THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

March 21, 2024

2023年次レポート

序文

私たちはこの年次レポートを作成するにあたり、二つの目標を掲げました。一つは攻撃者のプレイブック（戦略・戦術）に対する洞察的知見を提供すること、もう一つは将来想定されるシナリオを評価し、お客様の組織が合理的にそれらのシナリオに備えられるようにすることです。

2023年には、アタックサーフェス（攻撃対象領域）が拡大し、ソフトウェアのサプライチェーンの脆弱性が広範に悪用されたほか、
生成AIの利用拡大により、悪意のあるコンテンツが大規模に拡散する速度が速まりました。

攻撃者のTTP(戦術、技術、手順)のプレイブックから知見を獲得します。

このレポートは、2023年のインテリジェンスについて、業界で最も包括的に分析した内容となっています。その中では、現在のセキュリティ態勢における盲点をなくすべく、脅威アクター（攻撃者）とその標的、手法、攻撃のプレイブックが網羅されています。お客様にはその手口に関する情報が提供されます。

脅威アクターによる企業向けソフトウェアの大規模な悪用が確認できました。Fortra社のGoAnywhereやProgress Software社のMOVEitといったサードパーティのマネージド・ファイル転送（MFT）サービスに対するランサムウェア集団「CL0P」の攻撃などの例が挙げられます。

LinuxやmacOSシステムを標的にした攻撃ツールが増加しています。ランサムウェアのキットはWindows環境以外にも広がり続けており、被害者の範囲も拡大しています。

中国と関連のあるSpamouflage Dragon（Insikt GroupはEmpire Dragonとして追跡）のように、情報工作の向上のため、AIが生成した画像を国家が既に使用していることが確認できています。

2024年以降のロードマップにおいて、来るべき脅威に備えます。

本レポートでは、主な脆弱性、サードパーティの脅威、恐喝グループなどに関するRecorded Futureの今後の予測も掲載しています。お客様の脅威インテリジェンスへの取り組みがどの段階にあっても、このレポートをロードマップとして活用することができます。このレポートは各種業務を強化し、将来を見据えた戦略を策定するとともに、組織が保有するデータや知的財産、またブランドの評価を保護するのに役立ちます。

Ransomware groups will likely increase their targeting of technologies supporting hybrid and remote work.

The “phishing” landscape will become the “spearphishing” landscape as generative AI helps attackers create particularized lures.

The rise of passwordless logins will likely drive criminal activity away from infostealers and back to email-based credential harvesting.

Levi Gundert

チーフ・セキュリティ・オフィサー（CSO）

エグゼクティブサマリー

2023年は、予測とは異なる活動が確認できた年でした。一部で危惧されていた世界同時不況は現実化しませんでした。ウクライナの反転攻勢は、侵攻を続けるロシアとの紛争の流れを決定的に変えるものではありませんでした。イスラエルとサウジアラビアの和解に向けた動きは、10月7日のハマスによるイスラエルへのテロ攻撃、そしてガザ地区での新たな紛争の勃発によって大きく後退しました。ChatGPTをめぐる当初の触れ込みにもかかわらず、生成AIの本格的な応用の実現については、まだ数年先のことになりそうです。

こうした状況にあっても、Insikt Groupは、その混沌と不確実性に乗じてデータを窃取し、諜報活動を行い、地政学的な対立相手を混乱に陥れるサイバー脅威アクターを追跡し続けました。時には、これらの攻撃の目的がコンバージ（統合・複合）することもありました。中国政府に関連する脅威アクターらは、半導体業界における経済的・政治的な優位性を獲得するため、ますます台湾の半導体企業を標的にするようになりました。同時に、利益を追求するアクター（行為者）は、ハクティビズムの急増に乗じて、ツール（DDoS-as-a-serviceなど）を販売したり、「ハック＆リーク」作戦を収益化したりしました。

2023年は企業向けソフトウェアハックの年

「ゼロ・トラスト」は企業セキュリティの流行語になってるかもしれませんが、実際には、インターネットはこれまで以上に「信頼」に依存しています。リモートワークの時代となり、「as-a-service」の企業向けソフトウェア、共有クラウドインフラ、仮想化ワークスペースの採用が加速しました。結果として、セキュリティを重視する企業でさえ、仕事をこなすために、膨大な数のサードパーティ・サービスやツールに依存するようになっています。

サイバー犯罪者は、相互接続化が加速する現在の環境を利用して、ますます攻撃を強めています。企業向けソフトウェアにおける武器化された脆弱性の数は、前年比4倍に増加しました。2023年は特に、企業保有のシステムやサービスを標的とした一部の攻撃において、データ流出に見舞われたセカンドパーティやサードパーティの数が多かったことが注目されます。同年5月に発生したMOVEit File Transfer Applicationの悪用がその一例です。MOVEitの背後に存在したランサムウェア集団であるCL0Pは、このハッキングだけで7500万～1億ドルの利益を得たと推定されており、この種の攻撃が2024年まで続くことを示唆しています。

脅威アクターが信頼あるテクノロジーやサービスを悪用する方法は、企業向けソフトウェアを利用したものに限りませんでした。Recorded Futureが行ったある調査では、メッセージングプラットフォームやクラウドサービスといった正規のインターネットサービスの悪用が、マルウェアファミリーの約25%で検知されています。こうした悪用により脅威アクターは、通常のトラフィックに紛れて自らのコマンド＆コントロール（C2）通信を隠蔽することができるようになります。また、脅威アクターがLinuxやmacOS用の不正プログラムを攻撃シーケンスに組み込む事例が増えています。これにより、攻撃者は今まで比較的安全とされてきた環境も含め、より多様なシステムでランサムウェアを展開できるようになります。さらに脅威アクターは、ビジネスプロセス組織（BPO）に侵入し、SIMスワッピングやその他のソーシャルエンジニアリング詐欺も容易にしました。

主な調査結果

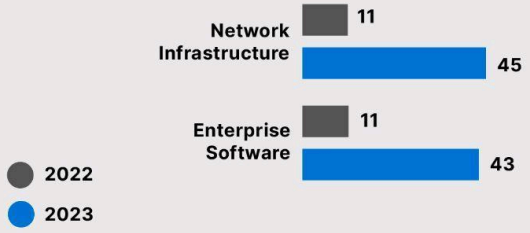
- アタックサーフェス（攻撃対象領域）の拡大により、脆弱性を大規模に悪用する機会が増えています。つまり、2023年を通じて、サードパーティ製品に存在する1つの脆弱性につけこみ、複数の被害企業を攻撃できるような脆弱性を好む脅威アクターが増加しているのです。ハイブリッドおよびリモートワークの環境が継続されていることが、この傾向を助長しているようです。
- 生成**AI**の初期の悪意ある利用については、ソーシャル・エンジニアリングと影響力工作に焦点が絞られました。つまり、生成AIの悪意ある利用のユースケース（使用事例）が、説得力のある詐欺的なコンテンツの大量作成を後押ししたのです。ダークウェブで販売されている大規模言語モデル（LLM）の修正バージョンが、正規ツールの安全ガードレールをユーザーが回避することを容易にしてしまいました。
- 依然として、ソフトウェア・サプライチェーン攻撃が蔓延しています。ソフトウェアの相互依存性が高まっているため、二重のソフトウェアサプライチェーン侵害が初めて確認されるなど、脅威アクターが新たな方法でサードパーティおよびフォースパーティの依存関係を悪用することができるようになりました。
- サイバー犯罪者は、ソーシャル・エンジニアリングを容易にするため、ビジネス・プロセス組織を標的にしました。具体的には、ビジネス・プロセス・アウトソーシング（BPO）を利用したソーシャル・エンジニアリング詐欺を通して、SIMスワッピングなどの詐欺を容易に行えるようになりました。
- 信頼されてきたツールが、合法的なインターネットサービスを通じて悪用されています。脅威アクターたちは組織のインフラにアクセスし、かつ発見されないようにするために、信頼あるツールやサービスをますます悪用するようになりました。これには、コマンド＆コントロール（C2）のためのクラウドサービスの悪用も含まれます。
- 規制の乱用は定着しませんでした。ランサムウェアや恐喝キャンペーンの事例では、被害者に対して支払いを迫るために、規制当局に攻撃者が自ら侵害を報告するなどの方法が試みられました。しかし、その後の政府による監視の強化により、攻撃者はこの恐喝手法を再考するようになったとみられます。
- 攻撃ツールは、**Linux**や**macOS**システムを標的にするケースが多くなっています。ランサムウェアのキットはWindows環境以外にも広がり続けており、被害者の範囲を拡大する機会をも提供しています。
- ガザでの戦争は、混乱に乗じてハクティビストの活動を活発化させました。そのほとんどの主張は虚偽または誇張されたものでしたが、ハクティビストの活動は、10月7日のテロ攻撃を取り巻く恐怖と混乱の一因となりました。ハクティビストはエクスプロイト、「雇われDDoS」（DDoS-for-Hire）やその他のサービスを販売することで、自分たちの大義に対する「草の根」レベルの関心の高まりをますます悪用しようとしています。
- フィッシングの手口が進化する一方、初期アクセスにおいて有効なアカウントが使用されるケースが増えています。フィッシング防止策が高度化する中、脅威アクターは、新たなフィッシングの手口や、有効なアカウントを含むその他の初期アクセス・ベクトル（アクセス方法）を採用することでそれに適応してきました。
- イデオロギーグループ間の「影響力工作のナラティブ（物語）」が統合されつつあることが確認できます。2023年の特徴として、中国による影響力工作で使用されるナラティブと、ロシアの偽情報エコシステムや米国国内の暴力的過激派に由来するナラティブとがますます統合されつつあり、同時にオルトテック・プラットフォームでの存在感も増していることが挙げられます。

目次

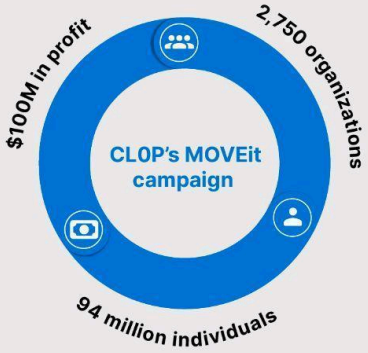
2023 by the Numbers

Increased Attack Surface Drives Mass Exploitation

Internet-facing appliances are a threat actors' best friend. This year saw an **increase in network infrastructure and enterprise software exploits**.



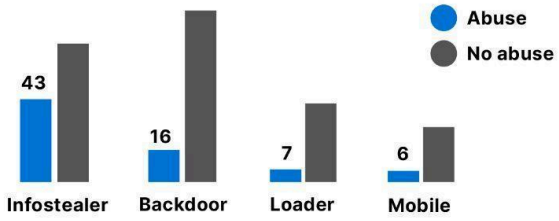
Called **"the biggest hack of 2023"**, CL0P's MOVEit campaign had far-reaching effects for organizations and industries globally.



