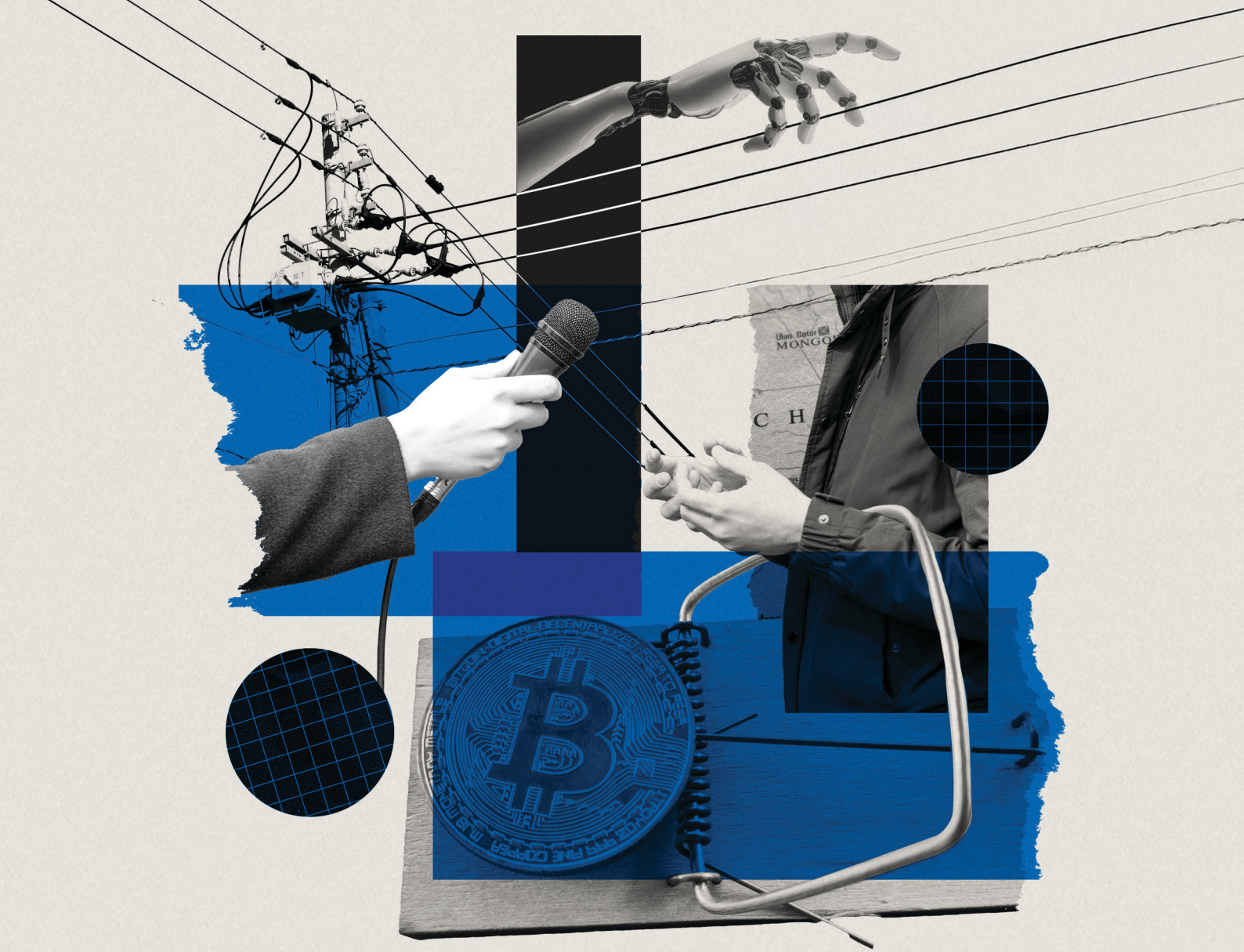
CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

January 28, 2025



2024年次レポート

2024年の最も重要な攻撃により、SaaSアプリケーションの急増により、盗難された認証情報の影響がいかに増幅するかが明らかになりました。MFAの欠如やその他の設定ミスが、脅威アクターが機密データにアクセスする原因となりました。

法執行機関の行動をきっかけに、犯罪集団が急増しました。ランサムウェア攻撃の数は昨年と同程度でしたが、ファミリーと亜種の数は増加しています。

生成AIは、国家が影響力工作を拡大するのに役立ちました。70か国以上で重要な選挙が行われる、敵対的な影響力工作は生成AIツールを使って偽のコンテンツを増幅させました。

序文

Recorded Futureの年次脅威レポートでは、脅威アクターの主要なTTP（戦術、手法、手順）と、過去1年間の動機について詳説し、来年予想されるTTPを導出します。この情報を使用することで、脅威をより適切に検出し、サイバーリスクを管理できます。

攻撃者の**2024**年のプレイブックから学び、セキュリティ体制を強化。

本レポートでは、企業のアタックサーフェス（攻撃対象領域）が拡大し続け、注目度の高い法執行機関の行動にもかかわらずサイバー犯罪活動が継続し、国家支援型の脅威アクターが重要なインフラストラクチャと選挙を狙った、2024年の業界で最も包括的なインテリジェンス分析を示しています。

主要な脅威アクターとその標的、使用されたTTPに関連する詳細を以下で確認し、システムのセキュリティ制御のギャップを特定して対処できるようにしましょう。以下について解説しています。

- 脅威アクターが特にChange Healthcareに対するALPHVおよびRansomHubランサムウェア攻撃や、Snowflakeに対するUNC5537の攻撃において、SaaS（Software-as-a-Service）のセットアップと有効な認証情報を悪用した方法。
- 法執行機関の対応がLockBITやALPHVなどの主要なRaaS（Ransomware-as-a-Service）グループに混乱を招き、ランサムウェアの活動が前年比で一貫しているという事実にもかかわらず、新たなランサムウェアグループの数が増加した事実。
- 世界中で20億人以上の有権者が投票に向かう中、中国、ロシア、イランがAI生成コンテンツを使用して、悪意ある影響力工作の一環として世論形成を試みた方法。

2025年以降のロードマップで将来の攻撃を阻止。

メモリセーフコーディング、仮想通貨詐欺、サードパーティのリスク管理などに関する予測を確認し、この情報を使用して、データ、ブランドの評判や収益を保護するのに役立つ脅威インテリジェンス戦略を策定します。当社の予測には以下が含まれます。

- 開発者はAIを使用してより安全なコードへの移行を加速。
- 仮想通貨詐欺が市場を不安定にする事象の原因に。
- 生成AIのエンタープライズワークフローへの実装や効果的なかなりすましのためのAI悪用に起因する大規模な侵害発生の可能性。
- 中国の事前配置（Pre-positioning）活動を報告する企業が増え、中国が幅広い重要産業で破壊的な作戦を実施する能力を実証。

Recorded FutureのInsikt Groupを代表して、本レポートが攻撃者の一歩先を行き、2025年にビジネスの混乱を回避する上で役立つことを願っています。

Levi Gundert
Chief Security & Intelligence Officer

エグゼクティブサマリー

2024年のサイバーセキュリティの状況は、法執行機関による中断措置の増加と企業のアタックサーフェス（攻撃対象領域）の複雑化に直面した犯罪ネットワークのレジリエンスという2つの並行したトレンドを形作りました。サイバー犯罪市場は、犯罪者が再編を通じて法執行機関の執拗な取り締まりに耐えられるように適応し、回復力を示した一方で、より重要なビジネスプロセスがサードパーティのクラウドベースのアプリケーションに移行する中でエンタープライズネットワークがあまりに複雑化しています。

2024年を通じて、LockBitなどのランサムウェアの運用、サービス拒否オペレーター、MaaS(Malware-as-a-Service)プロバイダーを対象に複数の法執行機関による措置が取られ、中断が発生しました。法執行機関による押収などの措置の直後にランサムウェアの被害者は一時的に減少しましたが、攻撃の全体的な報告件数は大幅に減少してはいません。この適応性は、サービスベースの犯罪エコシステムにより、脅威アクターが運用の継続性を維持しながらプロバイダー間を迅速に移動できることを示しています。さらに、サイバー犯罪を推進する基本的な市場力学は依然として堅調で、これが犯罪者が挫折をものともせず適応するための動機となっています。

一方、平均的な企業では現在、371種類のSaaS（Software-as-a-Service）製品を採用しており、これがアタックサーフェス（攻撃対象領域）の拡大につながり、効果的な防御がますます困難になっています。SaaS製品や環境の認証情報の侵害は、Change HealthcareとSnowflakeに影響を与えたインシデントからも明らかなように、重大な侵害につながっています。Ivanti社製品やConfluenceなど、広く利用されているエンタープライズ製品に重大な脆弱性が存在することも、広範なセキュリティ侵害を引き起こしています。

同時に、国家支援型の脅威アクターとその代理人であるハクティビスト（主に中国とロシアと関連）は、地政学的な目的を推進するために、水道施設などの重要なインフラネットワークに対して破壊的な攻撃を仕掛けました。サイバー攻撃に加えて、中国、ロシア、イランは生成AIを使用して情報操作を行い、偽の政治コンテンツを世界中に広めました。また、これらの脅威アクターは、産業技術と情報エコシステムの両方で複雑さが増していることを利用して、これらの活動への政府の関与の証拠隠蔽を試みています。

サイバー犯罪業界が堅調であり、第三者による検討事項が多岐にわたり、国家支援型の脅威アクターの力がますます強まる中、組織は従来の境界ベースの防御を超えて、より堅牢でスケーラブルな自動化されたセキュリティアーキテクチャを採用する必要があります。これらのセキュリティソリューションは、企業の運用環境の複雑さと、ますます高度化する脅威アクターツールセットの急増に対応する必要があります。とはいえ、2024年のSnowflakeのような大規模な侵害を踏まえると、組織はまず、新しく複雑なセキュリティツールよりも、MFA（多要素認証）のような単純で効果的なソリューションを優先する必要があります。

主な調査結果

- **SaaS**アプリケーション採用の拡大に伴い、**ID**エクスプロイトがより効果的になりました。
  2024年に発生した最も重要な攻撃からは、企業環境でのSaaSアプリケーションの急増が、インフォスティーラー（情報窃取型）マルウェアによって窃取された認証情報の影響をどう増幅させたかが見て取れます。
- 法執行活動の強化にもかかわらず、犯罪集団が急増しました。
  法執行機関は、LockBitを含む主要なRaaS運営者の阻止に成功しました。しかし、2024年後半には、犯罪者が公開されたソースコードとビルダーを使用して独立した活動を開始したため、ランサムウェアファミリーと亜種が急増しました。
- 混乱とデータにより、サイバー犯罪は割に合うものとなりました。
  製造業とヘルスケアは、2024年もランサムウェアや恐喝の運営者が最も狙う業界であり続け、サイバー犯罪者が業務の中断をかたに脅迫することから継続的に利益を得ていることを示しています。一方、犯罪フォーラムで販売されているデータベースの数は昨年に比べて20%増加し、通信、医療、教育関連のデータベースの価格が最高となっています。
- 世界的な紛争や衝突の増大が重要インフラの混乱を招きました。
  国家が支援する脅威アクターとその代理人であるハクティビストは、重要なインフラに対する脅しを武器に、地政学的な目標を推進しました。中国と関連する脅威アクターは、重要なネットワークに事前配置を行っていることが確認され、ロシアとイランが支援するハクティビストは、可視性を最大化するために水道施設を標的にしていました。
- 国家支援を受けた脅威アクターは生成**AI**を活用して影響力工作をレベルアップしました。
  70か国以上で重要な選挙が行われた今年、中国、ロシア、イランは影響力工作として、生成AIツールを使ってコンテンツの制作とリーチを拡大しました。3か国とも生成AI研究への投資を続けています。
- **TTP**（戦術、技術、手順）では、防御回避が重視されています。
  かつては国家資金が背後にある高度な脅威アクターに限定されていた戦術が、犯罪活動ではますます一般化しています。正規のツールを使用して検出を回避したり、GoおよびRust言語でマルウェアを開発したりすることが確認されています。

目次

SaaSの採用拡大が引き起こすIDの悪用

2024年には、相互接続されたSaaS（Software-as-a-Service）アプリケーションの採用増加に伴い、サイバー脅威アクターにとっての侵害された認証情報の有用性が増し、SSO（シングルサインオン）やMFA（多要素認証）ポリシーのギャップや設定ミスを悪用して企業のエコシステムにアクセスするようになりました。

SaaSアプリケーションが窃取された認証情報悪用の新たな機会を提供

平均的な企業は約371種類のSaaS（Software-as-a-Service）アプリケーションを使用しており、これは2021年（266種類）から39.4％増加し、2025年を通じてさらに増加すると予想されています。これらのアプリケーションには、通常、それぞれ独自のブラウザベースのログインポータルが付属しており、エンタープライズSSO（シングルサインオン）ソリューションに統合できます。ただし、ユーザーが承認されたIAM（IDアクセス管理）環境外のアプリケーションにアクセスする場合、その統合は必ずしもシームレスとは限りません。この急速に拡大するID攻撃対象領域は、ほぼ確実に、脅威アクターが盗難または公開された認証情報を悪用する機会を増やしており、ウェブアプリケーション攻撃の77％で使用されています。犯罪者は、SaaSへの依存度の高まりと公開された認証情報の組み合わせを利用して、2024年に最も注目された2つの攻撃、（Change HealthcareとSnowflakeの侵害）を実行しました。

