2022 年上半期サイバーセキュリティレポート

～「侵入」する脅威が浮き彫りにする「サプライチェーンリスク」～

はじめに

「2022 年上半期サイバーセキュリティレポート」は、2022 年 1～6 月の半年間における世界と日本の脅威動向をまとめたレポートです。トレンドマイクロがブロックした 630 億件以上の脅威とともに 2022 年上半期のサイバーセキュリティ状況での注目すべき出来事や新たな傾向について調査しました。使用する脅威データは 2022 年 1～6 月の期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 2022 年 8 月までに発生したものにも言及している場合があります。

本レポートが、企業や組織、個人の利用者にとって、刻々と変化する脅威状況を正しく把握し、セキュリティインフラやポリシーに関する意思決定を行う上で貴重な知見を提供できることを願っています。

※註 1 ： 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 2022 年 7 月 15 日付の統計データが出典となります。またグラフ上は実数で表示しますが、本文内では表現上読みやすいよう四捨五入などで表記する場合があります。割合を示す数値は割り切れない場合もありますので四捨五入表記が基本となります。その場合、グラフ上の数値の合計が「100%」にならないことがあります。

※註 2 ：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 3 ： 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。

2022 年上半期脅威動向総括：
広がり続ける「アタックサーフェス」を守るために

2022 年上半期、多くの企業や組織はコロナ禍における行動制限から、再び職場環境を変化させる必要性に直面しています。ある社員はオンサイトの職場に何らかの形で戻り、ある社員はリモートワークを継続し、またある社員は在宅勤務（WFH）とオンサイト勤務の両方を組み合わせたハイブリッド型に移行しました。業務統合に関する技術のニーズも高まる中、こうした変化は企業や組織にとっての「アタックサーフェス（攻撃対象領域）」が広がり続けることを意味しています。実際、時間の経過とともに攻撃者の活動はより危険な存在となり、その規模も巧妙さも増しています。こうした中、単一の攻撃キャンペーンにおいて、複数のアタックサーフェスの侵害が試みられるようになったことは不思議ではないでしょう。さらにサービスベースで利用できるマルウェアも普及し、サイバー犯罪者も攻撃を仕掛けやすくなり、マルウェア開発者も、自らの痕跡を巧みに隠ぺいすることが可能となりました。これはセキュリティ部門にとっては、自組織の IT インフラのあらゆる部分を防御するという課題に取り組まなければならないということであり、できる限り多くのセキュリティギャップを埋めるためアタックサーフェスを可能な限りカバーするための追加リソースが求められています。

法人組織を取り巻く具体的な脅威の状況

法人組織のセキュリティリスクとなる具体的な脅威に目を移すと、現在の法人組織にとって最大の脅威となっているランサムウェアの攻撃者は、より有利で効率的な収益化手法へのシフトを続けています。特に「RaaS （Ransomware-as-a-Service＝サービスとしてのランサムウェア）」モデルは、ランサムウェア攻撃が急速に拡大した主な理由の 1 つとされています。今年上半期には、3 つの RaaS 型ランサムウェア、Conti、LockBit、BlackCat、が他を圧倒していました。それぞれの 2022 年上半期の検出台数は、前年同期比で大幅に増加しました。これらの事実は、サービスの提供側と利用側の双方にもたらすメリットから、サイバー犯罪者が RaaS パートナーシップにますます傾倒していることを示しています。また、Black Basta、Nokoyawa、Hive といった比較的新しいランサムウェアファミリーも、大物の標的を狙う注目度の高い攻撃に使用されていることも確認されました。現在のランサムウェア攻撃が、データ暗号化に加えた窃取情報の暴露など多重の恐喝方式を採用したことは、最新のランサムウェア攻撃に対する防御が、企業や組織にとって最優先事項となったことを意味しています。