Exploits of Legitimate Internet Services Take Advantage of Trust

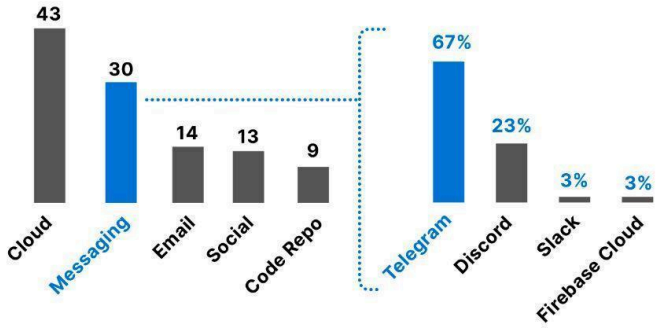
Malware

Infostealer malware most commonly exploited legitimate internet services (LIS). Among abused LIS, cloud services were the primary target, closely followed by messaging apps.



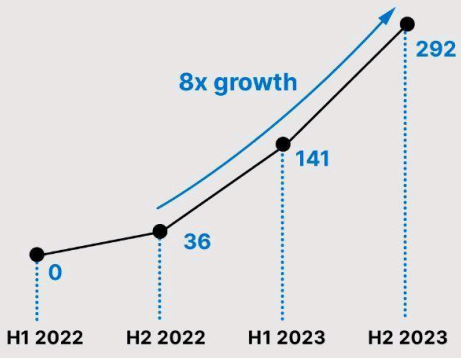
Services

Within messaging we can see Telegram and Discord are the leaders, but **Telegram is by far a fan favorite for attackers**.



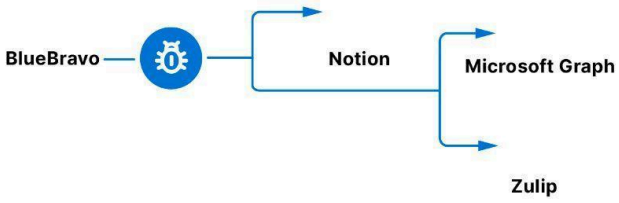
Hacktivist Resurgence

Mentions of DDoS-as-a-Service



DDoS-as-a-service mentions became significantly more common in the second half of 2023.

Examples of an APT abusing LIS



Active Hacktivist Groups
First 18 days

103 hacktivist groups were active within the first few weeks of the war in Gaza, compared to 25 active in the same time period following the invasion of Ukraine.

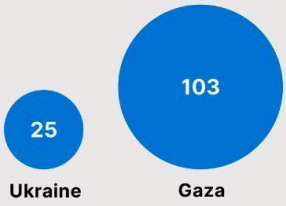


図1: 2023年のサイバー脅威における主要テーマ関連指標

セクション1：ステージ設定――技術、地政学、経済学、政策

主な技術トレンド

生成型人工知能（AI）をめぐる普遍的な議論を抜きにして、2023年の技術開発の動向を語るのはほぼ不可能です。特に、2022年11月にOpenAIがChatGPTをリリースした後においては、その状況はより一層明確になっています。ChatGPTの直接的な用途は、顧客対応AIチャットボットを導入するグローバル企業向けから、医療関連分野の研究向けまで多岐に渡ります。また、マイクロソフトによるExplainable Boosting Machines（EBM）の研究や、あるモデルがどのように結論に至ったかをユーザーに理解してもらうため透明性を重視したAIモデルなど、さまざまな種類のAIモデルの開発も見られました。こうした人工知能の動向、特に脅威アクターがAIをどのように利用しているかについては、本レポートの「サイバー脅威の進化」のセクションでさらに詳しく説明しています。

2023年には、クラウドコンピューティングや生成AIといったサービスに対する需要が高まり、ベンダーはコンピューティング能力の向上を求めるようになりました。ほとんどの企業は、少なくとも2つのInfrastructure-as-a-Service（サービスとしてのインフラ）にアプリケーションを導入していると報告しており、その半数近く（47%）が、自社への新しいアプリケーションの導入に際してはクラウドファースト戦略に則っているとしています。報告によると、現時点の予測では、OpenAIは顧客の需要を満たすために、3万弱のGPU（グラフィック・プロセッシング・ユニット）が必要になると見込まれています。需要を満たすためにクラウド・サービス・プロバイダー（CSP）が拡大することは、クラウド・コンピューティング・データセンターの集積地となっている東南アジアのような特定の地域が、テクノロジー業界全体にとって戦略的に重要な拠点になるという意味を帯びます。

テクノロジー製品、特に顧客対応アプリケーションにおけるもう一つの傾向としては、マジックリンク方式をはじめとするパスワードレス認証の提供の増加が挙げられます。セキュリティとユーザーの利便性を両立させるため、一部の企業では、例えばマイクロソフトなどのアカウントへのログインについて、ユーザー、さらには従業員に対してさえも、受信トレイに配信されるリンクの使用を通して許可するようになりました。マジックリンクの使用はGoogleが発売したパスワードレス製品に付随するもので、現在、ユーザーは携帯電話の認証方式を使ってGoogleアカウントにサインインできるようになっています。

地政学的事象――グローバルな紛争が戦略的パートナーシップを再構築する

ロシアの本格的なウクライナ侵攻は2年目に突入し、双方が領土を獲得・奪還するために、そして揺らぐ世界の関心を維持するために戦闘する段階に入りました。2023年に入ってからも戦闘状態は収まらず、ロシア、ウクライナ両国ともにリソースの枯渇や人員不足の懸念を抱え、軍事攻勢面でも現時点では思うような成果を上げていません。ウクライナにとっては、2023年の外国からの支援は前年よりも不透明なものとなりました。ウクライナに対するNATOの「揺るぎない」支持は、2023年にはEU加盟国がウクライナへの支持を表明する一方、米国の資金援助が連邦議会の紛糾により停滞したため、条件的にトーンダウンしました。他方でロシア政府はイラン、中国、北朝鮮のパートナーに働きかけて、兵器の輸送ルートと兵站を確保しました。ロシアは2023年以降、着実に地歩を固めつつあります。引き続き防衛産業基盤（DIB）への資金注入を行っており、その投資額はソビエト連邦崩壊以降の最高水準に達しています。

NATO加盟国からの支援の維持に腐心するウクライナを一層苦しめているのは、2023年10月7日にハマスのテロリストが行ったイスラエルへの物理的攻撃をきっかけとしたイスラエル・ハマス紛争という、もうひとつの地政学的紛争

の脅威です。この攻撃に対してイスラエルは、米国から30億ドルの軍事支援を受けて、ガザ地区で軍事作戦を開始しました。現在進行中の紛争を特徴づけているのは、地域的な戦闘激化への懸念です。特に、イランが支援するレバノンの民兵組織ヒズボラを筆頭とする、イランの代理勢力による地域的紛争地点での戦闘を考えれば、そのことは明らかです。一方、ロシアはこのテロ攻撃を機に、中東におけるアメリカの外交戦略の失敗が、暴力連鎖の直接的な原因であると捉え直しています。ロシア政府がイランとの結びつきを強めたことにより、かつては友好的だったイスラエルとの関係に亀裂が生じました。さらに、西欧（特に米国）の覇権主義に対するロシアのイデオロギー上の直接的な反発心が、改めて浮き彫りになっています。

中国は年間を通じて、反欧米感情を通じて結びつきを強めるロシアやイランとの戦略的パートナーシップを政治、経済、軍事面で推進しました。強固な貿易関係と地政学的利害の共有を通して、イランと中国は緊密な関係を築いてきました。中国は、ウクライナへの侵攻を続けるロシアに対し、軍事的・経済的支援を続けてきました。それでも、中国がウクライナ紛争に関して提示した「和平プラン」は、ロシアとの結び付きによって米国や欧州から疎外されないようにするための試みであることを示しました。他方、米国は中国を「競争相手」および「挑戦者」と見なし続けています。こうした両国関係は、昨年に実施したマイクロチップ技術に関する一連の関税措置や規制によって例証されています。

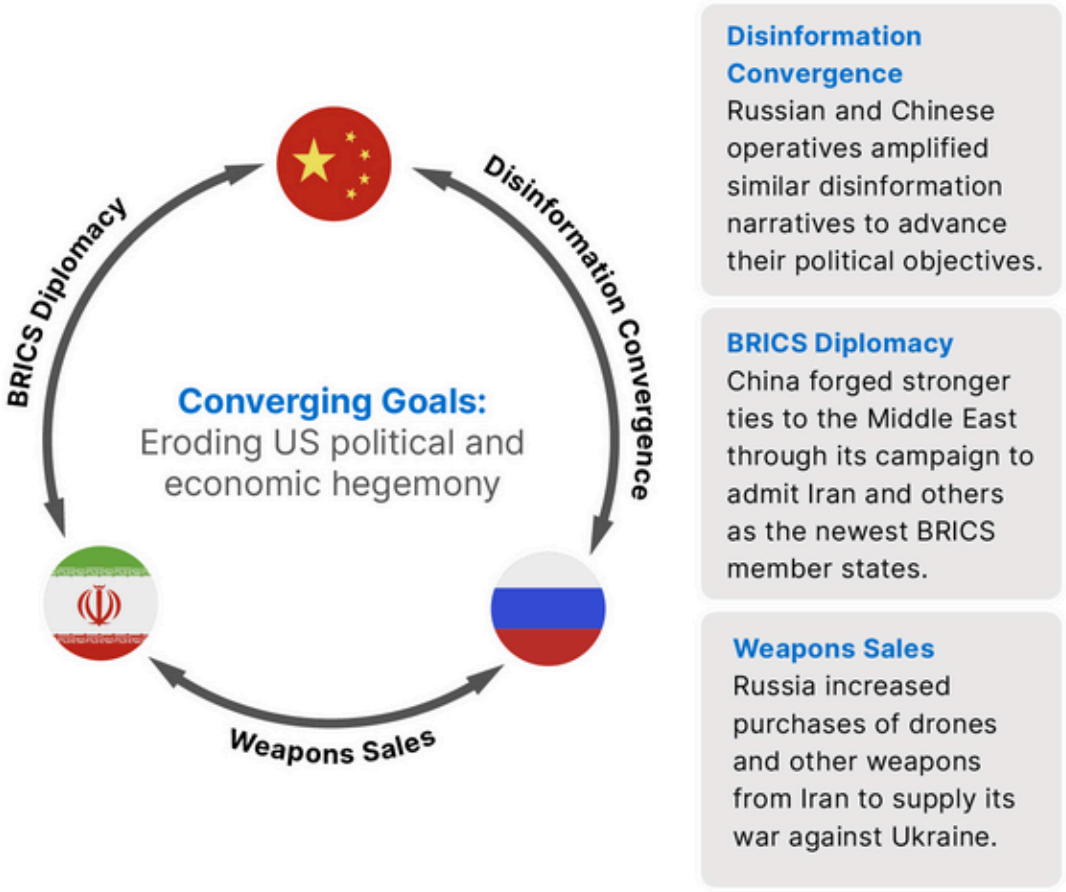


図2：ロシア、中国、イランの三国関係は統合された目標に基づいている

マクロ経済トレンド

マクロ経済は、2023年に入ってからは進行する世界的な健康危機、成長鈍化、地政学的不確実性、貿易相手の変化といった逆風に直面しました。同年第1四半期には大量解雇の波も襲い始めましたが、これは雇用側がそれまでの数年間の大量雇用の後、再調整の動きを加速させたためでした。この人員削減はテクノロジー部門に最も大きな打撃を与え、2023年には26万人の雇用が失われました。サイバー犯罪の点から見れば、失業者が急増することにより、求職者は雇用不安や求職プラットフォームを利用した詐欺キャンペーンにさらされることになります。また企業戦略的には、テクノロジー部門が人材とイノベーションの潜在的損失に見舞われる可能性が出てきます。

