2024年版 ThreatLabz ランサムウェア レポート

目次

本書の要旨 3

主な調査結果 4

ランサムウェアの状況：主な傾向と標的 5

- ランサムウェア攻撃の全体的な増加 6
- ランサムウェアの影響を最も受けた業界 7
- 被害組織の地理的分布 9
- 2023～2024年に最も活発だったランサムウェア グループ 12
- ランサムウェア攻撃に利用される主な脆弱性 13

ランサムウェアの総括：注目のニュース 14

- 医療業界におけるランサムウェアの脅威 14
- SECのサイバーセキュリティに関する規則による影響 15
- 法執行機関の作戦による影響 16

2024～2025年に警戒すべきランサムウェア ファミリーのトップ5 20

- #1 Dark Angels 20
- #2 LockBit 21
- #3 BlackCat 22
- #4 Akira 23
- #5 Black Basta 24

ThreatLabzによるランサムウェア メモのアーカイブ 25

2025年の予測 26

Zscalerが提供するシンプルなランサムウェア対策 29

- 攻撃チェーンの各段階での包括的な保護 31
- Zscalerの関連製品 32

ランサムウェア対策ガイダンス 33

調査方法 35

- ThreatLabzについて 35
- Zscalerについて 35

本書の要旨

ランサムウェア攻撃は、過去1年間でこれまでにないほど巧妙で大胆なものに進化し、特に脅迫型攻撃は著しく急増しています。ThreatLabzの調査では、ランサムウェア攻撃の増加以外にも、**7,500万ドルという前例のない身代金が支払われた被害事例**も確認されています。この金額は1社による支払いとして史上最高額であり、これまでに公表されている最高支払い額のほぼ2倍に相当します[1]。2023年だけでも身代金の支払いは10億ドルを超えており、こうしたサイバー犯罪による経済的影響が世界全体に幅広く及んでいる実態が浮き彫りになっています。

ランサムウェア攻撃に使われる手法もますます高度化し、悪質になっています。注目すべきは、脅威アクターが組織の従来の境界を超えた攻撃を仕掛けるようになったことです。例えば、より高額な身代金をより早く要求するために、幹部の子どもを標的にするといったケースも確認されています[2]。重要インフラ[3]や大企業[4]のみならず、中小規模の企業までが攻撃キャンペーンや進化する攻撃の標的になるのは時間の問題といえるでしょう。

法執行機関が脅威グループを撲滅するために行った「(エンドゲーム作戦(Operation Endgame)」や「ダック ハント作戦(Operation Duck Hunt)」で多数のイニシャル アクセス ブローカーが解体されたにもかかわらず、最も大規模で活発なランサムウェア ファミリーのほとんどが、解散後すぐに再編成して新たな攻撃を続けています。残念ながら、ランサムウェアの脅威アクターの多くは法執行機関の手が届かないところにいるため、刑事訴追を事実上免れています。本レポートで詳述しているように、法執行機関は報奨金や制裁、挑発行為、ランサムウェアの背後にいる人物の指名手配など、さまざまな心理的戦術を用いて圧力を強めてきました。

脅威アクターはランサムウェアの手法を常に進化させているため、脅威の状況がどのように変化しているかを常に把握しておくことが重要です。

2024年版 Zscaler ThreatLabzランサムウェア レポートでは、2023年4月から2024年4月までのランサムウェアの脅威の状況とあわせて、最新の傾向や攻撃の標的、ランサムウェア ファミリー、効果的な防御戦略の詳細を解説します。

ThreatLabzの調査により、Zscalerクラウドでブロックされた攻撃試行回数を基に計算されたランサムウェア攻撃の前年比増加率は17.8%であったこと、また、データ リーク サイトの分析で特定されたランサムウェア攻撃は57.8%という急激な増加率を示したことが明らかになりました。最も狙われた業界は製造、医療、テクノロジーであり、重要な業務とインフラが攻撃の矢面に立たされていることがわかります。

本レポートで示す調査結果は、容赦なく迫るランサムウェアに対する防御策の策定が喫緊の課題であることを明白に物語っています。ここに記載された洞察と戦略は、ランサムウェア対策を改善するための重要な手引きとなります。最新の傾向と脆弱性を理解し、推奨されるベスト プラクティスを実装すれば、ランサムウェアの被害者になるリスクが大幅に軽減され、組織の重要な資産とデータをより適切に保護できるようになります。

[1] Bloomberg、**CNA Financial Paid $40 Million in Ransom After March Cyberattack**、2021年5月20日
[2] Business Insider、**Hackers are now targeting the children of corporate executives in ransomware attacks**、2024年5月12日
[3] Dark Reading、**Ascension Healthcare Suffers Major Cyberattack**、2024年5月10日
[4] CyberScoop、**Boeing confirms attempted $200 million ransomware extortion attempt**、2024年5月8日

主な
調査結果

Zscaler ThreatLabzの調査で7,500万ドルという過去最高の身代金が支払われたことが判明しました。
これは1社が支払った身代金の額としては史上最高であり、これまでに公表されている最高支払い額のほぼ2倍に相当します。

Zscalerクラウドによってブロックされたランサムウェア攻撃は17.8%、データ リーク サイトで身代金を要求された組織は57.8%と、それぞれ前年比で増加しました。インフラの押収、逮捕、刑事告発、制裁など数多くの法的措置が行われたにもかかわらず、増加傾向となりました。

製造、医療、テクノロジーの業界がランサムウェア攻撃の最大の標的となりました。一方、エネルギー業界への攻撃は前年比で500%の急増となりました。この業界は重要インフラを保有しており、業務の中断による影響が大きいため、サイバー犯罪者の格好の標的となっています。

米国は依然としてランサムウェアの最大の標的であり、攻撃全体の49.95%を占めています。英国、ドイツ、カナダ、フランスがそれに続きます。

ThreatLabzは分析期間中に19の新しいランサムウェア ファミリーを特定しました。追跡開始以降に特定されたランサムウェア ファミリーの合計数は391となっています。

最も活発なランサムウェア ファミリー
はLockBit (22.1%)、BlackCat (別名ALPHV) (9.2%)、8Base (7.9%)でした。

脆弱性は依然としてランサムウェアの主な攻撃ベクトルとなっています。
パッチが利用できない場合でも保護を提供するゼロトラスト アーキテクチャーを基盤に据え、適切なタイミングでパッチを適用したり、統合型の脆弱性管理などの対策を強化したりすることが重要です。

音声ベースのソーシャル エンジニアリング攻撃が増加しています。
これは企業ネットワークへのアクセスを目的とするもので、Scattered SpiderやQakbotといった脅威グループが使用する手法です。

ランサムウェアの状況：主な傾向と標的

動的な性質を持つランサムウェアへの備えは、近年、セキュリティ上の最重要課題となっています。脅威アクターは人工知能(AI)技術、流出したソース コード、高度な暗号化を活用して攻撃と脅迫の手法を絶えず進化させ、その影響と収益を最大化しています。

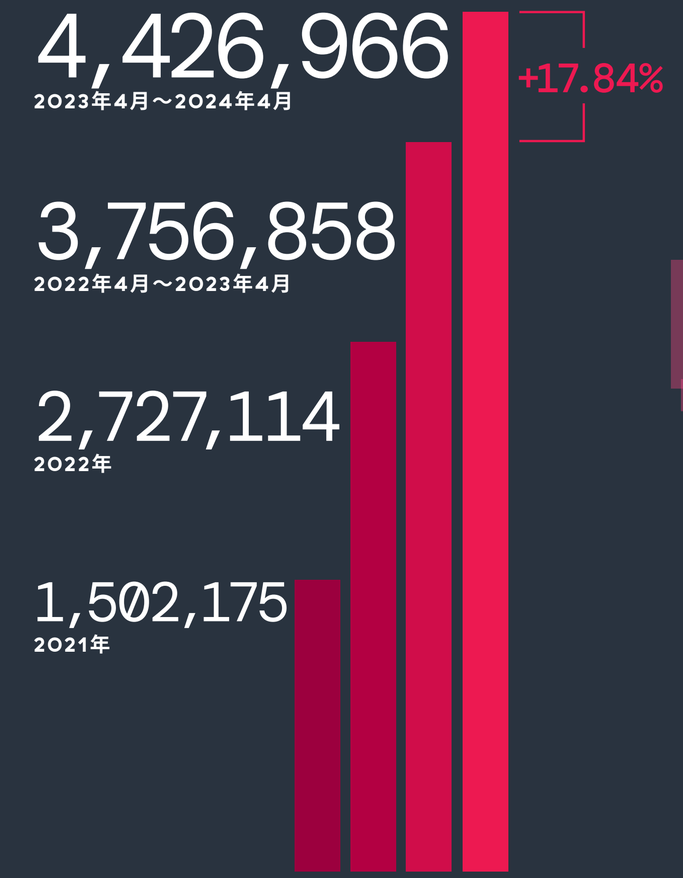
本レポートでは、2023年4月から2024年4月に発生したランサムウェア攻撃を調査し、以下の点を考察しました。

- ランサムウェア攻撃の全体的な増加
- ランサムウェアの影響を最も受けた業界
- 被害組織の地理的分布
- ランサムウェア グループとイニシャル アクセス ブローカーに行われた法執行
- 主なランサムウェアの脅威と過去最高となった身代金支払い額

ランサムウェア攻撃の全体的な増加

ThreatLabzの最新の分析により、Zscalerクラウドでブロックされた攻撃件数を基

にしたランサムウェア攻撃が前年比で17.84%増加しているという懸念すべき傾向が明らかになりました。このような攻撃を受けると業務の中断が発生し、ダウンタイムの長期化、大量のデータ流出、高額な復旧コストなどの問題が発生します。経済的負担は相当なものであり、身代金が要求されるだけでなく、システムの復旧と被害の管理にも多額の費用がかかります。こうした脅威が増大するなか、**堅牢な ランサムウェア対策**の必要性はかつてないほど高まっています。



ランサムウェアの影響を最も受けた業界

あらゆる規模や業界の組織がランサムウェア攻撃の重大なリスクにさらされています。これらの攻撃から、機密データの侵害、多額の財務損失、事業継続の中断、信用の失墜に至る可能性があります。事業の運営方法、取り扱うデータ、技術インフラなどは業界によって異なるため、各業界が抱えるランサムウェアの課題もまた多様です。

動向の変化はあるものの、ランサムウェアによる脅迫型攻撃は一貫して増加しており、データ リーク サイトに掲載された被害組織の数は昨年から57.81%増加しています。最も狙われた業界は製造となっており、653件の攻撃を受けています。これは、他のどの業界よりも2倍以上多い数です。

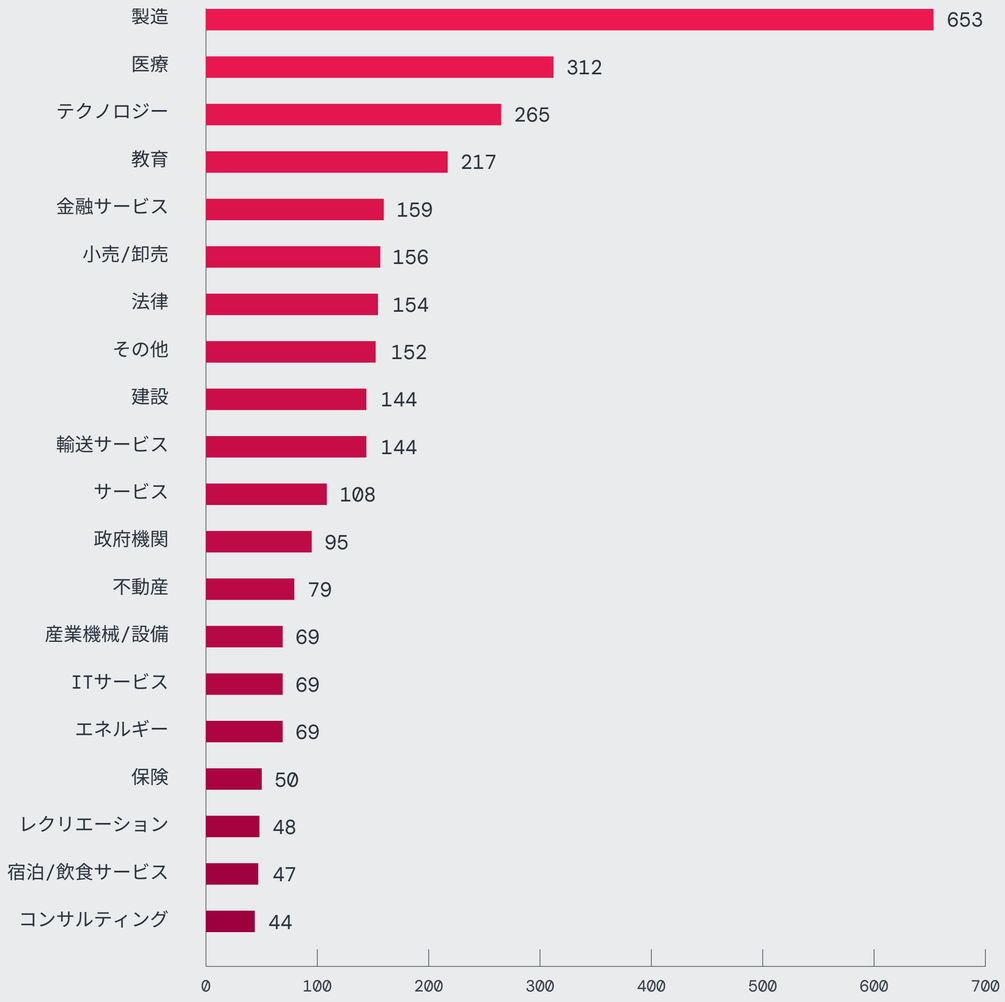


図1: データ リーク サイトに掲載された被害組織を基にしたランサムウェア攻撃の業界別件数(上位20の業界のみ)

