュリティ制御を展開していることを示すほど、保険コストは減少します。これは、企業によるセキュリティプログラムの強化を効果的に促進します。

この目的のために、世界中の組織は、アクセスを制御するゼロトラスト・ソリューションを実装し、詳細な可視性と制御を実現してラテラルムーブメント（横方向の移動）を検知、防止、阻止するマイクロセグメンテーションを使用して、ランサムウェア攻撃に対する回復力を高めています。次のような地域的なユースケースが考えられます。



APAC ではゼロトラストの実行をシンプル化



LATAM では迅速なポリシー適用によって攻撃を阻止



EMEA ではマイクロセグメンテーションによって回復力を向上



北米ではスマートポリシーによってランサムウェアに対抗

APAC ではゼロトラストの実行をシンプル化

シンクタンクとコンサルティング・サービス・プロバイダーは、ゼロトラスト・アクセス制御メカニズムの展開と管理を容易にし、自社のネットワークと重要なインフラのクライアントのセキュリティを強化する方法を必要としていました。脅威アクターは、侵入の障壁を下げるために生成 AI を採用する傾向が高まっているため、従業員や外部委託企業に貸し出しているデバイスの可視性と制御性が向上することで、データ漏えいやネットワーク全体でのマルウェアの拡散を防止できます。

ソフトウェアベースのマイクロセグメンテーションにより、コンサルティング・サービス・プロバイダーの従業員とそのサードパーティアソシエイトに対してゼロトラストの原則を適用するためのネットワークの可視化ときめ細かなアクセス制御を実現できるようになりました。この概念実証では、ランサムウェアが依存するラテラルムーブメント（横方向の移動）などの好ましくないふるまいを阻止し、内部のアタックサーフェスを減らせることが実証されました。

EMEA ではマイクロセグメンテーションによって回復力を向上

国際的なブランドでは、サイバーセキュリティポスチャを強化して内部の脅威から身を守る必要がありました。設置されていた少数のネットワークファイアウォールではネットワーク全体のラテラルムーブメントを防止できず、通信パスと潜在的なセキュリティリスクを可視化できませんでした。

特権アクセスときめ細かなセグメンテーションを展開することで、許可されていないリモートアクセスを制限し、ユーザーベースのセグメンテーションをより効果的に定義することでゼロトラストを実現できました。回復力をテストするために、ランサムウェアの侵害テストを実施し、不正なマシンを迅速に特定して隔離することで、侵害の拡大を防ぐことができました。

LATAM では迅速なポリシー適用によって攻撃を阻止

在宅勤務モデルへの移行直後、大規模銀行の重要なデータベースがランサムウェア攻撃の被害を受けました。セキュリティチームとITチームは、機密性の高い財務データの損失を抑えるために迅速な措置を講じる必要がありました。最初の攻撃ベクトルを特定してセキュリティを確保し、ランサムウェアがバックアップサーバーや本番環境へ横方向に拡散するのを防がなければなりません。

ソフトウェアベースのセグメンテーションは、すでに銀行の他の部分で展開されていました。そのため、チームは迅速に行動することができました。わずか3日間で、攻撃ベクトルを特定し、強制力のあるポリシーを適用するために必要なプロセスレベルの可視性を得ることができました。チームは、ランサムウェアのさらなる拡散を阻止し、その後のリモートアクセスのセキュリティを強化しました。

北米ではスマートポリシーによってランサムウェアに対抗

あるヘルスケア企業は、拡大するランサムウェアの脅威に直面しました。脅威を迅速に分離して排除し、セキュリティインシデント中もアプリケーションの可用性を維持するために、従来のファイアウォールをはるかに超えた可視性を必要としていました。

マイクロセグメンテーションを導入したことで、他のアプローチよりもコストを削減しながら、アプリのリングフェンスを改善し、ランサムウェア防止ポリシーを迅速に実装することが可能になりました。同社のITチームは、1日目に4,000件のサイバー攻撃を阻止したほか、ネットワークのトラブルシューティング、インシデント調査、ポリシーの作成と適用の迅速化など、想定以上のメリットを得ました。

緩和策

ランサムウェアに対する堅牢な防御には、多層的なアプローチ、エッジでのデータ保護に対する強力な取り組み、攻撃が横方向に拡散しないようにするためのセグメンテーションの使用が必要です。これにより、脅威アクターは内部リソースに到達することがなくなります。また、脅威を特定するためには、広範な可視性が不可欠です。最新の高度なテクノロジーは、こうしたニーズに対応でき、サイバー犯罪者が使用するますます高度化している AI 搭載ツールに対する防御としても欠かせません。ランサムウェア攻撃から組織を保護するために推奨される緩和戦略には、次のものがあります。