国際的なビジネスや企業の意思決定者は、地政学的な事象がマクロ経済に及ぼしているサイバーおよび非サイバーの影響と向き合うことを余儀なくされました。例えば、中国のサイバー諜報プログラムは、過去半世紀でより成熟、ステルス化し、組織化されてきました。中国のサイバー脅威集団は2023年、戦略的技術、防衛産業、政府関連、重要インフラなど、地政学的な対象に的を絞って攻撃をしかけてきました。これらの対象はすべて、中国が軍事的近代化と地域覇権を目指して推進している産業分野でもあります。欧米諸国によるロシアへの経済制裁が続くことで世界市場は分断され、サプライチェーンは緊張の度合いを増しています。ウクライナ支持派とロシア支持派に分かれる中、欧米市場とロシア市場のいずれかの選択を迫られ、ロシア市場からの撤退を決めた結果、サイバー攻撃やhack-and-leak（ハック・アンド・リーク）作戦の標的になった企業の例もあります。

サイバー政策の厳しい戦い

サイバーセキュリティ関連の法執行という意味で2030年は、ランサムウェアの恐喝ドメインに加え、ダークウェブのフォーラムおよびマーケットプレイスをはじめとするサイバー犯罪のテイクダウン（削除・閉鎖）が、顕著に活発化した年となりました。これは主に、長期に及ぶ捜査よりも直接的なテイクダウンに重点を置くという米司法省の明確な戦略に基づいています。こうしたテイクダウンは、米国、英国、ドイツなどの国々による国際的な協調と努力の成果でした。ただ、多くの摘発作戦がサイバー犯罪のインフラを解体することに成功した一方、結局はその代わりのものが出現しました。結果的には、これらの取り締まりの努力が、犯罪活動の水準を長期にわたって低下させることにつながるかどうか、あるいはそうした取り組みが国際的な強制力の誇示として機能するかどうかの判断には、引き続きの活動と観察が必要です。

2023年、特に米国では、運輸業界や医療業界などに影響を及ぼす、業界固有のサイバーセキュリティ規制が数多く導入されました。2024年にはさらなる規制が予定されており、https://therecord.media/hhs-proposes-cyber-requirements-for-hospitals例えば米国政府は、医療分野の事業体に対するサイバーセキュリティの最低衛生基準（他の分野別の取り組みを反映したもの）の導入を検討しています。しかし、おそらくこの年最も期待されたサイバー政策の成果のひとつは、2022年半ばまで遡る業界からのフィードバックを受け、「重要性」のあるインシデントを発生から4営業日以内に報告するよう対象事業体に求めることを内容とする証券取引委員会（SEC）の規制が最終決定に至ったことです。この規制の効果や意味合いはまだ完全には見えて来ないのですが（特に一部の米議員による再検討に直面しているため）、導入初期の影響としては、サイバー攻撃を報告した当日に株価が下落したと明かした企業の例があります。

その一方で、あらゆる産業でサイバーセキュリティの規制に焦点が当てられていることも確認されています。シンガポールのサイバーセキュリティ法では当初、重要インフラ産業（CII）の規制に重点が置かれていました。しかし、同法については2023年後半、CIIに対する要件をさらに追加する一方で、より多くの非CIIの事業体を規制するべく、対象

範囲を拡大するための改正案が議会に提出されています。ブラジルでは、国営電気通信庁（ANATEL）が国内規制を更新し、対象事業体に対する既存の最低セキュリティ要件を厳格化し、パスワード規定やソフトウェアの脆弱性更新情報などに関する具体的な要件を追加しました。どちらの国のケースも、重要な転機となったサイバーセキュリティ政策の実施初期において、効果的に規制するにはサイバーセキュリティ要件の対象範囲が広過ぎたと考えられたため、各国政府がそれを微調整した例となっています。世界的な動きを見ると、国連のサイバー犯罪特別委員会が2023年の交渉会合を経て、サイバー犯罪と闘うための国際的な法的基準を定めようとしたのですが、最終的な条約文の採決に至りませんでした。つまり、同委員会は、実行可能な国際条約を成立させるために、会期の延長を余儀なくされたのです。

加えて私たちは、サイバー脅威アクターが極端な恐喝戦術を用いた例を2件確認しました。その手口は、被害者をそれぞれの関係規制当局に通報するという内容でした。通報の口実は、脅威アクターが被害者を実際に侵害・攻撃できたことから、当該の被害者のサイバー防御は不十分であり、従って様々な規制を遵守していなかったのではないかというものです。それでも、私たちは、こうした恐喝戦術が一般的になる可能性は低く、世間の注目を集めることを目的としている可能性が高いと評価しています。この傾向については、本報告書の「恐喝の傾向」セクションで詳しく説明します。

セクション2：サイバー脅威インテリジェンス

悪用される脆弱性の変遷

アタックサーフェス（攻撃対象領域）の拡大が脆弱性を大規模に悪用する機会を増やす

脅威グループは2023年、特定のサードパーティツール（GoAnywhere、MOVEit、Citrix NetScalerデバイス）の複数の脆弱性を大規模に悪用し、数千の組織に広範な損害を与えることに成功しました。近年、集団攻撃・搾取に成功する事例が増えていることについては、部分的には2つの要素から説明できます。その要素とは、一つは企業のハイブリッド・ワークやクラウド・コンピューティングへの広範な移行により複雑化し、管理が難しくなっているアタックサーフェス（攻撃対象領域）であり、もう一つはゼロデイ脆弱性の開発・悪用など、自らの戦略や手口を改善し、巧妙化するランサムウェア集団です。一部のセキュリティリサーチャーは、この1年間に多数の大規模悪用イベントで標的になったような企業向けソフトウェアは、リアルタイムのパッチ展開には適さない定期的メンテナンスサイクルを通じて更新されるため、格好の餌食になるとも指摘しています。

この年最も注目を集めた悪用例は、CL0Pランサムウェア集団（CL0P）が、FortraのGoAnywhere MFTとProgress SoftwareのMOVEit MFTという2つのサードパーティのマネージドファイル転送（MFT）サービスに対して行った大規模攻撃です。特に懸念されるのは、事例研究によると2023年5月から2023年8月中旬にかけて、MOVEitに対するCL0Pの攻撃だけでも2,750社におよぶ企業と約9,400万人もの個人に悪影響を与えたと推定されていることです。CL0Pはまず、これらの攻撃を可能にする脆弱性について、その開示とパッチ適用前にゼロデイ攻撃の形で悪用しました。さらに、組織がシステムの脆弱性を特定してパッチを適用するのに手間取る一方で、脆弱性が修正された後にも当該の脆弱性を組織的に悪用しました。CL0Pが脆弱性の開示とパッチ適用に先行してゼロデイ攻撃の手法を開発したことが、脆弱性の開示後においても、それらの脆弱性の引き続きの悪用を成功させる後押しをしたとみられます。

大規模悪用のもう一つの顕著な例としては、2023年8月から12月にかけて、国家とランサムウェアの両方の脅威アクターがCitrix Bleed（CVE-2023-4966）を悪用してNetScaler ADCとNetScaler Gatewayデバイスに影響を及ぼし、数百の組織への攻撃を成功させた例が挙げられます。繰り返し強調すると、報告された攻撃事例の大半を占めるのはやはり、LockBitギャング、Medusaギャング、ALPHVといった著名なグループを含むランサムウェア集団の活動によるものです。

大規模悪用を可能にする製品の脆弱性には、いくつかの共通点があります。この年に観察された集団的脆弱性悪用の各事例については、次のような共通した特徴がありました。

- こうした脆弱性は、インターネットに接続されているインフラを公開スキャンすることで発見可能であり、脅威アクターは容易にその脆弱性を発見し、エクスプロイトを展開することができます。
- これらの脆弱性は、ゼロデイとして公開されパッチが適用される前に悪用され、さらに公開後も、各企業がパッチ適用に苦闘する中で広範囲にわたり悪用され続けます。

ゼロデイ脆弱性が懸念される一方、大規模悪用のほとんどの事例では脆弱性が公開され、パッチが適用された後に攻撃が成功していることに留意すべきです。この傾向は、おそらく被害組織のリソースのレベルの違いを映し出しています。高度なセキュリティプログラムを導入し、ゼロデイ脆弱性の悪用に対抗するための挙動分析を行っている組織がある一方で、最も基本的な日和見的攻撃を防ぐために必要なパッチ管理対策の実施に至っていない組織も少なくありません。マイクロソフトの最近の調査では、強力なパッチ管理プログラムの維持、ゼロトラスト原則の適用、XDR（拡張検知・対応）ソリューションの使用、MFA（多要素認証）の使用といった基本的なセキュリティ対策によって、サイバー攻撃の99%を防ぐことができるとしています。

繰り返し悪用された技術製品タイプ

仮想化の進展とクラウドへの移行により、狭隘化するベンダーのサプライチェーンへの依存度が高まり、企業環境に新たなセキュリティリスクをもたらしています。2022年の傾向と同様、脅威アクターは2023年も引き続き、マイクロソフト、グーグル、アップル、シスコといった主要ソフトウェア・ベンダー各社のオペレーティング・システムの脆弱性を標的にしました。しかしながら、2022年に観察された高リスクの脆弱性悪用事例と比較すると、2023年には、企業のソフトウェアやネットワークインフラの脆弱性を標的とした能動的な悪用の例が増加していることが観察されました。図3を見ると、2023年には、企業向けソフトウェアに対する攻撃で悪用された脆弱性の数が件数ベースでも、標的とされたソフトウェア別でも、2022年と比較して約290%増加したことが示されています。こうした製品は企業環境で広く使用されていたるめ、危険性の高い脆弱性の悪用を通じて、企業環境やランサムウェア集団が欲する機密データへの不正アクセスが広く行われる可能性があります。同様に、ネットワーク・インフラに対する攻撃で悪用された脆弱性の数は309%増加しています。