前年比の傾向

エネルギー業界ではランサムウェア攻撃が前年比で527.27%増加しましたが、その原因としては重要産業であること、身代金を支払う可能性が高いことが考えられます。

レストラン/バー/食品サービスの業界でもランサムウェア攻撃が333.33%増加しており、高度なPOSシステムやオンライン注文プラットフォームの導入による急速なデジタル化が件数増加につながったとみられます。これらのテクノロジーは運用を合理化し、カスタマー エクスペリエンスを向上させる一方で、脆弱性となる恐れもあります。

このような増加傾向はランサムウェア攻撃の蔓延を浮き彫りにしていますが、攻撃の全容を捉えていない可能性もあります。多くの攻撃は報告されないか、身代金の支払いによって非公開に解決されます。したがって、これらの数字は、脅威の状況全体を包括的に表すものではなく、ランサムウェア攻撃の大まかな傾向として捉える必要があります。

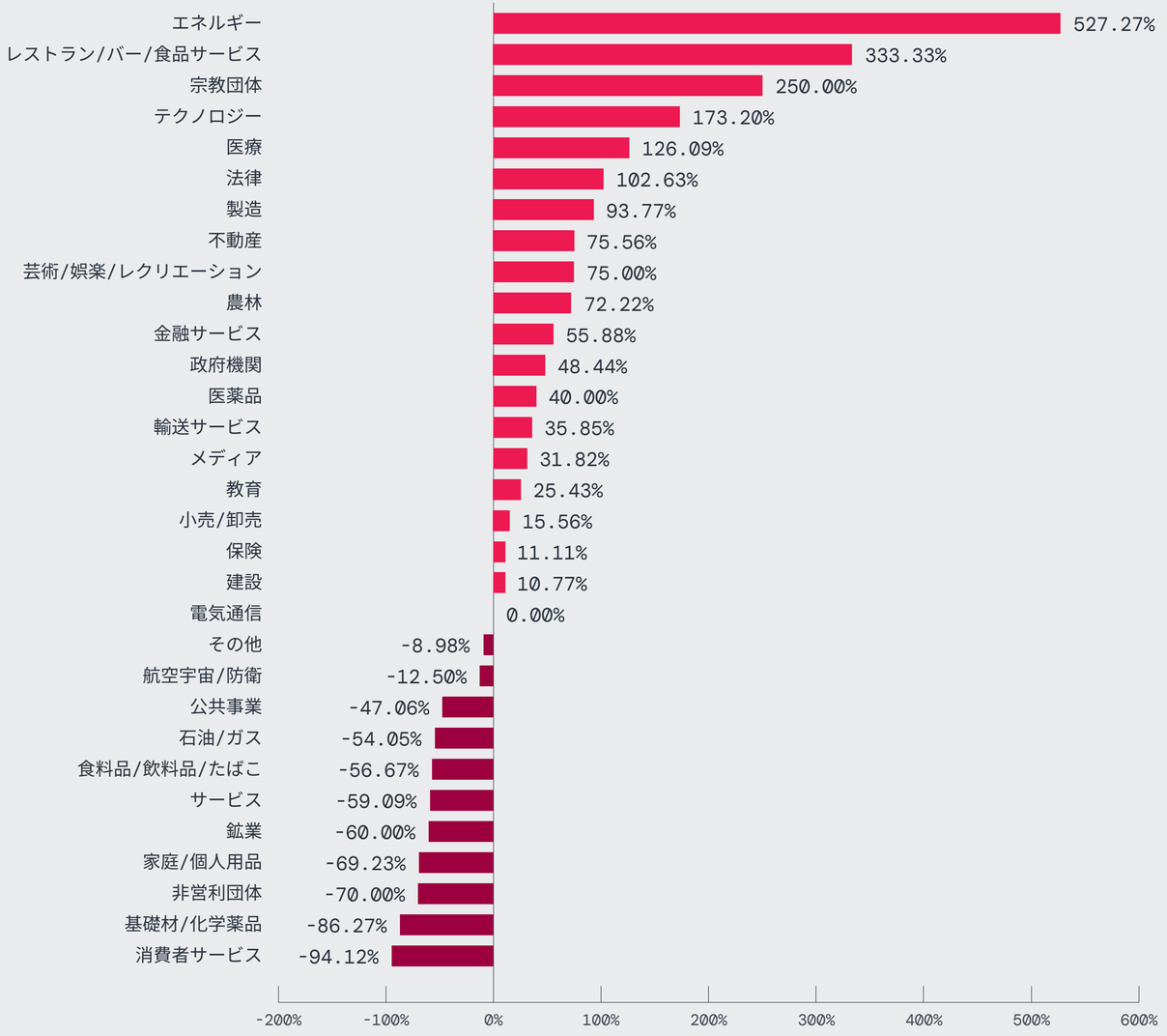


図2: ランサムウェアによる脅迫型攻撃における前年比割合の変化(業界別)。一部の業界では、基準値である前年レポートでの攻撃件数が比較的低かったため、増加率が大きく見える点に注意してください。

被害組織の地理的分布

米国は他のどの国よりも著しく多いランサムウェア攻撃を受けており、世界の攻撃全体の約50%を占めています。これに対し、2番目に狙われた英国では約6%となっています。次にドイツ(4.09%)、カナダ(3.51%)、フランス(3.26%)が続きます。図3は、2023年4月から2024年4月の間に身代金脅迫型攻撃の影響を受けた国を示しています。

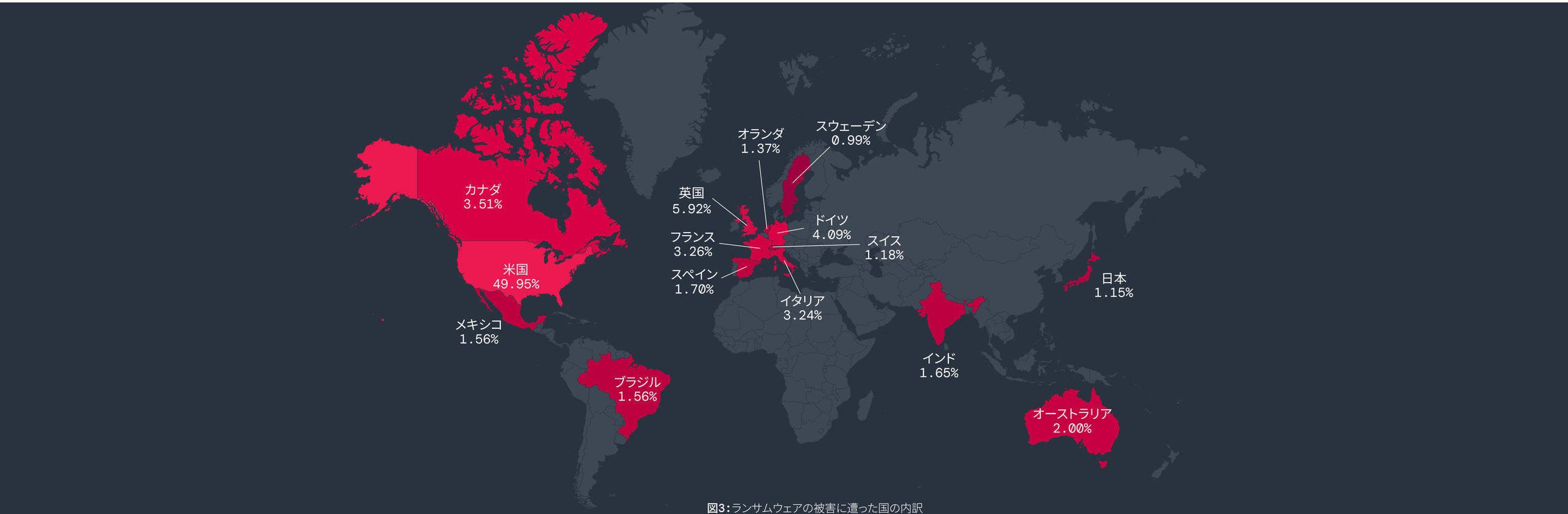


図3: ランサムウェアの被害に遭った国の内訳

ランサムウェア攻撃の地理的分布を把握することは、ランサムウェアの脅威に対抗するためのリスク評価、リソース配分、ポリシー策定、国際協力、意識向上の取り組みに不可欠です。

リスク評価

重点的に狙われた地域を分析することで、その地域の組織は自社が直面しているリスクの高さを評価し、より強力なサイバーセキュリティを実装できます。ThreatLabzの調査によると、米国が世界のランサムウェア攻撃の50%を占めているため、米国内の組織には厳格なセキュリティ対策を優先事項として取り組むことが求められています。

リソース配分

政府や組織は攻撃に関する詳細なデータを活用してリソースを戦略的に配分し、脅威レベルが最も高い分野へのサポート、資金調達、専門知識を優先することでセキュリティ態勢を強化できます。

ポリシー策定

政府は地域のランサムウェア攻撃から得た知見を、法整備、セキュリティ基準の改善、国際協力や官民部門の情報共有の促進に活用することができます。最近の注目すべき例として、SECの新しいサイバーセキュリティ規則は、脅威が増大するなかで透明性と説明責任を強化するための大きな一歩となっています。

国際協力

最も狙われた国を特定することで、法執行機関、組織、政府の間で協調的な取り組みが可能になり、ランサムウェアに国レベルおよび世界レベルで対抗できます。ダック ハント作戦とエンドゲーム作戦は、国際協力によってサイバー犯罪活動を阻止できることを示した好例といえます。

意識向上

頻繁に攻撃されている国を明確に示すことで、個人、組織、政府に対し、サイバーセキュリティのトレーニングやインシデント対応計画を策定し、防御技術に投資するなど、積極的な対策を講じるよう促進できます。

前年比の傾向

ThreatLabzは本年版と2023年版のThreatLabzランサムウェア レポートのランサムウェア攻撃を比較し、割合の変化を評価しました。最も狙われた上位15か国のうち、米国が前年比101.88%増と大きな伸びを示しました。スウェーデンは攻撃全体に占める割合は非常に小さかったものの、350%という驚異的な増加となっています。

ランサムウェアの傾向を世界レベルで分析することは非常に有意義ですが、世界のさまざまな地域での具体的な動向を理解することも重要です。地域別の内訳を理解することで、組織は自社に合わせたセキュリティ計画を、政府はより効果的なサイバーセキュリティ ポリシーを策定できるようになります。

標的となった上位15か国におけるランサムウェア攻撃の変化の割合

国	国別のランサムウェア攻撃（2023年）	国別のランサムウェア攻撃（2024年）	変化の割合
米国	902	1,821	101.88%
英国	144	216	50.00%
ドイツ	110	149	35.45%
カナダ	151	128	-15.23%
フランス	87	119	36.78%
イタリア	63	118	87.30%
オーストラリア	69	73	5.80%
ブラジル	38	57	50.00%
スペイン	36	62	72.22%
メキシコ	31	57	83.87%
オランダ	17	50	194.12%
インド	62	60	-3.23%
スイス	32	43	34.38%
日本	44	42	-4.55%
スウェーデン	8	36	350.00%

図5：ランサムウェア攻撃の前年との比較（国別）

欧州／中東／アフリカ（EMEA）におけるランサムウェア攻撃の変化の割合

国	ランサムウェア攻撃の影響を受けた組織（2023年）	ランサムウェア攻撃の影響を受けた組織（2024年）	変化の割合
英国	144	216	50.00%
ドイツ	110	149	35.45%
フランス	87	119	36.78%
イタリア	63	118	87.30%
スペイン	36	62	72.22%
オランダ	17	50	194.12%
スイス	32	43	34.38%
スウェーデン	8	36	350.00%
ベルギー	16	34	112.50%
南アフリカ	13	24	84.62%
オーストリア	15	24	60.00%
アラブ首長国連邦	12	21	75.00%

図6： 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）

アジア太平洋（APAC）におけるランサムウェア攻撃の変化の割合

国	ランサムウェア攻撃の影響を受けた組織（2023年）	ランサムウェア攻撃の影響を受けた組織（2024年）	変化の割合
オーストラリア	69	73	5.80%
インド	62	60	-3.23%
日本	44	42	-4.55%
タイ	13	25	92.31%
インドネシア	15	23	53.33%
マレーシア	14	20	42.86%
台湾	23	17	-26.09%
フィリピン	7	16	128.57%
シンガポール	8	16	100.00%
中国	21	15	-28.57%
韓国	12	10	-16.67%
ベトナム	10	10	0.00%

図7： 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）

2023～2024年に最も活発だったランサムウェア グループ

LockBit (22.1%)、BlackCat (9.2%)、8Base (7.9%)は過去1年間で最も活発だったランサムウェア ファミリーであり、それぞれが相当数の攻撃を行っていました。図8は、この期間中にデータを流出させられた被害者の数をランサムウェア ファミリー別に示しています。