2022 年上半期には、高度なツールキットと広大なインフラを攻撃キャンペーンに採用した標的型攻撃が出現しました。これらの標的型攻撃では同時に、コモディティ化した旧来のマルウェアにも目を向け、その能力と信頼性からこれらのツールを攻撃活動に組み込んでいく傾向が続いています。この傾向はより一般的なサイバー犯罪者にも広がっています。

攻撃者はそもそも、どのような状況でも利益を際限なく追求し、その時々の話題に便乗した攻撃を仕掛けます。2022 年これまでに発生した事件の中でも最も衝撃的だったのは、2 月に始まったロシアによるウクライナ侵攻に間違いありません。サイバー犯罪者はこの侵攻とその背後の敵対関係に乗じて攻撃を仕掛け、どちらの側であろうと、この戦争に関心を持つ人々を食い物にしています。

さらにサイバー犯罪者は、Windows 以外のオペレーティングシステムにも活動の幅を広げようとしているようで、Linux がますます攻撃対象になることが予測されています。同時にクラウド環境は、攻撃者にとって依然として人気のある標的であり、設定ミスなどの古くから存在する問題を利用する攻撃者もいれば、クラウドインフラストラクチャを攻撃するためにより新しく、従来とは異なる方法を開発しようとする攻撃者もいます。クラウドサービスのように、企業や組織がインフラを物理的に管理しない技術が普及している中で効果的なセキュリティを実現するには、利用間での責任共有モデル等を積極的に理解することが必要な状況となっています[1]。

様々な攻撃で使用される脆弱性に目を移すと、トレンドマイクロが運営する脆弱性発見コミュニティ Zero Day Initiative（ZDI）によれば、2022 年上半期には、脆弱性アドバイザリの公開件数全般、および深刻度の高い脆弱性の公開件数が増加しました。本レポートでも、macOS や Linux に影響を与える脆弱性にも注目しつつ、企業や組織のシステムで利用される重要な業務ツールやソフトウェアを対象とした注目すべき重要脆弱性を取り上げています。また今後に大きな影響を与えかねない脆弱性として、特に IoT/IIoT の分野で使用されているデータ配信サービス規格（DDS）と、この規格を利用する端末やデバイスに影響を与える可能性のある脆弱性についても掘り下げました。

アタックサーフェスの拡大への対応に必要な「多層防御」

このような脅威状況を踏まえた中、アタックサーフェス管理（ASM）の必要性が叫ばれています。ASM の第一段階は、自組織にとってのアタックサーフェスそのものを特定することです。企業や組織は、自社の資産を調査し、資産の重要度、潜在的な脆弱性、脅威活動のレベル、資産から収集される脅威情報の量などの要素から領域特定のための判断を下します。また、それぞれ利用可能なセキュリティ対策がどのように相互にリスクを相殺するか等を評価することも、ASM を計画する上での重要な準備段階となります。ASM において不可欠な要素の１つは可視性であり、これは潜在的な脅威に関する貴重な情報を提供することでもあります。こうして ASM は、潜在的な脅威に関する貴重な情報を提供し、企業や組織がリスクを判断し、そのリスクを軽減するために必要な措置を講じることを可能にします[2]。

[1] https://www.trendmicro.com/en_us/research/19/j/the-shared-responsibility-model.html

[2] https://www.trendmicro.com/en_us/ciso/22/d/attack-surface-management.html

適切なセキュリティプロトコルとベストプラクティスは、企業や組織が攻撃から自社のシステムを保護する上で大きな助けとなります。例えば、攻撃者がシステムの脆弱性を悪用する可能性を最小限に抑えるための最優先事項は、アップデートを迅速に実施することです。しかし直ちにアップデートを実施できない場合には、「仮想パッチ」などの技術的対策を適用するなどの方法で各端末を保護することも可能です。一方、クラウドの利用者は、クラウドのインフラが適切に設定され、正しいセキュリティプロトコルが適用されていることを確認し、設定ミスを突く攻撃を阻止する必要があります。個々のエンドユーザは攻撃者が企業や組織のシステムの他の部分にアクセスする際の「弱点」となるケースが多いため、社員のリテラシーをあげるためのセキュリティ教育も重要な要素となります。