Change Healthcareに影響を与えたALPHVおよびRansomHubランサムウェア攻撃には、他のリソースにピボットする前にデスクトップへのリモートアクセスを可能にするCitrixアプリケーションにアクセスするための有効な認証情報の使用が含まれていました。Change Healthcareのネットワークへのリモートアクセスの SSOインターフェイスとして機能していたCitrix Gatewayは、多要素認証が有効になっていなかったため、非常に一般的なIDの脅威（認証情報の悪用）が、非常に一般的なIDおよびアクセス管理手段（SSO）を利用できるという形で要因の最悪の合流点が発生しました。アクセスが確立されると、脅威アクターはネットワーク内を横方向に移動し、患者データを収集して流出させ、ランサムウェアのペイロードを展開しました。Change HealthcareはALPHVに最初の2,200万ドルの身代金を支払い、その後、再度の恐喝に続いてRansomHubの関連会社に追加の身代金を支払ったいう証拠がありますが、確認はされていません。

Snowflakeの複数のクラウドストレージアカウントが同時に侵害されたことで、数百の組織の認証情報が窃取されました。金銭的な動機を持つこの脅威アクターUNC5537は、情報窃取型マルウェア感染によって窃盗した認証情報を使用して、複数の企業のSnowflakeインスタンスからデータを侵害しました。Change HealthcareのCitrixポータルと同様に、UNC5537はMFAで保護されていない環境にアクセスできるようになりました。アクセス権を取得すると、UNC5537は単純なSQLクエリを使用して偵察を行い、関心のあるデータを特定し、Snowflake環境からデータを流出させました。その後、被害組織に個別の恐喝メッセージを送信し、既知のアンダーグラウンドおよびダークウェブフォーラムでそのデータを販売しました。これらの攻撃を同時に実行することで、UNC5537は当初、侵害の発生源をめぐる混乱を引き起こし、初期の報告では、Snowflakeプラットフォーム自体が侵害されたと考えられていました。

情報窃取型マルウェア感染が個人デバイスを狙う傾向を強め、感染1件当たり認証情報を取得数を増やし、SaaSエコシステムへのリスクが増大

ChangeとSnowflakeのデータ侵害の両方で、初期の有効な認証情報は情報窃取型マルウェア感染を通じて取得されました。Recorded Futureは、2024年の情報窃取型マルウェア感染の大半が個人または中小企業の所有するデバイスに影響を与えたことを確認しました。通常、個人用デバイスは、エンタープライズデバイスと同じ

監視、使用制限やセキュリティリソースの対象外であるため、情報窃取型マルウェアを阻止できない可能性が高くなります。さらに、Snowflakeの侵害で使用された認証情報の一部が2020年に盗難されていたことをMandiantが発見したように、認証情報は最初の情報窃取型マルウェア感染後も長期間公開されたままになる可能性があります。

また、2021年以降、デバイス1台当たりの盗難認証情報の数は着実に増加していますが、これはおそらく、ユーザーが企業環境と個人のデバイスの両方で日常的にログインするアプリケーションの数が増えていることが原因であると思われます。これにより、これらの認証情報の少なくとも1つが企業リソースへのアクセスを提供する可能性が高くなります。デバイス間でのログイン数の増加は、特にユーザーが企業の一元化されたID管理システムの外部でログインしている場合、セキュリティチームにとって管理が困難になる可能性があります。

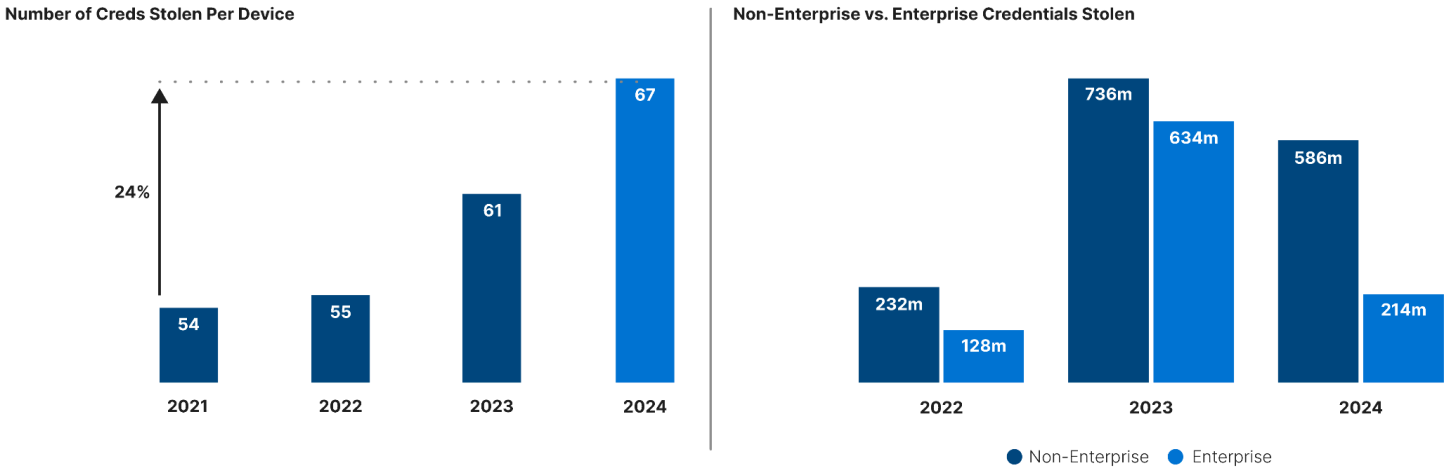


図*1*:個人用デバイスはエンタープライズデバイスよりも頻繁に狙われ、デバイス当たりの盗難認証情報の数は過去3年間で増加(出典:*Recorded Future*)

リモートワークなどに起因するインサイダー脅威リスクの増大

SaaSと仮想化クラウド環境の採用は、オンプレミスとリモートの作業環境を接続する必要性などから推進されてきました。しかし、リモートアクセスにより、脅威アクターは盗まれた認証情報だけでなく、盗まれたID全体を利用して企業の機密リソースにアクセスすることもできるようになりました。2024年12月、FBI(アメリカ連邦捜査局)は、盗難されたIDを使用してリモートワーカーを装い、アメリカ企業に就職した疑いで、14人の北朝鮮国民を起訴しました。これらの労働者の1人を知らずに採用したあるサイバーセキュリティ企業は、この新入社員が「盗難された有効なアメリカを拠点するID」を使用していたと報告しています。これによりこの社員は、身元調査、4回のオンライン面接、その他の採用前の審査をパスすることができました。

今後の見通し:クラウド*ID*を保護するための措置を実施

2025年までに業務の22%が完全なリモートになると予想される中、採用から解雇までのID管理は依然として複雑な取り組みとなる可能性があります。Insikt Groupが昨年指摘したように、ハイブリッド勤務の形態において、事業運営をサポートするためにサードパーティのインフラストラクチャやソフトウェアに依存する企業が増えています。昨年、Insikt Groupは、CVE-2023-34362(MOVEitファイル転送の脆弱性)の悪用によって注目を集めた大規模な脆弱性悪用の脅威を観察しましたが、今年は、組織の複雑さを悪用するために別のアプローチを取っている脅威アクターが注目されました。多要素認証はChangeとSnowflakeの両方の侵害を防ぐのにほぼ確実に役立ったでしょうが、複雑であり、クラウドベースのインフラストラクチャ全体で一貫した構成を行うことは実際には難しいのが現実です。

SaaSアプリケーションに対する脅威の増大に対応して、企業はより成熟した、または標的になりにくいID管理ソリューションへの投資を拡大しています。ある調査によると、2024 年にはパスキーの採用が400%に増加し、現在では100を超える有力アプリケーションがパスキーをサポートしています。これらの投資は成果を上げているようで、83%の企業がIDセキュリティへの投資がID関連のリスク軽減に役立ったと報告しています。しかし、これらのソリューションが効果的に機能するためには適切な構成と一貫したメンテナンスが不可欠であり、攻撃者は保護におけるギャップを悪用する新しい方法を探し続けます。

法執行機関の行動にもかかわらず、恐喝グループが急増

2024年の法執行機関の措置により、LockBitや主要な情報窃取型マルウェア、フィッシングキット、DDoSサービスの運用が一時的に中断されましたが、犯罪者は主要なRaaSアフィリエイト以外の小さなグループに再編成することで適応し、運用上の回復力を示しました。

法執行機関の措置が二大主要組織に混乱

2024年のランサムウェアの状況は、RaaS（Ransomware-as-a-Service）の二大グループであるLockBitの混乱とALPHVの離脱により、2つの大きな変化を遂げました。2024年2月、アメリカ、イギリス、いくつかの欧州諸国の法執行機関は「Cronos」と呼ばれる一斉作戦でLockBitの運営を中断し、同グループのネットワークリソースのいくつかを押収し、関係者2名を逮捕し、暗号通貨アカウントを凍結したと発表しました。2024年10月にも捜査は続けられ、法執行機関はLockBitの運営に対して行われた追加の措置を明らかにしています。これらの措置には、LockBitに関連する5人の追加逮捕と、同グループのインフラストラクチャの一部であった9台のサーバーの押収が含まれていました。一方、ALPHV（別名BlackCat）は、Change Healthcareから2,200万ドルの支払いを受けた直後の2024年3月にアフィリエイトネットワークをオフラインに移行しました。リサーチャーらは、この突然の閉鎖が法執行機関の注目が高まる中での出口詐欺の一部であり、関連会社への支払いを避けるための行動であったと疑っています。
LockBitとALPHVの活動の中断の影響は甚大でした。Recorded Futureのデータによると、Lockbitは2023年のランサムウェア活動全体の23%を占め、前年で特に活発だったグループの1つとなっています。また、ALPHVは昨年、最も活発なランサムウェアグループの上位5位にもランクインしました。

2024年の法執行機関の行動はRaaSだけに焦点を当てていたわけではありません。その他の注目すべき措置には、IcedID、Smokeloader、Pikabot、Bumblebeeなど、少なくとも4つのマルウェアグループを支えるインフラストラクチャをシャットダウンした「Operation Endgame」が含まれます。また、アメリカの法執行機関は、犯罪グループScattered Spiderとハクティビストグループ Anonymous Sudanのメンバーを起訴しました。後者は、直接攻撃を行うだけでなく、DCAT（分散型クラウド攻撃ツール）と呼ばれるDDoS（分散型サービス拒否）ツールへのアクセスの販売も行っていました。

ランサムウェアやMalware-as-a-Serviceのエコシステムに対する法執行機関の措置にもかかわらず、報告された攻撃の全体的な件数は大幅には減少していません。ランサムウェアグループは、再編成とブランドの変更で混乱に適応しました。Recorded Futureのデータによると、LockBitの恐喝ウェブサイトに投稿されたランサムウェアの被害者は昨年から着実に減少し、第1四半期の205件から第4四半期にはわずか4件に減少しています。しかし、LockBitマルウェア種は、2022年にリーク されたLockBit 3.0ランサムウェアビルダーが継続的に使用されているため、さまざまな新興グループによって使用され続けていました。LockBitマルウェアを使用するグループの例としては、ハクティビストの脅威アクターからランサムウェアグループに転身したDragon Forceや、

Recorded Futureが2020年から追跡している小規模なサイバー犯罪者アクターのCosmicBeetleなどがあります。

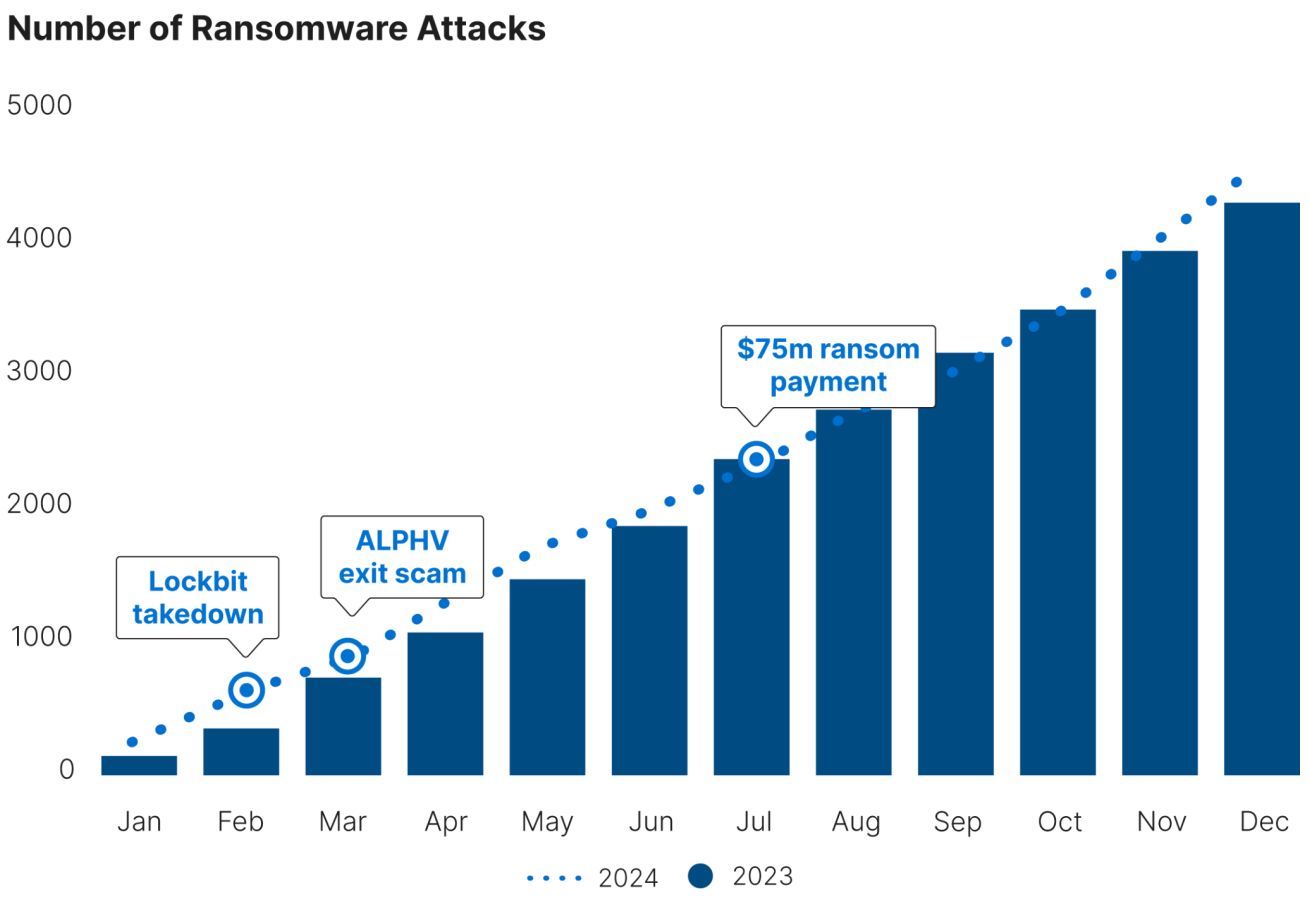


図**2**：*2024*年*8*月には攻撃の速度がわずかに低下するも、*2024*年*9*月から*10*月にかけて攻撃は過去*2*年間のペースに回帰（出典：*Recorded Future*）