- **ゼロトラスト・アーキテクチャの実装。**ゼロトラスト・アーキテクチャには、重要資産のセグメンテーションと、クラウドベースの[ゼロトラスト・ネットワーク・アクセス](#)による[セキュアなアプリケーションゲートウェイ](#)が含まれ、垂直方向（North / South）および水平方向（East / West）の通信を保護します。厳格なアクセス制御により、エッジ防御を回避できる[脅威を制限](#)し（[NIST Zero Trust Architecture](#) に準拠）、企業内でのランサムウェアのラテラルムーブメント（横方向の移動）を減らし、データ窃取の検知と防止を支援し、ベストプラクティスに従う組織の[ランサムウェアへの対応時間](#)を大幅に短縮することができます。
- **AI で強化された攻撃への対処、**および AI を利用した攻撃のスピードと適応性への対応。[AI 搭載](#)の脅威検知機能を展開することで、進化し続ける新たなランサムウェアの戦術に対するリアルタイムの自動応答とインシデント対応の迅速化を実現できます。
- JavaScript、Web アプリケーション、API 攻撃に対する防御を含む[包括的なエッジ保護を提供](#)し、ゼロデイ脆弱性やワンデイ脆弱性の高まる脅威に対処し、[すべての公開されているシステムのセキュリティを強化](#)します。
- 複数の環境で[意識を高める](#)と同時に脅威検知を迅速化して滞留時間を最小限に抑え、迅速な可視化と緩和を実現する機能を導入し、インサイダーの脅威や防御を回避した脅威を検知する戦略へ移行し、セキュリティ強化プロバイダーや[脅威ハンティングチーム](#)との連携による内部機能の強化を検討します。
- **MITRE ATT&CK フレームワークを使用して、**攻撃者の戦術にセキュリティ制御をマッピングし、既知の脅威アクター（DragonForce、CLOP など）を阻止できる場所を特定します。フレームワークは、保護のためにリソースを展開する方法を可視化するのにも役立ちます。
- 機密性の高いトランザクションやアクセス要求に対する[フィッシング対抗の多要素認証](#)、あるいはその他の多段階承認プロセスなど、強力な検証プロトコルを確立して、[ソーシャルエンジニアリングやディープフェイクの脅威に対抗](#)し、Single Points of Failure を防止します。ディープフェイクのリスクについてスタッフを教育します。

- URL 検査機能を備えたソリューションを使用してフィッシング攻撃を検知およびブロックし、フィッシングメールやペイロードからの悪性アクティビティを警告するエンドポイント検知を使用することにより、アウトバウンドトラフィックが感染した Web サイトに接続するのを防止します。
- セキュリティ制御とデータ保護対策が製品およびサービスのライフサイクル全体（垂直方向（North / South）のトラフィックと水平方向（East/West）のトラフィックを含む）にわたって統合されていることを確実にすることで、設計によるコンプライアンスを実現します。
- 包括的な事業継続性と災害復旧計画を策定し、ランサムウェア攻撃中および攻撃後の損失、復旧コスト、運用の安定性を管理するための財務サポートが得られるサイバー保険に加入することで、回復力を強化し、適切なリスク管理を推進します。
- バックアップ防御を継続的に強化してテストし、変更や削除を防ぐために、メインネットワークから物理的または論理的に分離した状態を維持します。
- 脆弱性を管理し、スキャンを行い、インターネットに公開されているシステムや機微な情報を含むシステムを優先するツールおよびプロセスを使用することにより、攻撃が行われる前に攻撃者を捕捉します。すべてを一度に解決するのではなく、最も重要な問題を迅速に解決することに重点を置きます。

結論

ランサムウェアの犯罪経済は、ハクティビズム、暗号資産（仮想通貨）の普及、RaaS ビジネスモデル、生成 AI および LLM、コンプライアンス要件と法律の拡大、法執行措置などの要因が複雑に絡み合い、動的かつ急速に変化し続けています。こうした脅威が急増する中、組織はサイバーレジリエンスを再定義し、包括的な保護を実現するための実践的なフレームワークを実装する必要があります。

以前は、回復力とはデータバックアップの維持を意味していました。現在、多くの組織は、攻撃が成功した場合の影響を回避するために身代金を支払わざるを得ないと感じているかもしれません。しかし、ほとんどの国の政府はそうすることを勧めていません。

最終的には、「侵害を想定する」という考え方を取り入れることで、防御者は侵害の兆候を警戒し、攻撃が成功して侵入を許す前に対応することができます。攻撃側と防御側、両方の戦術の知見を融合させた、パープルチームを展開することで、防御者はより効果的に高度なランサムウェアの脅威に対抗できます。このアプローチは、インシデントの検知と対応力を向上させるだけでなく、持続的で適応性の高い攻撃者に対する全体的な回復力の強化を可能にします。

