サイバー脅威レポート

2023年6月

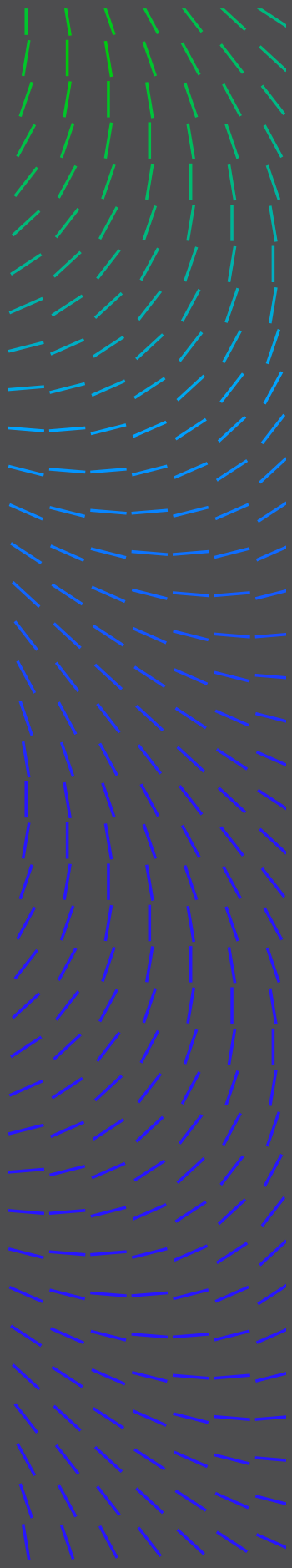
専門家、センサー、テレメトリ、
インテリジェンスから成る
グローバルネットワークから得られた
インサイト

提供

Trellix ADVANCED RESEARCH CENTER

サイバー脅威レポート

Trellix の Advanced Research Center による本レポートは、(1) サイバーセキュリティ脅威について、複数のソースの重要なデータから得られたインサイト、インテリジェンス、ガイドラインを紹介し、(2) このデータの専門的、合理的、妥当な解釈を展開して、サイバー防衛のベストプラクティスにつながる情報をお届けします。今回のレポートでは、2023 年 1 月 1 日から 2023 年 3 月 31 日までに収集されたデータとインサイトに焦点を当てています。



サイバー脅威は進化と増加を続けています。
その変化は急速で、大規模です。

SecOps チームは情報、資産、運用の防御に忙殺されており、脅威の状況をすべて完全に把握することはとうていできません。

なぜでしょうか？ 明晰な展望には広い視野が欠かせないからです。複数のソース、データ ストリーム、生のインテリジェンス。膨大なテレメトリが必要なのです。

真のインサイトには、多くの組織と業界を横断する戦略的な視点が必要です。複数の地域と、複数の攻撃対象に関する視点です。

サイバー脅威レポート 2023 年 6 月号へようこそ。

攻撃者が標的にしているリスク、脅威、脆弱性を理解し、積極的に突き止める

私は平素から、役員会のメンバー、CEO、CISO、CIO、CTO など、国や政府機関、さまざまな業界の民間企業などでサイバー防衛を担っているリーダーを相手にしています。

扱うトピックは多岐にわたります。グローバルな研究調査、イノベーション、インテリジェンスから、SecOps チームにおける最新のサイバー防衛対策の現状などにまで及んでいます。その人たちが抱えている課題については、Trellix が最近ソートリーダーシップについてまとめた「The Mind of the CISO (CISO の考え方)」でも明らかです。あまりにも多い情報ソース (35%)、変化の絶えない規制義務や法的要件 (35%)、増大する攻撃対象 (34%)、熟練スタッフの不足 (34%)、社内他部門からの賛同や利用の不足 (31%) などが指摘されました [1]。

こうした回答のほとんどは、直接的にだろうと間接的にだろうと、脅威を取り巻く環境の性質に関わっています。どんな攻撃が出現しているのでしょうか。特に影響力の大きいランサムウェア グループはどれでしょうか。標的になっているのはどんな脆弱性で、最も活発に活動している国家はどこなのでしょうか。メールやネットワークのセキュリティについて追跡している脅威にはどんな傾向があるのでしょうか。

「役員会のメンバー、CEO、CISO、CIO、CTO、あるいは SecOps チームのメンバーを務めている皆さんのミッションにとって、本レポートや Trellix の豊富なガイドライン、情報、視点のライブラリで共有されている知識は多くの場面で不可欠です」

Trellix からお伝えできることはいろいろあります。私たちは日々、セキュリティの最前線にいるからです。私たちは、世界中の 10 億以上のセンサーから届く膨大なセキュリティ インテリジェンス、インサイト、データを活用しています。役員会のメンバー、CEO、CISO、CIO、CTO、あるいは SecOps チームのメンバーを務めている皆さんのミッションにとって、本レポートや Trellix の豊富なガイドライン、情報、視点のライブラリで共有されている知識は多くの場面で不可欠です。

John Fokker は、Trellix が誇る Advanced Research Center チームで脅威インテリジェンス業務を率いる私の同僚であり、今回こうして素晴らしいレポートをまとめてくれました。チームの集中を図ってプロセスを強化し、適切な XDR テクノロジーを導入するうえで、ここにまとめられたインサイトをご活用ください。皆さん組織を安全に保って発展させるために、今後のレポートで特集として取り上げたい点があれば、ぜひお知らせください。

Joseph (Yossi) Tal
SVP 兼 TRELLIX Advanced Research Center 長

サイバー セキュリティの最前線に立つヒーローを支援するために

私の仕事相手はヒーローです。私のチームのことではありません。官民を問わずさまざまなキャリアを通じてスーパーパワーを発揮してはいますが、それを指しているわけではないのです。

ヒーローとは、皆さんのことです。私がヒーローと呼んでいるのは、Trellix のシステム、インサイト、インテリジェンスといった高度なリサーチ機能を利用してサイバー攻撃から組織を守っている世界中の人々やチームのことです。CISO、CTO、CIO はもちろん、ユーロポール、FBI、NSA、サイバーセキュリティ・社会基盤安全保障庁 (CISA)、オーストラリアのサイバー セキュリティ センター (ACSC)、英国の国家サイバーセキュリティセンター (NCSC-UK) など各機関の同僚も当てはまります。それと同じくらい、いえおそらくそれ以上に重要なのは、私のいうヒーローが SecOps チームのメンバー全員だということです。

「日々の業務で皆さんもよくご存じのように、サイバー セキュリティは目まぐるしく進化しています。テクノロジーのブレークスルーや XDR への強力なシフトなどです」

SecOps のミッションを根本から変えるものは何だと思いますか？同僚の Yossi が上で言及している Trellix のレポートによると、サイバー セキュリティ リーダーの関心は世界中どこでも変わりません。可視性の向上 (44%)、重要事項の優先順位付けの強化 (42%)、マルチベクトルの攻撃に対処できる広範なコラボレーション (40%)、精度の向上 (37%) といったことです。[2]

どの要素でも、土台として必要なのは正確なインサイト、情報、データであり、ちょうど本レポートがそれに当たります。

日々の業務で皆さんもよくご存じのように、サイバー セキュリティは目まぐるしく進化しています。テクノロジーのブレークスルーや XDR への強力なシフト。法律や法的責任をめぐる規制の変化。脅威の状況の移り変わり。革命が、すなわち SecOps チームが次世代のサイバー攻撃の「一歩先」を行くための改革が進みつつあるのです。勝利はいつもインサイトから、現状の理解から始まります。

ともに進みましょう。Trellix は皆さんを支えます。このレポートは皆さんに向けて作成されました。

John Fokker
Threat Intelligence 責任者
兼プリンシパル エンジニア
TRELLIX Advanced Research Center

[1] Trellix、2023 年レポート：「The Mind of the CISO (CISO の考え方)」、2023 年
[2] Trellix、2023 年レポート：「The Mind of the CISO (CISO の考え方)」、2023 年

はじめに

戦略的な背景：不安定な世界

本レポートのデータを正しく読み取るには、世界規模の「大きな全体像」を理解しなければなりません。世界中の組織に対するサイバー脅威は、技術の世界だけで起こっているわけではないからです。サイバー リスクの主な要因のなかには、戦争をはじめとする不可抗力、経済サイクルの大規模な変化などもありますが、ビジネスモデルや主要なパートナー、コア プロセス、テクノロジーの導入、法規制の遵守といった要因に変更を加えるたびに出現する新たな脆弱性もあります。2023 年第 1 四半期の脅威データに影響を与えている要因の例を以下に示します。

ロシアによるウクライナ侵攻と欧米に対する非対称的な戦争：政治的、経済的、領土的野心のために大国がしかけるスパイ活動、戦争、偽情報を目的としたサイバー活動は激しくなる一方です。欧米の企業、政府、インフラに対してハッカーがしかけるサイバー攻撃はさらに巧妙になっています。