さらに、2024年を通じて、新しいグループや恐喝ブログの数が増加しています。2023年、Insikt Groupは32の新しいランサムウェアグループを通年で追跡しました。一方、2024年の6月から8月には14の新しいブログサイトと62の新しい亜種が確認されており、最も多いグループ（RansomHub）の投稿でも恐喝投稿全体の12%に過ぎませんでした。比較して、その前の6か月間では、LockBitだけで恐喝の投稿全体の35%を占めていました。この活動状況は、統合された注目度の高いRaaSモデルから、特定のグループが法執行機関の注意を引きにくくなる、より細分化された犯罪エコシステムへの転換を示しています。新たなランサムウェアの亜種の観測数の増加は、ソースコードの漏洩と、攻撃者の間でビルダーがより広く共有されるようになったことが要因であると考えられます。

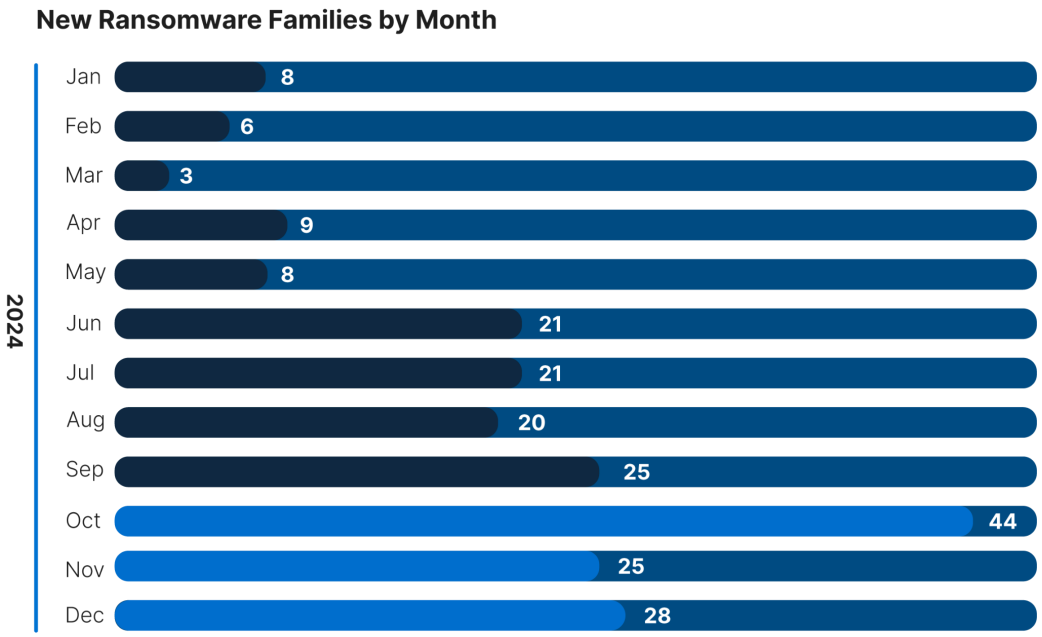


図**3**：*2024*年上半期を通じ、毎月検出される新しいランサムウェアファミリーの数は大幅に増加（出典：*Recorded Future*）

ランサムウェアの活動が依然として確認できるのは、2024年6月までの身代金の累積支払額が4.598億ドルに達し、2024年がランサムウェアの身代金支払額で過去最高の収益を上げる年となる見込みであるなど、ランサムウェアが依然として収益を産む犯罪行為であるためです。Chainalysisは、2024年にランサムウェアグループが知名度の高い組織に対して、非常に高額な身代金の支払いを強要したことをいくつか観測しました。これは「大物狩り」として知られる行為です。例えば、2024年には、あるFortune50企業に対してDark Angelsが約7,500万ドルの支払いを強要し、過去最大のランサムウェア身代金の支払いが行われました。それ以前の最高記録は、2021年にCNA Insuranceから行われた4,000万ドルの支払いでした。

利益が上げられるだけでなく、ランサムウェアの運営者は、欧米の法執行機関の措置からもほぼ影響を受けないという点も指摘されます。措置による中断がランサムウェア経済に及ぼす影響は短期的にとどまる傾向があり、下のグラフに示すように、ダークウェブ上のランサムウェア被害者の恐喝投稿は措置の後急速に回復します。起訴対象者がCIS（独立国家共同体）構成国など、アメリカや西欧に引き渡すことができない国に居住し、働いている場合、起訴の影響はさらに少なくなります。ロシア政府は、自国の影響力の及ぶ範囲外を標的とするサイバー犯罪者を罰することはあまりありませんが、今年は少なくとも2件の事件で、アメリカの組織に対して攻撃を仕掛けた脅威アクターが逮捕されました。

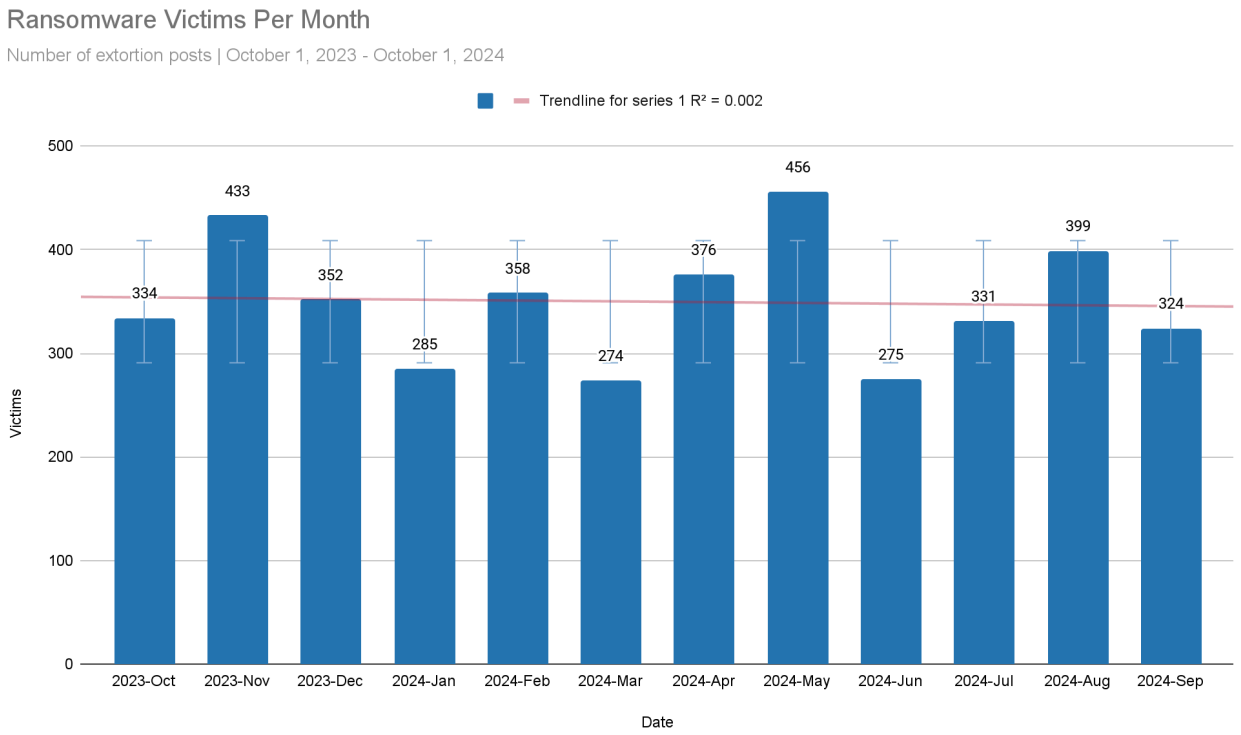


図**4**：年間を通じた法執行機関の措置にもかかわらず、恐喝ブログに投稿されるランサムウェアの月次被害者数への影響は限定的（出典：*Recorded Future*）

今後の見通し：ランサムウェアエコシステムの多様性への適応

特定のグループが漏洩したソースコードや他のランサムウェアグループからコードを取得してブランドを変更したり、再構築したりすると、適応して武器を拡大することができます。グループ間の協力、運営用ブランドの変更、小規模の独立した脅威アクターの台頭により、中央集権的なグループが残した空白が埋められ、亜種エコシステムが拡大しています。亜種の増加は、プロアクティブな脅威ハンティングとアトリビューションがより困難になるため、防御側にとって新たな課題となります。防御側は、コードベース内の異なる構文に焦点を当てたYARAルールで成功する可能性が低くなります。これは、攻撃によって異なる可能性が高いためです。しかし、目立つ機能や攻撃チェーンを構築する人材プールが亜種の急増に呼応して急拡大する可能性は低いため、ランサムウェアの暗号化ツールの実行に共通する前兆のヒューリスティックな検出は一貫しています。

業界分析から得られる脅威アクターの優先事項に関する洞察

上記のようにサイバー犯罪の手口に変化が生じているにもかかわらず、過去数年間、恐喝攻撃と盗難データベースの両方において、業界固有のターゲティングパターンは一貫しています。Recorded Futureのランサムウェア被害者データによると、ランサムウェアグループが最も狙う業界は製造業、ヘルスケア、建設業であり、製造業は3年連続でトップに立っています。

恐喝に対する支払額を増やすために緊急性を高めようとする脅威アクター

ランサムウェアの運営グループは、ITとセキュリティへの投資が限られていること、運用上のダウンタイムのコストが高いこと、IT・OT（運用技術）ネットワークの複雑さが組み合わされる製造業 https://www.verizon.com/business/resources/reports/dbir/での攻撃に対してより大きなリターンを認識する可能性があります。さらに、製造業は世界でも最も大きな産業の1つであり、脅威アクターにとって高い関心のあるターゲットとなっています。

- 一貫性のないネットワークセグメンテーションが運用技術の中断を招く結果に：製造業では、ITシステムやOTシステムを使用する複雑な環境を擁する企業が多くあり、これらは一様に高密度のセキュリティ対策によって保護されているわけではありません。例えば、イギリスの化学会社を対象とした2022年の調査では、74%の企業が企業のITネットワークからOT環境にアクセスできると報告していました。その1年後、OTセキュリティ企業のDragosは、OTに影響を与える攻撃の70%がITシステムから発生していると報告しています。
- 運用の中断はダウンタイムの高コストにつながる：製造業におけるダウンタイムのコストは、1分あたり8,662ドルから33,333ドルに上ると報告されており、大手自動車メーカーは特にコストの高さが顕著です。サイバー攻撃後の平均ダウンタイムは、数時間から4か月以上までと大きく異なります。

ヘルスケア業界もまた、患者の健康と安全への悪影響を最小化するべく、ダウンタイムに対する許容度が低い特徴があります。2024年5月、アメリカの民間医療機関であるAscensionはランサムウェア攻撃を受け、136の病院の多くで業務が中断され、救急車の転用と薬局の閉鎖を余儀なくされ、重要なITシステムが6週間オフラインになりました。金銭的なコストに加えて、病院に対するランサムウェア攻撃により、影響を受けた病院だけでなく、地域の他の病院でも緊急治療室の待ち時間が増加することが示されています。患者のケアや、場合によっては患者の生活に直接的な影響を与えることから、医療施設でのランサムウェアインシデント解決の緊急性がさらに高まり、企業にさらなる支払い圧力がかかります。