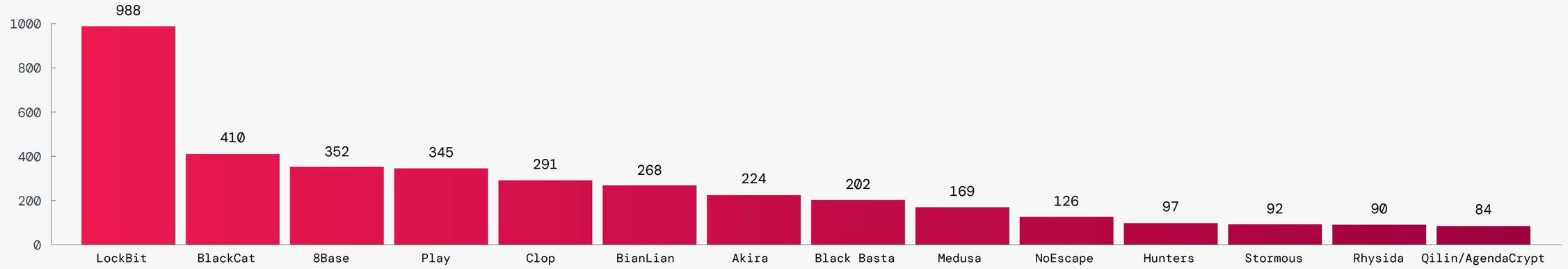


図8: 悪意を持って運営されているデータ リーク サイトで明らかになったランサムウェア攻撃の件数

新たに確認されたランサムウェア グループ

図9は、脅迫戦略の一環としてリーク サイトにデータを公開し始めた新しいランサムウェア グループを時系列で示しています。

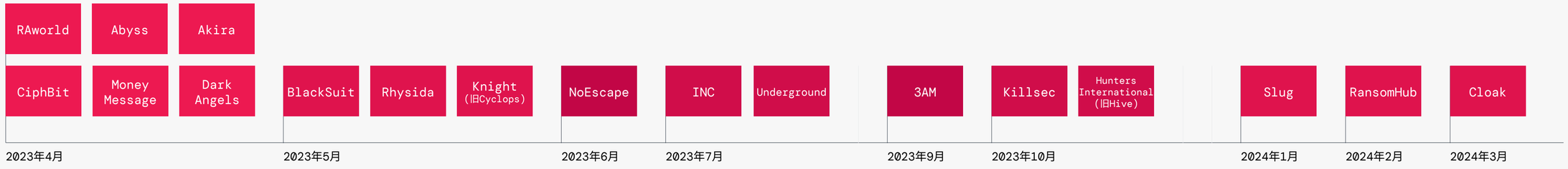


図9: データ リーク サイトを保有する新しいランサムウェア グループ

ランサムウェア攻撃に利用される主な脆弱性

ソフトウェアやシステム、デジタル インフラなどの脆弱性は、ランサムウェア攻撃の重要な侵入経路となる可能性があるため、これらの脆弱性を理解し、対処するための予防的な対策を講じる必要があります。

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、ランサムウェア グループが積極的に悪用している脆弱性を含む、脆弱性の完全なリスト[5]を管理しています。このリストを定期的に確認し、記載されている脆弱性の軽減に優先して取り組むことを強くお勧めします。予防的な脆弱性管理は、サイバーセキュリティ態勢全体を強化するうえで不可欠です。

ランサムウェア グループが悪用する脆弱性は多くの場合、ゲートウェイやVPN、その他のリモート接続テクノロジーなど、組織の外部の攻撃対象領域にあるインターネットに接続された資産に影響を与えます。これらの資産はインターネットに接続されているため、攻撃者は簡単にスキャンして悪用することができます。CISAの最新のガイダンス[6]ではさらに、VPNとリモート接続ソリューションの脆弱性が重要な懸念事項として強調されており、きめ細かなアクセス制御ポリシーに基づいたゼロトラスト アーキテクチャー、SSE、SASEなど最新のアプローチを採用するよう推奨されています。

過去1年間、世界的に有名なランサムウェア ファミリーは図10に示した脆弱性を悪用して、幅広いシステムに大きな影響を与えました。

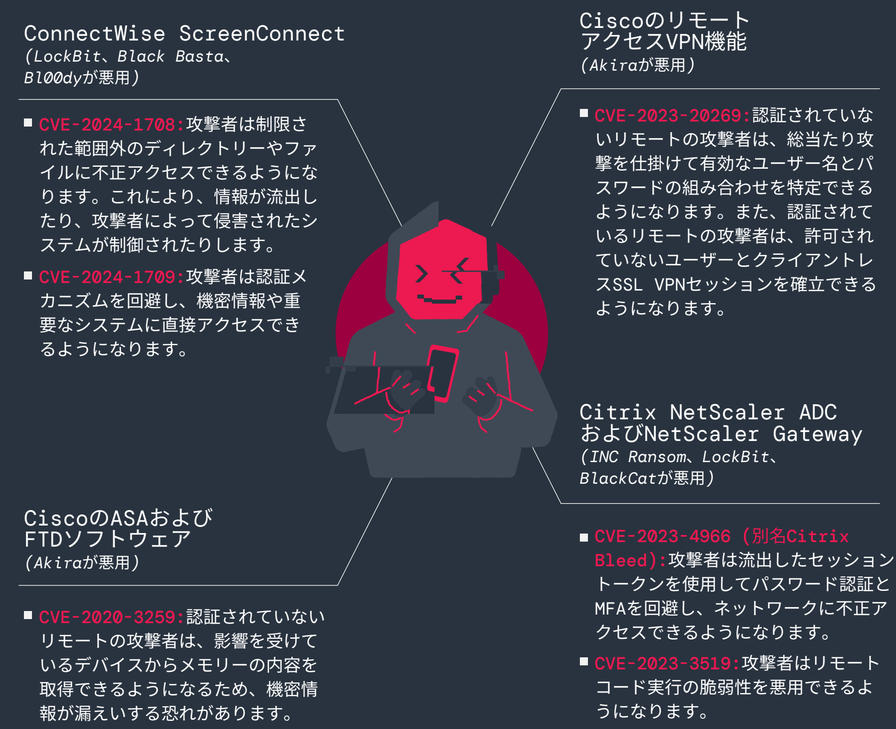


図10: 2023年4月～2024年4月に確認された脆弱性

これらの脆弱性に対して利用可能なパッチはできるだけ早く適用し、同時に以下の緩和策も講じる必要があります。

- サーバーへのリモート アクセスを無効にする
- 強力なパスワードと多要素認証を使用する
- 不審な振る舞いがないかサーバーをモニタリングする

[5] 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、Known Exploited Vulnerabilities Catalog、2024年6月25日にアクセス
[6] 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、Modern Approaches to Network Access Security、2024年6月18日

ランサムウェアの総括：注目のニュース

ランサムウェアは業界の垣根を超えて蔓延しています。あるグループを解体しても、別のグループが復活したり、新たに出現したりします。以下に紹介する最近の事件からも、ランサムウェアがいかに深刻な脅威であるかが改めてわかります。

医療業界における ランサムウェアの脅威

医療業界は、2023年から2024年にかけてランサムウェア グループから集中的に狙われ、深刻な事態に直面しました。医療業務の中断による影響は重大で、救急車のルート変更や処方箋の遅延、そして必要不可欠な治療の延期を余儀なくされます。また、機密性の高い医療データが盗まれると、個人情報の漏洩や医療詐欺などにつながり、医療エコシステムの脆弱性をさらに悪化させる恐れがあります。

身代金の支払いがもたらした予期せぬ結果

決済ソリューションを提供する、ある医療技術系企業がBlackCatグループのランサムウェア攻撃を受け、攻撃者の要求に従い2,200万ドルの身代金を支払いました。しかし、事態は予期せぬ展開をみせました。BlackCatは、攻撃を実行したアフィリエイトに身代金の一部を支払うという契約を反故にしたため(いわゆる「出口詐欺」)、アフィリエイトが医療技術系企業に対して機密データを公開すると脅迫したのです。

これはつまり、「盗人に仁義なし」という古い格言がランサムウェア攻撃にも当てはまるということです。身代金を支払ったとしても、脅威グループが窃取したデータを公開する可能性はゼロではなく、また、データが必ず削除されるという保証もありません。さらに、ランサムウェア復号ツールにはデータの正常な復旧を妨げるバグが含まれているケースもあるため、バックアップからのデータ復旧よりも時間がかかる場合があります。

二重脅迫、二重被害

2023年2月、米国のある大手医薬品販売業者は自社のITシステムが侵害され、子会社1社が被害に遭ったことを確認しました。盗まれたファイルは後にLorenz ランサムウェア グループによって流出させられています[7]。その後、同じ販売業者が2024年2月に再度ランサムウェア攻撃を受ける事態が発生しました[8]。ThreatLabzでは、1社が1年以内に複数のランサムウェア攻撃に見舞われるケースが増えていることを確認しており、これはその一例にすぎません。

[7] BleepingComputer、Drug distributor AmerisourceBergen confirms security breach、2023年2月8日

[8] BleepingComputer、Pharmaceutical giant Cencora says data was stolen in a cyberattack、2024年2月27日

SECのサイバーセキュリティに関する規則による影響

SECは2023年、上場企業の透明性と説明責任を強化するために新しいサイバーセキュリティ開示規則を導入しました。2023年12月15日に発効したこの規則により、重大なサイバーセキュリティ インシデントの適時報告が義務付けられ、組織におけるサイバーセキュリティのリスク管理、戦略、ガバナンスに関する詳細な情報提供が求められるようになりました。SECの規則に新たに追加されたForm 8-KのItem 1.05により、重大なサイバーセキュリティ インシデントについては、会社が重大度を決定してから4営業日以内に報告することが義務付けられます。さらに、Form 10-Kでは、2023年12月15日以降に終了する会計年度から、サイバーセキュリティのリスク管理と戦略について年1回報告することが義務付けられるようになりました。外国民間発行体も、Form 6-KとForm 20-Kの同等の開示に準拠する必要があります。

この規則では企業に攻撃の全容の開示が求められるため、上場企業に非公開の決済サービスの利用を要求するランサムウェアの脅威アクターにとっては新たな課題となります。プラス面として、この新たな義務によって暗号化しない脅迫型攻撃の効力が低下することが挙げられます。この攻撃では、脅威アクターがデータを盗み出し、公開すると脅迫して身代金の支払いを要求する手法が使われています。

新しい規則が組織に与える影響

SECのサイバーセキュリティに関する規則は、コンプライアンスとリスク管理の面で組織に深刻な課題をもたらす可能性があります。同規則は、透明性と投資家保護の強化を目的としていますが、組織に対しては複雑な報告要件を満たし、重大なインシデントを迅速に開示することを求めています。

大きな影響の一つに考えられるのが、組織に対してサイバーセキュリティ インシデントの正確な定量化と評価を求める圧力が高まることです。サイバーセキュリティ インシデントの重大性と被害の規模を判断するには慎重な分析が必要であり、これにはコストがかかる可能性があります。組織は規模の大小を問わず、インシデント対応手順を見直し、SECの要件を満たすために開示を更新する必要があります。

さらに、要件を満たす期限が組織の規模や報告状況によって異なることも、複雑さの要因となっています。中小規模の企業の報告期限は異なる場合が多く、一般的に大企業よりも長くなっています。大企業はより厳しい期限を遵守する必要がありますが、規模が大きいがゆえにサイバーセキュリティ インシデントの重大度を分析するためにより多くのリソースを割くことができます。

新しい開示要件により、上場企業は秘密裏に身代金を支払うことができなくなるため、侵害に関する情報の公開後に発生する信用の失墜や世間の反発は避けられない可能性があります。

SECの規則に違反している組織の存在

SECの明確なガイドラインが存在するにもかかわらず、一部の組織ではすでに新しいサイバーセキュリティの規則が遵守されていないことがわかっています。複数の有名企業からの最近の開示により、コンプライアンス違反やインシデント報告の適切性について懸念が提起されています[9]。これらの開示の多くは、サイバーセキュリティ インシデントの財務上および運用上の影響に関する定量的なデータや詳細な評価を欠いていますが、これこそまさにSECが現在義務付けているものです。サイバー インシデントの不十分な開示はSECの規則に違反するものであるため、一貫性のある効果的なコンプライアンスを確保するために、今後、ガイダンスと規制監督の強化が求められる可能性があります。

SECのサイバーセキュリティに関する規則は、インシデント報告の透明性と説明責任を向上させることを目的としており、規制の重要な転換を示すものです。これらの新しい規則を一貫して遵守するには、規制当局、組織、業界関係者の間で継続的に協力し合う必要があります。

[9] Forbes、**Companies Are Not Complying With The New SEC Cybersecurity Incident Disclosure Rules**、2024年3月4日

法執行機関の作戦による影響

Qakbotインフラを解体した「ダック ハント作戦」

連邦捜査局(FBI)と司法省(DOJ)は2023年8月29日、多国間の協調的な取り組みの一つであるダック ハント作戦に関する発表を行いました。Zscaler ThreatLabzはこの作戦において、多大な技術的支援を提供しました[10]。図11に示すように、Qakbotでは解体の試みに耐性がある多層的なインフラが使われていました。

このインフラには回復力が多層的に組み込まれていたため、各層を解体するには協調的な取り組みが必要でした。インフラの第1層にはスーパーノード プラグインを実行する感染システムが含まれていましたが、これはQakbotのマスター バックエンド サーバーを隠すように設計された複数の上流プロキシにトラフィックを中継するものです。

ダック ハント作戦では、図12に示すように、スーパーノードの上流プロキシ サーバーをシンクホール サーバーにリダイレクトさせ、Qakbotのインフラを即座に乗っ取りました。