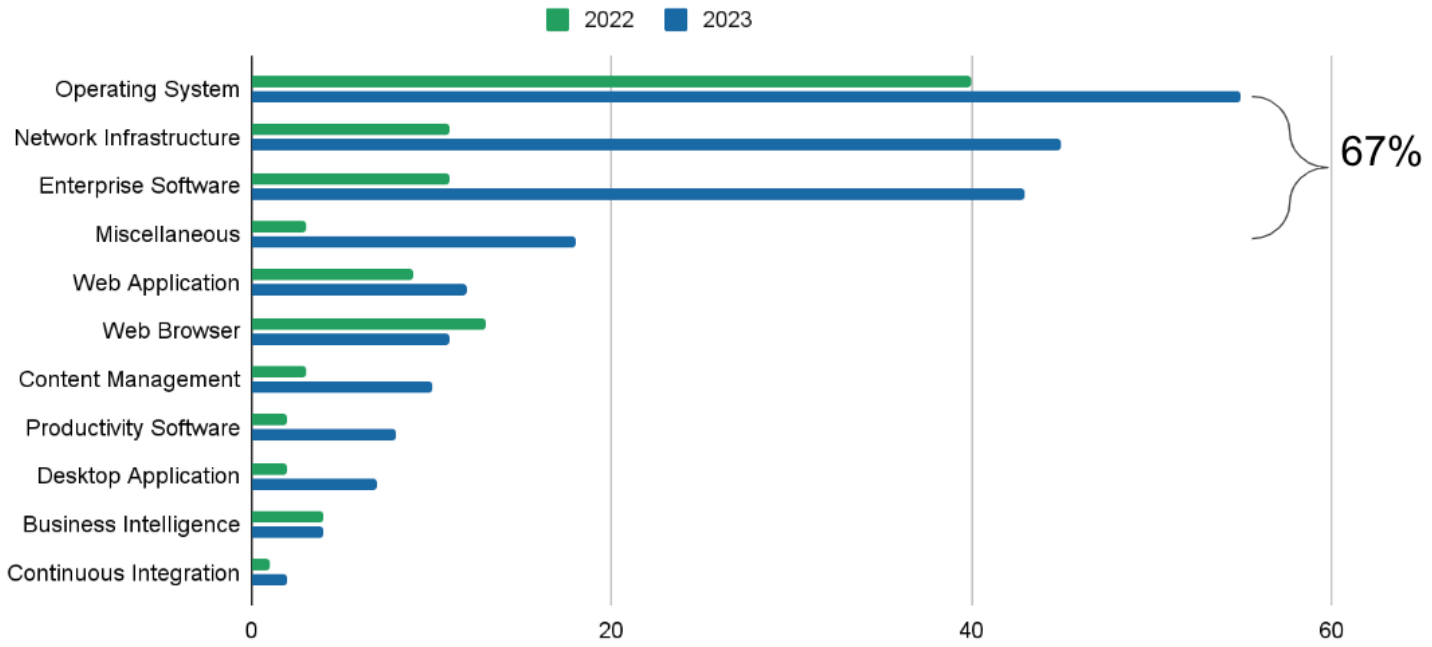


*図**3**：Recorded Future® Intelligence Cloudにおいて2022年と2023年に能動的に悪用された高リスクの脆弱性*

一部のランサムウェア脅威アクターは、恐喝オペレーションの一環として、意図的にファイル転送ソフトウェアの脆弱性を狙いました。この傾向の最も顕著な例は、CVE-2023-34362 に対して脆弱なProgress Software MOVEit Transferのインスタンスを標的としたCL0Pのデータ盗難キャンペーンです。その他にも、CL0P、ALPHV、LockBitによる、GoAnywhereのセキュアなマネージド・ファイル転送（MFT）ソフトウェアに悪影響を及ぼすCVE-2023-0669の悪用や、Reichsadlerによる、Progress SoftwareのWS_FTP Serverにおける CVE-2023-40044の悪用といった類似例がありました。さらに、IceFireとBuhtiは、IBMのAspera Faspexファイル共有ソリューションに影響を及ぼすCVE-2022-47986の悪用を行ったことが確認されています。こうした例が示す通り、ファイル転送プラットフォームは、明らかにランサムウェア集団の標的になっています。ファイル転送プラットフォームには大量の機密データを含めることができるため、組織が大規模に侵害される可能性があります。

2023年には、新たに特定されたUNC4466などのALPHVランサムウェア・ギャングも、バックアップ・ソフトウェアの脆弱性を悪用し、ネットワークへの初期アクセスを行いました。UNC4466 は、中小企業向けのデータ復旧ソリューションであるVeritas Backup Execを標的とし、2021 年にパッチが適用された3つの脆弱性を悪用しました。キューバ・ランサムウェア・ギャング（Cuba Ransomware Gang）は、仮想環境向けに開発されたVeeam独自のバックアップ・ソフトウェアであるVeeam Backup & Replicationを標的とし、新たな脆弱性ではあるものの既にパッチが適用されているCVE-2023-27532の悪用を通して、米国の重要インフラ組織や中南米のIT企業を攻撃しました。このCVE-2023-27532には2023年3月にパッチが適用されましたが、キューバ・ランサムウェア・ギャングは2023年6月に攻撃キャンペーンを行っています。脅威アクターはCVE-2023-27532を悪用することにより、コンフィグファイルから認証情報を抽出することができるため、バックアップ基盤ホストへのアクセスが可能になりました。

進化するサイバー脅威

*生成**AI**の初期の悪用は、ソーシャル・エンジニアリングと影響力工作に焦点を当てている*

生成AIはパラダイムシフトを起こす新技術であり、既に広く使われています。例えば、スマートフォンユーザーの95%以上は、AlexaやSiriのような音声アシスタントを通じてAIを利用した経験があります。2023年には生成AIがブレークし、新サービスが急増しました。攻撃の防衛側は脅威インテリジェンス、インシデント対応、コードへのパッチ適用のためにAIを実験的に使用してきましたが、一方でサイバー犯罪者や国家レベルの脅威アクターは、AIを使用して自らの戦術を可能にし、増幅させる新しい方法を試みています。

現在の生成AIに関する最も明確なリスクは、各種オペレーションへの影響力工作、ソーシャルエンジニアリング、データプライバシーの侵害、さらに知的所有権の侵害に関係しています。セキュリティリサーチャーは、脅威アクターがAIを搭載したチャットボットを使用して説得力のあるフィッシングメールを作成し、詐欺行為をサポートしているほか、電子商取引業者の不正防止システムを分析して、支払い詐欺を後押ししていることを確認しています。よりセンセーショナルな想定としては、AIが複雑なサイバー攻撃戦略を自律的に開発し、実行するといった脅威が挙げられますが、まだ概ね想定・推測の域を出ておらず、現実世界で観測されたことはありません。

まだ十分に理解されていない新たな懸念は、検閲されていない大規模言語モデル（LLM）が悪用される可能性です。インディアナ大学が2023年末に行った調査によると、一般にはChatGPT Plusに似たサブスクリプション・サービスとして宣伝されていた悪質なサービス向けのLLMが14件、ダークウェブで宣伝されていた悪質なオープンソースのLLMプロジェクトが198件、発見されました。これらのモデルの多くは、マルウェアやフィッシング・メールを作成したり、すぐに使える詐欺サイトを構築したりする能力を喧伝しています。しかし、ここで再確認しておきたいのは、AIが作成したマルウェア、フィッシング、詐欺サイトの現実世界での使用や影響については、まだ決定的かつ包括的な研究は行われていないということです。

脅威アクターがいずれAIを悪用してより高度な攻撃を行うようになることはほぼ確実ですが、その能力が成熟するには時間がかかるでしょう。サイバー空間の合法的な実務者と同様、脅威アクターたちも、2023年にはハルネーション（もっともらしい誤情報の生成）、処理能力、コンテキストウィンドウの制限、さらに問題・分野に特化したデータセットの必要性など、生成AIの限界と格闘しなければならなかったのはほぼ確実です。高度なサイバー脅威工作にAIを効果的に統合するという複雑な作業を行う際には、今やほぼどこにでもあるLLMへのアクセスの方法だけではなく、LLMがどのように機能するかについての深い理解と、LLMを使用するための独自のスキルセットが必要となります。また、脅威アクターがLLMを真に高度なサイバー工作に利用できるようになるには、高度なプロンプト・エンジニアリング技術の知識と、大規模なコンテキスト・ウィンドウを処理できるモデルへのアクセスを必要とします。その結果、サイバーセキュリティ・コミュニティにとっては、このような新たな脅威に備え、適応する好機が到来している。脅威アクターがAIを活用した工作を成熟させるために必要な時間軸は、脅威の種類によって大きく異なるとみられます。国家を後ろ盾とする脅威アクターはほぼ間違いなくAIを採用済みであり、サイバー犯罪者も、より高性能なマルウェアを開発するために、AIの高度な利用方法を試していることでしょう。

サードパーティの脅威

ソフトウェアサプライチェーンへの攻撃は依然として蔓延し、進化し続けている

Insikt Groupは2023年、ソフトウェアサプライチェーン攻撃の報告件数が前年比11.8%増になっていることを確認しました。PyPI（Python Package Index）やnpm（Node Package Manager）といったパッケージマネージャーは、サイバー犯罪の脅威アクターが最も頻繁に標的とする技術であり続けました。これは、脅威アクターがインフォスティーラー（情報窃取型マルウェア）を配置する際、ソフトウェアのサプライチェーンサイクルの開発段階に焦点を当てていることを示唆しています。また、北朝鮮の脅威アクターは、3CX、Jetbrains、CyberLinkのソフトウェア製品を標的としたマルウェアの展開を通して、サプライチェーン攻撃が、地政学的な目的を支援する国家的な諜報や窃取などの工作活動にいかに役立つかを実証しました。

脅威アクターはソフトウェアサプライチェーンを侵害する際、正規のパッケージになりすます手法をはじめとする既知のテクニックを引き続き使用しており、そのテクニックを広範に悪用して、マルウェアの配布や情報や暗号資産の窃取を行いました。とはいえ、私たちは攻撃ベクトルの進化を示す2つの傾向を見出しました。1つ目は、2023年を通じて、脅威アクターが悪意のあるパッケージを隠蔽し、感染の可能性を高めるために、新たなテクニックを使用していたことです。これには、PyPIに対するおそらく最初のサプライチェーン攻撃が含まれており、難読化のために実行するPythonバイトコード（PYC）を悪用しています。PyPIが標的に選ばれた理由は、セキュリティ製品がPythonソースコード（PY）ファイルのみをスキャンすることが多く、さらにはPYCを使用することで、悪意のあるコードがフラグを立てられブロックされるのを防止できるためであると思われます。また、脅威アクターは、過去バージョンのパッケージマネージャーの巨大数に関連付けられ、かつ放置されたAmazon S3バケットも使用して、データ窃取マルウェアを拡散させました。このようなバケットのキャパシティ（最大能力）を利用したのは、工作規模を拡大するためだと思われます。

上記のソフトウェア・サプライチェーン攻撃では、そのような攻撃の多くが有する「1対多」の性質が強調されていますが、攻撃者はより標的を絞った方法でもソフトウェア・サプライチェーンを悪用することができます。サイバー犯罪者は2023年に初めて、銀行セクターを標的としました。この攻撃では、標的となった銀行のオンラインリソース内の特定のコンポーネントに悪意のある機能をアタッチし、データをインターセプトして顧客のログイン情報を盗むように設計されたnpm（Node Package Manager）のパッケージが使用されています。

最後に、2023年には、ソフトウェアのサプライチェーンが二重に侵害されるという初の事例が発生しました。これは、3CX Desktop Appソフトウェアを標的としたサプライチェーン侵害攻撃で発生したもので、北朝鮮の国家的脅威アクターであるLazarus Groupの活動によるものとみられています。このLazarus Groupによる3XCの侵害は、Trading Technologiesのウェブサイトにホストされ ているX_TRADERトレーディング・プラットフォームのトロイの木馬化されたソフトウェア・インストーラーを含めた、以前のソフトウェア・サプライチェーン侵害によって開始されたといわれています。これらを総合すると、ソフトウェア・サプライチェーンへの脅威の状況においては、企業はセキュリティ戦略に関して、サードパーティおよびサードパーティの依存関係を考慮する必要にますます迫られているといえます。