ランサムウェアの身代金支払いの緊急性を高める要因は、工場や病院の閉鎖による現実世界への影響だけではありません。主要なサードパーティベンダーやサービスプロバイダーが狙われると、業界全体でサービスの混乱が生じる可能性があります。2024年6月、CDK Globalは、BlackSuitランサムウェアの侵入を受け、データセンター、電話、アプリケーションをシャットダウンしました。その結果、これらの緩和策により、北米の約15,000の自動車販売店のサービスが中断されました。CDK Global は2,500万ドルの身代金を支払ったことが広く報じられています。アメリカを拠点とするコンサルティング企業のAnderson Economic Groupは、CDK Globalの閉鎖により、わずか2週間で自動車ディーラーに6億ドル以上の損害が発生したと推定しています。2024年8月のDetroit Free Pressによると、ドイツのメーカーAEGでは、サイバー攻撃を受けた3週間における自動車ディーラーの直接損失総額が10億2000万ドルに達し、2024年6月の自動車販売台数は前年比で5%以上減少したと推定しています。高額なコストと広範な混乱により、脅威アクターの恐喝要求の緊急性が高まり、CDK Globalが支払いを強いられた可能性が非常に高いと考えられています。

将来の収益化の可能性で高まる盗難データの価値

犯罪者は、データ漏洩の脅威で企業を恐喝するだけでなく、盗んだデータを販売したり、ネットワークに直接アクセスしたりすることで、被害者のネットワークへのアクセスを収益化します。Recorded Futureのデータによると、2024年のダークウェブ犯罪フォーラムへのIAB（初期アクセスブローカー）からの投稿数は、2023年からほぼ横ばいです。しかし、提供サービスの種類ごとに投稿を分けると、公開されるデータベースの数は増加している一方で、侵害された組織への直接アクセスは2022年のピークから減少傾向にあるようです。これらの犯罪広告で最も多く取り上げられた業界は消費財で、全投稿の13%を占め、次いでテクノロジーと政府/公共部門（いずれも全投稿の7%）となりました。

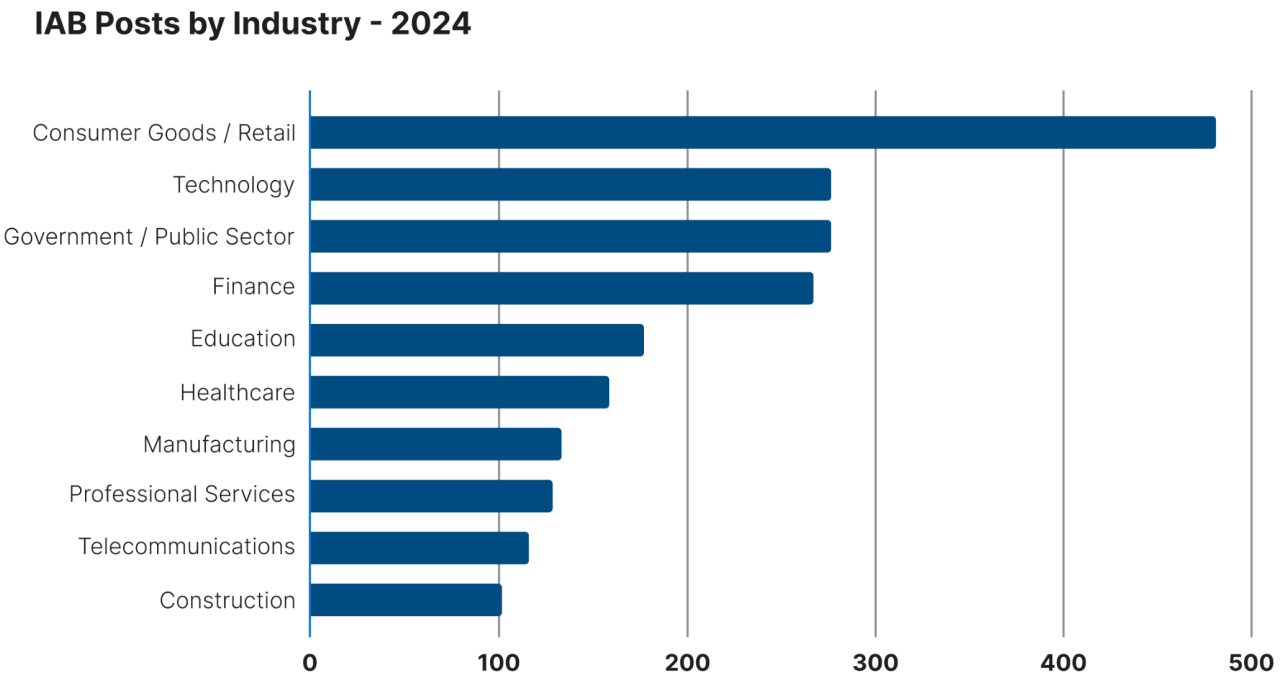


図*5*：犯罪フォーラムで販売されるデータとして最もシェアが大きいのは消費財/流通企業（出典：*Recorded Future*）

広告されているデータベースの価格を詳しく見てみると、参照頻度の低い業界は価格が高くなる傾向があることがわかります。例えば、小売業界のデータベースが最も一般的で、リスティングあたりの価格の中央値は320ドルで、全体の中央値である500ドルを下回っていました。（Insikt Groupが中央値を使用しているのはデータセットの外れ値を考慮するためです。）ヘルスケア業界のデータベースと電気通信業界のデータベースの中央値は、2023年から2024年の間に大幅に上昇しました（それぞれ100%と163%の上昇）。電気通信業界は、リスティングあたりの価格の中央値が1,000ドルで、最も高価な業界データとなっていますが、リスティング全体に占める比率はわずか3%です。教育業界から盗まれたデータベースは、2022年の298ドル、2023年の43ドルから2024年には700ドルとなり、最も大幅な価格上昇が起こった業界の1つとなりました。

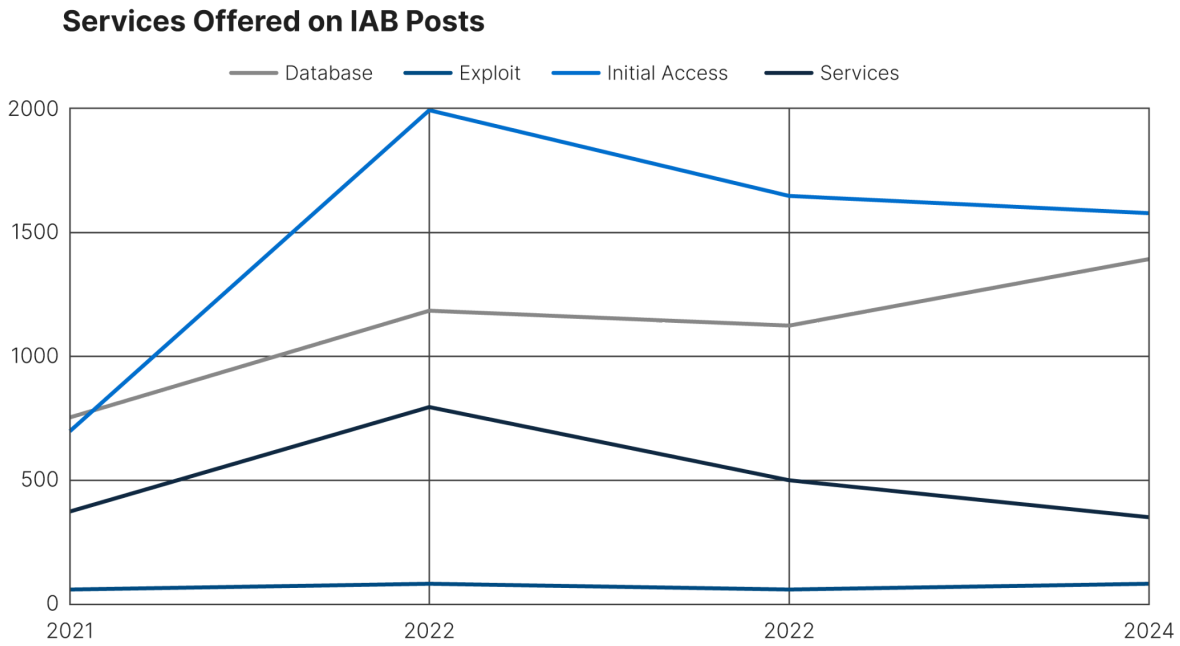


図*6*:*2022*年のピークにもかかわらず、初期アクセス提供投稿数は犯罪フォーラムのデータベースよりもわずかに多いだけ(出典:*Recorded Future*)

データベースの価格は、データの品質、被害者組織のプロファイル、個人情報の盗難やその他の詐欺のためにデータをさらに収益化できる可能性など、複数の要因によって左右されます。個人情報の盗難の状況に関する広範なレポートは、公開されたデータの有用性をコンテキスト化する上で役立ちます。アメリカ連邦取引委員会によると、2024年の第1～第3四半期に最も多かったのはクレジットカード詐欺でした。金融セクターのデータにはクレジットカード詐欺に役立つ情報が含まれている可能性が高いですが、ヘルスケア、公益事業、教育機関などの他のセクターでは、過去の住所、家族の名前、社会保障番号などの個人的かつ不変のデータが主に収集されます。また、電気通信業界の顧客データは、2要素認証を回避し、他の種類の詐欺を犯すために広範に使用されている方法であるSIMスワップ詐欺の実行にも役立つ可能性があります。

今後の見通し:「感染収益率」改善への期待

犯罪者がネットワーク、資産、データへのアクセスをどのように収益化しているかを理解することは、緩和戦略を立てる上で役立ちます。金銭的な動機を持つ脅威アクターは、国家支援型脅威アクターのように特定の企業を狙うことはありませんが、ターゲットの優先順位付けにおいては「感染収益率」の最も高い業界に引き続き焦点を当てる可能性が高いと思われます(2024年には製造業、ヘルスケア業界、金融業界が金額ベースで上位でした)。これは、Recorded Futureの観察結果とほぼ一致しており、ランサムウェアの恐喝投稿が最も多かったのは、製造業、ヘルスケア、産業機器、建設、サービスの各業界の企業でした。

世界的な敵対行為の激化が重要インフラの標的化を推進

イラン、中国、ロシアに関連する脅威アクターグループとそのハクティビストの代理人は、破壊的なサイバー攻撃で民間の重要インフラを標的にし、否定可能性を利用し、ハイブリッド紛争を通じて目的を推進しました。

中国国家の支援する事前配置は米国の重要インフラを破壊する能力を実証

2024年2月、アメリカのサイバーセキュリティ担当高官は、Volt Typhoonとして知られる中国の国家支援型脅威アクターがアメリカの重要インフラネットワークに事前配置しようとしていると警告しました。警告によると、この「事前配置」は、地政学的紛争が激化した場合に、脅威アクターが戦略的なタイミングでサイバー攻撃を実行するための重要なネットワークにアクセスできるようにすることを意図しています。Volt Typhoonの活動に関する報告は2023年にさかのぼり、この際にはMicrosoftが「重要な通信インフラを混乱させる可能性のある能力の開発を追求する」意図を持つと思われるアメリカの組織での活動を検出しました。重要インフラネットワーク上で観測されたVolt Typhoonの活動は、過去には産業スパイや地政学的なスパイ活動が特徴であったアメリカに対する中国のサイバー脅威活動の変化を表しています。事前配置活動の他の事例は、最近の緊張緩和にもかかわらず、インドの発電所が引き続き偵察活動の標的となっている中印国境 https://www.bbc.com/news/articles/ckg0gwy0nlyoでの紛争に関して発生した可能性が高いと考えられます。

事前配置活動の成功と、高度なスパイ技術の継続的開発（下記の「Salt Typhoon」を参照）は、ほぼ10年にわたる「ステルスへの移行」に努力の成果です。中国政府は、ゼロデイ脆弱性の研究やエッジデバイスの悪用など、ステルス技術の開発に多額の投資を行っており、後者は主に台湾の組織を標的としたスパイ活動で検出されています。

2024年を通じての事前配置活動は、米中間の敵対関係の激化という近年の傾向を背景に行われました。アメリカと中国は、南シナ海における中国の領土拡大と中国政府の台湾に対する領土主張、人権、技術移転、貿易、諜報活動をめぐって衝突を続けています。さらに、トランプ政権は、中国の世界的な影響力の増大に対抗することについて率直に発言している数人の人物を、国家安全保障および外交の主要な地位に任命しました。

*Salt Typhoon*の大規模な通信ハッキングと米中関係

2024年10月、Wall Street Journalの報道、中国のハッカーがアメリカの通信会社に侵入し、裁判所命令による盗聴作戦に使用された個人の通信やシステムに関連するメタデータにアクセスしたと伝えられました。この侵害の程度に関するさらなる詳細は、アメリカ議会へのブリーフィングで明らかに なり、数十の通信会社が狙われており、侵入がまだ進行中であることが明らかになりました。「Salt Typhoon」と称するこの脅威アクターは、これらの企業へのアクセスを利用して、 https://www.washingtonpost.com/national-security/2024/11/21/salt-typhoon-china-hack-telecom/ 著名な政治家の電話を標的にしたと報じられています。この活動は、アジアや中東の通信会社を標的にして諜報活動を行う従来の中国のスパイ活動と整合しています。さらに、2月の「i-Soon Leaks」の証拠からは、世界中の通信会社の通話データ記録を標的にすることへの関心が示されています。