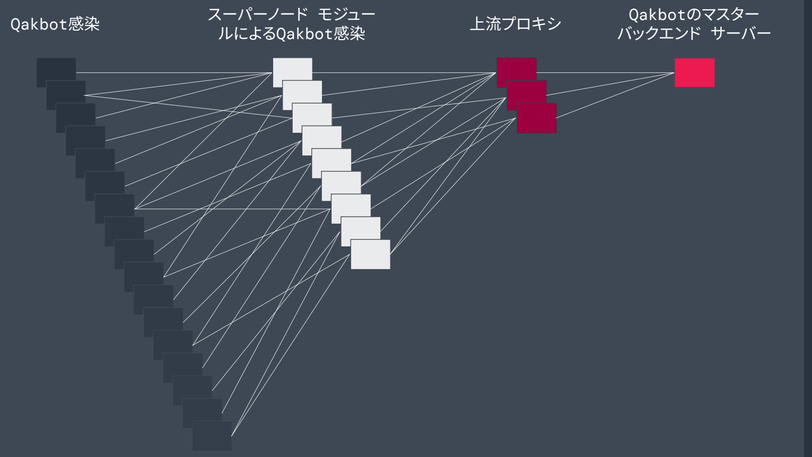


図11： Qakbotの多層的なインフラ

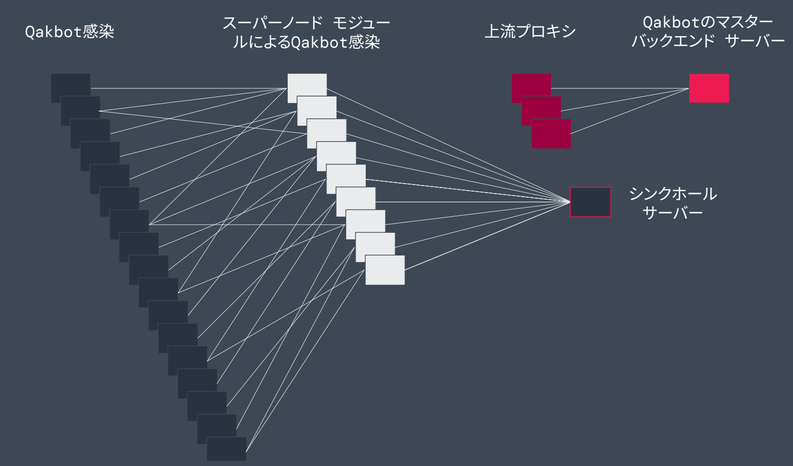


図12：各スーパーノードの上流プロキシをリダイレクトさせた後のQakbotのアーキテクチャー

FBIがスーパーノードを乗っ取ると、シンクホール サーバーは被害者のコンピューターにシェルコードをダウンロードするよう指示しました。このシェルコードはマルウェアを無効化するDLLを読み込むもので、これによってマルウェアの除去とさらなる攻撃の阻止に成功しました。

Qakbotは解体時点で世界中の70万台以上のコンピューターに感染しており、米国だけでは20万台以上に上ります[11]。**15年近く活動を続けたQakbot**は当初、クレジット カード詐欺や電信送金詐欺を目的としていましたが、2019年にConti、ProLock、Egregor、REvil、MegaCortex、Black Bastaなどのランサムウェア グループのイニシャル アクセス ブローカーへと方向転換しました。

Qakbotマルウェアは通常、悪意のある添付ファイルやリンクを含むスパム メールを介して配布され、一度感染すると、Cobalt Strikeが展開されてラテラル ムーブメントが発生し、最終的にランサムウェアが展開されるというものでした。

残念ながら、どの脅威アクターに対しても逮捕や起訴状の公開は行われませんでした。そして、Qakbotは**2023年12月に再び登場**し、64ビット版のWindows向けにマルウェアをさらに進化させました。このマルウェアでは内部構成フォーマットが変更されたほか、ネットワーク通信にAES暗号化を使用するよう修正されています。本レポートの後半で説明しますが、Qakbotの脅威アクターはダック ハント作戦以降、戦術、技術、手順(TTP)を大幅に変更しています。

[10] 米国司法省、**Qakbot Malware Disrupted in International Cyber Takedown**、2023年8月29日
[11] TechCrunch、**How the FBI took down the notorious Qakbot botnet**、2023年9月1日

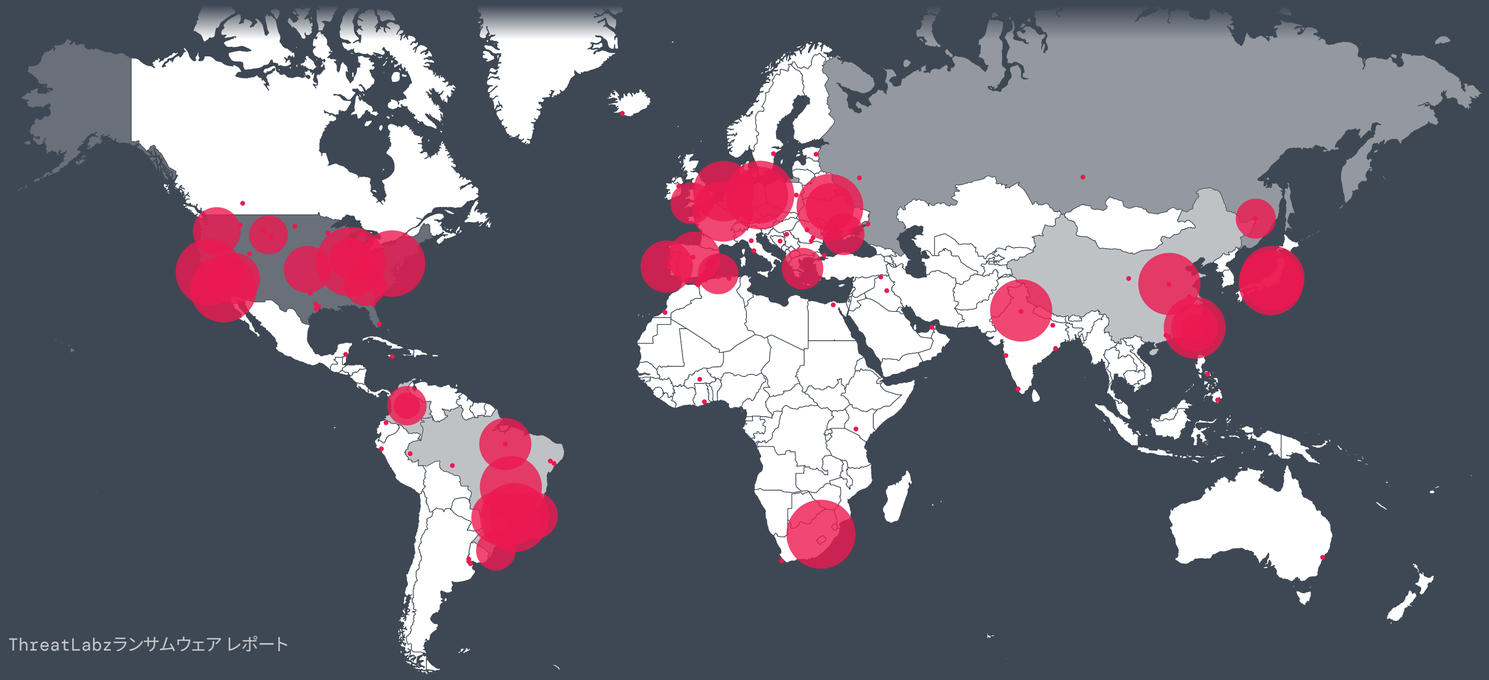
複数のイニシャル アクセス ブローカーを同時に狙った「エンドゲーム作戦」

欧州警察機構(ユーロポール)は2024年5月28日、多数の国際的法執行機関と連携し、複数のイニシャル アクセス ブローカーに狙いを定めた「エンドゲーム作戦」を発表しました。この作戦の結果、全世界の10か所以上で捜索が行われ、数人が逮捕されました。また、犯罪活動に使用されていた100台以上のサーバーも閉鎖されました。これらのサーバーは、被害者のコンピューターに侵入してランサムウェアなどを展開するさまざまなマルウェア ダウンローダー(別名「ローダー」)の動作に不可欠なものでした。

この作戦で標的となったマルウェア ファミリーは、医療施設や重要インフラのサービスを含む世界中の何百万台ものコンピューターに感染していました。作戦の一環として、SmokeLoader、Pikabot、Bumblebee、IcedIDに対して法的措置が取られました。

Zscaler ThreatLabzは、エンドゲーム 作戦のSmokeLoaderのシンクホール化と修復作業で重要な技術支援を提供しました。

SmokeLoaderは2011年に登場し、Raspberry RobinやStop (別名DJVU)などのランサムウェアを展開する目的で、複数のイニシャル アクセス ブローカーによって使用されてきました。エンドゲーム作戦では、これらの脅威グループが使用していた1,000を超えるSmokeLoaderドメインが押収され、その後、法執行機関が管理するシンクホール サーバーにリダイレクトされました。図13のマップは、SmokeLoaderに感染したシステムとシンクホールとの通信を示しています。



このマップからも、SmokeLoaderが世界中に大きな影響を与え、中南米、アジア、北米、欧州で深刻な感染が発生していることがわかります。

図13:エンドゲーム作戦のシンクホールと通信するSmokeLoaderに感染したシステムのマップ(出典:Zscaler ThreatLabz)

SmokeLoaderに感染したシステムがシンクホール サーバーに接続すると、マルウェアに組み込まれたアンインストール コマンドを受信します。図14に示すように、感染した4万台以上のシステムからSmokeLoaderが除去されました。

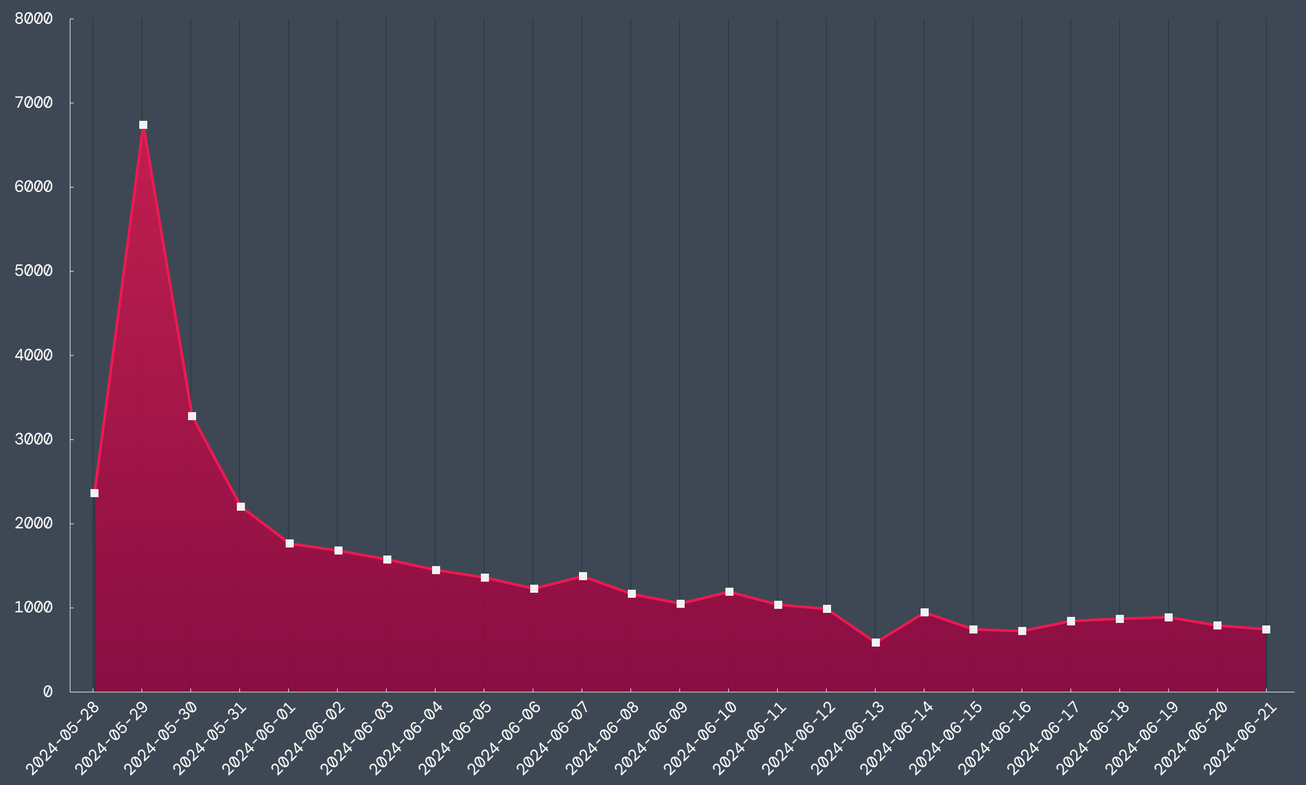


図14：エンドゲーム作戦によってSmokeLoaderが除去されたシステム

Pikabotは2023年の初めに登場し、同年後半に活発化しました。増加の理由は、ダック ハント作戦によるQakbotの解体後、Black Bastaランサムウェアがこのマルウェアをイニシャル アクセス ブローカーとして採用するようになったためです。2024年2月、コード ベースと構造を大きく変更したPikabotが再び登場しました。ThreatLabzは、PikabotがCobalt StrikeとMetasploitのMeterpreterを定期的に展開していることを確認していました。

2022年3月に登場したBumblebeeは、以前のContiランサムウェア グループに関連していることがわかっています。Bumblebeeは同グループのBazarLoaderマルウェア ツールの後継であり、ContiとDiavolによるランサムウェア攻撃のイニシャル アクセスに使用されていました。ThreatLabzでは、BazarLoaderとBumblebeeのどちらもCobalt Strikeペイロードを展開し、ラテラル ムーブメントを発生させていることが頻繁に確認されていました。また、BumblebeeはAkiraやBlack Bastaのランサムウェア攻撃にも関与しています。