習近平による中国の集中支配とその地政学的な野心：中国の国家的な目標、強硬な外交政策、産業スパイ活動は、中国が関与する持続型脅威 (APT) グループが世界的な状況を支配するなかで、サイバー リスクをあおり続けています。

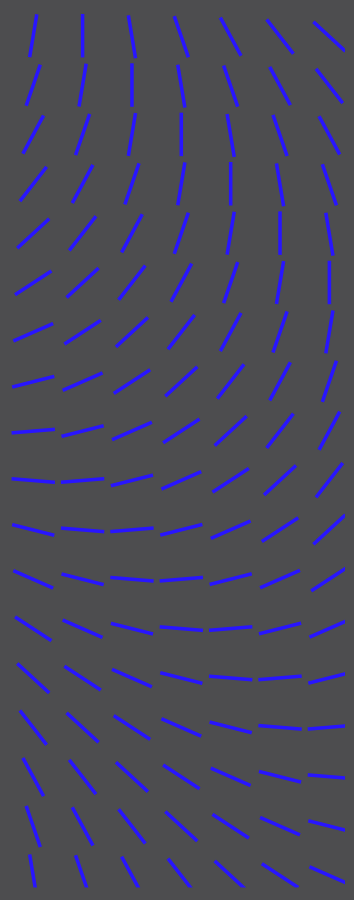
発展途上国の経済とインフラの急速な拡大：発展途上地域の多くが、経済成長に伴ってインフラや技術の規模を拡大しているため、サイバー セキュリティは最優先事項になりにくく、重要なインフラにサイバー関連の脆弱性がいくつも発生する結果になります。

世界的なインフレとその経済的および政治的影響：今期は、市場の変動性、金融危機、政治危機、そして支出の優先順位やサイバー セキュリティ予算への圧力などがありました。

コロナ禍以降も続くサプライチェーンの混乱：地域間の市場への新たな経路を切り開くには、パートナー、輸送網、情報共有、ひいてはサイバー リスクのシフトが必要でした。サイバー脅威は日々サプライチェーンに影響を及ぼしているため、ゼロ トラスト機能の必要性は業界全体で高いままです。

Apple 製品のセキュリティ環境が優れているという神話：攻撃者が Golang ベースのマルウェアを大規模に活用し始め、マルチベクトルの攻撃が多数のオペレーティング システムにまで広がっているため、macOS 環境はもはや安全とは言えなくなってきていますが、それでもこの状況は続いています。

人工知能が世界の舞台に登場し、破壊的な影響が濃厚に：サイバー防衛にとって、機械学習や自然言語処理などの進歩は味方にも敵にもなるものです。世界的なサイバー脅威が進化し、人間のチームが対処できる速度をはるかに上回る規模で発生しているため、人工知能ソリューションは企業のサイバー防衛にとって不可欠なものとなります。



サイバー セキュリティ : CISO の課題と SecOps 革命

今年の第 1 四半期、脅威を取り巻く環境は、社内の要因にも影響されましたが、影響の多くは、サイバー セキュリティのリーダーと最前線のチームが引き続き浴びている逆風を反映するものです。

サイバー セキュリティ担当者や SecOps チームにとって、最も重要な課題のひとつは何でしょうか?
脅威インテリジェンスに関する情報を迅速かつ大規模に消化し、実践的なインサイトを組織全体の脅威ハンティング チームやタスク フォースに即座に進めることです。

Trellix の目標は?その過程をシンプルにすることです。

では、どうやって? Trellix の XDR、ホスト保護、ネットワーク、およびメール製品に組み込まれている優れた脅威インテリジェンス、脅威ハンティング、セキュリティ オペレーション機能を利用して、組織が集中すべき対応に到達できる自動化レベルを提供することです。

時代遅れのテクノロジー : 多くの組織が SOAR や SIEM といったレガシー テクノロジーに今でも依存しています。実際、サイバー脅威から組織を保護するためにより今より優れたソリューションが必要であると回答した CISO は 96% にのぼりました。[3]

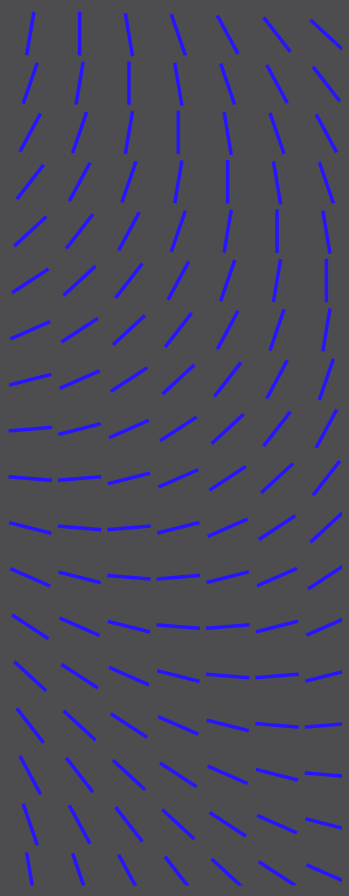
セキュリティ ツールの海 : SecOps チームはアラートで圧倒されており、その一方で時間の優先順位を付けるときに必要なものが不足しています。平均して、組織は 25 ものセキュリティ ソリューションとツールを採用しているのですから、混乱が起きるのは当然です。[4]

アラート疲労 : アラートが氾濫する状況で、SecOps チームは優先順位付け、誤検知、アラートの見逃しなどと闘っています。IDC によると、35% がアラートを無視しており、そのうち 45% は誤検知が理由だということです。[5]

人材不足 : SecOps の人材にも専門知識にも限界があるため、脅威に効果的に対抗することは困難です。SOC アナリストの平均勤続年数をご存じですか?約 2 年です [6]。

方法論 : データの収集および分析方法について

Trellix の Advanced Research Center に所属する、世界でもトップクラスの専門家は、本レポートを構成する統計、トレンド、インサイトを、クローズドかオープンかを問わずグローバルな幅広いソースから収集しています。収集されたデータは、弊社の Insights および ATLAS プラットフォームへ送られます。機械学習、自動化、そして人間の鋭敏な感覚を活用して、チームは集中的、統合的、反復的なプロセスをひととおり実施します。つまり、データを正規化して情報を分析し、全世界でサイバー セキュリティの最前線にいるサイバー セキュリティ リーダーや SecOps チームにとって有意義なインサイトを導き出すというプロセスです。当社の手法の詳細については、本レポートの末尾をご覧ください。



用途：本レポートの情報の使用方法

業界をリードする評価チームであれば、バイアスの影響を把握して認識し、可能であれば緩和することが欠かせません。バイアスとは、事実とその意味を受け入れるか、拒否するか、操作するかを左右する傾向のことであり、自然な場合も、仕組まれた場合も、目に見えない場合もあります。コンテンツの消費者についても同じことが当てはまります。

高度に構造化された制御ベースの数学のテストや実験とは違い、本レポートは本質的に便宜的なサンプルです。つまり医療やヘルスケア、心理学、社会学のテストでよく用いられもので、入手とアクセスが可能なデータを利用した非確率なタイプの調査ということです。

つまり、本レポートの調査結果は、私たちが観察できたことに基づいており、検出、報告、データ収集を回避した脅威、攻撃、戦術の証拠は含まれていません。

「完全な」情報や「完璧な」可視性がない以上、これは本レポートの目的に最も適したタイプの調査です。目的とは、サイバー セキュリティの脅威に関する重要なデータについて既知の情報ソースを明らかにし、このデータの合理的、専門的、倫理的な解釈を展開して、サイバー防衛のベストプラクティスにつながる情報を届けることです

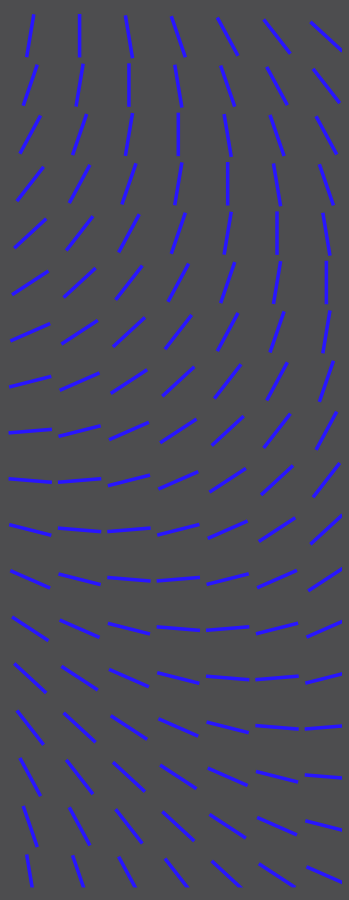
この調査倫理で中心となるのは以下の点です。

時間上のスナップショット：インターネットに接続されているシステムすべてのログにアクセスできるわけではありませんし、あらゆるセキュリティ インシデントが報告されているわけでもありません。被害者のすべてが侵害を受けてリーク サイトに掲載されることもありません。しかし、追跡できるものを追跡することで、各種の脅威について理解を深めることができ、分析と調査の盲点も減らすことができます。

