Trend Research

TREND MICRO

2024 年 上半期
サイバーセキュリティレポート

はじめに

「2024 年 上半期サイバーセキュリティレポート」は、2024 年 1～6 月における日本と全世界の脅威動向をまとめたレポートです。本レポートで使用する脅威データは 2024 年上半期 6 か月間の集計を基本としますが、個々の事件や重大なトピックに関しては本稿編集時点である 2024 年 7 月以降の状況に言及している場合があります。

昨年 2023 年、日本国内では法人利用者におけるランサムウェア被害、個人利用者におけるネット詐欺被害の双方が過去最大規模の被害[1]となり、サイバー犯罪の活発化はまさに最盛期に入った感があります。

2024 年に入ってもその傾向は世界的に継続しており、攻撃者たちは、素早く巧妙で高度な脅威とキャンペーンを生み出すため、常に新たな技術の悪用、世界的な重要イベントの悪用、そして適切に管理されていない脆弱な資産の侵害機会を探っています。

2024 年上半期におけるトレンドマイクロの観測では、サイバー犯罪者たちが人工知能（AI）などの新技術[2]を従来の攻撃手法に組み込み、オリンピックや国政選挙といった世界的イベントを悪用[3]し、さらに設定ミスや露出した資産を狙って密かにシステムに侵入し、機密データを盗み取る行為などが明らかになりました。

これまでの数年間、サイバーセキュリティは、ますます複雑化し巧妙になる攻撃に対応するため、進化を続けてきました。そして今後も、セキュリティ業界は、ビジネスリーダーやセキュリティチームが絶えず変化する脅威とリスクに立ち向かう中、確かなデータに基づく洞察と包括的なリスクベースのアプローチを通じて、システムとデータの安全を守るために、常に一歩先を行く必要があるでしょう。

このレポートでは、2024 年上半期の 6 ヶ月間にトレンドマイクロが注目した最も重要なサイバーセキュリティ事象と、顕著なセキュリティトレンドを紹介しています。また、サイバー脅威の現状をより明確に把握するため、当社の主力サイバーセキュリティプラットフォームである Vision One の一部を成す、拡張検知および対応（XDR）ソリューションと、サイバーリスクのライフサイクル管理ソリューションであるアタックサーフェスリスクマネジメント（ASRM）からのデータも掲載しています。

[1] https://resources.trendmicro.com/jp-docdownload-form-m681-web-2023-annualsecurityreport.html
[2] https://www.trendmicro.com/en_us/what-is/machine-learning/artificial-intelligence.html
[3] https://www.trendmicro.com/en_us/research/24/e/poll-security.html

※註１：データを含む本レポートの記述は編集時点での最新リサーチに基づくものですが、その後に新たな事実が判明することもあります。

※註２：本レポートに掲載されるデータ等の数値は特に明記されていない場合、トレンドマイクロのクラウド型セキュリティ基盤「Trend Micro Smart Protection Network（SPN）」による 2024 年 6 月 30 日付の統計データが出典となります。

※註３： 数値データに関しては表現上四捨五入などで表記する場合があります。四捨五入表記の場合、割合を示す円グラフ上の数値の合計が 100%にならない場合があります。

※註４： 本レポートで掲載した画像について、直接の危険や権利侵害に繋がりかねないと判断される部分には修正を施しています。

日本セキュリティラウンドアップ

国内法人利用者での脅威：ランサムウェア

国内個人利用者での脅威：ネット詐欺

まとめ

国内法人利用者での脅威：ランサムウェア

この数年、国内の法人利用者に最も甚大な被害を与えている脅威がランサムウェア攻撃であることには異論の余地がないでしょう。2024 年上半期に国内法人が公表したランサムウェア被害はトレンドマイクロで確認しただけでも 38 件を数えました。これは前年同時期となる 2023 年上半期と同数であり、過去最多となった 2023 年のペースが維持されていることに警戒が必要です。

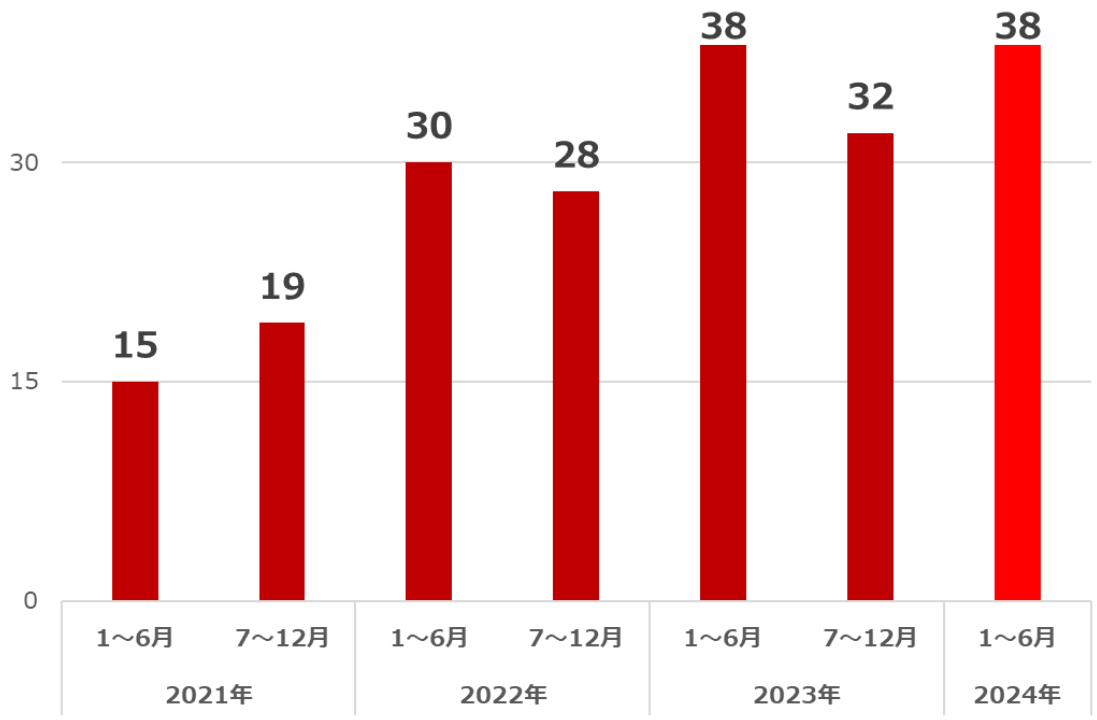


図 1：国内組織が公表したランサムウェア被害件数推移
（公表内容を元に整理、海外拠点での被害も含む）

重大なランサムウェア被害が示す法人組織のセキュリティ課題

攻撃者は常に侵入可能な法人ネットワークの弱点を探しており、ランサムウェア被害が発生してしまったことはすなわち、攻撃者になんらかの弱点を見つけ出されてしまったことを意味します。2024 年ここまでに発生したランサムウェア被害の中でも、特に注目を集めた重大事例において浮き彫りになった法人組織にとってのセキュリティ課題をまとめます。

・データセンターの侵害リスク

この期間に発生したランサムウェア被害事例の中でも、最も注目された事例として 6 月に発生した KADOKAWA グループの事例が挙げられます。公表によれば、6 月 8 日時点でグループ会社が運営するデータセンター内の複数サーバがアクセス不能となり、グループの複数の

ウェブサイト、特にドワンゴ社が提供する複数のウェブサービスが利用不可になりました[4]。その後、6 月 14 日にウェブサービスの停止原因として、データセンターに対する「ランサムウェアを含む大規模なサイバー攻撃」によるものであることがドワンゴ社より公表[5]されました。

データセンター内に構築したシステムが侵害を受けたという点では、2023 年 6 月発生のクラウドサービス「社労夢」[6]、および 7 月発生の名古屋港統一ターミナルシステム[7]に続く重大被害となります。名古屋港事例では脆弱な VPN が原因となった可能性が指摘されていますが、本事例では何らかの方法で窃取されたアカウント情報によって社内ネットワークに侵入されたことが根本原因と推測されることが 8 月に入り公表[8]されています。データセンターのプライベートクラウドはどこからでも遠隔で管理、運用が可能ですが、その管理、運用のための遠隔アクセスの経路が逆手に取られ、侵害を許している図式となっています。

このようなデータセンターの侵害が継続して発生している事実からは、データセンター上のプライベートクラウドサービスも攻撃者にとっては侵入可能なネットワーク、つまりアタックサーフェス（攻撃対象領域）の 1 つに過ぎないことを示しています。この事例の発端として、今後法人組織においては、自組織システムのクラウド移行はアタックサーフェス拡大の可能性を含んでいることを認識し、リスク管理を行っていく必要があるものと言えます。

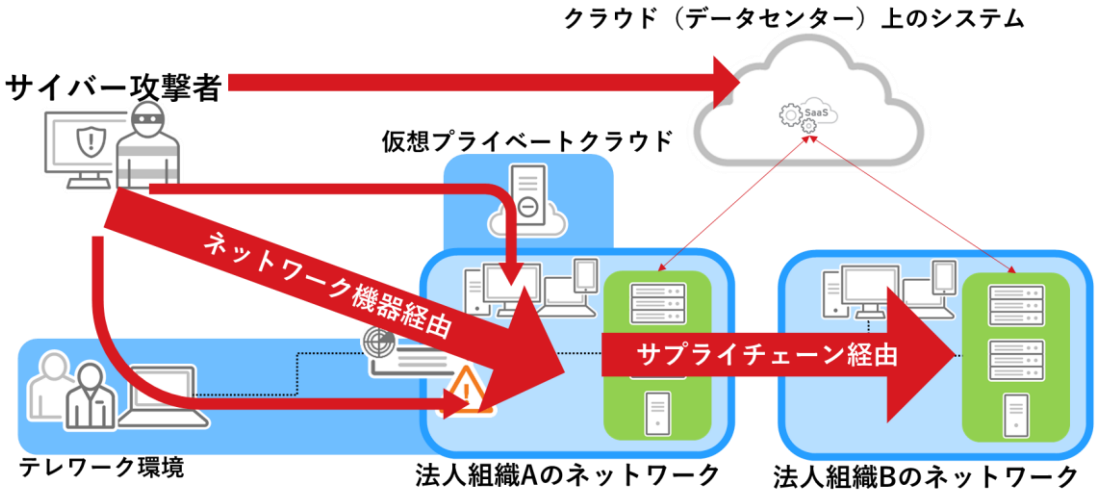


図 2：2024 年までに国内で発生したランサムウェア被害におけるアタックサーフェスの拡大を示す概念図

[4] https://prtimes.jp/main/html/rd/p/000014844.000007006.html
[5] https://dwango.co.jp/news/5131439897051136/
[6] https://contents.xj-storage.jp/xcontents/AS97180/33470ee8/09df/43be/8620/114a82ad17c8/140120230609500838.pdf
[7] https://meikoukyo.com/archives/3336
[8] https://dwango.co.jp/news/5109725381263360/