スパイ活動は、標的のネットワークを混乱させないことを明確に意図したものですが、アメリカの重要インフラネットワークへのこのような広範な侵入の発見は、米中関係悪化を招きました。本稿執筆時点では、アメリカ議会の反応は主に、古いルーターの存在や監視機能の欠如など、通信会社自体のセキュリティの過失に焦点を当てています。Salt Typhoonの侵害に関するインシデント後の調査では、アメリカ連邦サイバー機関のアクセス監視とインシデント対応に関連し認識された欠点にも焦点が当てられていますが、具体的な詳細は機密扱いのままで

す。サイバー攻撃に対する過去の議会の憤りから、重要インフラ向けサイバーインシデント報告法（Solarwindsの侵害を受けたもの）が可決されるなど、新たなサイバー法案が制定されています。しかし、バイデン政権は、侵害したロシアを罰するために制裁も課しました。この活動を受けて中国に対する制裁などの懲罰的措置が出てくる可能性も高く、米中関係のさらなる緊張が予測されます。

ロシア関連の破壊工作が間接的に戦争の目的を推進

同様に、ロシアは間接的にウクライナの同盟国を標的にすることで、ウクライナでの紛争目的を推進しようとしています。2024年5月上旬、サイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA）は、主に上下水道セクターの脆弱性を狙ったハクティビスト活動について警告を発しました。親露派のハクティビストが、ヒューマンマシンインターフェイス（HMI）を遠隔操作して、低水準の混乱や損害を引き起こしていることが確認されています。CISAは、これらのインシデントの多くが、インターネットに接続された脆弱なデバイスや、脆弱もしくはデフォルトのパスワードの使用によるものであると報告しています。ロシアの国家支援型脅威グループSandwormも、ハクティビストのペルソナとプロキシを使用してハッキング&リーク作戦を実施し、影響工作を通じて破壊的なサイバー攻撃の影響を増幅しています。12月には、Sandwormと関係のあるハクティビストグループ「Xaknet」が、ウクライナの国家登録簿を侵害し、データを盗み、市民がデジタルサービスにアクセスするのを妨げたとして犯行声明を出しています。Sandwormのハクティビスト代理人に対する支配と関係性はグループによって異なると思われますが、Mandiantは、最も近い運用上の関係はRussianCyberArmy_Rebornとの間にあると評価しています。

北大西洋条約機構（NATO）諸国は、サイバー的な混乱に言及するだけでなく、ヨーロッパの重要インフラに対して破壊工作を展開するロシアの「影の戦争」に対する注目を強めています。ロシアの破壊工作は、ほぼ確実にNATO同盟国を不安定化させ、NATOの戦闘能力を低下させ、NATOのウクライナ支援を妨害すること（例えばNATOがウクライナに提供を約束した軍事資産を狙うなど）などを目指しています。Insikt Groupは、ロシアの破壊工作と思われる攻撃が6月に少なくとも3件見られたことを特定しています（フィンランドの水処理施設への侵入、ポーランドの武器工場での爆発、ポーランドの鉄道ターミナルでの火災）。Insikt Groupはまた、同月に欧州全体で発生した21件の追加インシデントを特定しました。これらも破壊工作の可能性がありますが、確定するにはさらに情報が必要です。

今後の見通し：地政学とサイバーコンバージェンス

物理的な破壊工作や「ハクティビスト」によるサイバー攻撃によるロシアの活動は、敵を混乱させ、不安定化させるための非動的手段の使用を指す「戦略的情報攻撃」に当たります。この戦略を進める上で、間接的な攻撃は、大きな政治的反撃や軍事的報復を引き起こすことなく、望ましい効果をもたらすために十分な破壊力を持つ必要があります。

重要インフラへの間接的な攻撃は地政学的紛争の状況で発生するため、国家間の関係の変化により、サイバー脅威の活動がエスカレートまたは抑制される可能性があります。トランプ新政権の外交政策をめぐる不確実性を考えると、防御側は、さまざまな程度の混乱と否認を特徴とするサイバーおよび物理的な脅威の継続を予想する必要があります。悪意のある活動を加速させる可能性のあるシナリオには、中国が南シナ海での領土を拡大しようとする試みや、ロシアと西側諸国、特に欧州連合（EU）、イギリス、アメリカとの関係のさらなる悪化が含まれる可能性があります。

歴史的な選挙イヤーに生成AIが虚偽のコンテンツ拡散を加速

国家支援型の悪意ある影響力工作は、世界中の選挙に影響を与えるための欺瞞的で説得力のあるコンテンツを作成・配布するために、生成AIへの依存を深めています。

国家支援型の敵対者が影響力工作向けに生成AIの実験を継続

2024年を通じて、アメリカ、イギリス、インド、インドネシア、フランス、EUなど、世界中で20億人以上の有権者が国政選挙投票に向かいました。また、今回の選挙は、国家と連携する影響力工作アクターが、生成AIツールを使って作戦を加速させ、世論形成を図るに十分な機会を提供しました。ロシア、中国、イランはそれぞれ、欧米の民主主義を不安定化させ、政治的・社会的緊張を煽り、国民間の不和を植え付けて、自国の戦略的な地政学的目標を推進することを目的とした悪意ある影響力工作に従事しました。生成AIは、敵対者がソーシャルメディアネットワーク上で影響力工作を開始し、実行する上での速度と量を向上させます。効率性の向上にもかかわらず、こうしたキャンペーンは一般的に、対象オーディエンスにとり信頼できるコンテンツとなるには不十分でした。しかし、「オーバーロード作戦」に見られるように、信頼性が必ずしも主要な目的ではなく、情報環境を不実なコンテンツやジャンクコンテンツで圧倒し、ディスコースの全体的な質を低下させること自体が目的となる可能性があります。

特にロシアは、生成AIの使用を進化させ、より人間らしく説得力のあるコンテンツを作成し、より広範な国営キャンペーンを支える影響力工作の規模と範囲を拡大しています。例えば、ロシアが運営する「アンダーカット作戦」は、500件以上のソーシャルメディアアカウントを使用して、EUとEU市民を標的としたさまざまなロシア寄りのナラティブを宣伝するAI強化動画を拡散しました。アメリカ司法省（DOJ）によると、ロシアの国営メディア組織RTは、特別に設計された秘密ツールをAIで強化されたボットファーム「Meliorator」の作成・制御に使用しています。このツールは、生成AIを使用して、ボットアカウントよりも正当なアカウントに沿ったアカウント属性を持つ人工ペルソナのよりリアルなネットワークを作成します。Melioratorは、戦力を倍増させることを目的としていたと考えられており、複数のリアルなアカウントをまとめて作成・管理できるようにしていました。

一部のネットワークは、選挙結果を左右し、国民の信頼を損ない、世界的な不和の種をまくことを目的としていました。ロシアと連携する影響力工作「オーバーロード作戦」は、2024年のアメリカ大統領選挙、2024年7月のフランス大統領選挙、2024年のパリオリンピックで、疑念、混乱、不和の種をまくように仕組まれた悪意ある影響力キャンペーンを実施しました。このキャンペーンの主な特徴は、情報に遭遇した報道機関、研究者、民間人の限られた調査リソースを圧倒することを目的とした、AIによって生成された本物の報道機関になりすましたナレーションなど、コンテンツ提供の速度と量にありました。オーバーロード作戦は、説得力のある偽コンテンツを大量生成し、ソーシャルメディアを通じた配信を自動化することで、正当かつ時間的制約のあるリードの検証ではなく、証拠の収集と情報の信憑性の検証により多くの時間を費やすよう受け手に強制します。

一方、イランは、Insikt Groupが「Emerald Divide」と呼ぶ影響力ネットワークを利用し、イスラエル国民の間での反政府感情の醸成を狙いました。Emerald Divideは、イスラエルの政治環境の変化に対応して方向転換する能力を実証し、AIで生成されたコンテンツをイスラエル、ヒズボラ、ハマス、イランにおける紛争に合わせて調整しました。Emerald Divideは、少なくとも7つの主要なアカウントと、協調的な不正行動（CIB）に関与している250件以上のアカウントのネットワークを含むソーシャルメディアネットワークを使用しました。これには、イスラエルのラビを名乗る偽のアカウントが反LGBTQ+コンテンツを含むディープフェイクを公開し、Emerald Divideが支配する他アカウントが同じコンテンツを批判するキャンペーンが含まれていました。こうしたアカウントは、親イスラエル派と親ハマス派の両陣営で分裂を煽り、CIBネットワークを通じて配布されました。Insikt Groupは、Emerald

Divideが、反政府抗議行動や対象地域で観察されたポスターなどの観察可能な結果に基づいて、対象オーディエンスに影響を与えることに成功した可能性が高いと評価しています。

最後に、中国の影響力工作アクターは、物議を醸すアメリカの問題を議論し、バイデン政権を批判するAI生成コンテンツを宣伝しました。中国の影響力工作は、全体的に分断を増幅させ、民主主義を混沌とした望ましくない政治システムとして描こうとしています。そのソーシャルメディアのペルソナは、しばしば、政権の目標と公衆のニーズとの間で起きる不全や不一致の認識された例を強調しています。アメリカ大統領選挙以外にも、中国は、天安門事件に関連するハッシュタグをアメリカ国内の警察暴力を強調するコンテンツにリダイレクトするなど、好ましくないと思われる特定の出来事や問題について好意的なナラティブを増幅させました。中国の影響力作戦は、40以上の言語でコンテンツを作成しており、これはスポンサーの国際的志向を示しています。

国家支援型の脅威アクターはLLM（大規模言語モデル）の使用拡大を意図している可能性があるものの、攻撃自動化の障壁は依然として存在

2024年を通じて、中国、ロシア、イラン、北朝鮮に関連する脅威アクターは、偽コンテンツに加えて、AI使用を他の悪意のある用途に拡大しようと試みています。OpenAIは、国家が支援する脅威アクターが、マルウェア開発、ソーシャルエンジニアリングの偵察、影響力工作、スピアフィッシングのルアー生成にこのプラットフォームを使用したことを確認しました。サイバー脅威アクターがマルウェア開発に生成AIを使用していることを示す他の証拠は、VBScript（Visual Basic Script）と、このテクノロジーの使用を示すアーティファクトを含むJavaScriptコードの発見を通じて、すでに明らかになっています。

しかし、生成AIを完全自動化されたマルウェアの開発や配信に利用する試みは成功していません。セキュリティ研究者らは、AIプロンプトエンジニアリングとトレーニングを通じて、PoC（概念実証）マルウェアを開発しました。Insikt Groupは、PowerShellベースの情報窃取型マルウェアであるSTEELHOOKの亜種を作成し、LLMを使用して環境を推論し、YARAルールをバイパスするためにメモリ内のコードを更新しました。同様に、Hyasは、LLMを使用してポリモーフィックな動作を動的に生成するEyeSpyとBlackMambaという2つのPoCマルウェアをリリースしました。LLMは、実行時にキーロガーを駆動する悪意のあるコードを合成し、シグネチャベースの検出を回避します。

そうは言っても、上記の国々は、より自動化された攻撃作戦のためにAI機能に積極的に投資しています。特に中国は、軍事、民間、学術のAI能力を拡大し、物理的およびサイバー領域での攻撃作戦の強化を追求しています。ロシア、イラン、北朝鮮は、主にAI統合の初期段階または実験段階にあり、サイバー戦略におけるAIの可能性を探求することに重点を置いていますが、この分野のイノベーションの大部分を推進する民間企業への相応の投資が不足しています。

今後の見通し：*AI*運用の未来

2025年には、敵対的な国家がマルウェアの展開などの攻撃的な機能ではなく、主に生成AIを使用して不正コンテンツを生成する可能性が依然としてあります。ポリモーフィズム、ミューテックスメカニズム、メモリ内の悪意のある動作の隠蔽、これらのLLMが合成するその他の動作は新しいものではなく、既存のメカニズムはこれらの動作を検出するように設計されています。悪意のあるスクリプトやプログラムを生成するために、LLMは既存のマルウェアとキルチェーンでトレーニングを行い、サイバー攻撃の仕組みを理解する必要があります。現在のLLMは、利用可能なトレーニングデータに基づいて完全に新しい技術を発明するほど洗練されてはいません。さらに、生成AIの他の用途と同様に、アウトプットは一般に、人間による出力に比べて複雑ではありません。AIアプリ

ケーションは、2024年を通じてOpenAIが観察しているように、脅威活動の強化やトラブルシューティングに使用される可能性があります。

同時に、政治的な動機に基づくAIコンテンツの制作を制限する取り組みの優先順位は、今後数年間で下がる可能性が高いでしょう。Insikt Groupは、アメリカにおいて、不正なコンテンツネットワークに関する公開報道が減少すると予想しています。言論の自由に対する懸念に沿い、トランプ政権は初日から大統領令を発令し、連邦政府に対して、国内言論に「誤報」や「偽情報」とレッテルを貼って言論の自由を侵害することを禁じました。とはいえ、不誠実なコンテンツに関する研究の有効性は、ソーシャルメディアプラットフォームやホスティング企業が悪用ある者を排除する意志と能力と常に相関するため、今後数年間で政治的動機に基づくAIコンテンツの拡散をどの程度許容するかを決めるのは、公共部門ではなく民間部門です。AIで生成された政治コンテンツに対する国際法やアメリカの州法が可決されましたが、これらの法律が虚偽のコンテンツの開発と拡散に与えた影響は限定的です。

防御回避を重視する戦術とテクニック

TTP（戦術、技術、手順）は、かつては国家のリソースを持つ高度な脅威アクターに限定されていましたが、犯罪活動ではますます一般的になりつつあり、これに伴い防御回避技術の大幅な急増も観察されています。