誤検知と非検知：データを収集するための Trellix の特別な追跡システムとテレメトリ システムの高性能な技術的特性の一部として、誤検知および非検知の結果を緩和・除去するメカニズム、フィルター、戦術があります。これを通じて、分析レベルと調査結果の質を向上させることができます。

感染ではなく検出：テレメトリを話題にするとき、感染ではなく、検出がその焦点になります。検出は、ファイル、URL、IP アドレス、その他の指標を弊社のいずれかの製品が検出し、弊社に報告したときに記録されます。

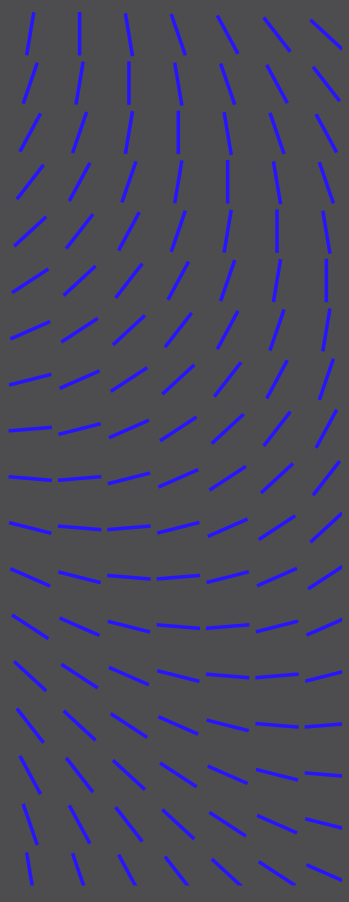
データのキャプチャは不均等：なかには、慎重な解釈が必要なデータ セットもあります。たとえば、通信データには、他の多くの産業やセクターで運営されている ISP クライアントからのテレメトリが含まれています。



国家の関与 : 同様に、国家に関与するハッカーやサイバー犯罪者が互いになりすましたり、悪意のある活動を信頼できるソースからのものとして偽装したりする一般的な現状を踏まえると、さまざまなサイバー攻撃や脅威に関する国家の責任を判断するのも、きわめて難しい場合があります。

今後の見通し : ガイドラインとリソース

本レポートに記載されている情報は、最前線に立つサイバー セキュリティのヒーローにとってどんな意味を持つのでしょうか。サイバー セキュリティに関するインサイトやデータは、それが行動に移されて、リスクの低減、意思決定の改善、SecOps 活動の効率と費用対効果の向上という結果が表れて初めて役に立ちます。その他のガイドラインとリソースについては、www.trellix.com を参照してください。



[3] Trellix、2023 年レポート :「The Mind of the CISO (CISO の考え方)」、2023 年
[4] Trellix、2023 年レポート :「The Mind of the CISO (CISO の考え方)」、2023 年
[5] IDC, The Voice of the Analysts、2021 年
[6] Ponemon Institute、2020 年

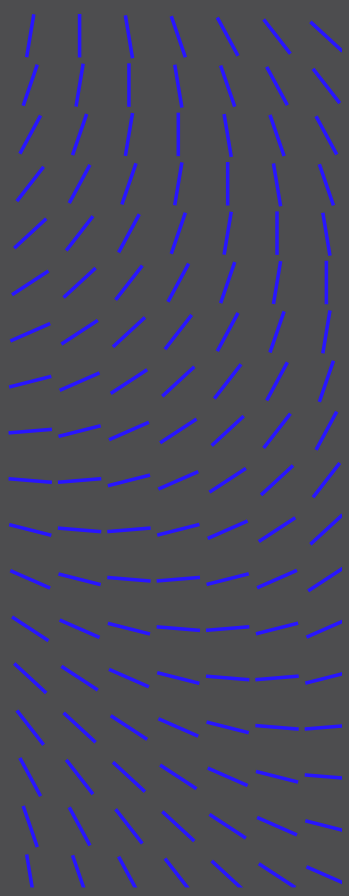
2023 年第 1 四半期のハイライト概要

ランサムウェアの状況

- **ランサムウェアの波 :** ランサムウェアは、膳世界で主要なサイバー攻撃としてその地位を保ち続けています。フィッシングのように、個人を欺き、操作して機密情報や個人情報を漏えいさせるソーシャル エンジニアリングの手口は、巧妙さが増しつつ、これまで以上に流行しています。
- **Cuba と Play が流行 :** 年明け早々には身代金に関連するサイバー犯罪活動の減少が見られましたが、第 1 四半期に最も流行したランサムウェア ファミリーは、Cuba (9%) と Play (7%) でした。
- **LockBit 根強く存続 :** 活動は 2 四半期連続で減少しているにもかかわらず、LockBit は依然として、身代金の要求に応じるよう被害者に圧力をかける特に攻撃的なランサムウェアとして存続しています。
- **Magecart グループが全盛に?**公的報告書によると、2023 年第 1 四半期には、このクレジット カード窃盗および E コマース攻撃グループの活動が驚異的な増加を記録しています。この脅威が、国家の関与する他の主要な APT ほどの規模で活動するのは稀であり、Magecart グループが世界的に再び台頭している可能性を示唆しています。

ランサムウェアの手口の進化

- **金銭目的 :** ランサムウェアの動機が依然として主に金銭であることに変化がないのは驚くことではなく、業種としては保険 (20%) と金融サービス (17%) で潜在的な攻撃が最も多く検出されています。
- **中規模企業の被害が最大に :** 当社のリーク サイト データを評価した結果、これらの攻撃による被害は、従業員数 51 ～ 200 人 (32%)、売上高 1000 万 ～ 5000 万ドル (38%) の中規模企業が最も多いことが判明しました。
- **主な標的は米国 :** ランサムウェア グループの被害を最も受けた国は米国 (15%) です。米国は、企業の被害者のうち、攻撃者から「データを買い戻す」と判断した人の割合が最も高い国 (48%) でもあり、次にランクインした英国の 6 倍という高さでした。
- **Cobalt Strike が攻撃手段に :** Trellix のテレメトリによると、Cobalt Strike はランサムウェアを使う攻撃にとても好まれています (インシデントの 28%)。ベンダー Fortra によって、2022 年第 4 四半期末には、攻撃者がこのツールを使いにくくすることを試みしましたが、グループの間では人気も使用率も高まっているようです。



国民国家の活動が危険な水域に

- **主な攻撃者：**第 1 四半期に国家を標的とした活動のなかでは、過去 6 か月間で Mustang Panda や UNC4191 など中国が関連する APT 攻撃者の活動が最も顕著でした。中国に関連する攻撃者は、全世界の環境に影響を及ぼしており、国家の関わる全活動のうち 79.3% を占めました。北朝鮮、ロシア、イランに関連する攻撃者がこれに続いています。
- **特に活発な APT グループ** Mustang Panda は、世界で最も活動的な APT グループ (72%) として 3 四半期連続で 1 位を維持しました。中国が引き続き、スパイ活動と阻害活動を目的として悪質なサイバー活動を続け、増やしているということです。

脆弱性インテリジェンス

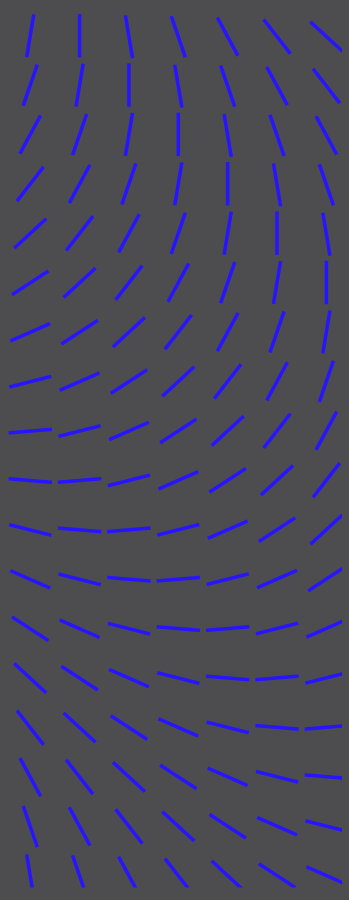
- **既知の脆弱性への対処の失敗：**今四半期でも特に重要な脆弱性の大半は、まだ対処されていない既知の脆弱性が原因でした。
- **古い情報：**今年 2 月に公開された Apple の脆弱性は、2021 年に NSO Group によって公開された Pegasus スパイウェアの一部として使用されていた FORCEDENTRY エクスプロイトまで遡ります。

メール セキュリティ

- **新たな攻撃経路：**Microsoft は、Office プラットフォームのマクロ添付ファイルをブロックし始めましたが、攻撃者は、SEO ポイズニング、OneNote、Zip 添付ファイルなど、引き続き Windows デバイスを狙う他の感染経路をすぐに使い始めました。
- **信頼性の低いブランド：**攻撃者は、一般的なフィッシングメールに加え、PayPal、Google、DWeb、IPFS など正規のブランド名やサービスを悪用して被害者を欺き、オンライン認証情報を詐取する傾向が増えています。