調査手法

このレポートに記載されている Akamai のランサムウェアデータは、毎月数十億件のイベントのデータを Akamai に提供している Secure Internet Access Enterprise の顧客から収集されたものです。Akamai は、100 以上のランサムウェアグループの侵害の兆候、TTP、武器化の取り組みなど、さまざまなアクティビティを積極的に監視しています。

このレポートでは、顧客から報告されたイベントと、その顧客の環境内で検知されたものに焦点を当てています。このコンテキストでは、「イベント」を、その結果に関係なく、脅威に関連付けられた IP またはドメインへの通信試行として分類します。Akamai の検知メカニズムは、信頼度と影響度に基づいて各イベント进行分类します。これは、アクティビティの悪性の意図と潜在的な影響の確実性を評価するのに役立ちます。

2024 年 1 月 1 日～ 2025 年 5 月 31 日までの 17 か月間のデータを使用しています。(注：2025 年 4 月にデータの供給が停止したため、同月のデータが欠落しました。)

寄稿者



Or Zuckerman
Akamai, Senior Security Researcher Lead

Or Zuckerman は、インシデント対応、フォレンジック調査、検知方法の開発など、セキュリティ分野のさまざまな業務に携わっている Akamai の Senior Security Researcher Lead です。



Maor Dahan
Akamai, Senior Security Researcher

Maor Dahan は、サイバーセキュリティ業界における 10 年以上の経験を持つ Akamai の Senior Security Researcher です。Maor は、オペレーティングシステムの内部構造、脆弱性調査、マルウェア分析を専門とし、EDR、EPP、仮想化ベースのセキュリティといった革新的なセキュリティ製品向けの高度な検知および防止メカニズムを設計および開発しました。



James A. Casey
Akamai, Vice President, Chief Privacy Officer

James A. Casey は Akamai の Vice President 兼 Chief Privacy Officer であり、Akamai Global Data Protection チームを統括しています。過去 20 年以上にわたりテクノロジー企業の社内弁護士として勤務し、インターネット、サイバーセキュリティ、情報サービス、情報分析、通信業界における新しいテクノロジーや製品イニシアチブのサポートにおいて豊富な経験を有しています。テクノロジーに関する法律と規制、公共政策、プライバシーと人工知能のガバナンス、輸出入と貿易のコンプライアンス、サイバーセキュリティなど、さまざまな分野で法的助言を行っています。顧問になる前、Jim の法律事務所は、国内外のデータ、通信、インターネット業界におけるテクノロジー規制やイニシアチブのサポート、米国および世界中の人々とのテクノロジープロジェクトや通信プロジェクトのサポートに注力していました。

クレジット

Research director

Kimberly Gomez

共同執筆者

Charlotte Pelliccia Badette Tribbey
Lance Rhodes Maria Vlasak

校閲およびテーマ別寄稿者

Tanya Belousov Reuben Koh
James Casey Richard Meeus
Maor Dahan Steve Winterfeld
Ori David Or Zuckerman

データ分析

Moshe Cohen Chelsea Tuttle

販促資料

Barney Beal Ashley Linares

マーケティング・出版

Georgina Morales Hampe Emily Spinks

インターネット／セキュリティの現状

高い評価を受けている Akamai の「インターネットの現状／セキュリティ」レポートのバックナンバーおよび今後のリリースについては、akamai.com/soti をご覧ください。

Akamai の脅威リサーチ

akamai.com/security-research では、最新の脅威インテリジェンス分析、セキュリティレポート、サイバーセキュリティリサーチを通じ、常に最新情報を把握できます。

このレポートに掲載されているデータ

このレポートに引用されているグラフや図のハイクオリティバージョンを以下のリンクからご覧いただけます。これらの画像は、出典元として Akamai を明記し、Akamai のロゴをそのまま残すことを条件に、利用および引用が可能です：akamai.com/sotidata

Akamai のセキュリティリサーチ

Akamai のセキュリティ・リサーチ・ブログでは、今日の最も重要な調査に関する迅速な回答の観点をご覧ください。

akamai.com/blog/security-research



Akamai セキュリティは、パフォーマンスや顧客体験を損なうことなく、ビジネスを推進するアプリケーションをあらゆる場面で保護します。当社のグローバルプラットフォームの規模と脅威に対する可視性を活用して、お客様と Akamai が提携して、脅威を防止、検知、緩和することで、ブランドの信頼を構築し、ビジョンを実現することが可能になります。Akamai のクラウドコンピューティング、セキュリティ、コンテンツデリバリー各ソリューションの詳細については、akamai.com および akamai.com/blog をご覧ください。X（旧 Twitter）および LinkedIn で Akamai Technologies をフォローしてください。公開日：2025 年 7 月