リモート管理ツールでありふれた場所に潜む行為が可能に

脅威アクターによるRMM（リモート監視・管理）ツールの悪用は、運用効率を維持しながら検出を回避するその能力に牽引され、2024年に急増しました。これらのツールは従来ITサポートで使用されていましたが、EDR（エンドポイント検出および対応）メカニズムを回避することを目的とした攻撃者による採用が増加しています。Huntressは、2024年1月から10月の間にRMMツールに関連するインシデントが214%増加したと報告しています。Recorded Futureのデータはこの傾向を裏付けており、2023年にはわずか50件だったのに対し、2024年には600件以上が言及されています。2024年初頭の言及は、CVE-2024-1709として追跡されているScreenConnectの認証バイパスの欠陥を含むエクスプロイトに関連しており、PoC（概念実証）のリリース後に広く悪用されました。2024年に言及が急増した2番目の大きな急増は、BlueBravoによるTeamViewerへの攻撃に関連しており、これにより、従業員データと暗号化されたパスワードがIT環境に流出しました。

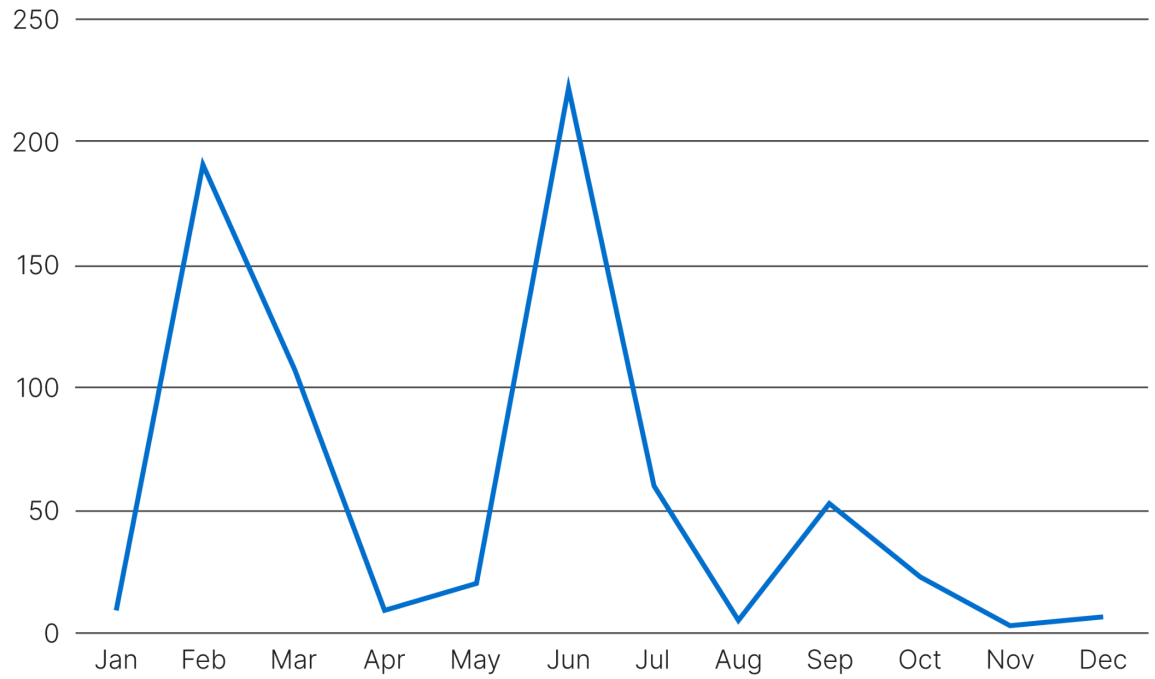


図7:リモート監視および管理ツールに言及したサイバー攻撃レポートは*2024*年の夏に大幅に急増(出典:*Recorded Future*)

脅威アクターは、ITヘルプデスク詐欺でAnyDeskやTeamViewerをダウンロードするようにターゲットを説得するBlackBastaのキャンペーンなど、ソーシャルエンジニアリングを通じてRMMを提供してきました。RMMプログラムがシステム上で実行されると、脅威アクターはそのアクセスを悪用して永続性を確立し、他のペイロードを配信することができます。

RMMの使用の増加は、EDR(エンドポイント検出および対応)ツールの採用の増加と、ConnectWise、AnyDesk、TeamViewerなどのRMMツールに依存してリモートITを可能にするハイブリッドおよびリモート作業環境の仮想化という2つのトレンドによって推進されている可能性があります。EDR機能の向上により、脅威アクターは、正当なプログラムの悪用など、EDRソリューションから活動を隠す戦術を採用するようになりました。仮想化の進展でRMMツールはIT環境の一部となり、防御側が正当な活動と悪意のある活動を区別することが難しくなっています。GitHubのプッシュが一般的なワークフローの一部である傾向があるため、脅威アクターは、RMMツールに加えて主にマルウェアペイロードの配信手段としてGitHubなどの信頼できるサイトも使用しています。他のランサムウェア運営者は、マルウェアをAnyDeskやScreenConnectなどの正当なRMMサービスに偽装して、ユーザーを騙し、プログラムをダウンロードさせます。

多様化を続けるmacOSとLinuxのマルウェア

Microsoft Windowsは依然として脅威アクターの主要な標的ですが、2024年はmacOSおよびLinuxシステムに対する攻撃が継続的に増加し、複数の種類のマルウェアが大幅に拡大しました。この傾向は、エンタープライズ環境やLinuxハイパーバイザー上で動作する多くのネットワーク関連機器やシステムでのAppleデバイスの採用増加が観察された事実に沿ったものです。Intel471は、2023年1月から2024年7月にかけて、ダークウェブフォーラムでmacOSデバイスを標的にした40人以上の脅威アクターを特定しました。2024年1月から2024年7月にかけて、21人の脅威アクターがmacOS固有のマルウェアまたはサービスに関心を示しており、これは2023年通年で観察された数と同数です。この発見は、macOSユーザーを標的とした情報窃取型マルウェアの地下販売が5倍に増加したとのGroup-IBの観察にも一致します。さらに、脅威アクターは、RustやGoなどのクロスプラットフォーム言語を使用するツールの開発を進めており、観察されたこれらの増加に貢献しています。Linuxシステムでもランサムウェアの活動が増加しました。

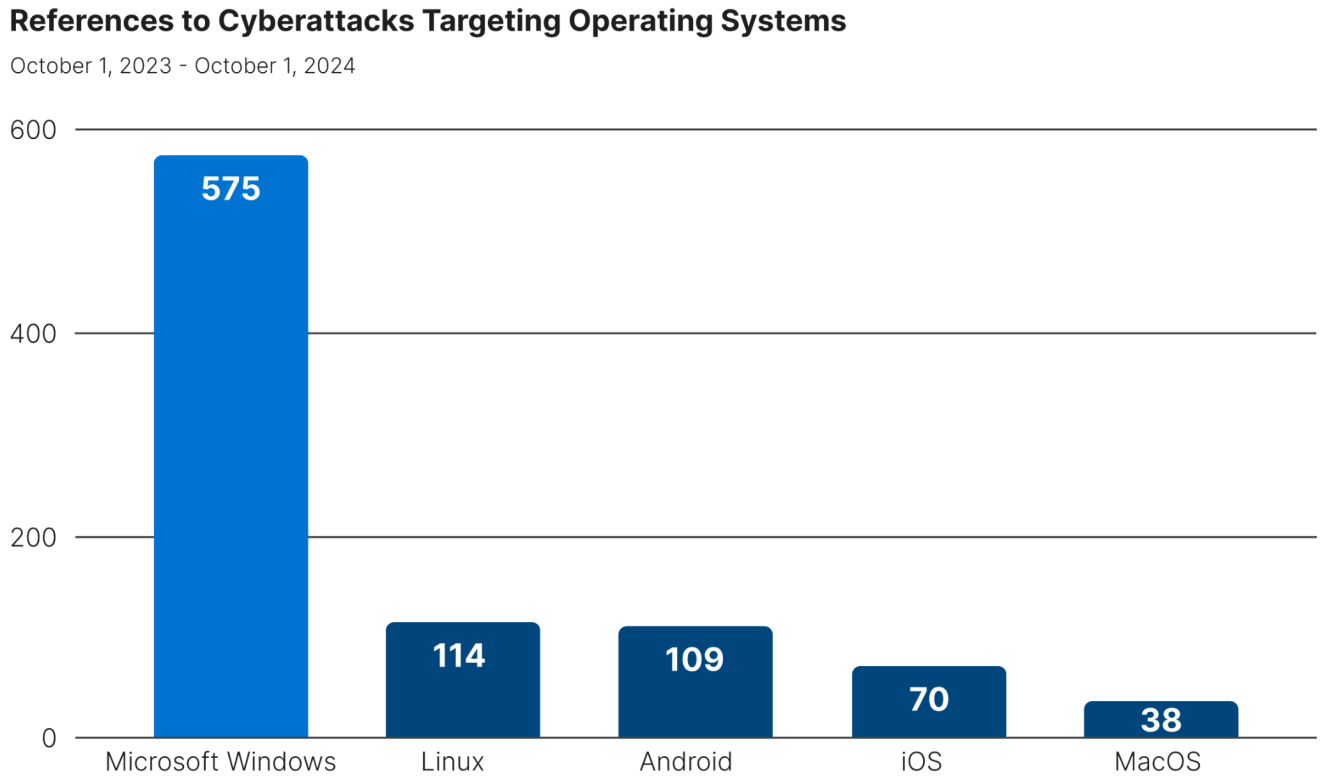


図**8**：*Windows*が依然として最も一般的に悪用されるオペレーティングシステムであるものの、*Linux*、*Apple*、モバイルデバイスの標的は増加傾向（出典：*Recorded Future*）

macOSに特化した情報窃取型マルウェアとトロイの木馬の増加と巧妙化

macOSを標的とするBANSHEE Stealer、Cthulhu Stealer、Atomic Stealer（AMOS）などの情報窃取型マルウェアはますます一般的になっています。この増加は、関心対象となるネットワークやユーザーのMacコンピューターを使用することが多いことから、macOS環境の悪用に対する脅威アクターの関心が変化していることを表しています。HZ Ratは、2024年4月に報告されたLightSpyモバイルフレームワークのmacOS向け亜種と同様に、以前はWindowsに重点を置いていたリモートアクセス型トロイの木馬（RAT）をmacOSに適応させたものです。この亜種は、2020年に発見されたiOSバージョンよりも洗練されており、コマンド&コントロール（C2）フレームワークを難読化するなどの改善点があります。また、2024年2月に確認されたTrojan.MAC.RustDoorなど、macOSに特化したトロイの木馬やその他のバックドアも出現しました。このバックドアは、脅威アクターがWindows、Linux、macOSなどのさまざまなオペレーティングシステムのネイティブバイナリに効率的にコンパイルする方法として、Rustで悪意のあるコードを作成する傾向を引き継いだものです。

サイバー犯罪者は、ソーシャルエンジニアリングや正規のインターネットサービスの悪用など、複数のベクトルを通じて、macOSの情報窃取型マルウェアとWindowsの情報窃取型マルウェアを配信し、操作しています。犯罪者はWeb3ゲームやビデオ会議ソフトウェアなどの一般的なプログラムになりすましてユーザーを騙し、複数のオペレーティングシステムで動作する情報窃取型マルウェアをダウンロードさせます。同様に、犯罪者はGitHubを使用して、AMOSを含むさまざまな情報窃取型マルウェアのコマンド&コントロールインフラストラクチャをサポートしていることが確認されています。GitHubなどの正当なインターネットサービスを使用することで、犯罪者は、ターゲット環境にすでに存在する可能性のあるプログラムを操作でき、検出を回避できます。RustDoor以外にも、ZuRuは諜報活動に特化したステルスmacOSバックドアとして登場しました。これは、そのモジュール型アーキテクチャにより、ターゲット環境に基づいて追加のコンポーネントを動的にロードすることができます。これらのペイロードは、画面キャプチャ、キーロギング、リモートシェルアクセスを可能にし、コード署名と

正規のApple開発者証明書を使用してmacOS GatekeeperとXProtectの防御を回避しました。情報窃取型マルウェアJaskaGOは、RustDoorと同様に、クロスプラットフォーム言語であるGo言語で記述されているため、攻撃者は単一のコードベースを使用して複数のオペレーティングシステムを標的にでき、開発時間とリソースを削減できます。Cuckooとして知られる多機能情報窃取型マルウェアおよびバックドアマルウェアも今年登場し、ZuRuと同様のステルス操作とモジュール型アーキテクチャで注目に値します。

有害なユーティリティ、ハイパーバイザー、クロスプラットフォーム機能で狙われる*Linux*システム

2024年、Insikt Groupは、Linuxシステムを標的とするMiraiボットネットをベースとする新しいワームを観測しました。このマルウェアのカスタマイズ版は、Linuxベースのサーバー、ルーター、ウェブカメラ、その他のIoT（モノのインターネット）デバイスを標的にしていましたが、DDoSプラットフォームではなく、悪意のあるクリプトマイナーとして機能していました。マルウェアがLinuxを標的とする能力を拡大した別の例では、研究者らは、感染したLinuxシステムのデータを完全に消去できるワイパーマルウェアであるBiBi-Linuxを発見しています。BiBi-Linuxは、イスラエルとハマスの紛争開始時に特にイスラエル企業を標的にしました。また、同じマルウェアのWindows版もあり、これも脅威アクターが複数プラットフォーム間で活動する傾向の強まりを示しています。