・第三者の行為による被害者への悪影響

この KADOKAWA グループの事例では、インシデントとは直接関係のない第三者の行動が被害者に大きく影響する事態が複数発生しました。その 1 つは 6 月 22 日の時点で身代金交渉のやり取りとされる内容を Web メディアが報じた[9]ことです。これに対し KADOKAWA は同日、「このような記事をこのタイミングで出すことは、犯罪者を利するような、かつ今後の社会全体へのサイバー攻撃を助長させかねない報道を行うメディアに対して強く抗議をする」という旨を発表[10]しています。またもう 1 つはランサムウェアギャングがリークサイト上で暴露した情報を、第三者が勝手に拡散する行為が見られた[11]ことです。6 月 27 日、ランサムウェアギャング「BlackSuit」のリークサイト上に本件に関連するデータが掲載されました。その後、匿名掲示板や SNS などにおいてリークサイトから取得した暴露情報をさらに拡散させる動きが確認されました。

交渉内容の報道にせよ、暴露情報の更なる拡散にせよ、復旧作業と共に攻撃者からの多重脅迫に晒されているランサムウェア被害者にとって対応すべき事項がさらに増えることになります。復旧に注力すべきタイミングでさらに対応事項が増えることは、被害者をさらに苦しい状況に追い込むことになり、結果的に脅迫を行う攻撃者を利することと言えます。

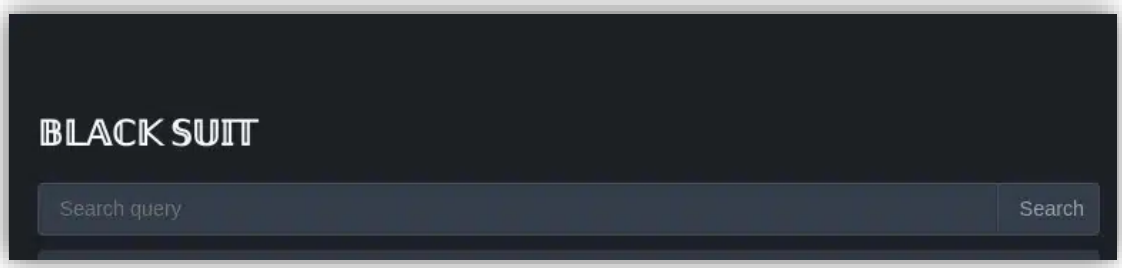


図 3：ランサムウェアギャング「BlackSuit」のリークサイト

・データサプライチェーンのリスク

5 月に発生した、印刷業務などの請負サービスを提供しているイセトー社のランサムウェア被害[12]は、公表当時は大きな注目を集めることはありませんでした。しかし、攻撃グループ「8 Base」がこの事例で窃取したとするデータを 6 月にリークサイト上で暴露したことで情報の漏洩が発覚[13]し、事態が一変します。情報漏洩の確認を受け、同社に業務委託してい

[9] https://newspicks.com/news/10160526/
[10] https://tp.kadokawa.co.jp/.assets/240622_release_zA69Tsjh.pdf
[11] https://dwango.co.jp/news/5108521951559680/
[12] https://www.iseto.co.jp/news/news_202405-3.html
[13] https://www.iseto.co.jp/news/news_202407.html

た全国の自治体や企業などが相次いで本事例に関連する情報漏洩被害を発表しました。その数は 7 月末時点で確認できただけでも 50 組織以上となっています。

図 4：ランサムウェアギャング「8 BASE」のリークサイト

本事例は業務上の関係性を経由してサイバー攻撃被害が拡大するサプライチェーンリスクの中でも、特に他組織への情報の委託、つまり「データサプライチェーン」に関するリスクを象徴する事例と言えます。近年では、このような業務委託上のリスクを回避するため、外部委託先監査の重要性が認識され始めています。ただし本事例の中では、本来個人情報を取り扱ってはならないはずの基幹系ネットワークに情報が保存されていたこと[14]や、委託業務の完了後に該当データを削除する契約になっていたが一部が保存されていたケース[15]や、削除の報告を受けたはずのデータが実際には削除されておらずに漏洩したケース[16]が確認されています。最悪を想定するリスク管理の上では、委託先でこのような不適切な処理が行われていることを監査で感知できなかった事態も勘案し、外部に預けた情報は漏洩する前提で対処を検討しておく必要があるかもしれません。

[14] https://www.pref.tokushima.lg.jp/ippannokata/kurashi/zeikin/7241915/
[15] https://www.sankei.com/article/20240607-IZJEXJ46WBPGJL3VC6DJFOQAQI/
[16] https://www.pref.tokushima.lg.jp/ippannokata/kurashi/zeikin/7241915/

国内個人利用者での脅威：ネット詐欺

ここ数年、個人利用者におけるネット上の危険は「ネット詐欺」に集約されてきました。2024 年上半期における各種詐欺サイトへの誘導件数は 2021 年以来初めて 2 千万件を切りましたが、なお高止まりの状況と言えます。

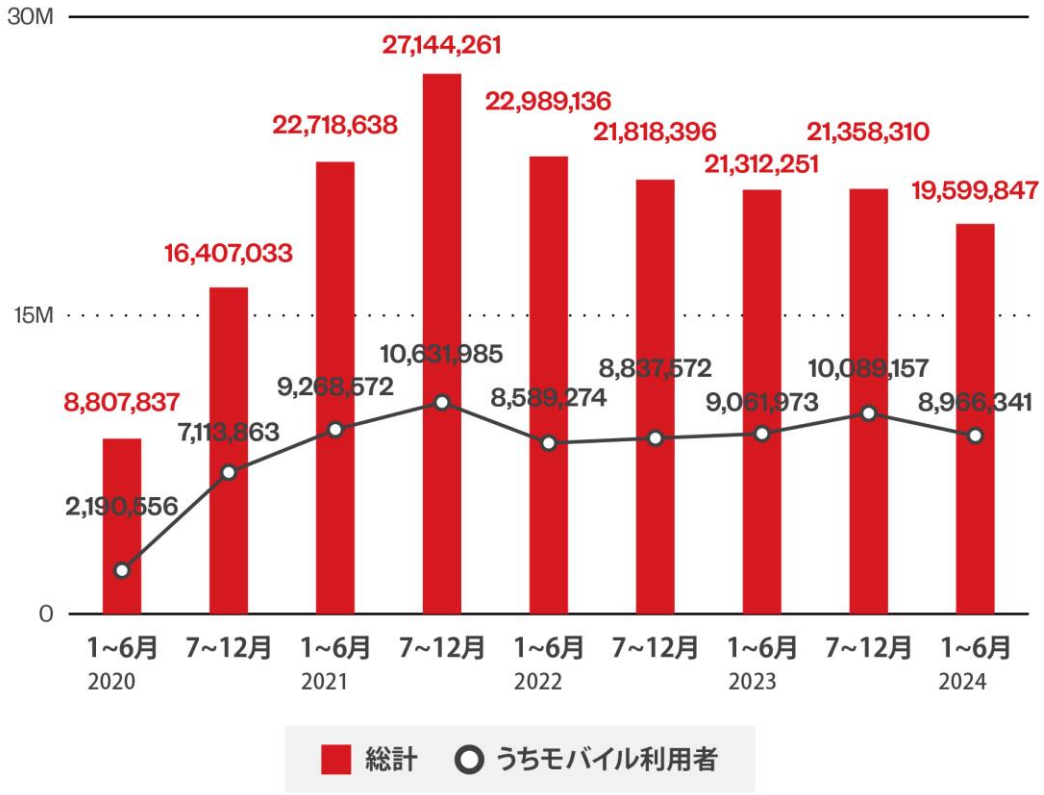


図 5：国内から各種詐欺サイトに誘導された利用者の端末台数[17]の推移と内訳

認証、決済、本人確認を脅かすフィッシング詐欺

フィッシングメールや誘導先の詐欺サイトで偽装される実在組織としては、各種の銀行、クレジットカードブランド、携帯キャリアから Apple や Google、Amazon などの有名企業をはじめとして、電気、ガス、水道などの公共料金関連、税金や給付金に関連した政府機関などを確認しました。