2017年に登場したIcedIDは当初、Qakbotと同様にバンキング型トロイの木馬として設計されましたが、後に、ランサムウェアのイニシャル アクセス ブローカーとしての活動に重点を移しました。IcedIDのマルウェア コードは長年にわたり、さまざまな目的で流用され、変更されてきました。さらに、同じ開発者がLatrodectusと呼ばれる新しいマルウェア ローダーを開発し、2023年11月にリリースしており、これもランサムウェアの展開に使用された可能性があります。

「エンドゲーム作戦」の後、1か月足らずで再登場したLatrodectusを除き、ほとんどのイニシャル アクセス ブローカーの活動は最小限に留まっています。しかし、脅威アクターは再結集することがあるため、今の落ち着いた状況は長続きしないとみられています。

Hunters Internationalとして再生したHiveランサムウェア

2023年1月、Hiveランサムウェア グループのインフラが閉鎖されました。FBIは7か月に及ぶ秘密作戦の後、Hiveのサーバーに侵入し、300を超える復号キーを回収して約1億3,000万ドルの身代金の支払いを阻止しました。Hiveグループは2021年6月から活動し、世界中の1,500を超える組織に被害を与え、1億ドル以上の身代金を手に入れています[12]。これらの攻撃により、病院や教育機関、金融機関など、さまざまな団体が被害に遭いました。しかし、Hiveに関連する逮捕者は出ないまま、2023年10月にこのグループはHunters Internationalにリブランドしました。大規模な混乱を引き起こした後にリブランドするという戦略は、脅威グループの常とう手段となっています。

図15に示すように、このグループは運用を大きく変更し、身代金の割引や被害者との交渉には一切応じない方針に切り替えました。

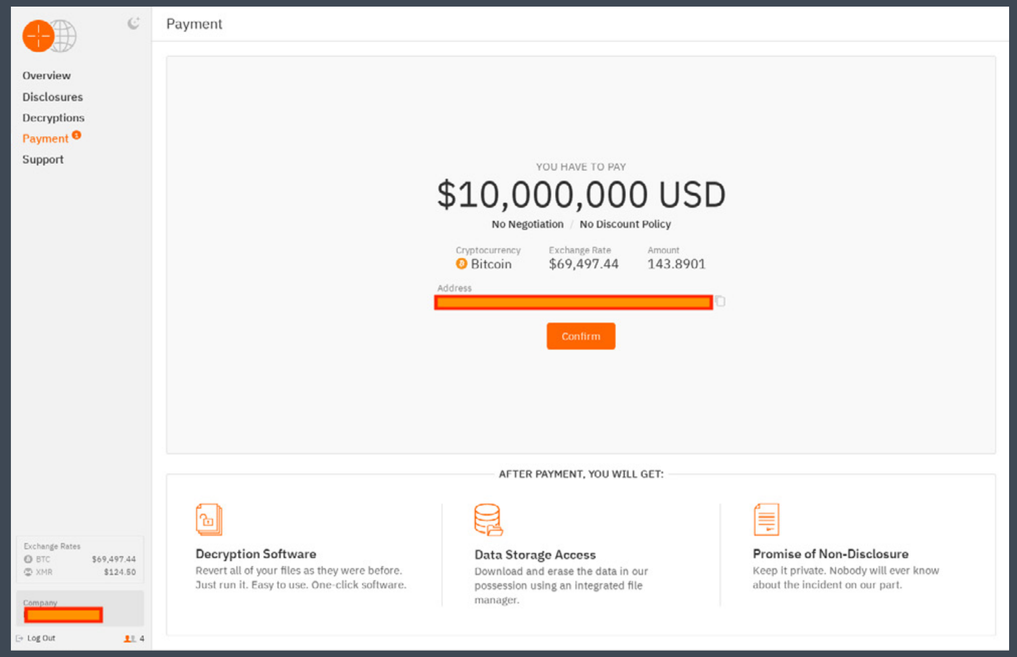


図15: 身代金の割引や交渉は受け付けないことを示すHunters International の被害者ポータル

身代金交渉に応じないという戦略は**非常に珍しく**、ランサムウェア グループは通常、元の身代金要求額から大幅な値引きを提示します。Hunters Internationalのこの方針転換により、全体的な支払い件数は減るものの、支払い総額は増加すると予測されます。

このグループは今なお新たな攻撃を仕掛けており、さらなる逮捕や刑事告発がなければ、今後も重大な脅威であり続けると考えられます。

[12] 米国司法省、U.S. Department of Justice Disrupts Hive Ransomware Variant、2023年1月26日

2024～2025年に警戒すべき ランサムウェア ファミリーのトップ5

ランサムウェアやその他のサイバー脅威はますます複雑かつ巧妙化しているため、効果的なセキュリティ態勢を維持するには、最も一般的で危険なランサムウェア ファミリーの情報を常に把握しておく必要があります。このセクションでは、組織にとって最も重大なリスクとなる5つのランサムウェア ファミリーを取り上げ、その手法、想定される被害、最新の活動状況を紹介します。

#1 Dark Angels

Dark Angelsランサムウェア グループは、データ リーク サイトのDunghillを運営しており、2022年5月頃に登場しました。これまで最大規模のランサムウェア攻撃をいくつか仕掛けたものの、注目を集めることはありませんでした。しかし、2024年初め、ThreatLabzはDark Angelsに7,500万ドルもの身代金を支払った被害者を確認しました。これは、今まで公表されてきた中で最も高額な身代金支払い額です。この成功は他の攻撃者への大きな刺激となり、Dark Angelsの手法(以降で説明)を採用して同様の成果を得ようとする攻撃者が増えることが予測されます。Dark Angelsは、医療、政府、金融、教育などさまざまな業界を標的としており、最近では産業、テクノロジー、通信分野の大手企業に対して攻撃を仕掛けたことが確認されています。

Dark Angelsグループは高度に標的を絞るアプローチを採用しており、通常、1度に攻撃する大企業は1社となっています。これは被害者を無差別に攻撃して、攻撃の大部分をイニシャル アクセス ブローカーやペネトレーション テスト チームのアフィリエイト ネットワークに依頼するという他のランサムウェア グループが採用しているアプローチとはまったく対照的です。Dark Angelsは攻撃対象を特定して侵入すると、会社のファイルを暗号化するかどうかを決定し、通常は1～10TBの膨大な量の情報を盗み出します。大企業に対しては、数日から数週間かけて10～100TBのデータを持ち出す場合があります。

Dark Angelsが最も注目を集めたのは、2023年9月に発生したビル自動化システムなどのソリューションを提供する国際複合企業への侵入でした。27TBを超える企業データを窃取して、同社のVMware ESXi仮想マシンを暗号化し、5,100万ドルの身代金を要求しました。この攻撃のファイル暗号化に使われたのが、RagnarLockerランサムウェアの亜種です。RagnarLockerとDark Angelsの関係は明らかではないものの、RagnarLockerに対して法的執行[13]が行われる前から、Dark Angelsはこのランサムウェアを使用しており、これが結果として2023年10月のRagnarLocker主要メンバーの逮捕につながりました。なお、Dark Angelsが登場した際はBabukの亜種を展開していましたが、その後RagnarLockerに切り替えています。

価値の高い少数の企業を標的にして多額の身代金を要求するDark Angelsランサムウェア グループの戦略は、注目に値する傾向です。Zscaler ThreatLabzは、他のランサムウェア グループがDark Angelsの成功に注目し、同様の手法を採用することで、価値の高い攻撃対象に狙いを定め、より重要なデータを窃取して金銭的利益を最大化する可能性があるとみています。

[13] 欧州警察機構(ユーロポール)、Ragnar Locker ransomware gang taken down by international police swoop、2023年10月20日

#2 LockBit

LockBitは2019年9月に初めて登場し、その大規模なランサムウェア アフィリエイト ネットワークにより急速に注目を集めました。LockBitはアフィリエイトを利用して侵害し、データを持ち出し、そしてランサムウェアを展開します。侵入は通常、悪意のある添付ファイルやリンクを含むスパム メールを介して始まります。他にも、リモート デスクトップ プロトコル(RDP)やVPN認証情報を標的としたパスワード総当たり攻撃を実行したり、窃取された認証情報をイニシャル アクセス ブローカーから購入したり、公開アプリケーションを悪用したりする手法も確立しています。LockBitのサイバー犯罪ネットワークは、製造、医療、物流などの重要な業界が保有する世界中の2,000以上のシステムに狙いを定め、被害者から1億2,000万ドル以上を入手しました。

LockBitは昨年も攻撃件数でトップとなっています。Dark Angelsとはまったく異なる戦略を用いるLockBitは、得られる報酬の大きさに関係なく、できるだけ多くの組織を攻撃するようアフィリエイトを促しています。このように攻撃件数が多いことから、標的にされた中小規模の企業に対しては通常、比較的低い身代金が要求されます。

LockBitランサムウェアは、WindowsとLinuxベースのシステムに展開されます。Windowsを標的とするLockBitには、LockBit Red (オリジナル)、LockBit Black (BlackMatterソース コードに基づく)、LockBit Green (流出したContiソース コードに基づく)の3つのバージョンがあります。**2023年版 ThreatLabzランサムウェア レポート**でも述べているように、LockBit Blackビルダーが流出した後、LockBitと提携していない多くのサイバー犯罪グループがこのビルダーを独自のランサムウェア攻撃に使用しました。LockBit Blackは依然として、このグループが最も多く展開している亜種となっています。現在、被害者のファイルの暗号化に使用されたLockBitランサムウェアの亜種が、身代金メモの被害者IDの横に表示されるようになっています。これは攻撃を実行する脅威アクターが展開された亜種を簡単に特定し、身代金の支払い時に適切な復号ツールを提供できるようにするためです。最近のLockBit Blackの身代金メモの例については、図16をご覧ください。

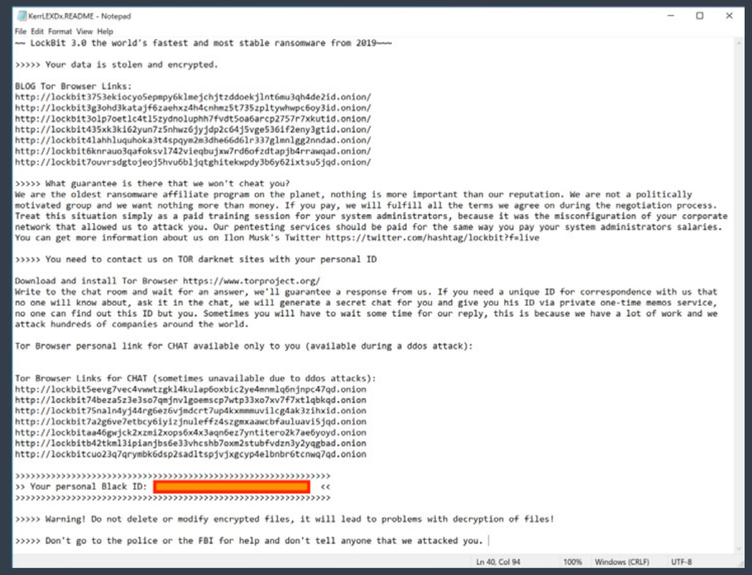


図16: 最近のLockBit Blackの身代金メモ

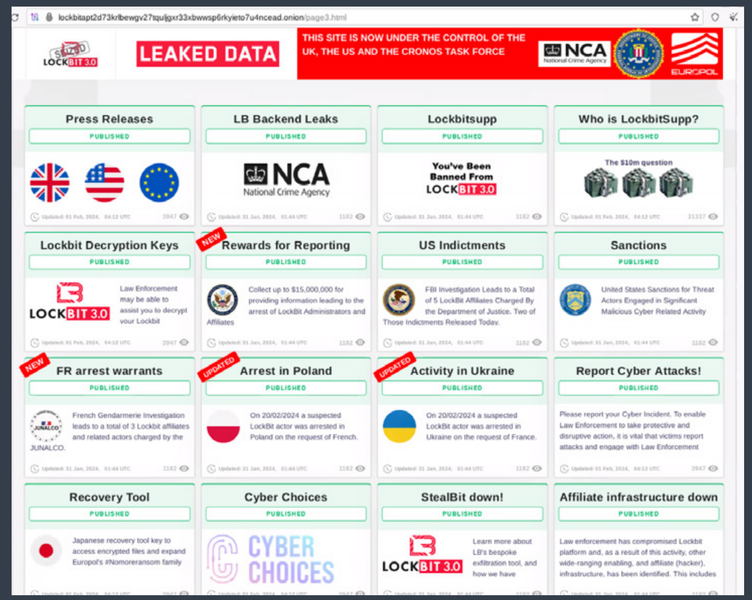


図17: 法執行機関が押収した
LockBitのデータ リーク サイト

FBIと英国の法執行機関は2024年2月20日、被害者の復号キー約7,000個を含むLockBitのインフラの一部を押収しました。法執行機関は押収後、LockBitのデータ リーク サイトを乗っ取り、下の図17に示すように、元のサイトに似せたミラー サイトを作成して、新しい情報が公開されるまでさまざまな記事やカウントダウン タイマーを表示させました。

しかし、この解体から数日後、**ThreatLabzはLockBitによる新たなランサムウェア攻撃を特定**し、さらに新たなデータ リーク サイトも確認しました。このグループは法執行機関による制裁以降も活動を続け、数十の組織に対して新たな攻撃を仕掛けています。