犯罪者はソーシャル・エンジニアリングを容易にするため、ビジネス・プロセス組織を標的にする

2023年には、サイバー犯罪者がビジネス・プロセス・アウトソーシング（BPO）組織を特に標的とし、ほぼ間違いなく金銭的動機に基づいて攻撃を行うという事例が複数確認されました。BPO組織は、サプライチェーンにとって極めて

重要な存在であるため、サイバー犯罪者の格好の標的になり得ます。脅威アクターは、BPO組織を標的にすることにより、単一の侵害ポイントを通じて多くの川下の顧客を侵害する能力を高めることができます。

具体的には、例えばScattered Spiderは、侵害された電気通信やBPO環境から携帯電話会社のネットワークにアクセスし、SIMスワッピングを実行し、暗号資産の窃盗といった直接の被害者以外への犯罪活動をさらに進めようとしました。近年増加しているSIMスワッピング攻撃の動機は、BPOが電気通信事業者と密接な関係にあるため、ほぼ間違いなくBPOへの攻撃の急増に繋がります。2023年にBPOが攻撃のターゲットになったことについて、考えられるもう一つの要因は、BPOによる企業データへのアクセス増加です。各企業は、コストを最適化し、専門スキルを利用し、事業継続性を確保するための選択肢として、BPOの活用を加速させています。BPOの市場規模は、2023年から2032年の間に2668億ドルから5448億ドルに成長すると予想されていることから、このセクターを攻撃の標的にするケースも、今後10年間で増加する可能性が高くなっています。

信頼あるツールが合法的なインターネットサービスを通じて悪用される

2023年に脅威アクターたちは、正規のインターネットサービス（LIS）を悪用してマルウェアを実行できるようにするとともに、C2通信を正規のトラフィックに紛れ込ませることで、検知される可能性を低下させました。最近のInsikt Groupの調査によると、400を超えるマルウェアファミリーのうち約25%が、C2インフラの一部として、何らかの形でLISを悪用しています。インフラのセットアップが容易であることから、データ窃取を目的としているインフォスティーラーが、C2インフラ用にLISを使用する可能性が非常に高くなっています。最も悪用されたLISはクラウドストレージプラットフォームで、次いでDiscordやTelegramなどのメッセージングアプリケーションとなっています。支払い詐欺も、脅威アクターによるLISのもう一つのユースケースとなりました。特にMagecartのEスキマー（Webスキマー）のペイロード（コード本体）を中継し、窃取したデータを流出させる場合に使用されています。2023年には、GitHubもよく悪用されるプラットフォームとして取りざたされました。

現在、比較可能なレポートやデータセットが存在しないため、LISの悪用事例の定量化を行うことは困難であり、明確な傾向を提示することさえできません。それでも、脅威アクターがソフトウェアのサプライチェーンに焦点を当てるようになっていることが一因となって、LISの悪用が増加し、手口も進化している可能性が高いとみられます。近年、いくつかのマルウェアファミリーは、そのインフラストラクチャにLISを徐々に組み込んでいます。最近のコモディティタイプのインフォスティーラー・ファミリーや悪意のあるPyPIパッケージは、とりわけC2通信向けにLISを悪用することが一般的になっています。また、ReversingLabsは2023年12月、PyPIパッケージに隠されたマルウェアが、GitHubのコミットメッセージをC2目的で悪用するという新しい手法について報告しました。

また、国家レベルのグループは、マルウェア通信を隠蔽するための合法的なサービスの悪用という点で、創造性と技術の急速な革新性を示しました。Insikt Groupは2023年1月、BlueBravoに起因するマルウェアGraphicalNeutrinoが、C2のために米国のビジネスオートメーションサービスNotionを悪用したと報告しました。BlueBravoは、ロシアの国家レベルのグループであるAPT29やNOBELIUMと活動内容や手口が重複する脅威アクターです。その数ヵ月後の2023年7月と8月、パロアルト（Paloalto）のUnit 42とEclecticIQは、APT29がC2のための新しいテクニックを使用していることを確認したと報告しました。このテクニックは、マイクロソフトのグラフAPIと、オープンソースのチャットおよびコラボレーションソフトウェアであるZulipの悪用を伴うものです。

恐喝の動向

規制の乱用は定着せず

2023年に米国と欧州の規制当局が新たなサイバー攻撃情報開示規則を定めたことにより、恐喝集団の手口が広範に変化することが懸念されました。しかし、今のところそのような変化は起きていません。米国では2023年7月、証券取引委員会（SEC）が上場企業に対し、業務に「重大な」影響を与えるサイバー攻撃が発生してから4日以内にその旨をSECに報告することを義務付ける新規則を提案しました。

その数ヵ月後の2023年11月、ランサムウェア集団のALPHV（BlackCat）が金融ソフトウェア会社MeridianLinkを標的とし、同社への恐喝予告をダークウェブのランサムウェア恐喝ブログに投稿した後、新しい開示規則に違反したとしてSECに通報しました。MeridianLinkはサイバーセキュリティ侵害があったことを確認しましたが（自社ネットワークへの具体的な不正アクセスはなかったとも主張）、一方で恐喝集団であるALPHVがMeridianLinkを規制機関であるSECに通報した時点ではまだ新規則が発効していなかったため、同社はSECの新規則に違反してはいませんでした。

MeridianLinkを攻撃したとする通報をALPHVが自らSECに行ったことを受け、サイバーセキュリティリサーチャーらは、他のランサムウェアグループもこの手法を実行しているか、あるいはALPHVがSECにさらなる被害者の通報を行っているかについて、その兆候を見出そうとしました。しかし、MeridianLinkの事案とSECの規制案が最初に公表されてから約2ヵ月を経ても、ALPHVとMeridianLinkが関わったような事例の報告は他には確認できていません。2023年夏には、別のランサムウェア集団が、攻撃者による身代金要求に応じない企業に対して、EUの包括的プライバシー法である一般データ保護規則（GDPR）違反の疑いで欧州の規制当局に通報すると脅しました。それでも、この手法が広く採用されたり、繰り返し使用されたりしている形跡は確認できていません。

LinuxとmacOSのシステムを狙う攻撃的ツールが増加

Microsoft Windowsが家庭環境と企業環境の両方で世界的に広く使用されているため、ほとんどのマルウェアや攻撃ツールは、macOS、Linuxやその他のUNIXライクなOSではなく、Windows OSを対象としています。しかしながら、報告によると、LinuxとmacOSシステムを標的としたサイバー攻撃とマルウェアは、2022年から2023年にかけて増加しています。Objective-Seeの報告によると、macOS環境を標的としたキャンペーンにおいて、少なくとも21の新たなマルウェア・ファミリーまたは亜種が出現しており、2022年の13という数字からは増加しています。トレンドマイクロの報告によると、Linuxのプラットフォームについては、2022年と2023年の両上半期を比較した場合、Linuxシステムにおけるランサムウェアの検出数は62%増えています。Rustのような複数のOSに対応するプログラミング言語を使用したマルウェア開発に移行している脅威アクターが存在しており、そのことが、macOSとLinuxの両方を標的とする脅威が増加している大きな要因であると考えられます。加えて、Linuxはサーバー、クラウド環境、重要なインフラストラクチャに広く普及してきており、機密データの窃取やサービスの妨害、大規模攻撃を試みる脅威アクターにとっては、そうしたLinuxの導入先は格好の標的となっています。特にこれらのプラットフォームのユーザー基盤が長期的に増大し続けていることから、攻撃者のTTPの変化は、脅威アクターの相変わらずの日和見主義、そしてターゲットになりうる対象を拡大したいという脅威アクターの願望を示唆しています。

Insikt Groupは2023年、敵対者が使用する可能性のあるツールやTTP（戦術・技術・手順）を分析したTTPインスタンスノートを公開しました。それによると、macOS、Linux、またはUNIX系のOSに関する記述が81件あり、2022年の17件から79%増加しています。2023年に公開された同様のTTPインスタンスノートのうち55件は、コード・リポジ

トリからダウンロード可能な攻撃ツールやエクスプロイト、あるいは野放し状態で観測されたマルウェア・サンプルに関するものでした。LinuxおよびUNIX系OSを標的とした攻撃的ツール（マルチプラットフォームツールやマルウェアを含む）について取り上げたTTPインスタンスノートは41件ありました。トレンドマイクロの調査と同様、LinuxおよびUNIX系OSを標的としたランサムウェアの蔓延がこれらのノートの中で浮き彫りとなった傾向の一つであり、例としてLinux、UNIXまたはESXiを標的とした22のランサムウェア・ファミリーが挙げられています。これらのファミリーのいくつかは、以前はWindows環境のみをターゲットとしていることが知られていましたが、2023年にはLinux、UNIXあるいはESXiの亜種がツールキットに加えられました。その亜種にはCactus、CL0P、Babuk、Monti、Akira、Agenda、Rhysida、IceFireが含まれています。私たちはBuhti、Dimorf、Ransomwhereなど、Linux環境のみを標的とするランサムウェア・ファミリーも確認しています。最後に、2023年に新たに発見されたNoEscapeのようなランサムウェアオペレーションについては、攻撃開始当初からWindowsとLinuxの両方のプラットフォームを標的としていたことも確認しました。

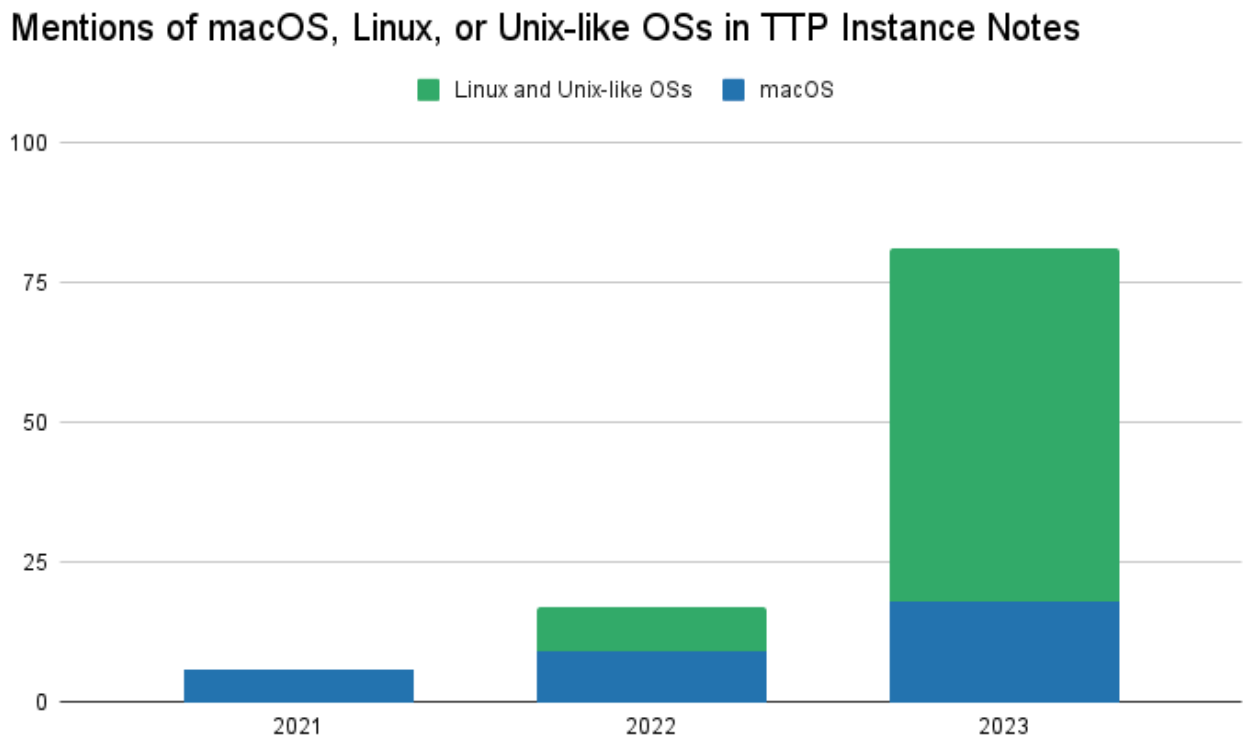


*図**4**：過去3年間のTTPインスタンスノートでmacOS、LinuxまたはUNIX系OSが言及された回数*
（出典：Recorded Future）

Insikt Groupは2023年、macOS環境を標的とした攻撃的ツールやエクスプロイトに関連する15のTTPインスタンスノートを公開しました。そのうちのいくつかは、前述のObjective-Seeの調査で強調されたマルウェア・ファミリー、すなわちTurtle、PureLand、JaskaGo、ObjCShellz、SparkRAT、XLoaderと重複していました。私たちは、2022年6月と2024年1月に、macOSの情報窃取者であるSparkRAT、MetaStealer、Atomicに関する個別のTTPインスタンスノートを公開しており、これらはすべてObjective-Seeの調査でも言及されています。また、CVE-2023-41993、CVE-2023-32407、CVE-2023-32422といったmacOSの脆弱性を標的としたPoCエクスプロイトも蔓延していました。