[17] SPN の問い合わせ IP のユニーク数を利用者の端末台数と定義

図 6：銀行のフィッシングサイトへ誘導するフィッシングメール（左）と
誘導先のネット銀行を偽装するフィッシングサイト（右）の例（2024 年 2 月確認）

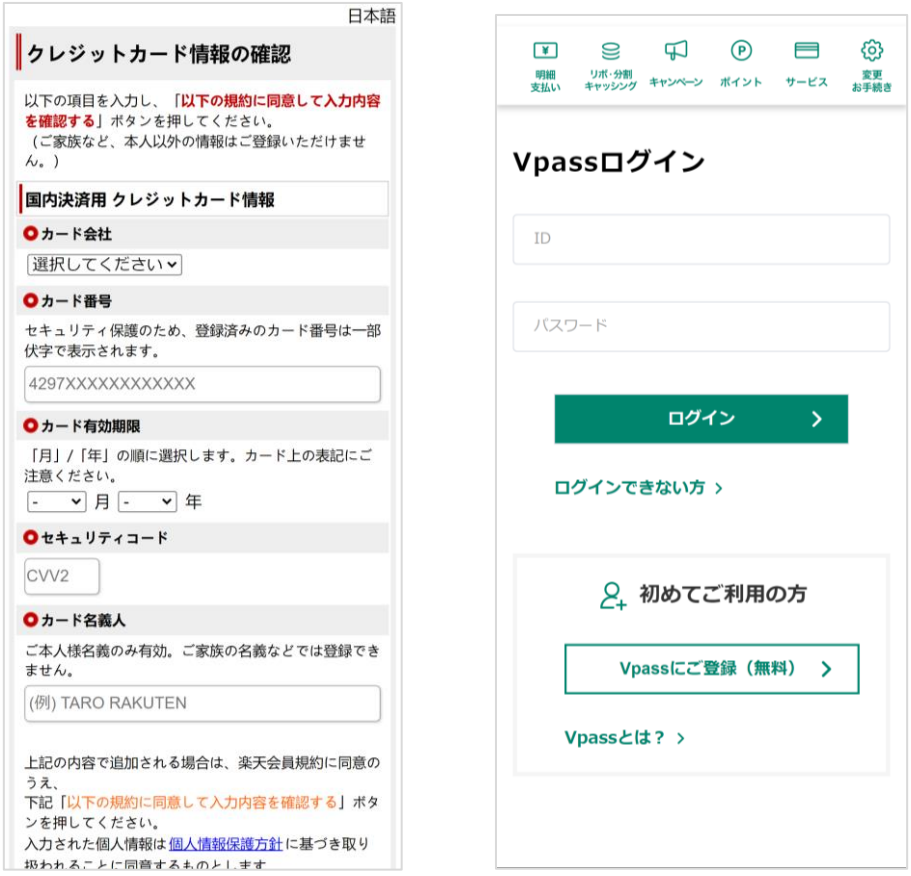


図 7：クレジットカード会社を偽装するフィッシングサイトの例（2024 年 5 月確認）

図 8：公共料金の滞納を偽装するフィッシングサイトの例（2024 年 5 月確認）
次に進むとクレジットカード情報の入力を促される

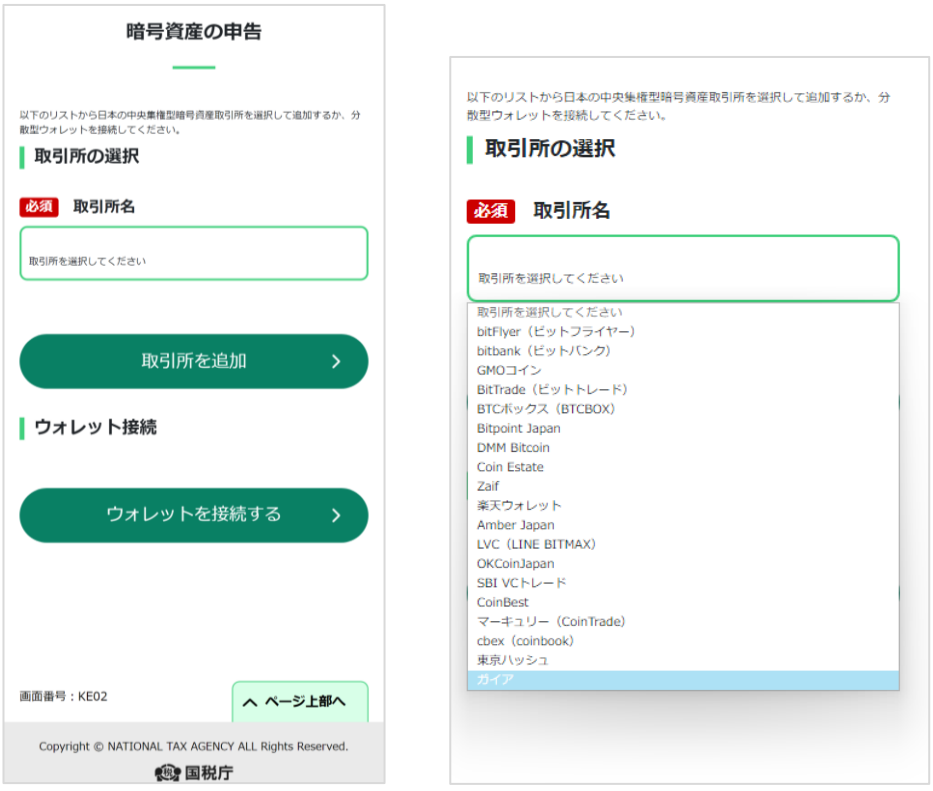


図 9：国税庁を騙り、暗号資産の詐取を狙うフィッシングサイトの例（2024 年 6 月確認）

ワンタイムパスワードなどの追加認証を突破するための「リアルタイムフィッシング」や、運転免許証、マイナンバーカード、パスポートなどの本人確認書類のアップロードを促す悪質な手口についても、以前から繰り返し確認しています。追加認証の突破はネットバンキングの不正送金などに直結する手口、本人確認書類の詐取は電子本人確認（eKYC）の突破に繋がる手口と言えます。特に eKYC の突破は昨今国内でも被害事例が報告されている SIM スワップ詐欺の被害[18]などに繋がっているものと考えられます。

図 10：リアルタイムフィッシングによる追加認証突破の概念図
ワンタイムパスワードなどの追加認証のための情報がその場で詐取され突破される

図 11：追加認証の突破を狙うフィッシングサイトの例（左：SMS 認証、右：スマホ認証）
（2024 年 6 月確認）

[18] https://www.itmedia.co.jp/news/articles/2405/30/news156.html

図 12：金融庁を騙り、運転免許証、パスポート、マイナンバーカードなど
本人確認書類のアップロードを促すフィッシングサイトの例（2024 年 6 月確認）

図 13：クレジットカードの手続きを偽装し本人確認書類のアップロードを促すフィッシングサイトの例
（2024 年 5 月確認）

スマートフォンの不正アプリによるスミッシングの拡散

詐欺サイトへの誘導手法としては SMS のフィッシングメッセージ（スミッシング）が主流となってきています。スミッシングメッセージ送信のインフラとしては引き続き、スマートフォンに感染した不正アプリが使われています。このスミッシング送信を担う不正アプリとしては、XLOADER（別名：MoqHao）と KeepSpy の 2 種が挙ります。これらの不正アプリが送信するスミッシングメッセージには、フィッシングサイトへ誘導する目的と共に、自身の感染を拡大するための不正サイトへ誘導するケースもあることは以前から変わりません。

図 14：KeepSpy によるスミッシングメッセージから誘導されるフィッシングサイトの例
（左）Android 端末でアクセスした場合には KeepSpy をインストールさせるサイトへ誘導
（右）iPhone でアクセスした場合には未払金の表示から電子マネーを詐取するサイトへ誘導

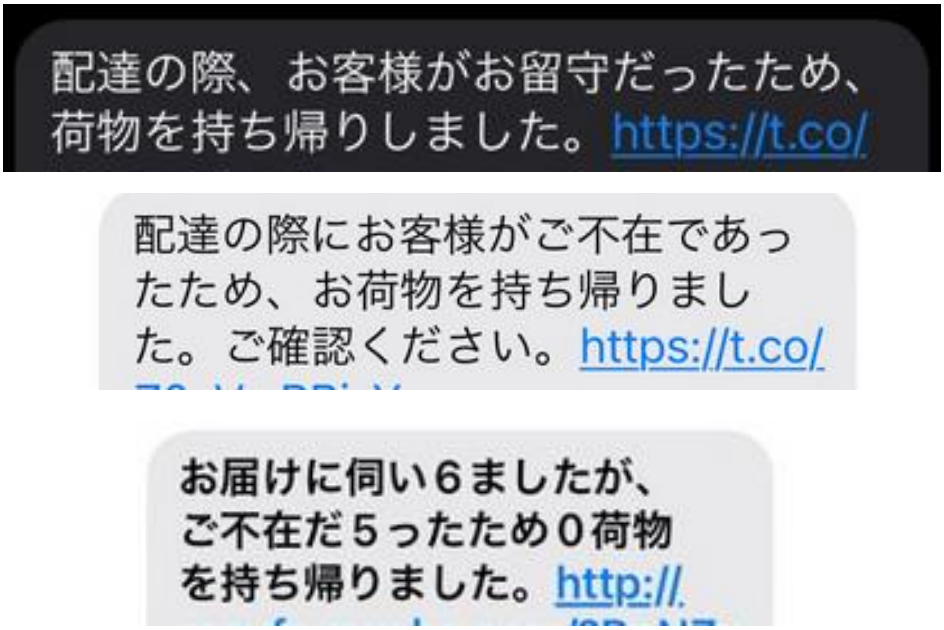


図 15：XLOADER による宅配荷物の不在通知を偽装するスミッシングメッセージの文面パターン例
6 月には 100 以上の文面パターンを観測したことも

図 16：警察を偽装するスミッシングメッセージと誘導先フィッシングサイトの例

RCS グループチャットを悪用したスパムメッセージ

「RCS（リッチコミュニケーションサービス）[19]」は、携帯電話における SMS/MMS や音声通話の代替を目指した規格です。規格自体は 2008 年にスタートしていますが、スマートフォンでの実装は比較的最近であり、Android OS では 2016 年に OS レベルで対応済み、iPhone では 2024 年 9 月に登場予定の iOS18 から対応開始が発表[20]されています。

トレンドマイクロの監視の中では 2024 年 4 月頃から、この RCS グループチャット機能を悪用したネット詐欺への誘導が観測されるようになってきました。今後 iPhone にも対象が広がることで RCS の悪用も拡大していくものと予測されます。

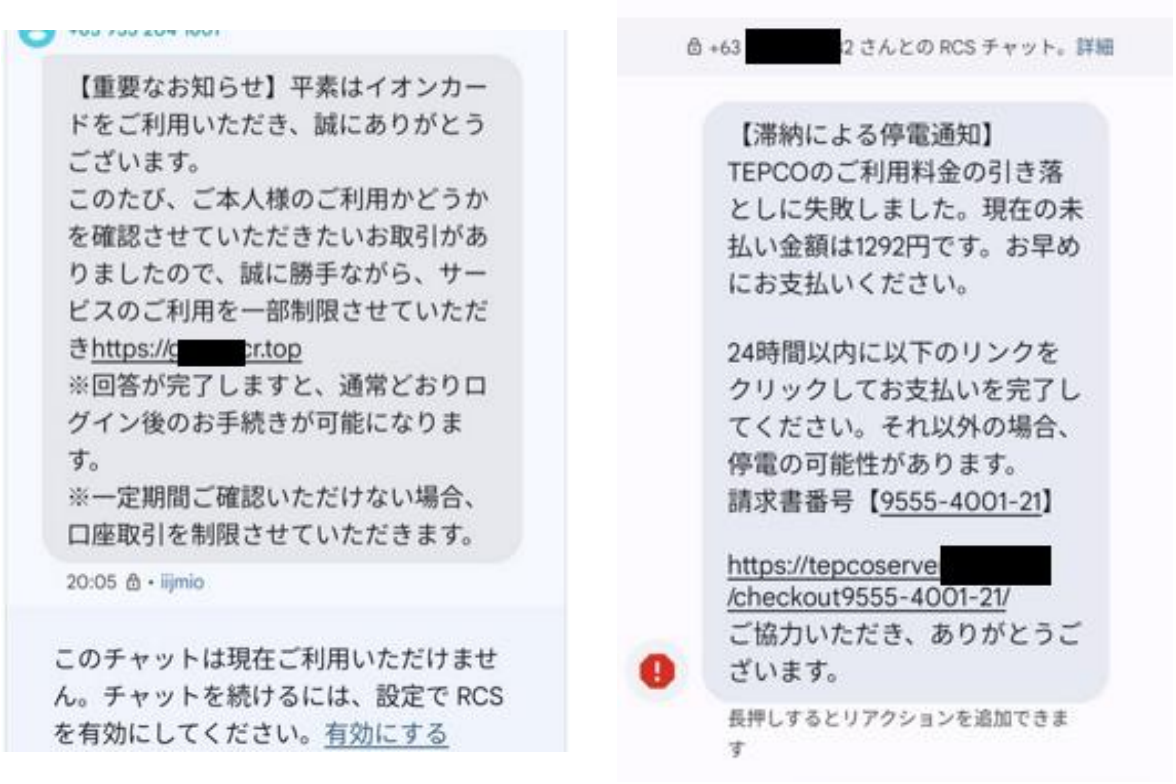


図 17：RCS グループチャットによるスパムメッセージ例（2024 年 4 月以降確認）

[19] https://www.gsma.com/solutions-and-impact/technologies/networks/rcs/

[20] https://wired.jp/article/guide-to-rcs-why-it-makes-texting-better/

サポート詐欺

2023 年に手口の悪質化と被害の深刻化が進んだサポート詐欺ですが、2024 年上半期にトレンドマイクロに入ったサポート詐欺の報告件数は 4715 件となりました。前年 2023 年は 1 年間で 4837 件であり、半年時点で昨年 1 年間とほぼ同数になっています。