クラウドへの不正アクセス

- **戦術がシフト：**オンプレミス インフラストラクチャから Amazon、Microsoft、Google など手頃で拡張性の高いオプションに移行する企業が増えるにつれて、クラウド インフラストラクチャへの攻撃も増え続けています。
- **有効なアカウント：**多要素認証、プロキシ、および API 実行を使用する高度な攻撃が台頭していますが、攻撃手法の主流は今もなお、有効なアカウントを使用するものであり、2 番目に多く使用されている攻撃ベクトルと比べても 2 倍以上の頻度で多用されています。サイバー犯罪者が正規のアカウントや Web サイトのログイン情報にアクセスしてそれを販売し、侵入して攻撃するという不正アクセスのリスクがまぎれもない現実であることの裏付けです。



レポート分析、インサイト、データ

セキュリティ インシデント

このセクションで取り上げるセキュリティ インシデントは、公的報告書に基づいたものです。2023 年第 1 四半期には、攻撃者が最も抵抗されにくい経路を悪用したため、Windows バイナリ、サードパーティ ツール、カスタム マルウェア、ペネトレーション テスト ツールが引き続き業務に影響を与えました。PowerShell と Windows Command Shell は引き続き、永続化、配備、抽出につながるタスクを生成する目的で悪用されています。

2023 年第1 四半期のイベントで使われた上位のWINDOWS バイナリ

1. PowerShell
2. Windows CMD
3. スケジュール タスク
4. RunDLL32
5. WMIC

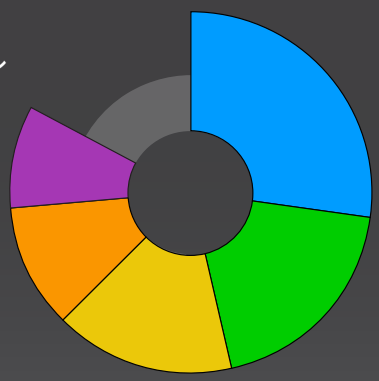
タスクのスケジューリング、悪意のある DLL ファイルの挿入、Windows Management Instrumentation を通じて実行されるコマンドが上位 5 位を占めました。スクリプトで実行される場合も、キーボードによる手動入力で実行される場合も、攻撃者が保護も監視もされていないバイナリを自由に利用している点は変わっていません。

多くの場合、サードパーティ ツール、フリーウェア、ペネトレーション テスト ツールは、攻撃のライフサイクルにおいて、攻撃者が永続性を設定する、スクリプトを実行する、標的情報を発見および収集する、権限昇格によって制限されたアカウントでは本来アクセスできない資産やデータにアクセスするの、などの行為を可能にする役割を果たします。また、権限昇格に使われると、攻撃者は昇格した権限でインストール プロセスを実行し、
制限されたアカウントでは本来アクセスできない領域、資産、またはデータにアクセスできるようになります。

2023 年第 1 四半期の公的報告書で使われた上位のサードパーティ ツール

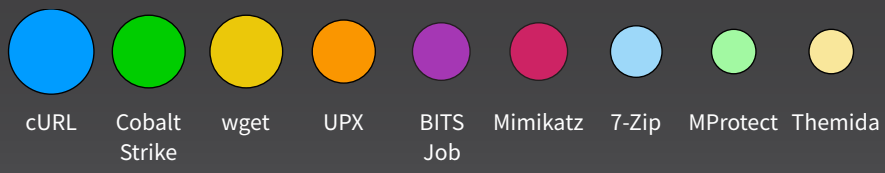
ツールのカテゴリ

- ファイル転送
- ソフトウェア パッカー
- エクスプロイト後のツール
- リモート アクセス ツール
- アーカイブ ユーティリティ



2023 年第 1 四半期の公的報告書で使われたサードパーティ ツール

具体的なツール



Cobalt Strike、Mimikatz、Sharphound などさらに悪質なサードパーティ ツールでは、合法的な場合も攻撃者が利用する場合も含めて、パスワードの収集、ビーコンの設定、特権昇格に利用されます。攻撃者が環境を侵害すると、cURL などのファイル転送ツールを使用してリモート ペイロードにアクセスしたり、Rclone を使用してデータをクラウド ストレージに流出させたりします。

2023 年第 1 四半期、金銭の収集、政府の機密の暴露、インフラ利用の阻害を目的として、地域またはセクター別にユーザーを標的とする最も活発な脅威グループおよび APT の上位は Magecart グループ、APT29、APT41 の 3 つでした。Magecart グループは、国家が関与する他の APT のような規模で活動することはほとんどないため、Magecart グループがリストのトップになったのは予想外でした。今後数か月間はこのグループの活動を監視し、今期のデータははたして、このグループが世界的な舞台で再び台頭してきたことを示す兆候なのかどうかを見極めたいと考えています。

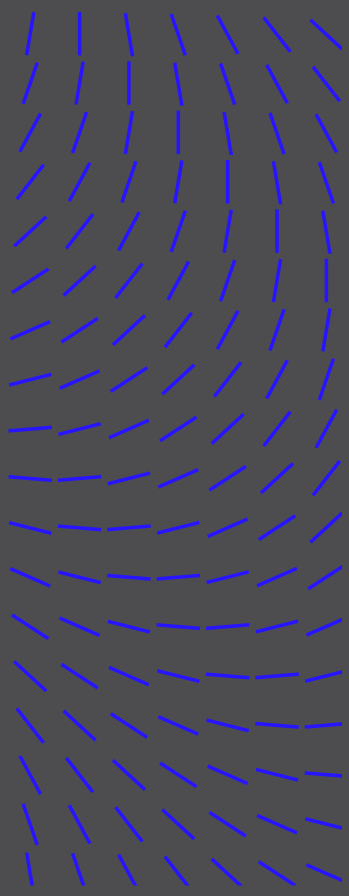
過去の世界規模のキャンペーンでは、クリックやダウンロードの多い人なら誰でも引っかかるように設計された、あまり高度ではないスプレー アンド プレイ手法がこの業種では問題でした。標的型攻撃はさらに巧妙に進化しており、製造業、金融、医療の各業種がますます執拗に狙われるようになっています。残りの 2 業種、通信とエネルギーは、グローバルに標的とされる頻度は低いようですが、どちらも重要な業種であることは変わらないので、この業種の組織が侵害を報告していない、あるいはインシデントに気づいていない可能性もあります。

2023 年第1 四半期の公的報告書で活発だったと報告された上位の攻撃者

1.	Magecart グループ	5%
2.	APT29	4%
3.	APT41	4%
4.	Blind Eagle	4%
5.	Gamaredon Group	4%
6.	Lazarus	4%
7.	Mustang Panda	4%
8.	Sandworm Team	4%

2023 年第1 四半期の公的報告書で標的と報告された上位の業種

1.	製造業	8%
2.	金融	7%
3.	健康	6%
4.	通信	5%
5.	エネルギー	5%



当社のリサーチ チームによって分析・検証され報告されたイベントには、個人の攻撃者、脅威グループ、またはより巧妙な APT に関する豊富な情報、相関関係、属性も含まれています。マルウェア ファミリーに伴うツール、テクニック、手順としては、ローダーやダウンローダーなどのマルウェア、RAT、情報窃取、ランサムウェアなどがあります。2023 年第 1 四半期に分析され、Insights を通じて利用できるイベントでは、ウクライナが最も頻繁に標的とされており、僅差で米国が続いています。

Royal Ransom、Trigona、Maui のランサムウェア ファミリーが、2023 年第 1 四半期に大きな被害をもたらしました。Trellix は先日、Royal Ransom の詳細な分析と、Windows および Linux の実行可能ファイルに関してその内部構造を発表しました。これは、特に当社の Insights プラットフォームから得られた統計ですが、グローバルにつながったインフラストラクチャ全体では、さらに多くのイベントが発生しています。報告済み、または非公開の既知のイベント、まだ特定・修復されていないイベントも含まれています。