2023年、複数の脅威グループがmacOSマルウェアを攻撃用の武器として加えましたが、これは、ランサムウェア工作がLinuxやUNIX系OSにまで拡大しているのと類似した傾向です。Jamf Threat Labsの研究者は2023年11月、macOS向けマルウェア「ObjCShellz」について、北朝鮮を後ろ盾とするAPTグループ「BlueNoroff」に起因するものだと述べています。このグループは、暗号通貨取引所、ベンチャーキャピタル企業や銀行を標的とした金銭的動機に基づく攻撃で知られています。公開された報告によれば、ObjCShellzの出現は、BlueNoroff向けmacOSマルウェアへの新たな拡大傾向を意味しています。同様に、LockBitランサムウェアのmacOS亜種（バリアント）の最初のサンプルが2023年4月、公に表面化しました。現在までのところ、LockBit macOS亜種を含む攻撃は報告されていません。しかしながら、前述のサンプルは、この亜種がまだ実験的なものであることを示していました。つまり、このサンプルの実行パスワードは "test "であり、流出や永続化のテクニックは実装されていません。LockBitグループは、Linux/ESXiを標的にした最初の亜種が世に表面化するまで2年以上活動していたため、macOSの亜種はなお開発中である可能性があります。

ガザ紛争でハクティビストの活動が活発化―― 混乱を利用

2023年には進行中の地政学的な紛争、さらに新たに勃発した地政学的な紛争に関連したハクティビストの活動が加速しました。2022年にロシアがウクライナに侵攻した後、草の根の活動や国家主導の活動が急増したのと同様に、2023年後半にはハマスによる10月7日のイスラエル攻撃後の混乱に乗じて、新たなハクティビストの集団や同盟がかつてない勢いで出現しました。これらのグループはイスラエルとパレスチナ双方の組織・団体を標的として、DDoS攻撃、ウェブサイトの改ざん、データ漏洩攻撃を仕掛けました。Insikt Groupは、これらの脅威アクターは主として重要インフラ、緊急サービス、政府ウェブサイトへの侵害を主張していたものの、その圧倒的多数は虚偽であるか、または侵害の影響力が誇張されていると指摘しました。

しかし、AnonGhostがイスラエルのRedAlertアプリケーションを侵害し、近く核攻撃を行うとの虚偽の通知を送信させるなど、顕著な効果を示す事象がいくつか見られました。例えば、アノニマス・スーダン（Anonymous Sudan）がエルサレム・ポスト紙を攻撃してウェブサイトを停止させ、Cyber Av3ngersがアイルランドの地方都市の水道システムを攻撃しました。アイルランドの事例では、イスラエル製のOT機器が標的となり、2日間の断水が発生しています。イスラエルとハマスの戦争では、ハクティビスト集団を自称するMoses StaffとPredatory Sparrowが、休止状態から再び表舞台に現れました。特にPredatory Sparrowは、イランの重要インフラに対する効果的なサイバー攻撃で知られており、実際に2023年12月18日には、イランのガソリンスタンドの70%をオフラインにしたサイバー攻撃を首謀したことを認めています。

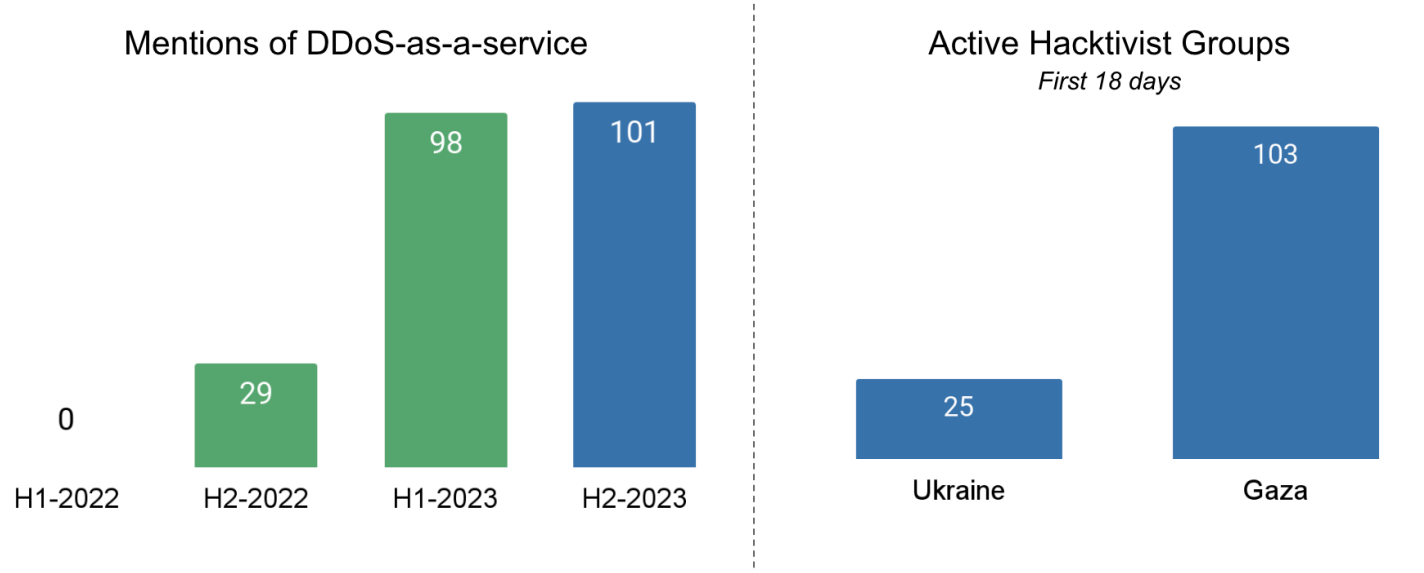


*図**5**：2022年から2023年にかけてのDDoS-as-a-serviceに関する言及回数と、ウクライナ、ガザ両紛争の最初の18日間に活動したハクティビスト集団の数（出典：Recorded Future）*

さらに、サイバー犯罪者たちは、地政学的な不安定さとハクティビズムに対する草の根レベルの関心をますます悪用しているようです。2023年後半のいくつかのグループは、伝統的にハクティビストよりもサイバー犯罪者に関連付けられてきたTTPを採用していました。こうしたグループは、特にイスラエルとウクライナの国民に影響を与える個人識別情報（PII）のような認証関連の漏洩情報を販売または共有しているほか、（Anonymous SudanとUserSecが行ったように）エクスプロイトや「雇われDDoS」（DDoS-for-Hire）サービスを販売するという、これまでに確認されている伝統的手法を継承しています。例えばKillnetは、暗号資産取引所の運営や、2023年1月と5月にそれぞれロシアのサイバー犯罪フォーラムとサイバー犯罪に焦点を当てた教育プラットフォームの両方を立ち上げるなど、ハクティビズムを金融、教育、イデオロギー系のサイバー犯罪のサイドプロジェクトにまで拡大し、一定程度の成功を収めていることが知られています。別の例を挙げると、2023年6月にアノニマス・スーダン、Killnet、REvilが欧州の金融機関を共同で攻撃する計画を発表していますが、その後そのような攻撃が行われたことは確認できません。

2023年に最も一般的だったハクティビズム関連のTTPは、DDoS攻撃、ウェブサイトの改ざん、インフラ侵害、一般向けアプリケーションの悪用でした。注目すべきは、親ロシア派のハクティビスト集団の活動が、DDoS攻撃やウェブサイト改ざんの報告にほぼ限定されているのとは異なり、中東や東南アジアを拠点に活動する数多くのハクティビスト集団が、hack-and-leakや脆弱性の悪用、さらには破壊的なワイパー型マルウェアの展開など、より広範なTTPを採用していることです。2023年12月、ウクライナ最大の通信プロバイダであるキーウスター（Kyivstar）に対してワイパー攻撃が行われ、同社は一時的な休業を余儀なくされました。当初はKillnetがこの攻撃を首謀したと主張していたのですが、その後、実はSolnstepek（ロシアのAPT SandwormやGRUと繋がりがあることで知られる）の活動による結果であったことが明らかになりました。これは、ハクティビストよりもロシアのAPTアクターの技術的能力が高いことを示しており、Killnetがこの攻撃に関連する恐怖、不確実性、疑念（FUD）を不当に利用しようとしたことをうかがわせるものです。また、ロシアのグループについては、攻撃者向けインフラストラクチャー・サービスの宣伝に一層、力を入れていることが確認されています。この動きは、そうしたグループが、より技術的に進んでいるロシア語のサイバー犯罪コミュニティに融合していることを示すもう一つの証であると考えられます。

フィッシングの手口が進化する一方、初期アクセスに有効なアカウントの利用が増加

2023年にInsikt Groupが観察した初期アクセスの手法うち、報告された攻撃の規模の大きさ、有効性、さらには新たに進化したトレンドの採用という点で際立っていたのは、フィッシング、外部リモートサービス、有効なアカウントの使用です。