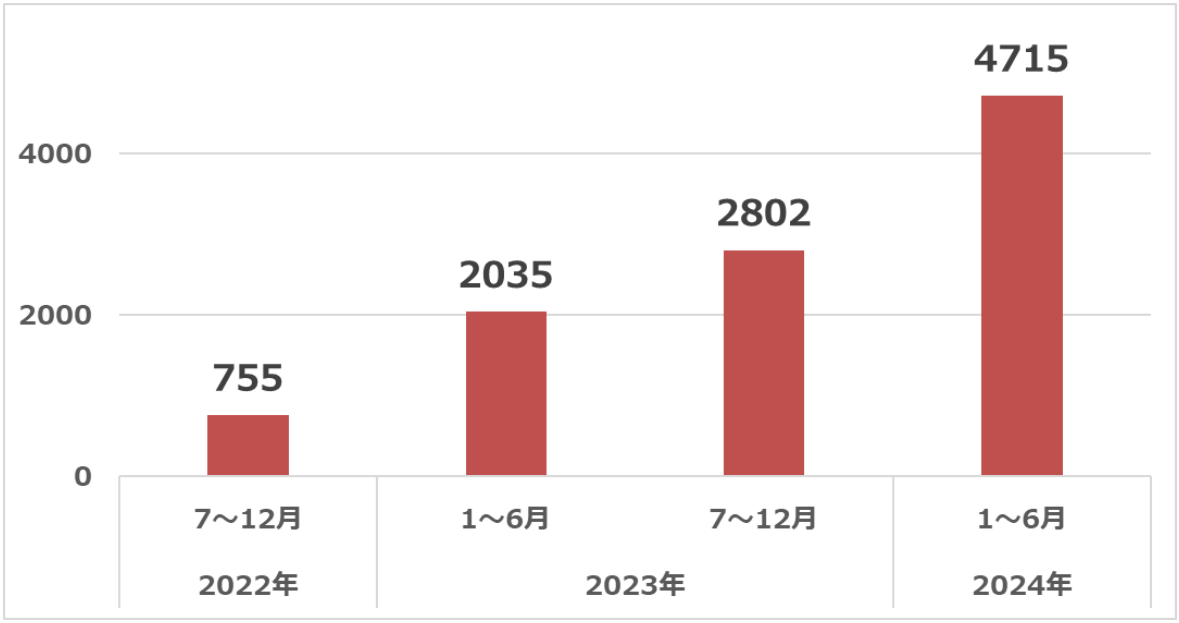


図 18：トレンドマイクロサポートセンターが受けたサポート詐欺報告件数の推移

偽警告表示を行うサポート詐欺サイトへの誘導に関しては、Web 上の不正広告経由の他、ブラウザ通知経由や Web 検索広告経由も確認しています。

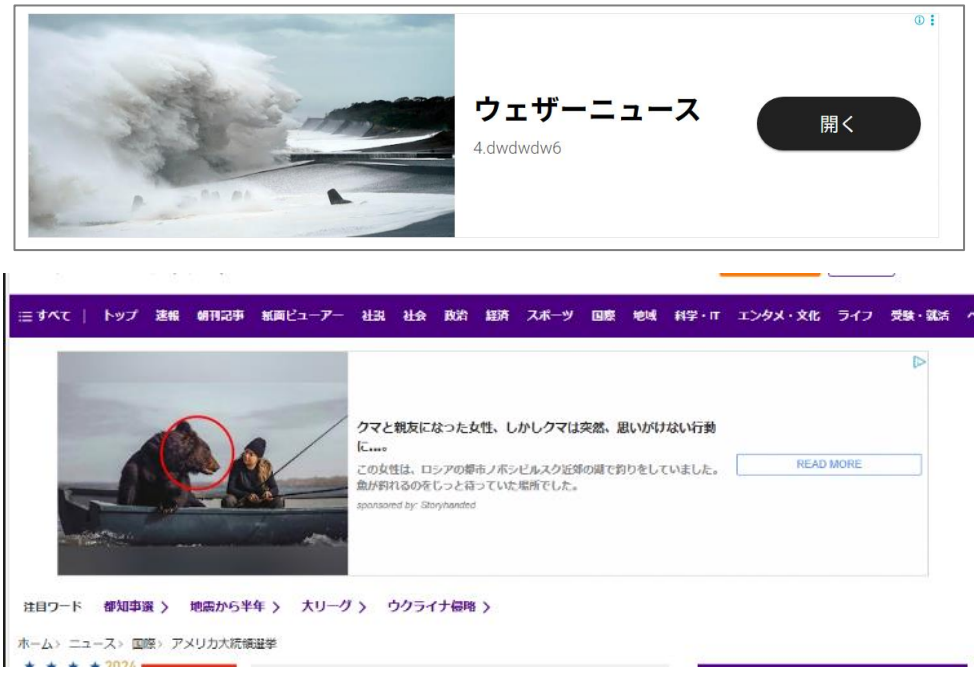


図 19：サポート詐欺（偽警告）サイトへの誘導を確認した不正広告の例
（上：2024 年 4 月確認　下：2024 年 6 月確認）

図 20：サポート詐欺（偽警告）サイトへの誘導を確認したブラウザ通知スパムの表示例（2024 年 4 月確認）

また Web 上の不正広告では利用者の興味を引くための記事的な広告表示ではなく、「続ける」、「広告をスキップ」など Web ページ上のボタンを偽装したものも確認しています。これは利用者の誤解からクリックすることを狙ったものと言えます。

図 21：Web ページ上のボタンを偽装した表示の不正広告の例（2024 年 6 月確認）

このような偽警告表示を行うサポート詐欺サイトへ誘導する不正広告は、けして不審なページだけに表示されるものではありません。一般のサイト上でも Google 広告など正規のネット広告の仕組みを経由して表示されてしまうことが常態化しています。一般の新聞サイトやポータルサイト上で不正広告が表示されたケースも 2024 年には確認しており、場合によっては Web を閲覧しているだけで広告をクリックしなくとも自動的に偽警告表示が行われたケースすら確認しています。