2023 年第1 四半期の公的報告書で標的と報告された上位の国

7% 

分析対象とした公開のイベントでは、攻撃者によって最も狙われた国はウクライナで、米国が僅差で続いています。

1.	ウクライナ	7%
2.	米国	7%
3.	ドイツ	4%
4.	韓国	3%
5.	インド	3%

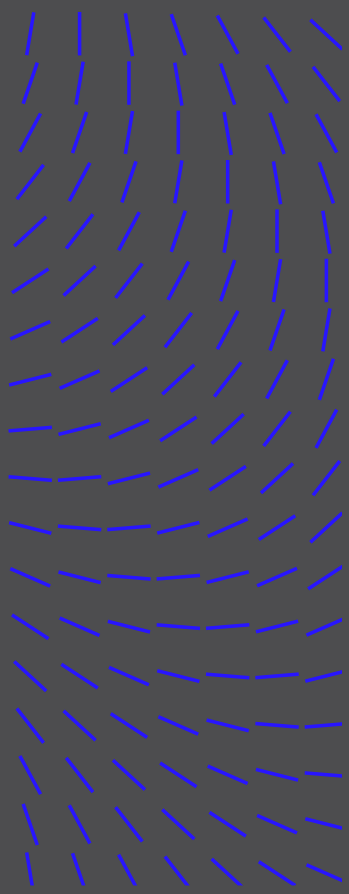
2023 年第1 四半期の公的報告書で取り上げられた上位のランサムウェア

1.	Royal Ransom	7%
2.	Trigona	4%
3.	Maui	4%
4.	Magniber	3%
5.	LockBit	3%

ランサムウェア

以下に示す統計はキャンペーンの統計であり、検出そのものではありません。弊社のグローバル テレメトリによると、さまざまなランサムウェア グループによる複数のキャンペーンに属する侵害の痕跡 (IoC) が確認されました。

年明け早々の 1 月にサイバー犯罪者の活動が低下することは珍しくありません。この傾向は、Hive と Cuba のどちらも活動が顕著に減少していることの説明になります。そのうえ、FBI とユーロポールが 1 月下旬に Hive の活動を妨害したことで、同グループの活動は大幅に妨害されたはずです。LockBit は引き続きランサムウェアの大きなファミリーであり、被害者に身代金の支払いを共用することに積極的で、特に成功しているように見えます。



2023 年第 1 四半期のイベントで使われた上位のランサムウェア

8%

最も活発だったランサムウェア グループは Cuba、次いで Play、LockBit の順でした。

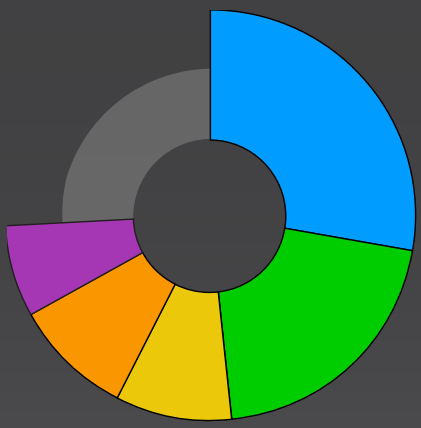
- Cuba
- Play
- LockBit 3.0
- Clop
- Hive

2023 年第 1 四半期に使われたランサムウェア

28%

CobaltStrike は、2023 年第 1 四半期のランサムウェア インシデントのほぼ 3 分の 1 で使用され、ツールの悪用を困難にする最近のアップデートがあったにもかかわらず、使用率は増加する一方でした。

- Cobalt Strike
- Mimikatz
- Empire
- BloodHound
- SystemBC

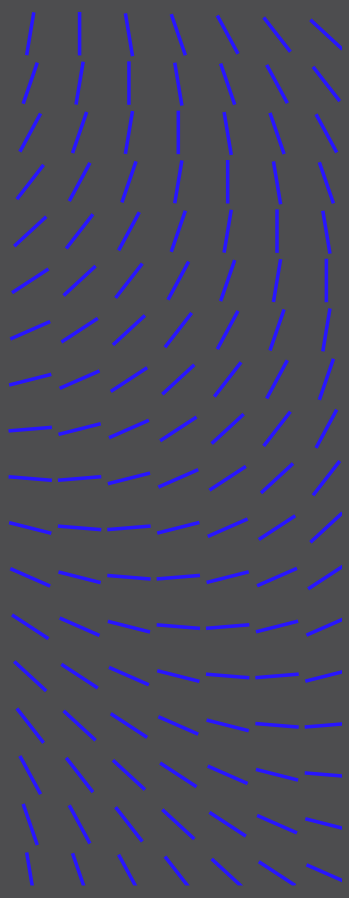


2023 年第 1 四半期にランサムウェア グループから最も影響を受けた国

15%

米国は引き続きランサムウェアの影響が最も大きい国であり、今期はそれにトルコが僅差で続いています。

1.	米国	15%
2.	トルコ	14%
3.	ポルトガル	10%
4.	インド	9%
5.	カナダ	9%



2023 年第1 四半期にランサムウェア グループから最も影響を受けた業種

1.	保険	20%
2.	金融サービス	17%
3.	医薬	7%
4.	通信	4%
5.	外部委託 & ホスティング	4%

ランサムウェア グループは、「リーク サイト」と呼ばれる Web サイトで被害者の情報を公開しており、被害者との交渉が頓挫している場合や身代金の支払いが拒否された場合には、その情報を利用して被害者を恐喝します。私たち Trellix の専門家は、オープンソース ツール RansomLook を使って、投稿記事からデータを収集し、その結果を正規化・強化して、匿名化された被害分析を提供しています。

なお、各リーク サイトでは、すべてのランサムウェア被害者が報告されているわけではありません。多くの被害者が身代金を支払っており、その場合は報告されていません。これらのメトリックスは、ランサムウェア グループが脅迫や報復を行った被害者の指標であり、被害者の合計と混同しないようにする必要があります。

2023 年第 1 四半期に最も多くの被害者を報告したリーク サイトごとのランサムウェア グループ

1.	LockBit	30%
2.	Hive	22%
3.	Clop	12%
4.	Royal Ransom	7%
5.	ALPHV	5%

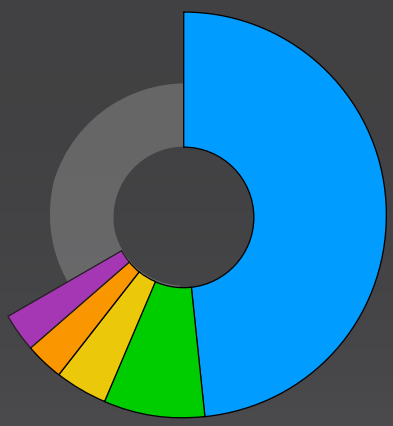
2023 年第1 四半期にランサムウェア グループから最も影響を受けたリーク サイトごとのセクター

1.	産業財・サービス	25%
2.	小売業	14%
3.	テクノロジー	11%
4.	小売業	8%
5.	金融サービス	6%

2023 年第 1 四半期にリーク サイトに掲載された企業の上位の国

48%

ランサムウェア グループのリーク サイトに掲載された被害企業のうち、米国を拠点とする企業の割合。



- 米国
- 英国
- ドイツ
- カナダ
- インド

2023 年第 1 四半期にリーク サイトに掲載された企業の規模

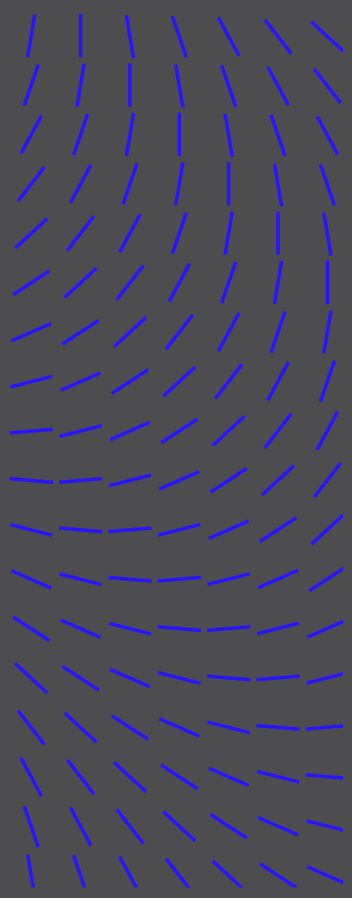
従業員数 (人)		年間売上高	
1. 51 ～ 200	32%	1. $10M ～ $50M	38%
2. 1,001 ～ 5,000	22%	2. $1B ～ $10B	23%
3. 11 ～ 50	15%	3. $1M ～ $10M	21%
4. 201 ～ 500	15%	4. $100M ～ $250M	11%
5. 501 ～ 1,000	15%	5. $500M ～ $1B	7%

国民国家の活動

国民国家の活動に関するインサイトは、脅威の状況をよりよく把握し、監視バイアスを減らすために複数のソースから収集されています。まず、国民国家グループの IOC と Trellix の顧客テレメトリの相関から抽出された統計を描いています。2 つ目に、セキュリティ業界が発行し、Threat Intelligence グループが厳しく吟味・解析・分析したさまざまなレポートから得られたインサイトを提供します。

前述したように、表示される統計は、キャンペーンの統計であり、検出そのものではありません。さまざまなログの集約、お客様による脅威シミュレーション フレームワークの使用、Threat Intelligence サポート情報との高度な相関により、データは私たちの分析目標を満たすように手動でフィルタリングされます。