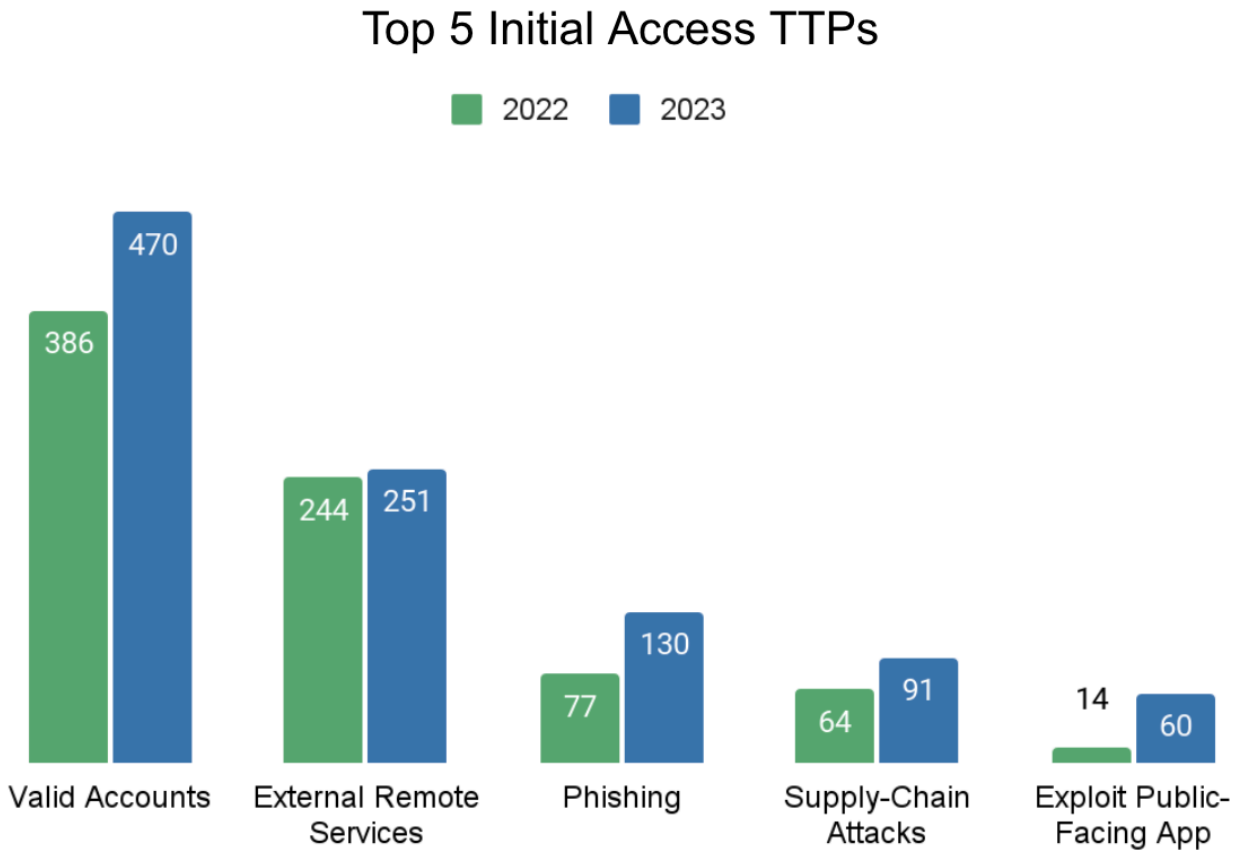


*図**6**：検証されたサイバー攻撃において初期アクセスに使用された上位5つのTTP（出典：Recorded Future）*

2023年、サイバー犯罪者や国家レベルの脅威アクターは、電子メール・セキュリティ・システムによる検知を回避し、進化するセキュリティ環境に適応するため、フィッシング攻撃の際にさまざまなファイル形式を使用するようになりました。2022年に私たちが確認したものと同様に、アーカイブ形式を使用した悪意のある添付ファイルには、ZIPおよびRARアーカイブ形式が広く使用されていました。これらのフォーマットは、特にパスワードで保護されている場合には、悪意のあるコンテンツをウェブプロキシ、サンドボックス、電子メールスキャナーから隠すのに役立ちます。加えて、攻撃者はコンパイル済みHTMLヘルプ（CHM）やLNKといったファイルを広範囲に使用していました。これらのフォーマットは、通常の通信では一般的かつ健全に使用されているため、電子メールセキュリティソフトウェアではしばしば無視されます。CHMの添付ファイルは悪意のあるスクリプトを偽装する一方、LNKファイルは信頼できるWindowsアプリケーションに対してマルウェアのダウンロードを促し、検出リスクをさらに低下させます。

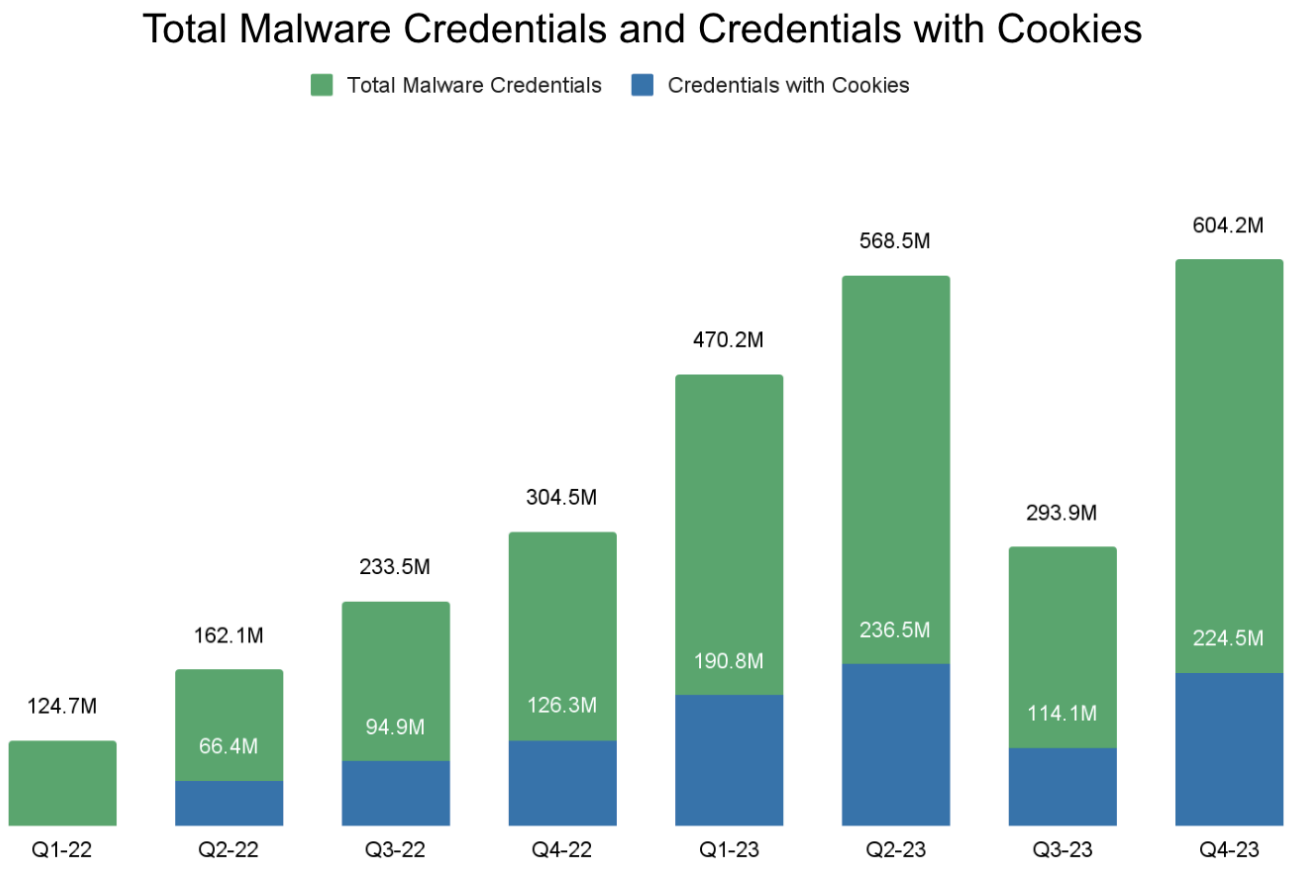


図1：Recorded Futureのマルウェアログで確認された盗まれた認証情報（出典：Recorded Future）

私たちは、Recorded Future® Identity Moduleとマルウェアのログを活用することにより、脅威アクターが利用できる有効なアカウントの数量が増加していることを確認しました。脅威アクターは、MFA（多要素認証）をバイパスするためにこれらのアカウントを使用する可能性があります。2023年には、収集された認証情報の総数が135%増加し、クッキーに関連する認証情報も166%増加しました。この増加は、部分的にはRecorded Futureのインテリジェンス・インデックスに含まれるソースのコレクションが拡大したことに起因しています。とはいえ、グラフに描かれた上昇傾向は、サイバー攻撃の全般的な成功数の増加と相関しています。

また、電子メール技術のセキュリティ管理により、脅威アクターは、マルウェアを配布したり、被害者をフィッシングウェブサイトにリダイレクトしたりする代替手段を見つけるようになっています。そうした代替手段には、QRコードフィッシング（クイッシング）、スミッシング（SMSフィッシング）、企業向けメッセージングアプリケーションの悪用などがあります。また、脅威アクターがフィッシングキャンペーンの際にマルウェアのペイロードを配布するために、Github Pagesのような正規のインターネットサービス（LIS）を悪用するという手口も増えています。これと並行して、脅威アクターは支払い詐欺を推進するための巧妙化努力の一環として、フィッシングページやマルウェアのペイロードを配信すべく、拡大するマルバタイジング・アズ・ア・サービス（malvertising-as-a-service）のエコシステムの中で正規のプログラム広告技術を広範囲に悪用しました。二要素認証・多要素認証（2FA・MFA）の広範な採用により、脅威アクターがフィッシングキャンペーンと並行して、敵対的中間者（AitM）攻撃やMFA疲労攻撃を行う割合を増やしたことはほぼ確実です。

イデオロギーの対立陣営間で統合する影響力ナラティブ

2023年は、秘密裏の影響力工作の点で前代未聞の年でした。Google、Meta、TikTokなどの企業は、ドッペルゲンガー（Doppelgänger）やSpamouflage Dragonを含めた過去最大級のインフルエンスネットワーク（影響力工作ネットワーク）の一部に対し、自社のプラットフォーム上でテイクダウン（削除・閉鎖）を行ったことを公表しました。ドッペルゲンガー、Spamouflage Dragonの両ネットワークについてはいずれも、生成AI採用の兆しも少しずつ見えてきました。

ロシアと繋がりがあるドッペルゲンガーは、現在運用されている最も永続的な影響力工作ネットワークの一つである可能性が非常に高くなっています。Insikt Groupは2023年10月から12月にかけて、ドッペルゲンガーとリンクした5,000以上のアカウントによって増幅された130のドメインを確認しました。この工作は、ウクライナとヨーロッパのウクライナ同志国、そしてアメリカを標的にした、ロシアのより広範な情報工作の一環であるとみられます。この広範な工作では、ウクライナ政府の腐敗を浮き彫りにしようとするTikTokアカウントや、欧米の各国内におけるウクライナへの支持を低下させるための偽の著名人による引用が使われました。ドッペルゲンガーについては、米国の政治を標的にしたウェブサイトでAI生成テキストを使用していることが確認されました。AI生成テキストはドッペルゲンガーが運営する広範な資産を横断して使用されてはいないため、生成AIの使用は依然として限定的であり、より幅広いロシアの影響力工作全体では体系化されていないとみられます。

中国と繋がりがあるSpamouflage Dragon（Insikt GroupではEmpire Dragonとして追跡）は、大量で関与度の低い工作を継続しました。このネットワークでは、2022年8月以降、情報工作が顕著に加速し、中国の力影響工作で使用されるナラティブ（物語）とロシアの偽情報に由来するナラティブの統合（コンバージェンス）が進みました。