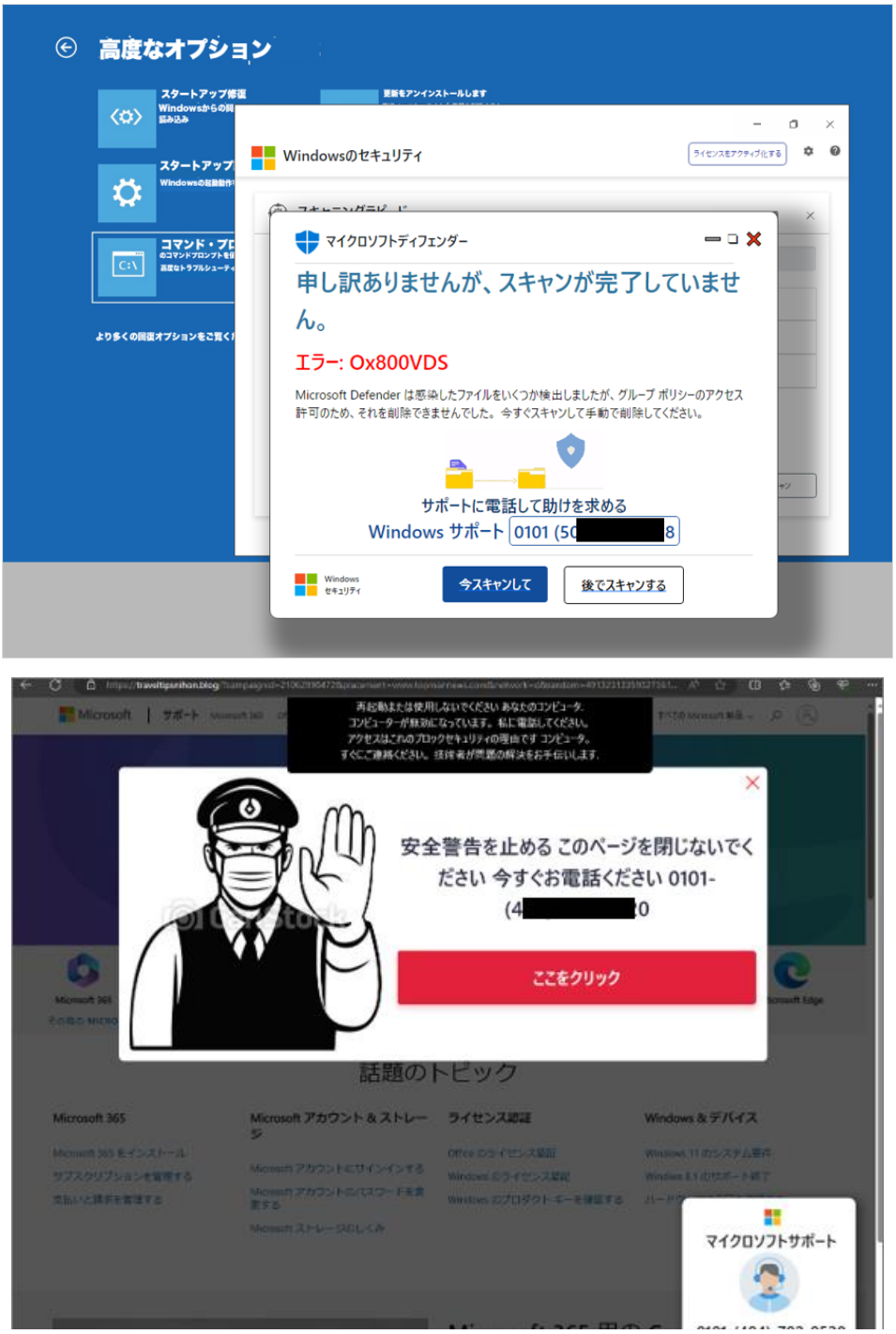


図 22：誘導先のサポート詐欺（偽警告）サイトの表示例（2024 年 4 月以降に確認）

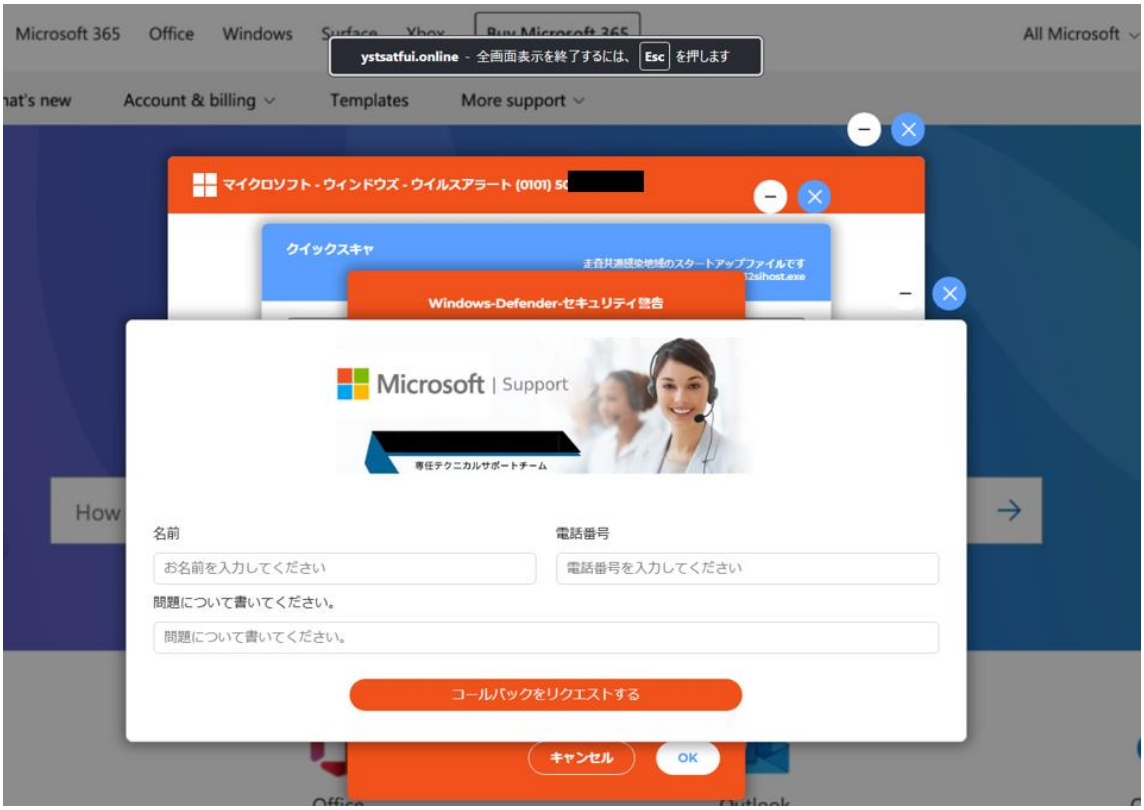


図 23：誘導先のサポート詐欺（偽警告）サイトの表示例（2024 年 6 月確認）
コールバックをリクエストするための入力フォームを持つ

サポート詐欺に関しては 2023 年から被害の高額化が進んでいましたが 2024 年もその傾向が続いています。報道が確認できただけでも、3 月に法人で 1000 万円の被害[21]、6 月に個人で 500 万円[22]、6 月に個人で 1100 万円[23]といった高額被害が相次いで発生しています。これらの高額被害はいずれも遠隔操作によりネットバンキングの送金を不正に行われたものと考えられます。特に 3 月の法人被害事例では、ネットバンキングの ID とパスワードを相手に教えた上、指示に従って PC の電源を切らずに一旦帰宅してしまったことが分かっています。

また、法人においては金銭以外にも情報漏洩の可能性を無視できません。サポート詐欺では被害者の端末が詐欺師に遠隔操作されるため、端末や組織のネットワーク上の共有ファイルにある情報が窃取される可能性があります。2023 年にサポート詐欺被害に遭った長野県の県立高校 2 校では、生徒の成績など合わせて 1 万 4231 人分の個人情報が流出した恐れがあるにもかかわらず個人情報保護委員会への報告が遅れたため、2024 年 2 月に行政指導が下されました[24]。もちろん個人においても端末内から個人情報や認証情報が窃取されることは、更なる被害の可能性が高まることになります。

[21] https://www.asahi.com/articles/ASS3L5W7ZS3LUZOB006.html
[22] https://www.iwate-np.co.jp/article/2024/6/4/164119
[23] https://www3.nhk.or.jp/lnews/tsu/20240612/3070013049.html
[24] https://xtech.nikkei.com/atcl/nxt/column/18/01157/061900113/

詐欺に対しては「手口を知る」ことが強力な対策になります。サポート詐欺の場合、全画面で表示される偽警告画面と警告音によって冷静な思考を奪う手口です。逆に電話番号を伴う全画面の警告表示や警告音があった場合にはサポート詐欺であることを強く認識することが騙されないことに繋がります。

SNS 型投資詐欺

海外で「Pig Butchering Scam」（養豚式投資詐欺）などと呼ばれていた投資詐欺[25]ですが、2023 年を通じ、国内で被害拡大しました。警察庁はこの状況から「SNS 型投資詐欺」として大々的な注意喚起[26]を行うと共に、ロマンス詐欺と共に認知状況などの発表を開始[27]しています。もっとも活発な誘導経路としては、有名人を無断で使用した Web や SNS 上の広告やメッセージから投資に関する LINE グループに招待されるケースがあります。LINE グループ内には指南役である有名人とそのアシスタントを名乗る人物や複数人の参加者と思しきメンバーが入っており、やり取りと共に推奨銘柄などの購入を促される、というのが一般的なパターンです。

図 24：著名人の写真を悪用した Web 上の広告例（2024 年 1 月確認）

[25] https://www.trendmicro.com/vinfo/ph/security/news/cybercrime-and-digital-threats/unmasking-pig-butchering-scams-and-protecting-your-financial-future

[26] https://www.npa.go.jp/bureau/safetylife/sos47/new-topics/investment/

[27] https://www.npa.go.jp/news/release/2024/20240516001.html

図 25：著名人の写真を悪用した SNS 上の広告例（2024 年 4 月確認）

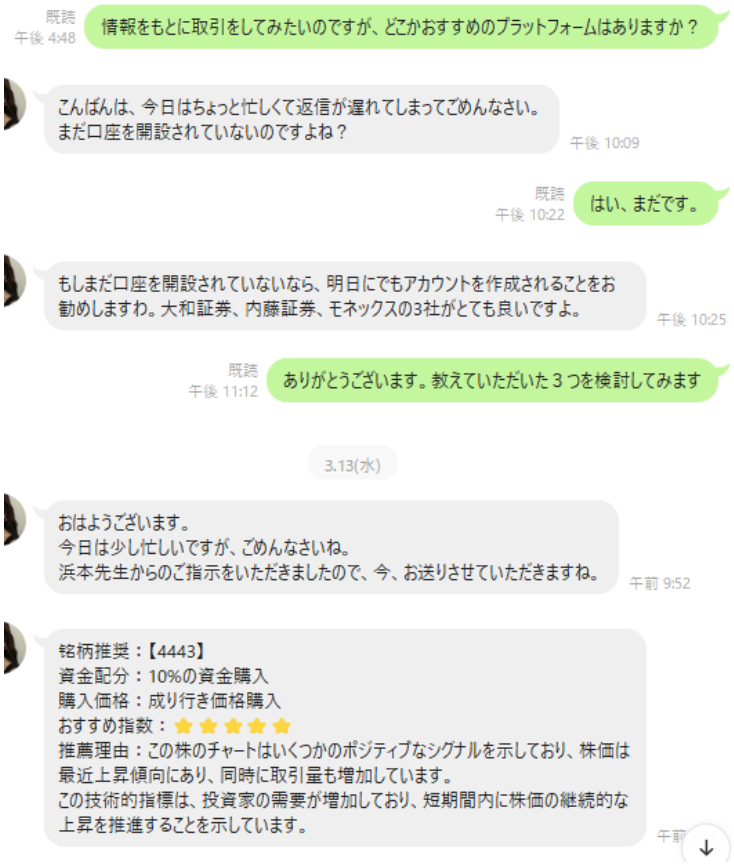


図 26：広告から誘導される投資関連 LINE グループの例

4 月には無断で広告に利用されていた著名人のうち、特に前澤友作、堀江貴文の両氏が SNS や政府に対し、対策と規制を訴えました[28]。その為もあってか、5 月以降は著名人を無断使用した広告が減少傾向にあるようです。

[28] https://www3.nhk.or.jp/news/html/20240410/k10014418321000.html

図 27：Meta 広告ライブラリによる検索結果例（2024 年 5 月確認）
著名人を無断使用したものと思われる広告コンテンツの削除が確認できる

また最終的な誘導先となっていた LINE も詐欺対応強化を行うことを 6 月に発表[29]しました。実際、トレンドマイクロが 5 月の調査時に収集した投資詐欺関連アカウント 224 件のうち、53 件が 6 月の調査時には無効になっていました。

6 月以降には投資詐欺グループのメンバー併せて 96 人の逮捕[30]も報じられるなど、投資詐欺への対策は進んでいます。ただし、有名人を使用しない広告は継続して確認されていると共に、高額被害も引き続き報道[31]されており、今後もさらに警戒を強めるべきであると言えます。

図 28：不審な LINE グループへの誘導を確認した有名人を使用していない広告の例（2024 年 5 月確認）

[29] https://www.lycorp.co.jp/ja/news/release/008622/
[30] https://www3.nhk.or.jp/kansai-news/20240820/2000086911.html
[31] https://www3.nhk.or.jp/lnews/kofu/20240820/1040024226.html

まとめ

フィッシングをはじめとするネット詐欺は利用者を騙して操るものであるため、個人個人がその手口を知って警戒することが有効な対策となります。併せて、技術的対策により偽サイトやメール、メッセージを判定し、警告やブロックを行うことも重要です。それでも情報を詐取されてしまったなどの可能性がある場合、被害を最小限に抑えるためにも、詐取された可能性のある情報のサービス事業者や警察のフィッシング報告専用窓口[32]など、関係機関への報告と相談を行ってください。