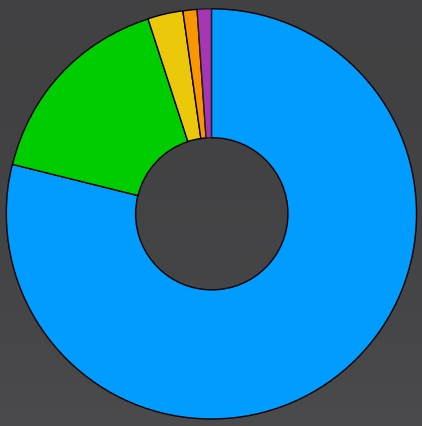
中国に関連する脅威は引き続き世界的な状況を支配しており、特に 2023 年第 1 四半期には、Mustang Panda が検出件数の大半を占めました。ステルス性を高めるためにサイドローディングその他の手法を全面的に利用しているため、中国が関連する APT グループは、他の脅威と比べてもマルウェア ツールのローテーション頻度が低い可能性があります。そうだとすれば、このような習慣が「予測バイアス」につながる、つまり中国が関連するハッシュの検出数の過大評価につながる可能性があります。



2023 年第 1 四半期の国民国家の活動の背後にある攻撃者の最も多い国

79%

2023 年第 1 四半期には、国家が関連する活動の大半を中国が占めました。



- 中国
- 北朝鮮
- ロシア
- イラン
- パキスタン

2023 年第1 四半期に最も多く確認された攻撃者

1.	Mustang Panda	72%
2.	Lazarus	17%
3.	UNC4191	1%
4.	Common Raven	1%
5.	APT34	1%

2023 年第 1 四半期の国民国家の活動で最も多用された MITRE ATT&CK 手法

1.	LDLL サイドローディング	14%
2.	ファイル / 情報の難読化解除 / デコード	11%
3.	イングレス ツール転送	10%
4.	ローカル システムからのデータ	10%
5.	ファイル / ディレクトリの探索	10%

2023 年第 1 四半期に国民国家の活動で最も多用された悪意のあるツール

38%

2023 年第 1 四半期、悪意のある国民国家の活動のうち 38% を PlugX が占めました。

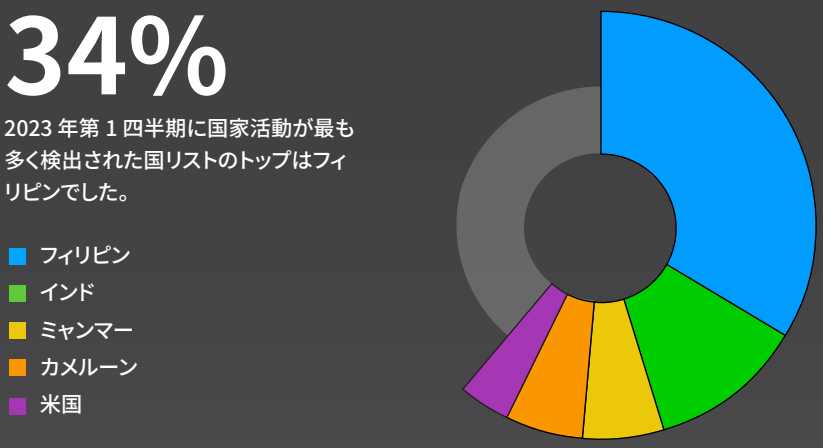
1.	PlugX	38%
2.	Cobalt Strike	35%
3.	Raspberry Robin	14%
4.	BLUEHAZE/DARKDEW MISTCLOAK	3%
5.	Mimikatz	3%

インドは、アジアおよび近隣地域のなかでも優れたサイバー プログラムを持つ主要国のひとつです。一部のグループ (主に中国に関連する攻撃者) は、インドの技術的、軍事的、政治的発展に多大なる関心を示しています。インドで検出が目立っているのは、Mustang Panda です。

2023 年第 1 四半期、国民国家による活動が最も多く検出された国

34%

2023 年第 1 四半期に国家活動が最も多く検出された国リストのトップはフィリピンでした。



2023 年第 1 四半期、国民国家による活動が最も多く検出された業種

脆弱性インテリジェンス

リバース エンジニアリングと脆弱性解析に関する Trellix Advanced Research Center の専門家は、最新の脆弱性を継続的に監視しながら、攻撃者がいかに脆弱性を利用しているか、またその攻撃の確率と影響をどう軽減するかについて、お客様にガイドラインを提供しています。

2023 年第 1 四半期において特に深刻で、にもかかわらず意外なほど知られていない発見があります。この期間に見つかった重大な脆弱性の多くは、その原因が古い CVE に対するパッチのバイパス、古くなったライブラリの利用から生じるサプライチェーンのバグ、あるいはかなり以前にパッチが公開された脆弱性にあることです。

たとえば、CVE-2022-47966 は、今年 1 月に話題になった Zoho の ManageEngine 製品に存在する致命的な脆弱性 (9.8) です。ManageEngine は全世界の多数の企業で使用されているので、この脆弱性の悪用が実際に検出されたとしても、それだけで驚くには当たりません。私たちを驚かせたのはその根本原因、すなわち Apache Santuario 1.4.1 が使われていることでした。驚くほど古く、XML インジェクトを許してしまう既知の問題が存在していたのです。

Zoho は 10 月に同社の製品全体にこの脆弱性のパッチを公開し、それからほぼ 3 か月後の第 1 四半期には、CISA が勧告を発表して、野放し状態の悪用を警告するとともに、ベンダーにパッチ適用を促しました。

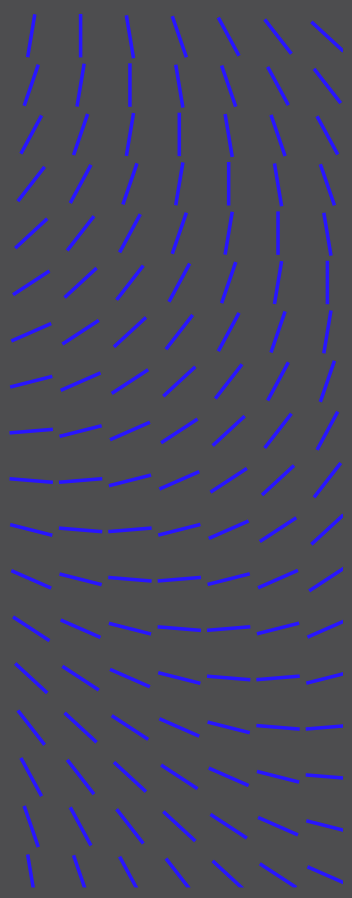
もうひとつの例が CVE-2022-44877、つまり Control Web Panel (CWP) に存在する重大な脆弱性です。直接の関連はありませんが、この脆弱性には前述の例と同じ特徴が多数存在します。前年の 10 月にパッチが公開されていたにもかかわらず、1 月にその悪用が広く確認されたもうひとつの 9.8 RCE だったのです。根本的な原因は、Black Hat トークにふさわしいものではなく、URL パラメータの標準的なシェル変数展開を使用したコマンド インジェクションでした。

3 つ目の例は、CVE-2021-21974 です。VMware ESXi の OpenSLP サービスに存在する脆弱性で、2021 年 2 月に対処されていました。広く悪用が確認された突然の流行から、実に 2 年も前のことです。2 月のバグレポートでこの脆弱性について報告したときには、インターネットに接続可能な約 48,000 台のサーバーでまだ脆弱なバージョンの ESXi が稼働しているという Shodan の指摘を報告しました。今日でもなお、その数はまだ 38,000 を超えており、22% 未満の変化にとどまっています。

日付	Shodan で報告された脆弱な ESXi サーバー
2023 年 2 月下旬	48,471
2023 年 4 月下旬	38,047

今年初めに Apple のデバイスを調査したとき、私たちも例をいくつか発見しました。CVE-2023-23530 と CVE-2023-23531 です。この 2 つの脆弱性は、その影響が RCE ではなくローカルの特権昇格に限定されるという点が、これまでの例とは異なります。といっても、2021 年には NSO Group がスパイウェア Pegasus を配備するために使った FORCEDENTRY エクスプロイトによって、これと酷似した脆弱性が利用されていたので、この脆弱性の重要性を見過ごしてよい理由にはなりません。実際、私たちが発見した 2 つの CVE は、FORCEDENTRY エクスプロイトのベースになったのと同じプリミティブ、つまり NSPredicate と呼ばれる無害なクラスを利用しています。残念なことに、FORCEDENTRY を緩和しようとする Apple のアプローチでは、広範な拒否リストが使用され、NSPredicate の悪用を補強する結果となりました。原因となる問題に対処できず、バイパスを許してしまっていました。

このような傾向を根拠として、ベンダーがセキュリティを真剣に考えていないと結論したり、攻撃者や研究者が古いエクスプロイトを再利用していることを嘆いたりしたくなりますが、その結論は正しくありません。脆弱性の研究者がさまざまな分析に取り組んでいるのは、有効な脆弱性研究が実際の攻撃者の優先順位をエミュレートするためであり、緩和策のバイパスや、パッチの進んでいない製品の古い CVE を発見できれば「車輪を再発明」するより ROI に有効だからです。