選挙への影響力工作もまた、Empire Dragonネットワークにとって優先事項となってきています。このネットワークは、カナダ選出議員を標的にしたことに加え、2023年12月の香港地方選挙と2024年1月の台湾総統選挙を標的として、影響力工作を試みたこともInsikt Groupが確認しています。さらにInsikt Groupは香港の選挙期間中、Empire Dragonのアカウントが、AI生成の画像を限定的に使用しているのを確認しました。

*図**8**：香港の地方選挙中にEmpire Dragonのアカウントがアップロードした生成AI*
（出典：Recorded Future）

ロシアと中国の影響力工作ネットワークはともに、それぞれの政府の地政学的目的に関連してオーディエンスを操作するという強い意図を示してきました。私たちは、その地政学的目的には、2024年に米国で行われる選挙の結果に影響を与えることも、ほぼ確実に含まれると推測しています。そのようなシナリオでは、影響力工作者（インフルエンサー）の目的が、ウクライナや台湾への政治的・軍事的支援に対する各国の国内感情を低下させることに集中する可能性があります。ロシアと中国は、米大統領選の候補者により、選挙結果に影響を与える手法が異なってくる可能性がありますが、両国とも選挙を前に民主的プロセスを弱体化させ、政治的分断を推進しようとすることはほぼ間違いないでしょう。

セクション3：2022年の予測に関する考察

過去の予測の精度を評価することは、インテリジェンスのライフサイクルの重要な部分であり、新たな予測と評価の策定に寄与します。次ページの図では、Insikt Groupが2022年のアニュアルレポートからの3つの主要な予測について振り返っています。これらの予測は大枠では正しいものとなりましたが、微妙に異なった展開もいくつか見られました。

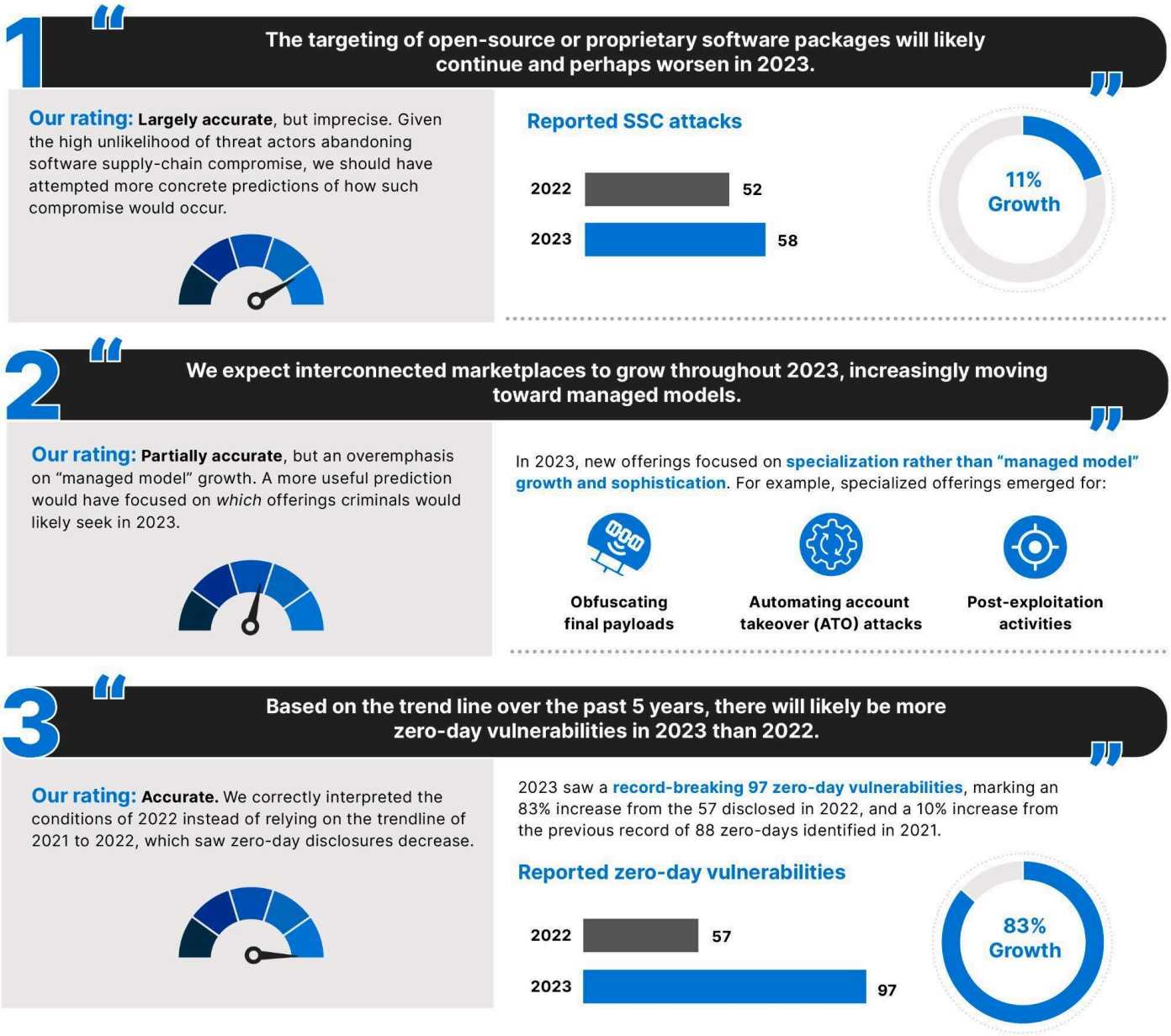


図9：2022年のアニュアルレポートからの3つの主要な予測に関する考察

セクション4：今後の展望

サイバーセキュリティの将来予測は、以下の2つの大きな問題に直面しています。

- 安全すぎる予測のため、あまり価値のある情報が提供されない
- あまりにも大胆に予測しすぎるため、防御する側の注意を誤った方向に向けてしまう

このジレンマに直面する私たちが2024年に望むのは、警戒よりも攻撃の側に立って多く間違えることです。なぜなら、私たちの評価により、防御側が新しい脅威やあまり報告されていない脅威に先手を打つ可能性が高まることを望んでいるからです。私たちがそうする理由は、効果的なサイバーセキュリティ戦略を開発する際には、脅威の状況のよく知られた属性に沿った一般的な説明よりも、それがたとえ不快である可能性があっても具体的な評価の方が、通常はより有用であると信じているからです。

これらの考慮事項を念頭に置いた上で、2024年のサイバー脅威の状況に関する私たちの予測を以下に示します。これには地政学や法規制など、サイバー脅威の状況に対するより大きな文脈上の影響に関する予測も含まれています。

サイバー脅威の状況

- 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私たちは予想しています。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でことしょう。
- 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%増加すると予想されます。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。
- 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、仮想プライベートネットワーク (VPN) を恐喝グループがますます標的にすることが予想されます。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。
- ハクティビズム：私たちはロシア・ウクライナ戦争の流れの変化により、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やアノニマス・スーダン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。
- 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私たちは予想しています。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。

- 情報工作：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、特に米国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予想されます。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。

文脈的な状況

- テクノロジー：企業は2024年にはほぼ間違いなく、Web 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、アカウント乗っ取り (ATO) 戦術から新規アカウント詐欺 (NAF) 戦術への移行が進む可能性があります。
- 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、米国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、地域での米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、米国と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。
- 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。

付録A：2023年に悪用された主な脆弱性

脆弱性	影響を受けた製品	説明	リスクスコア	CVSS
CVE-2023-44487	HTTP/2プロトコルを使用するすべての製品	HTTP/2プロトコルでは、リクエストのキャンセルにより多くのストリームを即座にリセットできるため、サービス拒否（サーバーリソースの消費）が可能になります。修正はベンダー固有となります。	89	7.5
CVE-2023-34362	Progress Software MOVEit Transfer	MOVEit Transfer Web アプリケーションにSQL インジェクションの脆弱性があり、認証されていない攻撃者が MOVEit Transfer のデータベースにアクセスできる可能性があります。	89	9.8
CVE-2023-23397	Microsoft Outlook	特権昇格の脆弱性	89	9.8
CVE-2023-4966	Citrix NetScaler ADC およびNetScaler Gateway	機密情報の漏えいにより、攻撃者がバッファの終了後に大量のメモリを読み取ることを可能にする脆弱性	89	9.8
CVE-2023-21716	Microsoft Office（Word）	Microsoft Wordのリモートコード実行の脆弱性	99	9.8
CVE-2023-24932	Microsoft Windows 10、11、サーバー	セキュアブートのセキュリティ機能がバイパスされる脆弱性	99	6.7
CVE-2023-28206	Apple macOS、iPhone OS、iPadOS	境界外書き込みの問題は、入力検証（バリデーション）を改善することにより対処されました。アプリはカーネル権限により任意のコードを実行できる可能性があります。	99	8.6
CVE-2023-2868	Barracuda Email Security Gatewayのファームウェア	リモートでコードが実行される可能性があるリモートコマンドインジェクションの脆弱性	99	9.8
CVE-2023-38831	RARLAB WinRAR	6.23より前のRARLAB WinRARでは、ユーザーがZIPアーカイブ内の無害なファイルを表示しようとすると、攻撃者が任意のコードを実行する可能性があります。	99	7.8
CVE-2023-41990	Apple macOS、iOS、iPadOS	Appleのみに存在するADJUST TrueTypeフォントの脆弱性により、悪意のあるiMessage添付ファイルを介してリモートコード実行が行われる可能性があります。Operation Triangulationの攻撃で悪用されました。	99	7.8
CVE-2023-43177	CrushFTP	10.5.1より前のCrushFTPは、動的に決定されたオブジェクト属性の不適切な制御による変更に対して脆弱です。	99	9.8

脆弱性	影響を受けた製品	説明	リスクスコア	CVSS
CVE-2023-47565	QNAP QVR Firmware 4.0	OSコマンドインジェクションの脆弱性により、認証済みユーザーがネットワーク経由でコマンドを実行できるおそれがあります	99	8.8
CVE-2023-4863	Google Chrome、Mozilla Firefox	Google Chrome 116.0.5845.187およびlibwebp 1.3.2より前のlibwebpでのヒープバッファオーバーフローにより、リモートの攻撃者が細工されたHTMLページを介してメモリの境界外への書き込みを実行する可能性がありました。	99	8.8
CVE-2023-4911（Looney Tunables）	64ビットのGNU glibc Fedora Red Hat Enterprise Linux	権限昇格によりRCE（リモートコード実行）を許可できるバッファオーバーフローの脆弱性	99	7.8
CVE-2023-7024	Google Chrome	120.0.6099.129より前のGoogle ChromeのWebRTCのヒープバッファオーバーフローにより、リモートの攻撃者が細工されたHTMLページを介してヒープ破壊の悪用を行うおそれがありました。	99	8.8

*表**1**：2023年に開示された上位の高リスク脆弱性（出典：Recorded Future）*

Recorded Future®

*Insikt Group®*について

Recorded Future の脅威研究部門である 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、クライアントのリスクを軽減し、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、技術ソース全体で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1,700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。