また、サイバー犯罪者は既に流出している情報を元にネット詐欺を仕掛けてくることがあります。最近ではアンダーグラウンドで流通している情報を知らせてくれるサービスなどもありますので、自身に関する情報がどの程度流出しているかを知ることが事前の心構えとして有効です。

[32] https://www.npa.go.jp/bureau/cyber/countermeasures/phishing.html

グローバルセキュリティラウンドアップ

サイバー犯罪の根本解決に向けた取り組み：ランサムウェア、ボット、フィッシングに対する法執行機関の大規模な撲滅作戦

ランサムウェア攻撃で注目された戦術、技術、手順（TTP）

ランサムウェア攻撃の各段階で最もよく使われたコマンドとプロセス

攻撃者が狙うクラウド資産の弱点：放置されたリソース、露出した認証情報、脆弱性

APT 攻撃グループが攻撃範囲を拡大するため、武器をアップグレード

AI の未開拓領域を狙う攻撃者たち

サイバー犯罪の根本解決に向けた取り組み：法執行機関の大規模な撲滅作戦

2024 年上半期、ファイル検出台数で最も多く確認されたランサムウェアは、LockBit でした。2024 年前半のランサムウェア攻撃では、銀行機関が最も大きな被害を受け、次いでテクノロジー業界の組織が標的となりました。

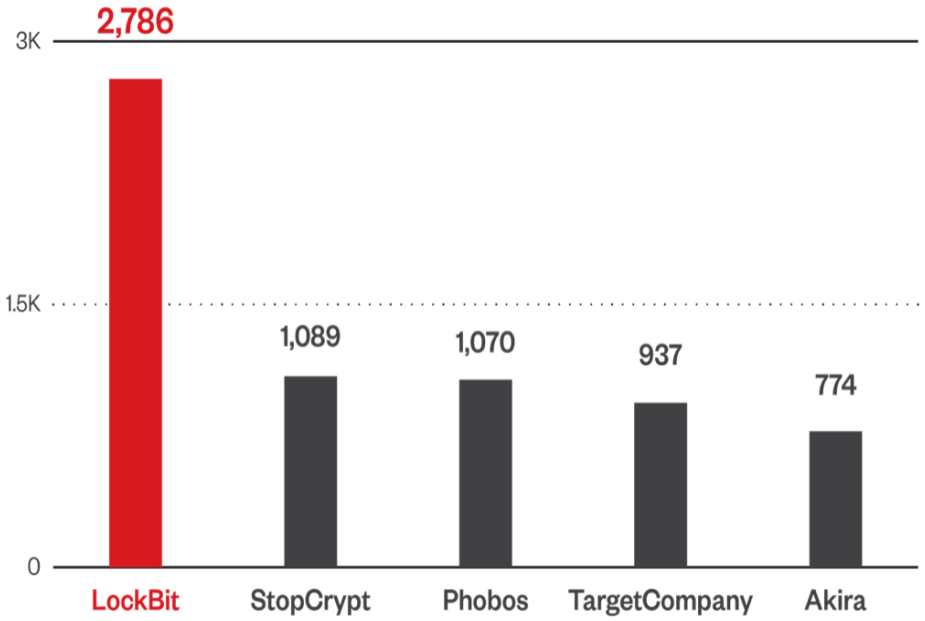


図 1：ファイル検出台数ランサムウェアトップ 5（2024 年 1～6 月）

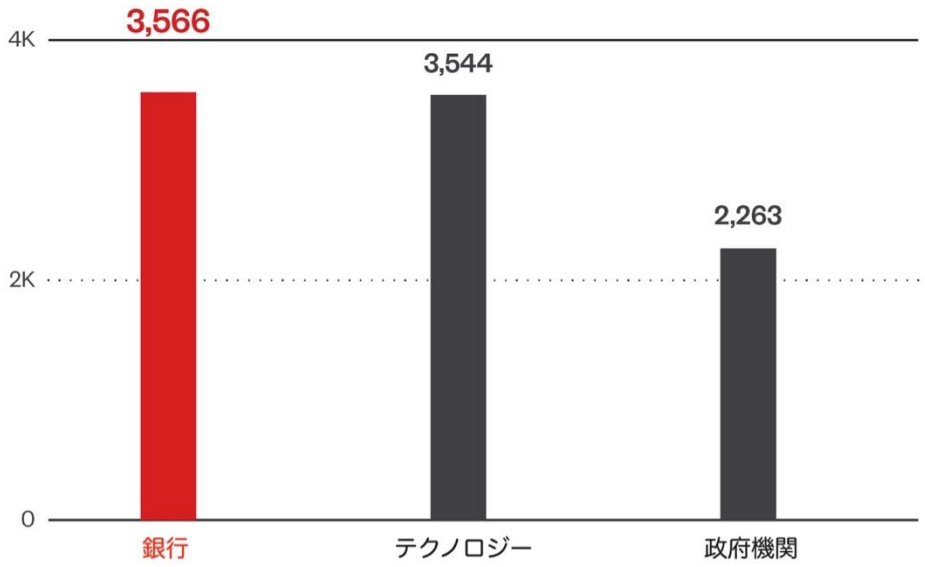


図 2：検出台数ランサムウェア業界別トップ 3（2024 年 1～6 月）

2024 年前半、法執行機関がランサムウェア攻撃グループを壊滅させるための大規模な作戦を展開しました。サイバー犯罪者がランサムウェアの配布やフィッシング攻撃に使用していたボットネットやプラットフォームが次々と阻害される様子が見られました。

クロノス作戦

2024 年 2 月、「オペレーション・クロノス（Operation Cronos）」[33]と名付けられた法執行作戦により、2023 年最大の金融脅威グループである LockBit の活動が大きく妨げられました。

活動を阻害され、評判を損ない、メンバーの身元が暴露されたにもかかわらず、LockBit は影響を受けていないかのように振る舞おうとしました。しかし、トレンドマイクロの分析では実際は異なる結果が出ており[34]、彼らの主張する数字が誇張されていることが明らかになっています。

LockBit のような経験豊富なランサムウェアグループは、ランサムウェア界での地位を保つために進化が必要だと理解しています。クロノス作戦中、我々は LockBit-NG-Dev（NG は「新世代」の意）と呼ぶ、全く新しいコードベースを持つ LockBit の開発中サンプルを分析しました。我々の分析によると、LockBit-NG-Dev は.NET で書かれ、CoreRT でコンパイルされており、様々なプラットフォームで動作すると考えられています。

すでに弱体化した組織と、進行中の関連ネットワークの解体に加えて、LockBit はクロノス作戦の一環として課された制裁によってさらなる打撃を受けました。2024 年 5 月に発表された作戦の第二段階[35]では、このランサムウェアグループの疑いのある管理者兼開発者に対して資産凍結と渡航禁止措置が取られました。この人物は現在、米国で 26 件もの罪状で起訴されています[36]。

エンドゲーム作戦

2024 年 5 月、「オペレーション・エンドゲーム（Operation Endgame）」[37]と呼ばれる、もう一つの大規模な法執行機関による撲滅作戦が実施されました。

[33] https://www.trendmicro.com/ja_jp/research/24/d/operation-cronos-aftermath.html
[34] https://www.trendmicro.com/ja_jp/research/22/e/ransomware-spotlight-lockbit.html
[35] https://www.europol.europa.eu/media-press/newsroom/news/new-measures-issued-against-lockbit
[36] https://www.justice.gov/opa/pr/us-charges-russian-national-developing-and-operating-lockbit-ransomware
[37] https://www.europol.europa.eu/media-press/newsroom/news/largest-ever-operation-against-botnets-hits-dropper-malware-ecosystem

この作戦では、IcedID[38]、Pikabot[39]、Smokeloader[40]、Trickbot[41]など、ランサムウェアに関連するボットネットやドロッパーの活動が阻止されました。この共同作戦[42]の結果、100 台のサーバが機能を停止し、2,000 以上の不正なドメインが押収されるという成果を上げました。

エンドゲーム作戦は、近年のボットネット対策としては最大規模[43]のものであり、多くのランサムウェアグループの活動に大きな打撃を与えました。しかし、ランサムウェア運営者たちは、重大な脆弱性の悪用、リモート監視・管理（RMM）ツールの不正利用、自前の脆弱なドライバー（BYOVD）攻撃の実行、独自のシェルスクリプトの使用など、新たな感染方法を探ると予想されます。

スターグルー作戦

2024 年 4 月、サイバー犯罪者たちは大きな打撃を受けました。「オペレーションスターグルー（Operation Stargrew）」[44]により、2021 年後半に出現したサイバー犯罪プラットフォーム「LabHost」が摘発されたのです。LabHost はフィッシング・アズ・ア・サービス（PhaaS）を提供していました。

摘発時、LabHost には 2,000 人を超える犯罪ユーザがいました。階層型の会員制モデルで様々なフィッシングサービスを提供し、月額料金は 179 ドルから 300 ドルでした。これらのフィッシングサービスは世界中の銀行や企業を標的としており、特にカナダ、米国、英国の組織が狙われていました。

スターグルー作戦は、英国の首都警察庁が主導し、国際的な法執行機関や、トレンドマイクロを含む業界パートナーとの協力で実施されました。作戦の結果、LabHost プラットフォームは無効化され、関連する不正サイトが押収され、さらに 37 人の主要人物が逮捕されました[45]。

[38] https://www.trendmicro.com/ja_jp/research/23/a/icedid-botnet-distributors-abuse-google-ppc-to-distribute-malware.html
[39] https://www.trendmicro.com/ja_jp/research/24/b/a-look-into-pikabot-spam-wave-campaign.html
[40] https://www.trendmicro.com/vinfo/ph/security/news/cybercrime-and-digital-threats/smokeloader-malware-spreading-via-fake-meltdown-spectre-patches
[41] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/group-behind-trickbot-spreads-fileless-bazarbackdoor
[42] https://www.businessinsider.com/operation-endgame-fbi-europol-cybercrime-malware-cybersecurity-2024-6
[43] https://therecord.media/dropper-malware-takedown-europol-operation-endgame
[44] https://www.trendmicro.com/ja_jp/research/24/d/labhost-takedown.html
[45] https://www.independent.co.uk/tech/metropolitan-police-manchester-luton-essex-police-b2530549.html

ランサムウェア攻撃で注目された TTPs

2024 年上半期、ランサムウェア攻撃者たちは既存のツールや脆弱性を悪用する多彩な手法を駆使しました。

ConnectWise ScreenConnect

今年初め、ランサムウェア BlackBasta[46]や Bl00dy などを扱う攻撃グループが、ConnectWise ScreenConnect ソフトウェアの脆弱性（CVE-2024-1708[47]と CVE-2024-1709[48]）を悪用し、システムに侵入してデータを盗み出し、業務を妨害したことを報告しました。