Insikt Groupが2024年にランサムウェアグループが最も標的にした製品の1つとして観察したものは、Linuxフレームワーク上に構築されたVMWare ESXiハイパーバイザーでした。Insikt Groupは、Hunters International、Play、INC、RansomHubなど、ハイパーバイザーやその他のLinuxデバイスを直接標的とする一般的なランサムウェアペイロードの特定の亜種を確認しました。ネットワーク内でのESXiの機能は非常に重要であるため、依然として優先度の高いターゲットとなっています。上記のmacOSマルウェアと同様に、ESXiを標的とする多くのマルウェアの亜種は、RustまたはGo言語で記述されています。これらは低水準言語として低遅延通信とリソース効率の高い実行に最適化されており、プロセスインジェクションやフックに使用できます。さらに、Rustはメモリの安全性に重点を置いているため、バグの可能性が減り、検出や中断が困難な信頼性と安定したペイロードが生成され、ヒューリスティックベースの検出ではメモリアクセスパターンと構造の検出がより困難になります。

防御回避を伴う**TTP**が最も増加

防御回避（TA0005）技術（デバッガー回避、反射型コードローディング、API（アプリケーションプログラミングインターフェイス）による実行）の顕著な増加は、ディスクにコードを書き込まない防御回避戦略に対する移行の傾向を浮き彫りにしています。NTP（ネットワークタイムプロトコル）ベースの時間回避と反射型コードローディングは、行動分析とフォレンジック検出の回避に敵対者の重点が置かれていることを示しています。

2023年から2024年にかけてMITRE ATT&CKの手法でInsikt Groupが観測した最も顕著な増加は、T1497.003（時間ベース回避）、T1622（デバッガー回避）、悪意のあるローダーソーの回避コンポーネントに通知するデータ収集に関連する手法でした。T1057（プロセス検出）とT1016（システムネットワーク構成検出）は、Insikt Groupが複数の攻撃やマルウェアサンプルで観察した手法で、ドロッパー、ローダー、またはその他のバイナリが環境からデータを収集し、デバッガー環境とサンドボックス環境のどちらで実行されているかを判断するために使用されます。特定のネットワーク設定、実行中のプロセス、または過去100日間にアクセスされたドキュメントの数などのその他のアーティファクトを使用して、ターゲットデバイスとサンドボックス環境を区別できます。

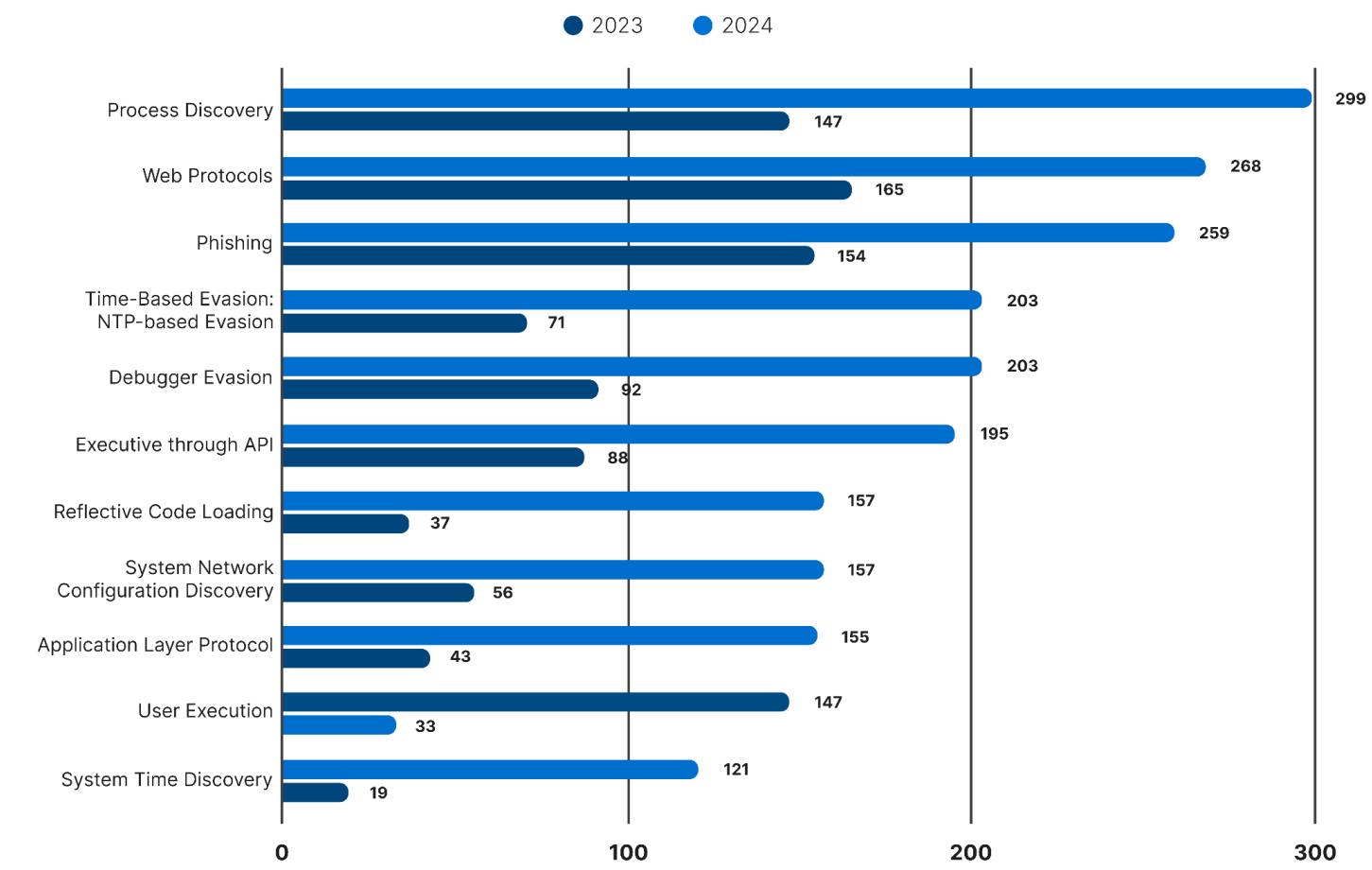


図**9**：*2023*年から*2024*年の間に観測された増加が最も大きかった*TTP*（出典：*Recorded Future*）

EDRの使用の改善がRMMツールの乱用増加の根拠であるという本レポートの上記の評価に沿って、Insikt Groupは、一般的なEDRバイパス技術に関連するTTPの増加も観察しました。T1106（ネイティブAPI）は、API呼び出しを使用して悪意のあるアクションを実行しながら、正当なシステムアクティビティに溶け込むため、セキュリティツールによる検出を回避できます。APIコールを悪用することで、攻撃者は従来のアラートをトリガーせずにコードを実行でき、システム機能を低水準で制御できるため、攻撃者は検出可能なサードパーティの実行可能ファイルへの依存を回避できます。同様に、T1620（反射型コードローディング）は、脅威アクターが悪意のあるコードをディスクに書き込まずに直接メモリにロードすることを可能にします。これにより、EDRスイートで一般的なファイルベースの防御を回避できます。Insikt Groupは、特にDLL（ダイナミックリンクライブラリ）サイドローディングを頻繁に使用する中国の国家支援型グループの間で、敵対者がシグネチャベースの防御やフォレンジック分析を回避するためにメモリ常駐型マルウェアを展開することが増えていることを観察しました。Cobalt Strikeやカスタムローダースクリプトなどのツールも、反射型コードローディングの使用の増加に貢献しています。

今後の見通し：ディスク外の敵対的アクションの追跡

EDRを始めとするセキュリティツールがますます一般的になる中、脅威アクターはセキュリティギャップを突いて検出を回避する方法を模索しています。こうした展開から浮かび上がるのが、進化する脅威を軽減するため、防御者が堅牢なメモリ分析、行動異常検出、高度な脅威インテリジェンス統合を採用することの必要性です。防御

側は、既知のプログラム構成の実行状態マッピングなど、より複雑な防御策を検討する必要があります。これにより、バイナリ実行やAPI呼び出しが中断される可能性があります（悪意のあるコードの挿入により、ライブラリが承認されたプロファイルと一致しない場合の悪意のあるDLLを含め）。実行状態のマッピングは、ヒューリスティック監視と組み合わせて、脅威アクターの行動の有効性を混乱させる可能性のあるポジティブおよびネガティブなセキュリティモデルにすることができます。こうすれば、フック解除や反射型DLLローディングなどのEDR回避技術を使用しても、ライブラリはポジティブモデルに従って既知の状態で動作しないため、悪意のあるバイナリは実行されません。これを利用すれば、ネガティブセキュリティモデルをさらに発展させ、防御側が将来の脅威アクターの行動を迅速に検出して阻止する能力を高めることができます。

独自にマルウェアを分析する能力や意欲が組織にあれば、インメモリサイバー攻撃の増加を受けて、人員の採用やトレーニングの強化といった方法で対処できるでしょう。より一般的には、行動ベースの検出、特に特定の種類の行動の順序（特定のプロセスがシャットダウンされる前のプロセスの列挙など）に重点を置くと、より簡単に追跡可能な指標やバイナリを超えて複雑化する脅威の状況においても、異常なアクティビティを特定しやすくなります。これは、認証情報のダンプなど、通常のユーザーとしては非典型的な動作といえる多くのラテラルムーブメント手法に特に当てはまります。

2023年の予測に関する考察

2023年の年次レポートにおいて、Insikt Groupは、当時の脅威の状況に基づき、最も的確である、または最も検討の価値があると思われる一連の予測をまとめました。ただし、予測は、十分な時間が経過した後に常に再検討して、そのパフォーマンスを確認する必要があります。そのため、本レポートでは、Insikt Groupの昨年の予測と、その精度の判断について紹介します。

2023年の予測	2024年の実績
脆弱性：ランサムウェア集団（特に CL0P）が企業向けファイル転送ソリューションの脆弱性を大規模に悪用して数千件の攻撃を成功させたことを考慮すれば（Accellionは2020年と2021年、GoAnywhereおよびMOVEitは2023年）、**2024**年には少なくとも**1**つのランサムウェア集団が、企業向けサードパーティファイル転送サービスの脆弱性を悪用して、数百のターゲットの侵害を成功させると**Insikt Group**は予想しています。この事象の影響は、2023年からのMOVEitキャンペーンのそれに匹敵することでしょう。	ほぼ予想通り：今年の最終週、CL0Pは、少なくとも60社の被害者企業に影響する新しいファイル転送アプリケーションの悪用を発表しました。このキャンペーンは、これらのアプリケーションの脆弱性が依然として特に有効であることを示していますが、今年の攻撃は昨年のMOVEitエクスプロイトほどの影響には達しませんでした。 さらに、2024年には、別の脅威アクターが、最初のMOVEitエクスプロイト時点である2023年5月に遡り、少なくとも25社 https://www.infostealers.com/article/massive-moveit-vulnerability-breach-hacker-leaks-employee-data-from-amazon-mcdonalds-hsbc-hp-and-potentially-1000-other-companies/に影響するデータのトランシェにアクセス可能である旨を主張しました。このインシデントは、出現する被害者の数が増える中、MOVEitの侵害の広範な影響を強化しています。
サードパーティの脅威：2024年には、ソフトウェアサプライチェーン攻撃が、攻撃の件数と重大度の点でサードパーティの脅威の大半を占め、報告される事象は少なくとも**15%**増加すると**Insikt Group**は予想します。その遍在性と公開される新しいパケットの量により、npmが今後も最も多くのサイバー攻撃を引き寄せる可能性が高くなります。	不的中：報告されたソフトウェアサプライチェーン（SSC）攻撃の件数は2023年から2024年にかけてほぼ横ばいであり、依然として広範な攻撃ベクトルであるにもかかわらず、他の悪用を上回っていないことを示唆しています。 注目すべきソフトウェアサプライチェーンインシデント：Insikt Groupが予想していなかったことの1つに、ある精巧なソーシャルエンジニアリング事例がありました。これは、広く使用されているオープンソースのソフトウェアコードにバックドアを挿入するというものでした。コードリポジトリポイズニングはSSC攻撃の新しい方法ではありませんが、脅威アクターが悪意のあるアップデートが見過ごされることを期待してコミュニティ内で信頼を築くために2年以上を費やしたという事実が、この攻撃を際立たせています。