FBIは2024年5月7日、LockBitの開発者兼運営者であるDmitry Yuryevich Khoroshevの起訴を発表しました。しかし、LockBitの運営者はFBIがこの人物を正しく特定したことをすぐに否定しました。これ以上の逮捕者が出ない限り、LockBitの攻撃は当面続く可能性が高いと予測されますが、ThreatLabzは監視が強化されていることもあり、ある時点でLockBitというブランドが廃止され、別の名称で運営を復活させると考えています。

#3 BlackCat

2021年11月に活動を始めたBlackCat (別名ALPHV)ランサムウェアは、2024年3月に活動を停止するまで最も悪名高い脅威の一つでした。BlackCatはLockBitと同様に、アフィリエイト ネットワークを活用して攻撃を開始し、身代金の支払いの一部を分配していました。

おそらく最も危険なBlackCatのアフィリエイトは、Scattered Spider[14] (別名Star Fraud)として知られるグループです。このグループは英語を話すメンバーで構成されているため、ソーシャル エンジニアリング攻撃で高い効果を発揮します。典型的な手口としては、音声通話でIT担当者やヘルプ デスクなどになりすまし、SIMスワッピング攻撃を実行して多要素認証を突破します。2024年6月15日、Scattered Spiderの首謀者[15]とされる22歳の英国人が逮捕されましたが、この逮捕がグループの攻撃継続能力にどのような影響を与えるかを判断するには時期尚早かもしれません。

BlackCatはプログラミング言語にRustを使用していることもあり、プラットフォーム間の互換性が最も高いランサムウェア ファミリーの一つでした。図18はグループが活動を停止する直前に、異なるプラットフォーム向けに提供していたBlackCatの復号ツールを示しています。プラットフォームにはWindows、ESXi、FreeBSDのほか、さまざまな種類のLinux OSとアーキテクチャー(ARM、x86/x64、PowerPCなど)が含まれています。

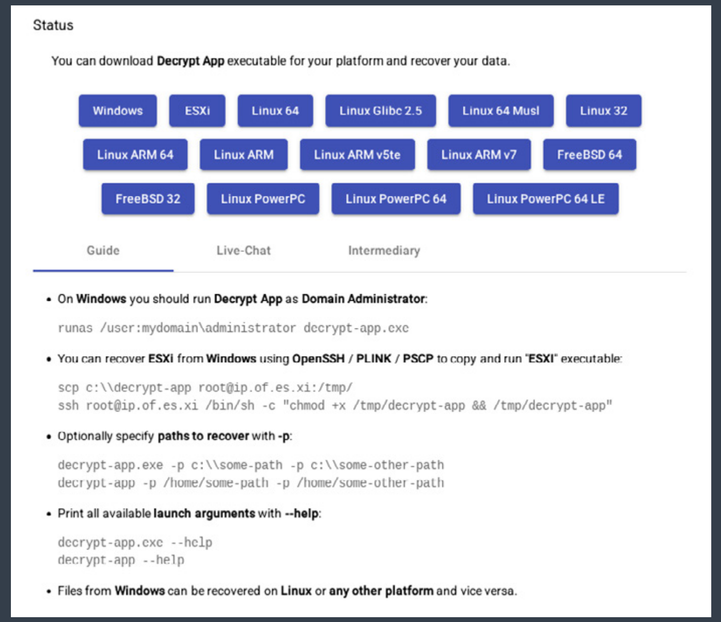


図18： 15種類の異なるOS、アーキテクチャー、プラットフォーム向けに提供されたBlackCatの復号ツール

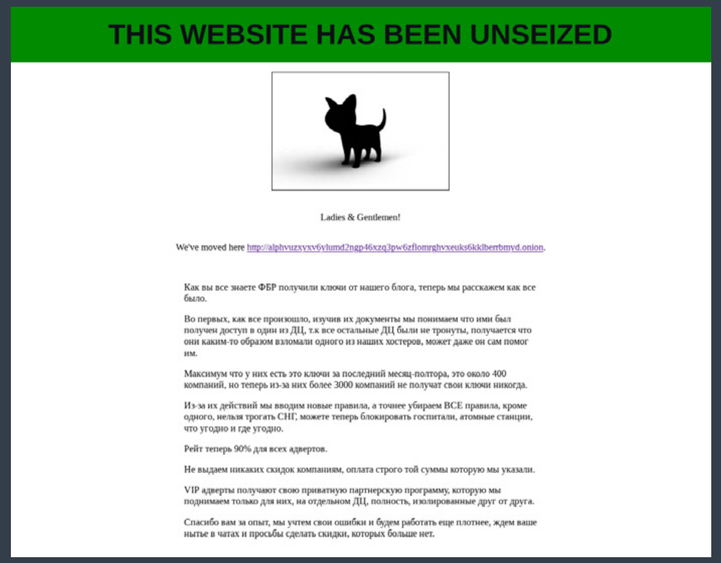


図19： 法執行機関の行動後に「押収を解放」したBlackCatのデータ リーク サイト

他のランサムウェア ファミリーは通常、WindowsやESXi、ごく一部のLinuxベースのプラットフォームだけを標的とするため、これほどまでに幅広いプラットフォームを対象としているのは異例といえます。これは、BlackCatのアフィリエイトができるだけ多くのシステム上でファイルを暗号化するために、対応するプラットフォームの追加を要求したためとみられています。

2023年12月、FBIはBlackCatのインフラの一部にアクセスし、このグループが所有する身代金交渉ポータルやデータ リーク サイトを含むTorベースのWebサイトを押収しようと試みました。しかし一転、下の図19に示すように、BlackCatはデータ リーク サイトを「押収から解放した」というメッセージを投稿し、FBIが操作できない新しいデータ リーク サイトへのリンクを掲載しました。

FBIとBlackCatのこのやり取りは、新しいデータ リーク サイトが十分に周知されたとBlackCatが確信するまで数日間にわたって行われました。なお、Torサイトの「押収」は、中央機関が裁判所命令に従って行うものではなく、暗号化の秘密情報を把握しているかどうか次第であるため、従来のDNSベースのWebサイトほど簡単ではありません。

BlackCatグループは2024年3月、FBIがインフラを侵害したことで活動を継続できなくなったとして解散を発表しました。しかし、解散のタイミングが2,200万ドルの身代金を受け取った直後であり、その後、医療技術系企業の侵害を支援したアフィリエイトに対して出口詐欺を働いたため、疑惑が生じました(本書で前述)。

BlackCatランサムウェアは現在活動していませんが、このグループの攻撃実行役となっていたアフィリエイトは、RansomHub (2,200万ドルの身代金を支払った医療技術系企業から窃取したデータをリークしたグループ)などの他のRansomware as a Serviceネットワークにくら替えしたとみられています。また、BlackCatランサムウェア グループ自体が実際に活動を停止した可能性は低く、新しい名称で再び登場すると予測されます。

[14] 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、Cybersecurity Advisory: Scattered Spider、2023年11月16日
[15] Krebs on Security、Alleged Boss of 'Scattered Spider' Hacking Group Arrested、2024年6月15日

#4 Akira

Akiraランサムウェアは2023年4月に突如登場し、そのアフィリエイトが実行した膨大な数の攻撃により急速にその名が知られるようになりました。Akiraの脅威グループは、消滅したContiグループの別の分派である可能性が高く、実際、Akiraのランサムウェア コードと流出したContiのソース コードに多くの類似点が確認されています。一方、このグループは最近、特撮番組「Power Rangers」のキャラクターであるMegazordを連想させるRustベースのランサムウェアを開発しています。

Akiraランサムウェアのアフィリエイトは、CVE-2023-20269の悪用を含むさまざまなイニシャル アクセス メカニズムを採用しています[16]。Bumblebeeを運営する脅威グループは、Contiランサムウェアと関係があり、Akiraのイニシャル アクセス ブローカーとしても知られています。本レポートで前述したように、エンドゲーム作戦でBumblebeeは解体されましたが、Akiraはほとんど影響を受けませんでした。

Akiraの攻撃をより深く理解するために、このグループが身代金を支払う被害者に提供した実際の情報を紹介します。ThreatLabzが入手したAkiraからのチャット メッセージには、イニシャル アクセス ブローカーを通じて企業ネットワークに最初にアクセスした方法だけでなく、ランサムウェア攻撃を今後防ぐためのヒントも記載されていました。

我々は、貴社のネットワークへのイニシャル アクセスをダークWebで購入しました。その後、kerberoastingを実行し、パスワードのハッシュを取得しました。次に、ハッシュに総当たり攻撃を仕掛け、ドメイン管理者のパスワードを取得しました。数週間にわたってネットワーク内で調査を行った結果、セキュリティ上の欠陥がいくつか検出されたので対処することを強くお勧めします。

1. 従業員は疑わしいメールやリンクを開封したり、ファイルをダウンロードしたり、ましてや自分のコンピューターで実行したりしてはいけません。

2. 強力なパスワードを使用し、できるだけ頻繁に変更してください(少なくとも月に1～2回)。パスワードは別のリソースと同じものを使用したり、繰り返し使用したりしてはいけません。

3. 可能な限り2FAをインストールしてください。

4. 攻撃に対する脆弱性が改善されている最新バージョンのOSを使用してください。

5. すべてのソフトウェアのバージョンをアップデートしてください。

6. ウイルス対策ソリューションとトラフィック モニタリング ツールを使用してください。

7. VPNのジャンプ ホストを作成してください。ドメイン1とは異なる一意の認証情報を使用してください。

8. トークン キーをサポートするクラウド ストレージを備えたバックアップ ソフトウェアを使用してください。

9. オンラインの安全対策について、できるだけ頻繁に従業員にトレーニングを実施してください。最も脆弱な要素は人的要因であり、従業員やシステム管理者などの責任の欠如が大きなリスクを招きます。貴社のますますのご発展をお祈りしています。ご協力いただきありがとうございました。セキュリティに対してはぜひ慎重な姿勢で取り組んでください。

Akiraから送られてきたこのアドバイスは非常に役立つものであり、こうした攻撃を理解して阻止するための基本といえます。

Akiraは法執行機関の妨害を直接受けていない、数少ない主要なランサムウェア グループの一つとなっています。結果として、現在最も活発なランサムウェア グループの一つでもあり、今後1年間にわたって新たな攻撃を仕掛け続ける可能性が高いとみられています。

[16] https://nvd.nist.gov/vuln/detail/CVE-2023-20269

#5 Black Basta

Black Bastaは2022年4月に初めて確認されたランサムウェアで、Contiランサムウェア グループの後継にあたります。Black Bastaのアフィリエイトは、企業ネットワークへのアクセスを得るためにさまざまな方法を採用しています。Black Bastaの主要なイニシャル アクセス ブローカーは、ダック ハント作戦(2023年8月)以前はQakbotでしたが、前述したように、Qakbot解体後の穴を埋めるためにPikabotが介入しました。しかし、Pikabotは2024年5月の「エンドゲーム作戦」を受けて解体されています。

ThreatLabzはそれ以降、TTPを大幅に変更したQakbotグループの新たな活動を追跡してきました。現在、Black Bastaはスパム メールを使用してシステムをQakbotに感染させる代わりに、ソーシャル エンジニアリング技術を組み合わせて使用しています。この脅威グループはスパム メールを何百万ものアドレスではなく、攻撃対象を入念に選定して、少数の企業に送信することから攻撃を始めます。その後、自社のIT部門をかたり従業員に電話をかけます。電話の発信者はその従業員に対し、MicrosoftのQuick Assistなどのリモート デスクトップ ソフトウェアを使用して画面共有セッションに参加し、「会社のスパム フィルターを更新する」よう指示します。従業員が脅威アクターにアクセス権を与えると、Windowsバッチ スクリプトが実行され、偵察、認証情報の窃取、被害者のシステムへのバックドアのインストールが行われます。使用されるバックドアは変わるものの、これまではQakbot、Cobalt Strike、SOCKSプロキシ ツールなどが仕掛けられています。バッチ スクリプトには、図20に示すようなコマンドライン インターフェイスが含まれています。

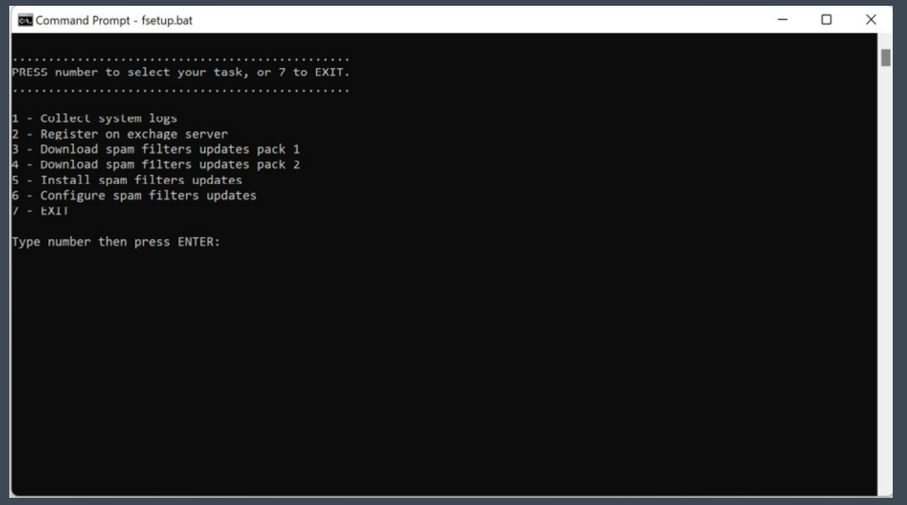


図20: Black Bastaランサムウェア攻撃の足掛かりとして、被害者のシステムにバックドアをインストールするために使用される悪意のあるWindowsバッチ スクリプト インターフェイス