組織がこの傾向を正しく認識していれば、次のように結論することが重要です。つまり、脅威の最新の状況において、最先端の脅威検出技術は不可欠ですが、勝利の多くは、パッチ適用プロセスやサプライチェーンの審査といった基本的な部分で勝ち取ることができるということです。

メール セキュリティ

メール セキュリティの統計は、全世界の顧客ネットワークに配備されている複数のメール セキュリティ アプライアンスから生成されたテレメトリに基づいたものです。

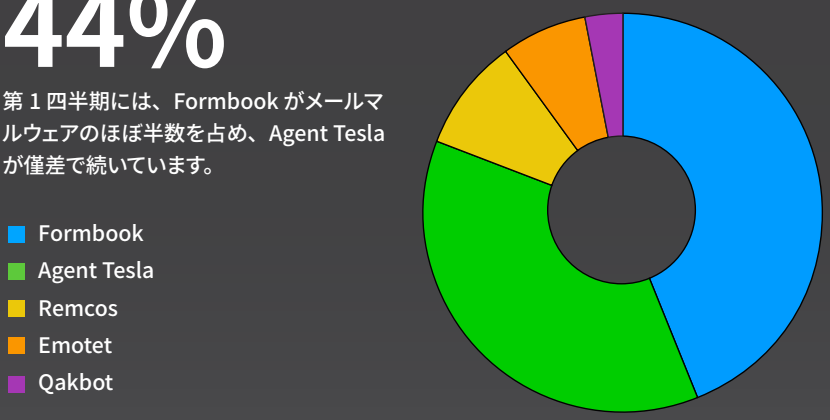
正規のブランドを利用してユーザーを欺き、認証情報を盗むフィッシング攻撃が増加しており、DWeb、IPFS、Google 翻訳がこのメール攻撃に多用されています。フリーメールや、PayPal Invoicing や Google Forms など同等のサービスを悪用して、ヴィッシング攻撃をしかけ、検知を回避している攻撃もあります。この期間には、Scribd、LesMills、Google Play ギフトカードなど新しいブランドも標的になっています。

また、こうした攻撃に使われた特定のマルウェアについては、Formbook と Agent Tesla のどちらも、昨年末と比べて 2023 年第 1 四半期には顕著な増加を示しています。これは、Remcos、Emotet、Qakbot に比べ、この 2 つのマルウェアの入手も配備も容易であることが原因だろうと考えられます。

2023 年第 1 四半期に最も多く見られたメール マルウェアの戦術

44%

第 1 四半期には、Formbook がメールマルウェアのほぼ半数を占め、Agent Tesla が僅差で続いています。



2023 年第1 四半期に最もメール フィッシング詐欺の標的となった国

30%

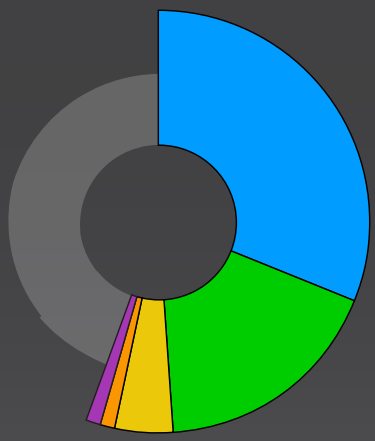
第 1 四半期には、米国と韓国がフィッシング詐欺の被害を受けた主要な国であり、両国をあわせると全世界のフィッシング詐欺の約 3 分の 2 を占めています。

1.	米国	30%
2.	韓国	29%
3.	台湾	10%
4.	ブラジル	8%
5.	日本	7%

2023 年第 1 四半期に最もメール フィッシング詐欺の標的となった製品およびブランド

38%

何百ものブランドが標的にされていますが、2023 年第 1 四半期に特に標的にされたのは Microsoft 製品でした。



に悪意のあるメールの影響を最も受けたセクター 2023 年第1 四半期

1.	政府	11%
2.	金融サービス	8%
3.	製造業	6%
4.	テクノロジー	6%
5.	エンターテイメント	5%

2023 年第 1 四半期の悪用度の高い WEB ホスティング プロバイダー

1.	IPFS	41%
2.	Google Translate	33%
3.	Dweb	16%
4.	AmazonAWS Appforest	3%
5.	Firebase OWA	3%

2023 年第 1 四半期にフィッシング攻撃で最も多く使われた回避手法

79%

2023 年第 1 四半期にフィッシング攻撃で最も多用された回避テクニックは、リダイレクトに基づく回避の 302 件でした。

46%

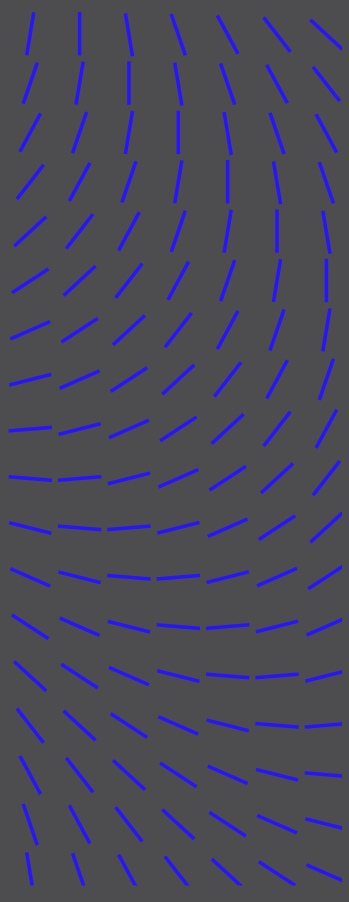
Captcha ベースの攻撃が、2022 年第 4 四半期と比較して第 1 四半期に大幅に増加しています。

ネットワーク セキュリティ

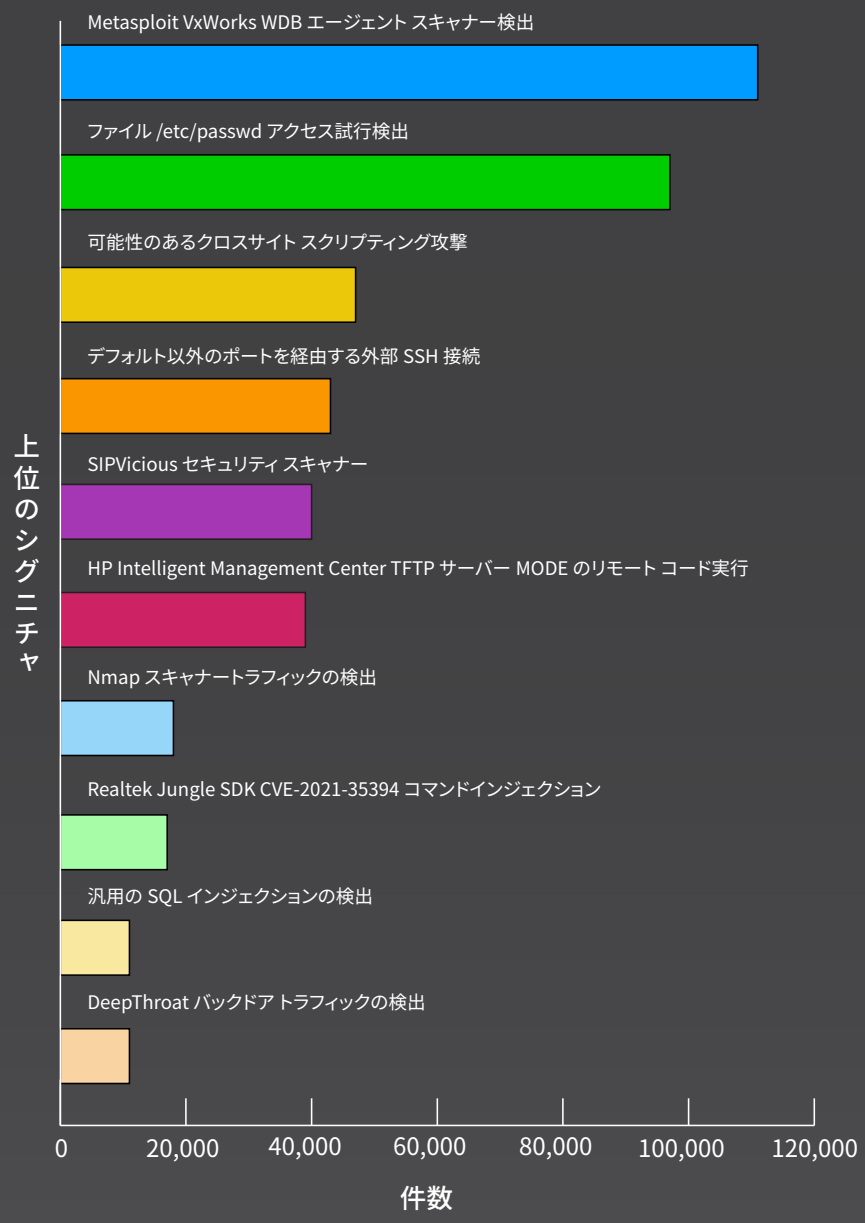
ネットワークリサーチチームは、お客様を脅かすネットワークベースの攻撃を検知してブロックするために、Trellix Advanced Research Center のネットワーク研究チームは、キル チェーンの各種領域、つまり偵察、初期侵害から C2 通信、ラテラル移動 TTP までを調査しています。