2023年の予測	2024年の実績
恐喝グループ：ハイブリッドおよびリモートのワークモデルを採用・維持する企業が増える中、ハイブリッドおよびリモートワークをサポートおよび保護するテクノロジー、特にクラウドベースのデータストレージやMFAソリューション、VPN（仮想プライベートネットワーク）を恐喝グループがますます標的にすることをInsikt Groupは予想します。そして、ランサムウェア攻撃の大部分には、そのような資産に対する攻撃が含まれることになります。	的中：リモート管理ツールの悪用の増加や複数のSaaS・クラウドベースの侵害の発生は、脅威アクターが仮想化環境を利用して既存の活動に紛れ込むことが増えていることを示しています。 • **165**社にSnowflakeの侵害が影響 • **12**倍 - 攻撃におけるRMMツールへの言及（Recorded Futureデータ）
ハクティビズム：Insikt Groupはロシア・ウクライナ戦争の変調により、特に紛争がガザ地区の他の地域に波及する恐れがあることから、KillnetやAnonymous Sudanなどのグループのハクティビスト活動が、戦略的にガザ紛争に向けられる可能性が高いと予測しています。NATOや欧州連合と連携する西側諸国が標的化される可能性は今後も引き続き高いものの、一方でイスラエルを支援する組織への注目度が高まる可能性もあります。	ほぼ予想通り：ハクティビストの活動は、特にガザ侵攻の初期の数か月間、イスラエル、ハマス、パレスチナに関連する標的へと移行しました。しかし、Insikt Groupが2024年にハクティビストの活動に関して観測した最も重要な戦略的転換は、金儲けへのシフトでした。Insikt Groupは、DDoS-as-a-Serviceツールによる Anonymous Sudanの利益を記録しています。2024年5月、KillMilk（旧Killnet）も、犯罪フォーラムで販売されている情報窃取マルウェアを宣伝しました。 注目すべき例外は2024年パリオリンピックを狙ったハクティビスト活動で、さまざまな政治的原因への注目を増幅させようと試みたものでしたが、イベントに与える破壊的な影響は限定的でした。
初期アクセスの手法：2024年には、組織がセキュリティの境界（ペリメータ）を強化するにつれて、攻撃者はパスワードスプレーやクレデンシャルスタッフィングなどの手法を駆使して、認証情報やIDを窃取することに一層注力する可能性が高いとInsikt Groupは予想しています。また、犯罪者が生成 AI を利用し、検出が難しく高度にパーソナライズされたキャンペーンを作成するための経験値とリソースを増強する中、フィッシングの脅威はますます「スピアフィッシング」の状況になると予測しています。	部分的に的中：Insikt Groupの認証情報窃盗に関する予測は的確で、本レポートの全セクションがその特定の脅威に特化しています。 リサーチによりAIがフィッシングメールを改善する可能性が実証されていますが、Insikt Groupは、大規模なスピアフィッシングの促進にAIが使用されているという証拠をまだ確認していません。 - **50%**増加 - 2024年第1四半期から第3四半期にかけての有効な認証情報の使用（Recorded Future TTP データに基づく） - **46%** - 2024年に報告された初期アクセスTTPにフィッシングが占める割合
影響力工作：世界中で注目を集める数多くの選挙が行われる年に突入しているため、特にアメリカのように有権者が顕著に二極化した国においては、ディープフェイクや偽情報工作に対する一般大衆の認識が、政敵重視の選挙キャンペーンの目的や活動以上に混乱をきたすと**Insikt Group**は予想します。有権者は真偽に関係なく不愉快な画像や報道について、人工的に生成されたものとして無視するよう条件づけられる可能性が高いとみられます。	予想通り：生成AIコンテンツの氾濫により、一般に、実際の写真を割り引いたり、既知の偽コンテンツを広く共有して政治的主張を進めやすくなりました。

2023年の予測	2024年の実績
テクノロジー：企業は**2024**年にはほぼ間違いなく、ウェブサイトにサインインするためのアクセスリンクの活用や生体認証ベースの認証など、パスワードなしのログインをユーザーに提供する機会が増えるとみられます。この変化により、ダークウェブ上で販売される特定の漏洩した認証情報の価値は大幅に低下し、脅威アクターは偽のアクセスリンクを記載した電子メールの作成など、パスワード不要のセキュリティを悪用する新しい方法を見つけるための自己改革を強いられることになります。マネーロンダリングや外部の顧客対応型の支払い詐欺の脅威については、パスワードレスログインへの依存度が高まることにより、ATO（アカウント乗っ取り）戦術からNAF（新規アカウント詐欺）戦術への移行が進む可能性があります。	ほぼ不的中：FIDO Allianceの報告では、ユーザーの不満と従来のパスワードに関連する多くのセキュリティ問題の両方により、2024年にパスキーに対する認識が**50%**改善したとされていますが、Insikt Groupは、今年、複数のクレデンシャルベースの攻撃が成功したことからも明らかなように、このシフトがサイバー犯罪に及ぼす二次的な影響を未だ確認できていません。
地政学：中国は、国内経済の状況が悪化し、また世界各地でそのことが触れられる中、自国民の不安を鎮めるために社会的監視と検閲を利用する可能性が高まります。中国は対外関係においては、不屈の精神を示し続け、アメリカなどの対立国が国内の不安定要素につけこむのを阻止するために、事前に破壊的サイバー工作を仕掛ける可能性があります。それでも、中国があからさまな陽動的紛争を始めるなどして激しく攻撃する可能性は低いでしょう。イランは今後も、自国周辺地域に不安を植え付けるべく、代理戦争とサイバー影響力工作を組み合わせた戦略に依存し続けるとみられます。その戦略には、イスラエルを孤立させ、地域でのアメリカ軍の駐留に反対する取り組みが含まれます。ロシアは、西側諸国の間で「支援疲れ」が認識されていることを利用して、アメリカとEUの選挙に先立って世論に影響を及ぼす可能性が非常に高いとみられます。それらの選挙結果を待って、ウクライナ戦争や西側諸国との関係について、次の行動方針を決定するでしょう。	予想通り： - 中国：Insikt Groupは、2月のVolt Typhoonの露呈後、これ以上の事前配置は確認していませんが、アメリカの通信ネットワークで広範な諜報活動が発見されたことは、中国のサイバー能力と意図に関する確かなメッセージとなりました。 - イラン：イランは2024年を通じ、イスラエルに対する代理戦争で何度も挫折を味わっています。主要代理組織であるハマスとヒズボラが著しく弱体化したため、イランは年初よりもはるかに悪い立場で年末を迎えることとなりました。 - ロシア：ウクライナへの支援拡大に対する抵抗はアメリカとEUの両方の選挙のテーマとなりました。しかし、このうちどの程度がロシアの影響力工作によるものなのか、それとも国内のポピュリスト的な言説によるものなのかを判断するのは困難です。
規制：脆弱性エクスプロイト（脆弱性を突く不正プログラム攻撃）の増加により、各国の規制当局の関心は、ソフトウェアの安全性に関する規制から、ソフトウェア責任法の改正に移行することになると予測されます。これにより消費者は、安全でないコードを作成するソフトウェア会社に対して法的手段をとりやすくなります。ただし、何がコーディング（プログラミング）における過失とみなされるのかを判断することは、政策立案者にとって難しい課題となるでしょう。**AI**企業は、**AI**に関する進行中の政策と規制に対応して、プライバシーと著作権の問題を回避しつつ、技術開発を加速し、脅威アクターによるデータポイズニング（**AI**訓練データの悪用）の危険性を低減するために、自社AIモデルの訓練用に合成データを使用する方向に移行する可能性が高まるでしょう。	一定程度予想通り：EUは、責任に関してソフトウェアを他の製品と同様に扱うように民法を改正 しました。これにより、個人は、集団訴訟を含め、デジタル製品によって引き起こされた損害について企業やプラットフォームを訴えることができるようになります。この改正がソフトウェアの安全性に及ぼす影響は、2025年に最初の訴訟が欧州の裁判所に持ち込まれる時点で初めて判明するでしょう。アメリカが同様のアプローチを検討していることを示唆し、バイデン政権は、ソフトウェアセキュリティの定量化に関するさらなる研究を呼びかけることで、最初の一歩を踏み出しました。こうした取り組みは次期政権でも続くと思われます。 一方、AI企業は、2024年を通じて規制や公的機関から

2023年の予測	2024年の実績
	の反発が限定的であったにもかかわらず、マイニングのための実データのソース探しを続けました https://www.theverge.com/2024/7/11/24196396/the-atlantic-openai-licensing-deal-ai-news-journalism-web-future-decoder-podcastshttps://www.nytimes.com/2024/04/06/technology/tech-giants-harvest-data-artificial-intelligence.html。

今後の展望：2025年の予測

- **SaaS**アプリケーションの次の大きな攻撃ベクトルとしての**AI**なりすまし：Insikt Groupは、大規模な侵害は、エンタープライズワークフローへの生成AIの実装または効果的ななりすましのためのAIの乱用という2つのAI関連要因のいずれかから発生する可能性が非常に高いと予測しています。いずれの場合も、SaaSアプリケーションが初期アクセスまたはデータ公開に一役買う可能性があります。昨年、OpenAI（SORA）、Meta（MovieGen）、Google（Veo 2）などの企業が、極めてリアルなフェイク動画や画像を作成するモデルをリリースしました。これらのツールを使用すると、詐欺グループは、ITヘルプデスクへのビデオ通話など、既存の詐欺をより説得力のある方法で実行できるようになり、機密データやシステムへのアクセスを詐欺により獲得することがはるかに容易になります。
- 新たなセクターに影響を与える新しい「**Typhoon**」活動の発表：2024年にも中国関連のAPT（持続的標的型脅威）グループによるアメリカの重要インフラへの侵入がすでに発覚していますが、Insikt Groupは、中国のAPTによる重要インフラへの注目度の高い侵害が2025年にさらに明らかにされると考えています。エネルギーおよび通信セクター以外の業界からも、破壊的な工作の事前配置目的で行われた可能性の高い、中国のAPTに起因する侵害が開示されると予測しています。
- **Windows**とクラウドに**MacOS**とモバイルの脅威が追加：マルウェアと脆弱性の傾向において、Insikt Groupは、2025年に大きな影響を及ぼすサイバーインシデントの1つがmacOSマルウェアまたはモバイルマルウェアに関連するものとなる可能性が高いと予測しています。これは、標的としてのmacOSへの注目の高まりや、モバイルデバイスを介した機密性の高い企業や財務データへのアクセスの増加など、特定の環境要因が限界点に達する結果であると考えています。
- 仮装通貨詐欺が市場を不安定にするイベントに：仮装通貨の価値の高騰も背景に、仮装通貨に優しい政策を追求するアメリカの新政権は、より積極的で野心的な詐欺の試みを推進するでしょう。仮装通貨詐欺は現在、最も一般的で収益性の高い投資詐欺の1つであり、犯罪者は暗号ブームによって大胆となり、市場を不安定にする詐欺を実行する可能性が高いと予測しています。この結果、少なくとも一時的に仮装通貨の価値が下がり、仮装通貨の使用を制限するよう求める声が高まりかねません。
- 開発者は**AI**の採用で新しいコードへの移行を加速：AIコーディング機能の向上 や欧州でのソフトウェア関連の責任の新たな推進の動きなどの複数の要因の結果として、Insikt Groupは、企業と脅威アクターの両方が、（企業向けのメモリセーフコードからマルウェア用のよりモジュール化されたコードに至るまで）最新のコードライブラリへの移行を加速するために生成AIへの依存度を高める可能性が非常に高いと予想しています。
- アメリカにおけるサイバー規制の調整に向けた動き：Insikt Groupは、新政権の規制緩和アジェンダと、規制の実施方法に関する議会の意図を明確にするよう議会に圧力をかける最高裁判所の判決が相まって、サイバー規制調整法可決への支持が高まる可能性が高いと予想しています。アメリカの複雑なサイバー規制環境の簡素化は、長い間超党派の支持を得ており、大規模なサイバーインシデントの余波を受けて国のサイバーセキュリティを改善するための行動を起こすことは、アメリカ議会にとって実現しやすい成功と見なされるでしょう。
- 危険にさらされる台湾の重要インフラ：武力紛争の勃発には至っていませんが、中国は台湾への威圧を徐々にエスカレートさせ続けており、次に起こるのが台湾のエネルギー、運輸、金融セクターを標的とした破壊的なサイバーキャンペーンだと考えるのは論理的帰結でしょう。これは、これらのセクターに対して過去に行われた小規模な破壊的行動（2020年、2021年後半、2022年初頭、そして（おそらく）2022年後半）と、2024年の後者の2つのセクターを狙った活動に基づくものです。破壊的なキャンペーンではないにしても、Insikt Groupは、台湾のネットワークから広く事前配置について開示されると予想しています。より一般的には、中国は引き続きサイバー能力を使用して、台湾やアメリカや日本などの仮想敵国の政策と準備を偵察すると考えられます。

*Recorded Future*のレポートには、米国インテリジェンスコミュニティー（*ICD*）*203*：分析基準（*2015*年*1*月*2*日発行）と一致する可能性のある表現が含まれています。また*Recorded Future*のレポートでは、米国インテリジェンスコミュニティーが採用する信頼レベル基準を使用して、分析的判断の裏付けとなる情報源の質と量を評価しています。

Insikt Group®について

Recorded Future の脅威リサーチ部門である *Insikt Group* は、政府、法執行機関、軍、諜報機関に深い経験を持つアナリストとセキュリティ研究者で構成されています。彼らの使命は、お客様のリスクを軽減し、具体的な成果を実現し、ビジネスの中断を防ぐインテリジェンスを生み出すことです。

Recorded Future®について

*Recorded Future*は世界最大規模のインテリジェンス企業です。当社のインテリジェンスクラウドは、攻撃者、インフラストラクチャ、標的に関する包括的なインテリジェンスを提供します。オープンウェブ、ダークウェブ、技術ソースにわたるインターネットをインデックス化して、拡大傾向にあるアタックサーフェスと脅威状況をリアルタイムに可視化し、お客様が迅速かつ確信を持ってリスクの軽減と安全なビジネス遂行に取り組めるように支援します。ボストン本社および世界各国のオフィスに従業員を擁し、*75*か国以上で*1,800*社を超える企業と政府組織と連携して、バイアスのかかっていない実用的なインテリジェンスをリアルタイムで提供しています。

詳細については、*recordedfuture.com*をご覧ください。