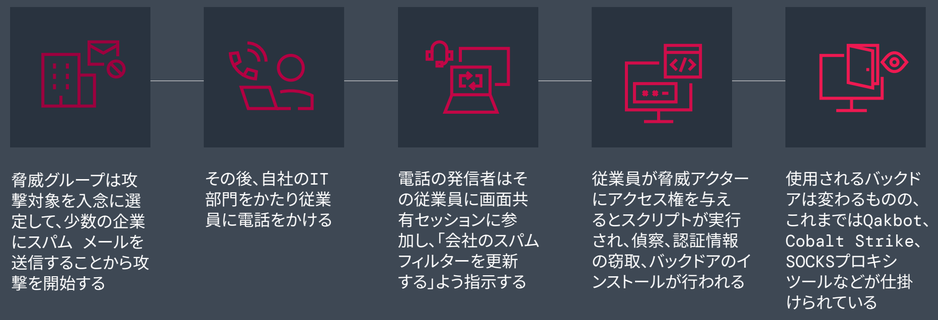


図21: Qakbotグループによって仲介されたイニシャル アクセスによるBlack Bastaランサムウェアの攻撃チェーン

このバックドアへのアクセスが確立されると、Qakbot脅威グループはラテラル ムーブメントとBlack Bastaランサムウェアの最終展開を担当するペネトレーション テスト チームにアクセスを渡します。

ダック ハント作戦は短期的には大きな影響を与えたものの、脅威グループは依然として活動を続けており、継続的に新しい手口を編み出し、実験しています。Qakbot脅威グループは今後1年間、Black Bastaなどのランサムウェア攻撃の主要なイニシャル アクセス ブローカーとして引き続き活動すると思われます。

ThreatLabzによる ランサムウェア メモ のアーカイブ

Zscaler ThreatLabzは、GitHubの公開リポジトリーを保持しています。同リポジトリーでは、本レポート執筆時点で391のランサムウェア ファミリーが追跡され、合計945件の身代金メモが含まれています。2023年4月から2024年4月の間には、19のファミリーと55件の身代金メモが追加されました。このアーカイブはデータリーク サイトや交渉戦術など、ランサムウェア グループの経時的な追跡や、文体測定で明らかになったリブランドしたランサムウェア グループの関連付けに役立ちます。

図22は、Conti (上)とBlack Basta (下)の身代金を要求するチャットの文体測定による比較を示しています。文の構造、言葉の使い方、さらには指示の内容が似ていることから、Black Bastaのメンバーはほぼ確実にContiの元メンバーであることがわかります。

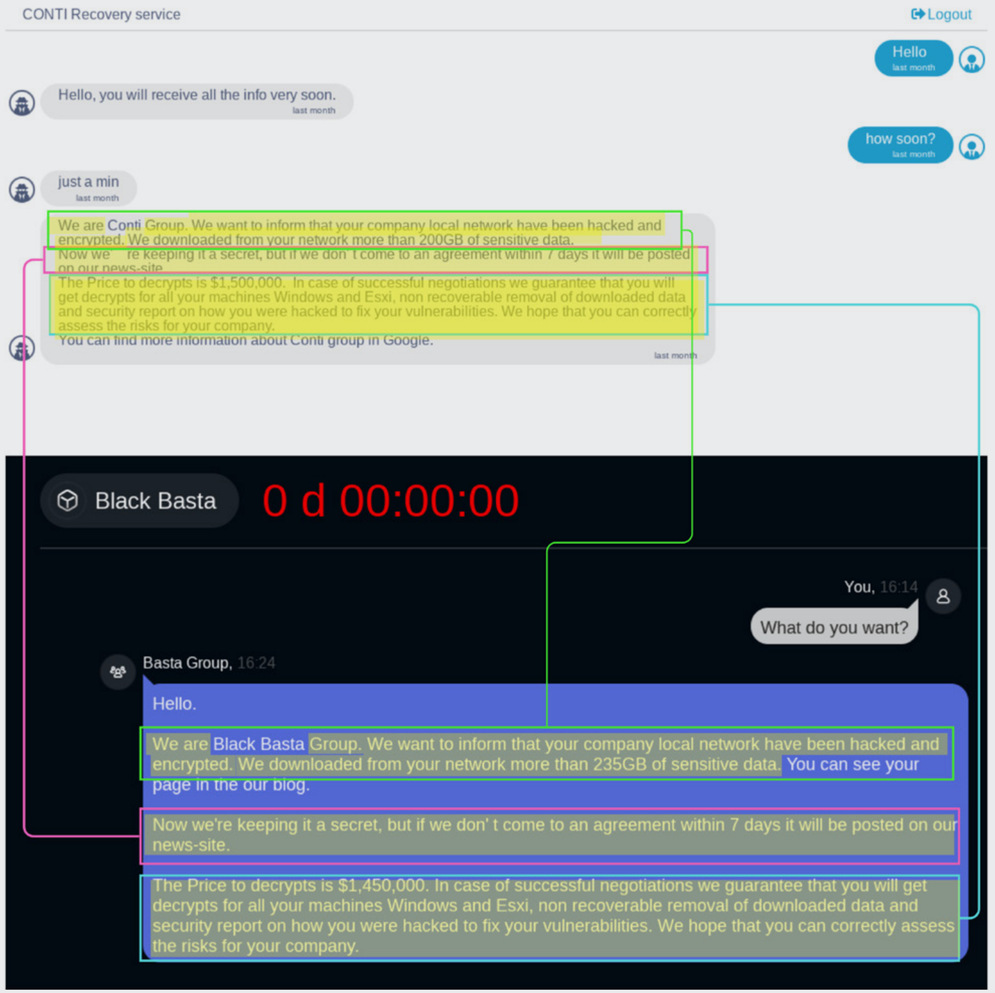


図22: 文体測定によるConti (上)とBlack Basta (下)の身代金を要求するチャットの比較

2025年の予測

1．ランサムウェアの脅威アクターは入念に標的を選ぶ攻撃戦略を採用します。

Dark Angelsは過去1年間、最も成功を収めた、有名ではないランサムウェアグループの一つです。数十億ドル規模の少数の組織を標的にして多額の身代金を要求するという独自の戦略を採用しています。この戦略には、法執行機関やセキュリティ業界からの監視を軽減する、そして、盗み出した膨大な量のデータを守るために、より多くのリソースを投入して多額の身代金を支払う用意のある大企業に侵入するという2つの目的があります。こうして、Dark Angelsは7,500万ドルという過去最高の身代金を受け取ることに成功しました。2025年には他のランサムウェアの脅威アクターが関心を持ち、このグループの成功を再現しようとする可能性が高いでしょう。

2．音声ベースのソーシャル エンジニアリングを使用した標的型攻撃が増加します。

2025年には、専門のイニシャル アクセス ブローカーによる標的型攻撃が増加すると予想されます。QakbotやScattered Spiderの活動例にみられるこの種のブローカーは、高度な技術を使用して侵入口を確保します。特に、音声ベースのソーシャル エンジニアリング攻撃(ビッシング)を利用して個人を欺き、企業環境へのアクセス許可を得ます。そして、そのアクセスによって最終的にデータを窃取し、ランサムウェアを展開するのです。この新たな傾向は、サイバー犯罪エコシステム内の連携が強化されている実態を浮き彫りにしています。このような進化し続ける脅威に対抗するためにも、警戒を怠らず、喫緊の課題として高度なセキュリティ対策に取り組むことが重要です。

3. 攻撃対象に合わせてローカライズされたより効果的なランサムウェア キャンペーンを展開するために、生成AIを採用する攻撃者が増加します。

脅威アクターは2025年以降も生成AIを悪用し、正確な文法と表記でスパム メールを作成したり、音声クローンを使用してスタッフになりすましたりして、特権アクセスを入手すると考えられます。AIが生成した音声は、今後数年間でその地域のアクセントや方言に合わせて調整できるようになるため、信憑性が高まり、成功につながりやすくなります。そのため、より説得力があり、検出されにくい攻撃を仕掛ける手法として広まっていくでしょう。

4. SECの新しい規則に沿って、より多くのサイバーセキュリティ インシデントが報告されるようになります。

SECの規則により、サイバーセキュリティ インシデントの報告がより厳格化されたことから、2025年にはランサムウェア インシデントを公表する組織が引き続き増加すると予想されます。これにより、透明性が向上し、説明責任と予防的な防御が促進され、サイバーセキュリティの手法が改善されることが期待されます。

5．大量のデータを持ち出すランサムウェア攻撃が増加します。

今後1年間で、暗号化しない攻撃も含め、大量のデータを持ち出す攻撃が大幅に増加するとみられています。この傾向は2022年に勢いを増し始めたもので、多くの脅威アクターはシステムを暗号化せずにデータを持ち出すことだけに焦点を当てています。このアプローチを採用すれば、これまで以上に迅速かつ日和見的な運用が可能になり、機密データが公開される恐怖心を利用して被害者に身代金の支払いを強要できます。これは、脅威アクターがより効率的で影響力の大きい手法にくら替えしていることを明確に示しています。

6．医療業界は特に今後もランサムウェア　グループによる執拗な標的型攻撃を受けます。

医療データの価値の高さは、2025年も引き続き注目を集めると予測されます。多くの医療組織では、従来のシステムから最新の高度なセキュリティ対策への移行が遅れており、特に脆弱になっているため、侵害や脅迫が繰り返される可能性があります。適切な対策を講じてゼロトラスト防御戦略を優先しない限り、ランサムウェア グループの標的になるリスクは今後も深刻さを増すでしょう。

7．サイバー犯罪組織に対峙するために、既存の取り組みを基盤とした国際協力が発展します。

法執行機関と民間組織は、主要なイニシャル アクセス ブローカーやランサムウェア グループの阻止など、ランサムウェア攻撃に対抗するための取り組みにおいて引き続き協力していきます。世界的な相互接続が増し、サイバー犯罪者が国境を越えて活動する傾向が強まるにつれて、国際的な協力がますます重要になります。このような協調行動において情報と専門知識を共有することで、世界のランサムウェア ネットワークをさらに効果的に解体できると期待されます。Zscaler ThreatLabzは過去1年間、こうした活動に対して最前線で技術支援を提供してきました。

Zscalerが提供する シンプルなランサムウェア対策

ランサムウェア攻撃の複雑さとコストがますます増えていくなか、ゼロトラストで組織を包括的に保護する必要があることはいうまでもありません。**Zscaler Zero Trust Exchange™**プラットフォームは、この課題を簡素化し、ランサムウェアを阻止するための総合的なアプローチを提供します。

Zero Trust Exchangeにより、攻撃のあらゆる段階でよりスマートな防御を展開できるようになります。Zscalerは最初にユーザーやアプリを見えなくし、許可されたユーザーやデバイスのみにアクセスを許可することで、攻撃者がこれらのエンティティーを検知したり、悪用したりするのを防ぎます。また、暗号化の有無に関わらず、インバウンドとアウトバウンドのすべてのトラフィックをインラインで検査します。認証されたユーザーやデバイスは、ネットワークではなく、必要なアプリケーションに直接接続されるため、攻撃者が侵入できたとしても、ネットワークを水平に移動してデータを盗んだり暗号化したりすることはできません。

ランサムウェア対策にゼロトラストが不可欠な理由
旧式のセキュリティ アーキテクチャーでは、ランサムウェア攻撃を阻止できません。

従来型からの脱却：通常、「次世代ファイアウォール」や「VPN」などの従来のセキュリティ対策やポイント ソリューションでは、死角や複雑さが生まれ、コストも膨大になります。これらのアプローチは暗号化されたファイルやトラフィックをコスト効率よく検査できず、可視性と制御のギャップを悪用するラテラル ムーブメントやランサムウェア攻撃に対して脆弱になるため、壊滅的な結果を招く恐れがあります。

ゼロトラストの採用：ゼロトラスト アーキテクチャーでは、どのユーザー、デバイス、接続も侵害される可能性があるとみなされるため、継続的な検証と厳格なアクセス制御が行われます。ゼロトラストはアイデンティティーを一貫して検証し、暗号化されたデータを含むすべての情報を検査することで、ネットワーク内で攻撃が広がるリスクを大幅に軽減し、被害が生じる前にランサムウェアの脅威を無力化します。

攻撃サイクルのあらゆる段階でランサムウェアを阻止——Zscalerは、最初の偵察や侵入からラテラルムーブメント、データ窃取、ペイロードの実行に至るまで、すべての段階で対処します。

攻撃対象領域の最小化：ゼロトラスト アーキテクチャーに基づいて構築されたZero Trust Exchangeは、VPNとファイアウォールのアーキテクチャーをリプレースします。こうした旧式のアーキテクチャーは悪用されやすいだけでなく、攻撃対象領域も拡大させます。Zscalerはユーザー、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し、インターネットから見えなくして検出されないようにすることで、攻撃対象領域を効果的に最小化します。許可された相手に通話を振り分ける交換機と同様に、許可された適切なユーザーやデバイスだけを特定のアプリケーションに接続させます。

初期侵入の防止：Zero Trust Exchangeは、広範なTLS/SSLインスペクション、ブラウザー分離、高度なインライン サンドボックス、ポリシー活用型のアクセス制御を備えています。これらの機能は、悪意のあるWebサイトへのアクセスを防止し、未知の脅威がネットワークに到達する前に検出するため、侵入自体のリスクが最小限に抑えられます。