Team City

攻撃者たちは、Team City On-Premises の 2 つの重大な脆弱性（CVE-2024-27198[49]と CVE-2024-27199[50]）も悪用し、感染したシステム上でリモートコード実行を行うことに成功しました。

Microsoft Quick Assist

Black Basta 集団が、Microsoft Quick Assist[51]を悪用し、音声フィッシング（ヴィッシング）、リモート管理ツールの導入、ランサムウェアの配信を含む、巧妙なソーシャルエンジニアリング的攻撃を行っているのが確認されました。

Martini ドライバー

ランサムウェア Kasseika[52]の運営者は、自前の脆弱なドライバー（BYOVD）攻撃を仕掛け、Martini ドライバーを悪用して、被害者のコンピューターのアンチウイルス関連プロセスを停止させました。

---

[46] https://www.trendmicro.com/ja_jp/research/22/j/ransomware-spotlight-blackbasta.html
[47] https://nvd.nist.gov/vuln/detail/CVE-2024-1708
[48] https://nvd.nist.gov/vuln/detail/CVE-2024-1709
[49] https://nvd.nist.gov/vuln/detail/CVE-2024-27198
[50] https://nvd.nist.gov/vuln/detail/CVE-2024-27199
[51] https://www.microsoft.com/en-us/security/blog/2024/05/15/threat-actors-misusing-quick-assist-in-social-engineering-attacks-leading-to-ransomware/
[52] https://www.trendmicro.com/ja_jp/research/24/b/kasseika-ransomware-deploys-byovd-attacks-abuses-psexec-and-expl.html

Rust 版マルウェア

ランサムウェア Agenda[53]の運営者は、独自の PowerShell スクリプトを使用する Rust 版を用いて、VMWare vCenter と ESXi サーバに感染を広げていることが分かりました。さらに、Agenda ランサムウェアは新機能として、接続されたプリンターに身代金要求文を直接印刷するようになりました。

独自シェルスクリプト

ランサムウェア TargetCompany[54]の攻撃グループは、独自のシェルスクリプトを使ってマルウェアの配信と実行を行う、新しい Linux 向けの亜種を公開しました。

ランサムウェア攻撃の各段階で最もよく使われたコマンドとプロセス

以下は、Trend Micro Vision One の 標的型攻撃検知データから、様々なランサムウェアグループが標的ネットワークに侵入し、横展開する際によく用いた、進化する戦術と執拗な攻撃手段をまとめたものです。

初期侵入

- 様々な手法が使い分けられている

永続化

- bitsadmin_transfer（BITS を使用したファイル転送）
- encoded_command（エンコードされたコマンド）
- anti_av（アンチウイルス対策）

クレデンシャルアクセス

- lsass_dump（LSASS プロセスのダンプ）
- esentutl_copy（Esentutl を使用したファイルコピー）
- ntdsutil_dumping（NTDS ファイルのダンプ）

水平移動・内部活動

- portscan（ポートスキャン）
- adfind（Active Directory 情報の収集）

[53] https://www.trendmicro.com/ja_jp/research/24/d/agenda-ransomware-propagates-to-vcenters-and-esxi-via-custom-pow.html

[54] https://www.trendmicro.com/ja_jp/research/24/f/targetcompany-s-linux-variant-targets-esxi-environments.html

攻撃者が狙うクラウド資産の弱点：放置されたリソース、露出した認証情報、脆弱性

2024 年上半期、リスクイベントの上位を占めたのは、高リスクのクラウドアプリケーションへのアクセスでした。特に、管理されていないデバイスでエンドポイント保護が最新でないことが、企業をさらなるリスクに晒しています。

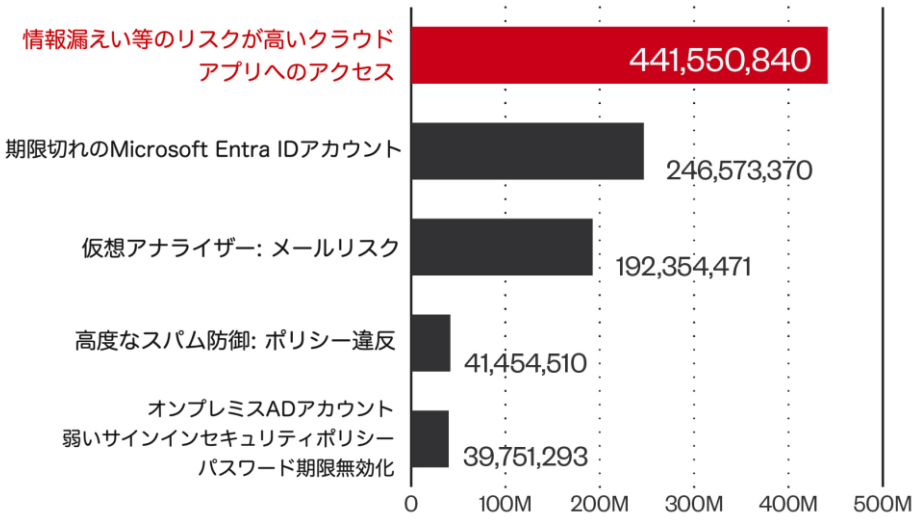


図 3：検知されたリスクイベントトップ 5（2024 年 1～6 月）

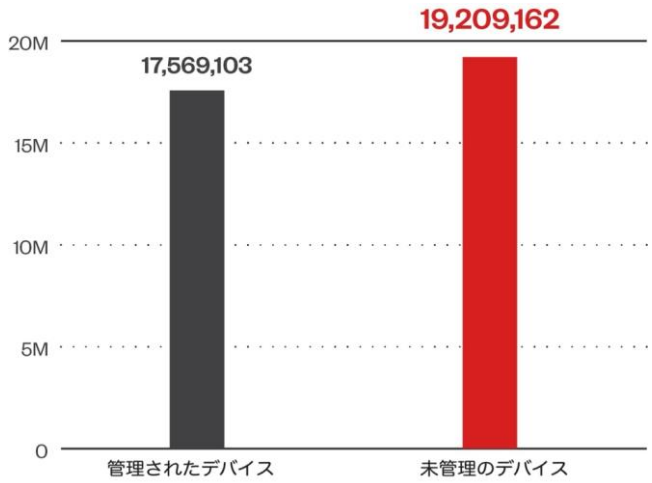


図 4：管理デバイスと非管理デバイスの検出数の比較（2024 年 1～6 月）

- **管理されたデバイス:** トレンドマイクロのエンドポイントセキュリティソリューションがインストールされ、組織の IT チームが積極的に監視・管理しているデバイス。
- **未管理のデバイス:** セキュリティソリューションによって検出されたものの、トレンドマイクロの管理下にない、または組織の IT やセキュリティ管理システムで監視されていないデバイス。

2024 年上半期、サイバー犯罪者の手法は必ずしも全て新しいものではありませんでした。彼らは依然として、実績のある攻撃手法を好み、被害者のシステムに侵入して重要な情報を盗むため、露出した機密情報を探し続けています。

1. 最近、ニューヨーク・タイムズがデータ侵害を受けたと報じられました。攻撃者がクラウド上の第三者プラットフォームの露出した認証情報を悪用したのです。匿名の 4chan ユーザが、360 万のファイルを含む 5,000 の暗号化されていない GitHub リポジトリ[55]にアクセスしたと主張しました。これには機密認証情報や、人気ウェブゲーム「Wordle」のソースコードまで含まれていたといいます。

2. 今年初め、露出した Docker remote API サーバを悪用する仮想通貨採掘キャンペーンについて報告[56]しました。分析によると、攻撃者が露出した Docker サーバを悪用し、開発者向けオープンソース GitHub プロジェクト「Commando」の Docker イメージを通じて仮想通貨マイナーを展開していました。また、正規だが設定ミスのあるツールが攻撃に利用されているのも確認しました。

3. 3 月には、開発者が APISIX API ゲートウェイの設定[57]を安全にする必要性について言及しました。特に、管理 API にアクセスするためのハードコードされたデフォルトのマスターAPI トークンを変更する必要があります。野放しの状態で多数の露出したインスタンスを確認しましたが、これらは攻撃者によるリモートコード実行（RCE）に悪用される可能性があります。

4. 2024 年前半にもう一つ注目したのは、Kong API ゲートウェイでした。トレンドマイクロの報告[58]では、2021 年以降増加傾向にある露出した Kong API ゲートウェイインスタンスの数と、そのような露出がバックエンドサービスを危険にさらす可能性について論じています。

5. 2024 年 5 月、オープンソースの監視ツール Container Advisor（CAdvisor）で見つかった設定ミスについて報告[59]しました。攻撃者が、機密な環境変数を露出した安全でない CAdvisor インスタンスを入手すると、偵察、横方向移動、権限昇格、サプライチェーン侵害、脆弱性悪用といった攻撃を行う可能性があります。

---

[55] https://www.darkreading.com/cloud-security/new-york-times-internal-data-nabbed-from-github

[56] https://www.trendmicro.com/ja_jp/research/24/f/commando-cat-a-novel-cryptojacking-attack-.html

[57] https://www.trendmicro.com/ja_jp/research/24/d/apache-apisix-in-the-wild-exploitations-an-api-gateway-security-study.html

[58] https://www.trendmicro.com/ja_jp/research/24/f/kong-api-gateway-misconfigurations-an-api-gateway-security-case-study.html

[59] https://www.trendmicro.com/ja_jp/research/24/f/2observability-exposed-exploring-risks-in-cloud-native-metrics.html

標的型攻撃：攻撃範囲の拡大と攻撃手法の更新

2024 年上半期、「APT」とも呼ばれる標的型攻撃集団は、より多くの被害者を捕らえるため、ツールと戦術のレパートリーを革新する新たな方法を模索し続けました。

1. **ルーターの乗っ取り：**インターネットに接続されたルーターの乗っ取り[60]は、匿名化の手段として、国家支援の攻撃者とサイバー犯罪者の双方に人気がありました。Sandworm のようなグループは独自のプロキシボットネットを使う一方、APT29 は商用の住宅用プロキシネットワークを好みました。Pawn Storm は 2024 年 1 月に FBI に阻止されるまで、Ubiquiti EdgeRouter デバイスの第三者プロキシボットネットを利用していました。

2. **政府インフラの侵害：**また、Earth Krahang[61]の攻撃キャンペーンと、政府のインフラを侵害して利用するという彼らの好む戦術についても報告しました。Earth Krahang と Earth Lusca という中国関連の攻撃者グループとの間に、インフラとバックドアの類似性を通じてつながりを発見しましたが、これらは独立して活動する 2 つの侵入グループである可能性もあります。