2023 年第 1 四半期で最も注目すべきマルウェア コールバックのトレンド

STOP ランサムウェア活動が減少	94%
Amadey によって配布された LockBit ランサムウェアの増加率	25%
Android マルウェアの活動の増加率	12.5%
Ursnif の活動の前年比	10%
Smoke Loader の活動の増加率	7X
Amadey の活動の増加率	4X
Cobalt Strike の活動の増加率	3X
Emotet の活動の増加率	2X



2023 年第 1 四半期に外部向けサービスに対する影響が最も大きかった攻撃



クラウド インシデント

Amazon、Microsoft、Google などが開発・提供するサービスに対するクラウド インフラストラクチャ攻撃は増加の一途をたどっています。以下の表は、顧客別およびクラウド プロバイダー別にクラウドベースの攻撃テレメトリ データについて説明したものです。

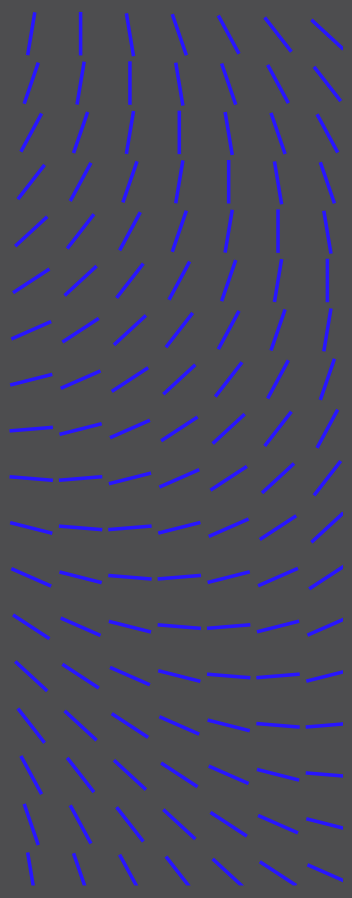
2023 年第 1 四半期の MITRE ATT&CK 手法別の上位 AWS 検出

	AWS	Microsoft Azure	GCP
有効なアカウント	3,437	4,312	997
クラウド コンピューティング インフラストラクチャ変更	4,268	0	17
比標準 ポート	115	0	17
多要素 認証	190	1,534	22
ネットワーク サービス検出	141	93	0
ブルートフォース	25	1,869	22
プロキシ	299	2,744	135
アカウント 検出	264	68	787
メール転送 ルール	25	0	22
API を介した実行	1,143	0	252

方法論

データ収集 : Trellix と当社の経験豊富な、世界でもトップクラスの専門家は、本レポートを構成する統計、トレンド、インサイトをグローバルな幅広いソースから収集しています。

- **クローズドのソース :** 場合によっては、公共と民間の両方のネットワークによって全世界に配備されている顧客のサイバー セキュリティ ネットワークと防御フレームワーク上でテレメトリが生成され、これには Trellix のセキュリティ ソリューションによって技術、インフラ、およびデータ サービスを提供するものも含まれます。このようなシステムは数百万に上り、10 億個のセンサーからデータを生成しています。
- **オープンソース :** その他のケースで、Trellix は特許取得済み、プロプライエタリ、オープンソースのツールを組み合わせて、インターネット上のサイト、ログ、データ リポジトリをスクレイピングしており、攻撃者がランサムウェアの被害者に関する情報や被害者の情報を公開する「リーク サイト」のようなダーク ウェブも活用することがあります。



正規化 : 収集されたデータは、弊社の Insights および ATLAS プラットフォームへ送られます。機械学習、自動化、そして人間の鋭敏な感覚を活用して、チームは集中的、統合的、反復的なプロセスをひととおり実施します。つまり、データを正規化して結果を補強し、個人データを削除して、攻撃手法やエージェント、業種、地域、戦略、結果などに関する相関関係を特定します。

分析 : 次に Trellix は、(1) 脅威インテリジェンスの広範なナレッジ ベース、(2) 高い評価と認定を受けた情報ソースからのサイバー セキュリティ業界レポート、(3) Trellix のサイバー セキュリティ アナリストや調査員、リバースエンジニアリング専門家、フォレンジック研究者、脆弱性専門家の経験と洞察力を参考にして、この膨大な情報を分析します。

解釈 : 最後に、Trellix チームは、サイバー セキュリティ リーダーと SecOps チームが (1) サイバー脅威の環境における最新のトレンドを把握し、(2) この視点に立って将来的なサイバー攻撃を予測、防止、防御する機能を向上させるうえで役に立つ有意義なインサイトを抽出し、確認して検証します。

リソース

脅威レポートのアーカイブ

The Mind of the CISO (CISO の考え方)

Trellix Advanced Research Center Discovers a New Privilege Escalation Bug Class on macOS and iOS

A Royal Analysis of Royal Ransom

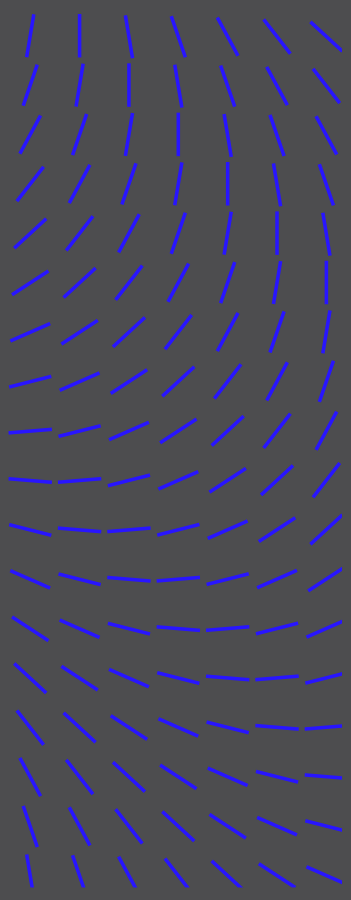
Feeding Gophers to Ghidra

TWITTER

Trellix ARC

脅威レポートのアーカイブを見る

Trellix Advanced Research Center

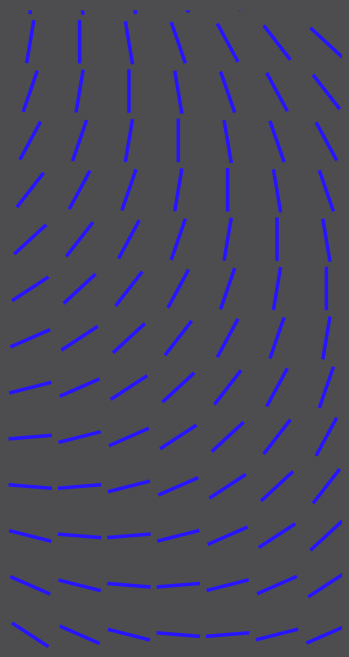


TRELLIX ADVANCED RESEARCH CENTER について

サイバー セキュリティ業界の最も包括的な憲章を掲げ、Trellix Advanced Research Center は、脅威を取り巻く環境全体の中で、新たな手法、トレンド、攻撃者の最前線に立ち、全世界のセキュリティ オペレーション チームにとって不可欠なパートナーとして活動しています。Trellix Advanced Research Center は、セキュリティ アナリストにインテリジェンスと最先端のコンテンツを提供することで、弊社の最新 XDR プラットフォームを支えています。さらに、Trellix Advanced Research Center の Threat Intelligence グループは、世界中のお客様にインテリジェンス製品やサービスを提供します。

TRELLIX について

Trellix は、サイバー セキュリティの将来と気持ちのこもった業務を再定義するグローバル企業です。今日の最も高度な脅威に直面している組織は、弊社のオープンでネイティブな eXtended Detection and Response (XDR) プラットフォームを使用することにより、業務の保護と耐久性に自信を持つことができます。Trellix は、広範なパートナー エコシステムとともに、機械学習と自動化を通じて技術革新を加速させ、生きたセキュリティによって 40,000 以上の企業や政府機関のお客様を支援しています。



詳細は、Trellix.com もご確認ください。

Trellix について
Trellix は、サイバーセキュリティの将来を再定義するグローバル企業です。今日の最も高度な脅威に直面している組織は、弊社のオープンでネイティブな eXtended Detection and Response (XDR) プラットフォームを使用することにより、業務の保護と耐久性に自信を持つことができます。Trellix のセキュリティ専門家は、広範なパートナー エコシステムとともに、機械学習と自動化を通じて技術革新を加速させ、40,000 以上の企業や政府機関のお客様を支援しています。

072022-05