ラテラル ムーブメントの排除：ユーザーとアプリ間またはアプリ間のセグメンテーションを活用し、ユーザーはネットワークではなくアプリケーションに(アプリは他のアプリに)直接接続されるため、ラテラル ムーブメントのリスクが解消されます。Zscalerはアクセス制御ポリシーを一元的に管理することで、インターネット トラフィックのセキュリティ チェックポイントのように機能し、ラテラル ムーブメントの経路を排除します。また、アイデンティティー脅威の検知と対応(ITDR)機能とデセプション機能により、外部の脅威や悪意のある内部関係者を問わず、潜在的な攻撃者のラテラル ムーブメントを特定して阻止することもできます。

データ流出の阻止：インライン情報漏洩防止策とフルTLS/SSLインスペクションを組み合わせて、データ窃取を効果的に阻止します。Zscalerは、転送中データと保存データの両方を確実に保護します。

AIを悪用する脅威には
AIとゼロトラスト イノベーションで対抗

AIを活用した以下の5つの機能により、Zscalerはランサムウェアに対する強力な保護を提供し、脅威が急速に拡大するなかでも包括的なセキュリティを確保します。

- ***AI*活用型のフィッシングと*C2*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 サイトやコマンド&コントロール(C2)インフラを特定してブロックします。
- ***AI*活用型のサンドボックス：**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。
- ***AI*活用型のセグメンテーション：**自動で推奨されるアクセス ポリシーにより、攻撃対象領域の最小化だけでなく、ユーザーのコンテキスト、振る舞い、場所、プライベートアプリのテレメトリーを使用したラテラル ムーブメントの阻止が可能になります。
- **動的なリスクベースのポリシー：**ユーザー、デバイス、アプリケーションに関連するリスクを継続的に分析し、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。
- ***AI*を活用したブラウザー分離：**ページを完全な画像のストリームとしてレンダリングすることで、ユーザーと悪意のあるWebコンテンツとの間に安全な緩衝ギャップを作成し、データの漏洩と活動中の脅威による配信を阻止します。
- ***AI*活用型のデータ検出と分類：**設定を必要とせずに、エンドポイント、インライン、クラウドのデータを瞬時に可視化して分類するため、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。

攻撃チェーンの各段階での包括的な保護

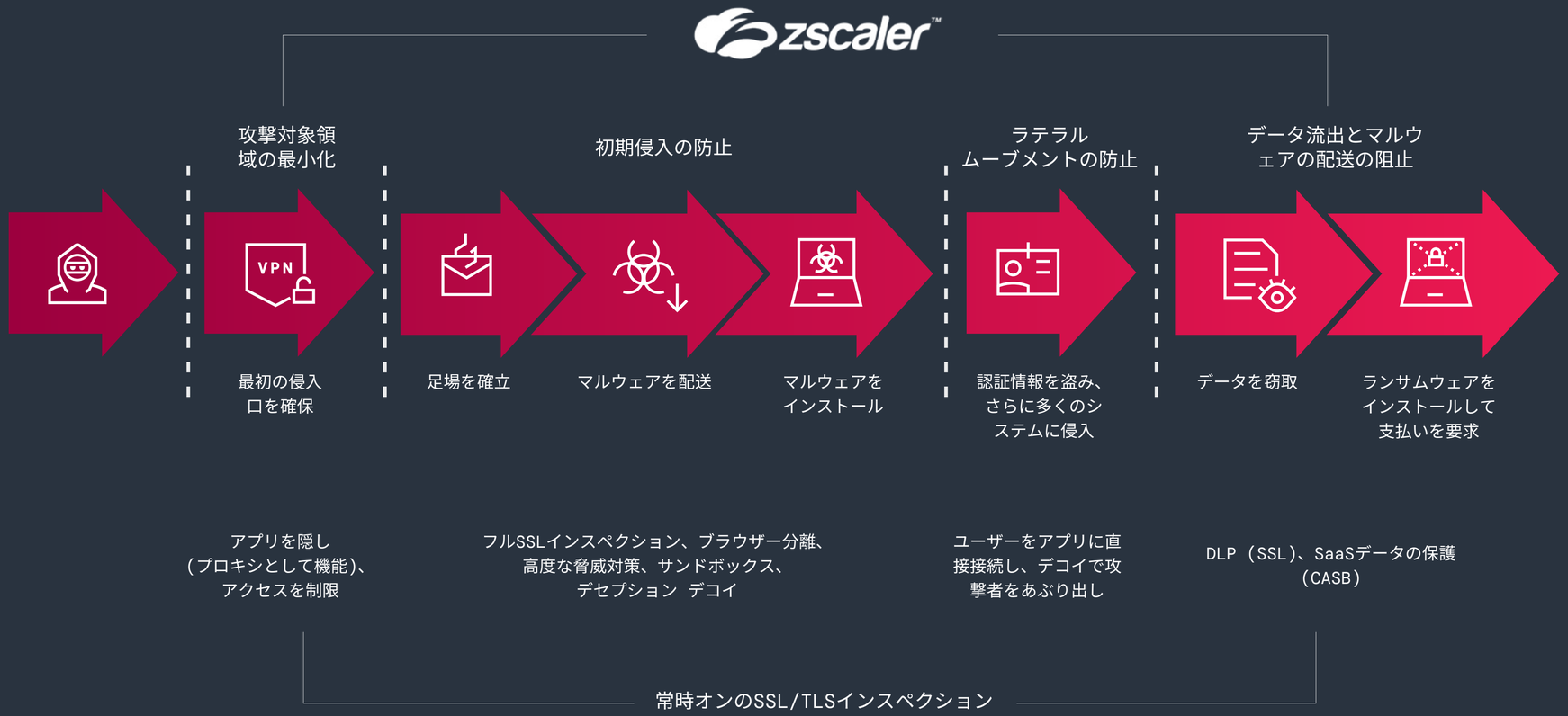


図23: ランサムウェア攻撃チェーン全体で機能するゼロトラスト アーキテクチャー

Zscalerの関連製品

Zscaler Internet Access™ (ZIA™)は、インラインの脅威対策を行い、インターネットへの安全な直接アクセスを提供します。ZIAの高度な脅威対策とサンドボックスの機能により、ランサムウェアのダウンロードとコマンド&コントロール(C2)通信が阻止され、ランサムウェアの侵入が防止されます。

Zscaler Private Access™ (ZPA™)は、ゼロトラスト モデルを採用し、インターネットに公開することなく内部アプリケーションへの安全なアクセスを可能にします。ZPAは、許可されたユーザーとデバイスのみが重要なアプリケーションにアクセスできるようにすることで、攻撃対象領域を減らし、ランサムウェア攻撃の試みを防ぎます。

Zscaler Zero Trust Firewallは、TLS/SSLトラフィックを傍受して検査することで、暗号化されたトラフィックに隠されたマルウェアを検出し、ネットワークへの侵入を防ぎます。

Zscaler Deceptionは、ラテラル ムーブメントや権限昇格を試みる攻撃者をデコイのサーバー、アプリケーション、ディレクトリー、ユーザー アカウントでおびき寄せ、それらを検知して封じ込めます。

Zscaler Sandboxは、制御された仮想環境で疑わしいファイルや実行可能ファイルを分析し、悪意のあるコードを特定してブロックします。これにより、組織はファイルベースのランサムウェアやゼロデイ攻撃に対して先手を打つことができます。

Zscaler Cloud Browserは、Webセッションを分離し、ピクセル データのみをデバイスにストリーミングして、ランサムウェアの実行者によって使用される可能性のあるドライブバイ ダウンロードやゼロデイ脅威のリスクを効果的に排除します。

Zscaler ITDR (アイデンティティー脅威の検知と対応)は、認証情報の窃取や権限の悪用、Active Directoryへの攻撃、リスクの高い権限付与などのアイデンティティーベースの攻撃を検知し、防御します。

Zscaler Data Protectionは、SaaSやパブリック クラウド アプリケーション全体にわたり、転送中データおよび保存データに統一されたセキュリティを提供することで、ランサムウェア攻撃による潜在的な被害だけでなく、データが持ち出されるリスクも低減させます。

ランサムウェア対策ガイダンス

ゼロトラスト アーキテクチャーを基盤とした防御戦略はランサムウェアの阻止に有効であることが実証されているセキュリティ対策ですが、この多面的な脅威に対抗するには予防的な計画、継続的なコラボレーション、戦略的投資が必要です。

ThreatLabzの専門家は、ランサムウェアのリスクを軽減し、既存の脅威と新たな脅威から組織を保護するための最新のベスト プラクティスをまとめました。

- **データの安全なバックアップを定期的に実施する。**オフラインのバックアップを含め、すべてのデータが定期的かつ安全にバックアップされていることを確認します。進化する脅威に合わせてバックアップ戦略を適応させることが重要です。
- **ソフトウェアを最新の状態に保つ。**既知の脆弱性に対処するために、最新のセキュリティ パッチを速やかに適用します。AIドリブンの脅威インテリジェンス プラットフォームを使用すると、セキュリティ パッチの優先順位を決定し、効果的に管理できます。
- **多要素認証(MFA)を有効にする。**MFAを使用してユーザー アカウントにセキュリティ レイヤーを追加し、不正アクセスのリスクを軽減します。MFAソリューションを統合すると、アカウントの乗っ取りを効果的に検出し、防止できます。
- **一貫したセキュリティ ポリシーを確立する。**すべてのユーザーがMFAや定期的なセキュリティ アップデートなどの一貫したセキュリティ手順に従うようにして、初期侵入を防止します。従業員が分散している場合は、セキュリティ サービス エッジ(SSE)アーキテクチャーを実装し、ユーザーがどこにいても保護することがさらに重要になります。
- **アプリケーションのセキュリティを強化する。**ランサムウェアの脅威アクターが脆弱性を悪用できないように、アプリケーションをパブリック インターネットから取り除きます。ランサムウェア攻撃から社内アプリケーションを保護するために、ゼロトラスト アーキテクチャーを実装します。
- **最小特権アクセスを施行する。**最小特権ポリシーを実装し、ユーザーのアクセスを必要なリソースのみに制限します。AIを活用したソリューションでユーザーの振る舞いを動的に分析し、それに応じてアクセス権限を調整します。
- **アイデンティティー保護を強化する。**ITDRツールを使用すると、アイデンティティーの設定ミスの可視化、権限昇格とラテラル ムーブメントに悪用されるActive Directoryの脆弱性の修復、ステルス性の高いアイデンティティーの脅威の検出が可能になります。
- **すべてのトラフィックを検査する。**現在、脅威の86%が暗号化されたチャネルを介して配信されていますが、これらのチャネルは検査されないことが多いため、高度な技術を持たない攻撃者でもセキュリティ制御を簡単に回避できます。侵入を防ぐには、暗号化されているかどうかに関係なく、すべてのトラフィックを検査する必要があります。
- **ゼロトラスト ネットワーク アクセス(ZTNA)を実装する。**ユーザーとアプリ間およびアプリ間のきめ細かなセグメンテーションを展開することで、最小特権アクセス制御を介したアクセスの仲介が可能になります、これにより、ラテラル ムーブメントの排除、データ漏洩のリスクの最小化、セキュリティ態勢全体の強化が可能になります。

- **AI活用型のブラウザー分離を活用する。**疑わしいインターネット コンテンツやリスクの高いユーザーをAIで隔離し、Webの脅威からユーザーを保護します。ブラウザー エクスペリエンスを分離し、有害となりうるアクション(認証情報の入力など)を制限することで、システムのセキュリティを危険にさらすことなく、リスクの高いURLやファイルに安全にアクセスできます。

- **AI活用型の高度なサンドボックスを採用する。**AI/ML分析を活用して未知の脅威や不審なファイルを自動的に検出および隔離するサンドボックスで、検出されにくい未知のマルウェアを阻止します。

- **インラインの情報漏洩防止(DLP)を展開する。**インラインのDLP対策を展開することで、データの持ち出しと漏洩を防ぎます。

- **デセプション テクノロジーを活用する。**デセプション ツールとハニーポットで攻撃者をあぶり出し、システムへの侵入に対する防御を強化します。

- **クラウド アクセス セキュリティ ブローカー(CASB)を活用する。**CASBでクラウド アプリケーションの使用状況を制御およびモニタリングし、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防止します。

- **従業員向けのトレーニングを継続的に実施する。**定期的なセキュリティ意識向上トレーニングを実施し、ランサムウェアの脅威について従業員を教育します。実際の攻撃シナリオに基づいてシミュレーションを行い、従業員の備えを強化します。

- **包括的なランサムウェア対応計画を策定する。**ランサムウェア攻撃が発生した場合に迅速かつ効果的に行動できるように、データ復旧、インシデント対応、通信プロトコルを含む対応計画を策定します。

*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リポジトリーも管理しています。

X @ThreatLabz | ThreatLabzのセキュリティ リサーチ ブログ

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。調査チームは、2023年4月から2024年3月にかけて以下のソースから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。

- **外部のインテリジェンス ソース。**ランサムウェアの攻撃者、攻撃対象、手法に関する追加情報を提供する脅威インテリジェンス フィード、オープン ソース調査、法執行機関のレポートなどの外部インテリジェンス ソースからデータを収集しました。

- **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の脅威インテリジェンス チームは、リバース エンジニアリングとマルウェア分析の自動化を通じて、ランサムウェア ファミリーを大規模に追跡し、効果的な対応戦略を開発しています。ThreatLabzは国際法執行機関とも緊密に連携しており、ダック ハント作戦やエンドゲーム作戦などの最近の活動で重要な役割を果たしています。

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.jp**)で公開しています。

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150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、**www.zscaler.jp**をご覧ください。