3. **ソーシャルエンジニアリング戦術：**Earth Lusca[62]の攻撃キャンペーンも、中国と台湾の関係を利用したソーシャルエンジニアリング戦術を特徴とする新たなキャンペーンを展開しました。2024 年初頭の台湾総統選挙の直前に、地政学の専門家から盗んだとみられる本物の文書を基にした偽のメールを使ってマルウェアを配布しました。

4. **高度な機能を持つマルウェア：**Earth Hundun[63]の攻撃キャンペーンは、常に更新され、高度な回避技術を多数持つことで知られる Waterbear バックドアを使った攻撃を続けています。Earth Hundun は最新版の Deuterbear[64]を使用し、さらに機能を追加しています。Deuterbear はシェルコード形式を持ち、メモリスキャン対策が可能で、そのダウンローダーと同じ通信キーを使用しています。

[60] https://www.trendmicro.com/ja_jp/research/24/e/router-roulette.html
[61] https://www.trendmicro.com/ja_jp/research/24/c/earth-krahang.html
[62] https://www.trendmicro.com/ja_jp/research/24/c/earth-lusca-uses-geopolitical-lure-to-target-taiwan.html
[63] https://www.trendmicro.com/ja_jp/research/24/d/earth-hundun-waterbear-deuterbear.html
[64] https://www.trendmicro.com/ja_jp/research/24/e/earth-hundun-2.html

AI の未開拓領域を狙う攻撃者たち

企業が AI 技術の新たな活用法を探る中、避けられない失敗が犯罪者に新たな機会を与える可能性があります。サイバー犯罪者もまた、AI の利点を活用しようと、新たな方向に舵を切ることで知られています。

1. 2024 年 6 月、Microsoft は AI ツールによるユーザ活動の追跡に関するプライバシーの懸念から、議論を呼んでいる「Recall」機能のリリースを延期[65]しました。Copilot+ PC において 6 月リリース予定だった Recall は、ユーザの PC 使用状況のスクリーンショットを撮影[66]し、ローカルに保存します。これが、ユーザの認証情報や他の機密データを狙う悪意ある攻撃者の標的になる可能性があります。

2. 2024 年前半、サイバー犯罪者が独自の大規模言語モデル（LLM）の開発から、既存 LLM の「ジェイルブレイク」にシフト[67]していることが分かりました。LLM の倫理的制限を回避するための「ジェイルブレイク・アズ・ア・サービス」[68]の提供が増加しており、仮説的質問、ロールプレイ、外国語での質問などを通じて LLM を操作する手法が用いられています。

3. AI 活用型詐欺[69]は、生体認証データを収集してディープフェイクを作成できるトロイの木馬「GoldPickaxe.iOS」[70]のようなツールにより、強力な脅威となっています。2 月には、ロンドンの企業 Asup の最高財務責任者をディープフェイクのビデオ通話[71]で偽装し、詐欺師が 2560 万ドルを騙し取るという事件も起きました。

4. OpenAI と Microsoft は、中国関連の攻撃グループ「Earth Lusca」[72]が、情報収集、フィッシング用のコンテンツや翻訳の生成、攻撃を微調整するスクリプト作成などに OpenAI のサービスを使用していたと特定しました。2 月の共同調査結果の発表以降、OpenAI はこの高度な標的型サイバー攻撃（APT）に関連するアカウントを無効化[73]しています。

---

[65] https://www.reuters.com/technology/artificial-intelligence/microsoft-delay-release-recall-ai-feature-security-concerns-2024-06-14/

[66] https://www.cnbc.com/2024/06/07/microsoft-says-its-upcoming-recall-featu.html

[67] https://www.trendmicro.com/ja_jp/research/24/e/back-to-the-hype-an-update-on-how-cybercriminals-are-using-genai.html

[68] https://www.trendmicro.com/ja_jp/research/24/h/surging-hype-an-update-on-the-rising-abuse-of-genai.html

[69] https://www.trendmicro.com/ja_jp/jp-security/24/h/cybersecurity-ai.html

[70] https://www.group-ib.com/blog/goldfactory-ios-trojan/

[71] https://edition.cnn.com/2024/05/16/tech/arup-deepfake-scam-loss-hong-kong-intl-hnk/index.html

[72] https://openai.com/index/disrupting-malicious-uses-of-ai-by-state-affiliated-threat-actors/

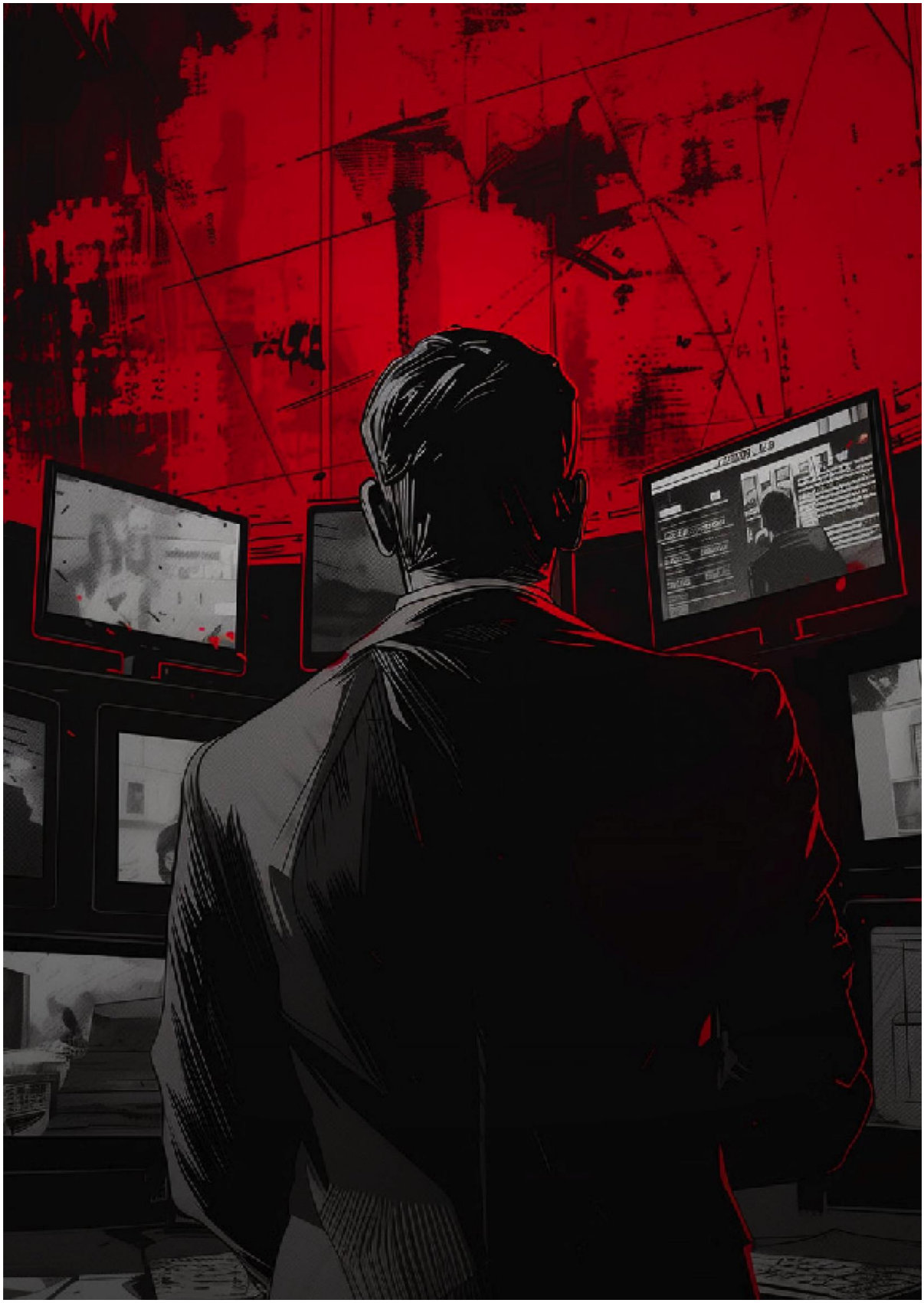
[73] https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/

5. サイバー犯罪者は、世界中での AI 技術への関心の高まりを利用しています。例えば、Void Arachne は中国語話者を標的とするキャンペーンで、正規の AI ソフトウェアに不正なプログラムを忍ばせていました[74]。より多くの潜在的被害者を捕らえるため、このグループは裸体化ツールや他のディープフェイク生成 AI ツールを含む悪意のあるインストーラーファイルも拡散しています。

6. 2024 年 5 月、日本で初めて生成 AI を悪用して「ウイルス」を作成したとする逮捕事例が発生[75]しました。警視庁の解析により作成されたウイルスは、データを暗号化したりメッセージを表示して暗号資産を要求したりする活動を持つランサムウェアであったことが確認されています。逮捕された 25 歳の男は「ランサムウェアを使って楽に稼ぎたかった」などと供述して容疑を認めています。男は 2023 年 3 月に自身のパソコンやスマートフォンから複数の生成 AI を利用して作成しましたが、専門的な知識はなく、ウイルス作成方法を生成ＡＩから聞き出す質問の仕方などはネット上で情報を得たとしています。また、SNS を通じて女性のスマホにランサムウェアを送信していましたが、何らかの原因で作動しなかったこともわかっています。

[74] https://www.trendmicro.com/ja_jp/research/24/g/behind-the-great-wall-void-arachne-targets-chinese-speaking-user.html

[75] https://www.jiji.com/jc/article?k=2024052800315&g=soc



TREND MICRO

〒160-0022
東京都新宿区新宿 4-1-6　JR 新宿ミライナタワー
https://www.trendmicro.com

トレンドマイクロはサイバーセキュリティのグローバルリーダとしてデジタル情報を安全に交換できる世界の実現に貢献します。私たちの革新的なソリューションはデータセンター、クラウド、ネットワーク、エンドポイントにおける多層的なセキュリティをお客様に提供します。

当社のリーダシップの根幹であるトレンドマイクロリサーチは、多くのエキスパートに支えられています。それは最新の脅威を発見し、重要なインサイトを公に共有し、サイバー犯罪の防止を支援することに情熱を注ぐ人材です。当社のグローバルチームは、日に数百万もの脅威を特定し、脆弱性の開示を先導し、標的型攻撃・AI・IoT・サイバー犯罪等における革新的な研究結果を公表しています。私たちは次に来る脅威を予測し、セキュリティ業界が進むべき方向を示しうる示唆に富んだ研究成果を提供するため、継続的に取り組んでまいります。

Trend Micro Research