しかし、インフラ、システム、エンドポイントを保護する際に直面する複雑な現実は、これらが整備されていても、適切なセキュリティツールがなければ、それぞれのポイントを保護することは困難であることも意味します。システムのさまざまな部分のセキュリティを個別に処理できる技術は存在しても、それぞれにサイロ化した各ソースからの異なるデータポイントを関連付ける手立てがない点が大きな課題となります。このため、企業や組織のセキュリティ部門は、攻撃がどのように発生し、どこから来たのかを判断する際に、一度にパズルの一部しか扱えないという制約に直面することになります。アタックサーフェス全体をカバーできる単一のプラットフォームは、特にリソースが限られている企業や組織にとって理想的なセキュリティソリューションといえます。包括的なプラットフォームがあれば、アタックサーフェスを完全に可視化できることはもちろん、さまざまな指標を関連付けることができるため、全体像に焦点を当てることができます。また、統合されたセキュリティプラットフォームは、多層的な保護を提供すると同時に、複数のセキュリティ技術に費やしていた費用を削減することができます[3]。最後に、潜在的なセキュリティギャップを最小化し、デジタル資産を継続的に保護する上でも、こうしたプラットフォームは設定可能であり、有効なセキュリティ対策となります。

本レポートでは、2022 年上半期にサイバーセキュリティの状況に影響を与えた最も重要なトレンドやインシデントを取り上げています。また、2022 年のセキュリティ予測についても、今年上半期のトレンドと合致するものがあるかどうかを検証しています。トレンドマイクロでは本レポートを通じ、個人ユーザや企業にさまざまな脅威を周知するだけでなく、アタックサーフェスが拡大する現在、実際に環境やシステムを保護するためのセキュリティ対策にも寄与できることを望んでいます。

[3] https://www.trendmicro.com/en_us/business/products/one-platform.html

日本セキュリティラウンドアップ

国内脅威動向総括：「侵入」する脅威が浮き彫りにする「サプライチェーンリスク」

事業継続を脅かすランサムウェア攻撃

復活後、さらに拡大する「EMOTET」の脅威

誰でも手が届く「クラウド」上のリソース侵害

個人利用者にとっての危険は「ネット詐欺」に集約

国内脅威動向総括：
「侵入」する脅威が浮き彫りにする「サプライチェーンリスク」

法人組織におけるサイバー脅威による被害は毎月・毎週の単位で報じられ続けています。これらの被害の中では、組織内ネットワークへ侵入されたことによる被害が顕著です。また、それらの被害がサプライチェーン、つまり組織間の関係性の弱点やリスクを浮き彫りにしている事例も目立っています。

侵入を前提とした脅威の拡大

まずネットワークへの侵入の面では、法人被害の中心的脅威となっているランサムウェア被害において、公表された事例のすべてが所謂「Human-Operated」型のランサムウェア攻撃によるものとなっています。日本では「標的型ランサムウェア攻撃」、「人手によるランサムウェア攻撃[4]」、「侵入型ランサムウェア攻撃[5]」などとも呼ばれるこの攻撃は、被害組織のネットワークに侵入した後、管理者権限の掌握、セキュリティ製品の無効化、情報窃取などの「内部活動」を経た後に、ネットワーク内でランサムウェアを拡散させるものです。ランサムウェアによる暗号化に加え情報の暴露などを行う「多重脅迫」にはネットワーク侵入後の内部活動が必須であり、現在のランサムウェア攻撃は組織内ネットワークへの侵入を前提とした攻撃と言えます。

これを対策側の視点で考えると、ネットワークへの侵入を許し内部活動を自由にさせてしまうことが被害の発生に直結してしまう、と言えます。そもそもの侵入を許した侵入経路として、トレンドマイクロのインシデント調査では外部から直接侵入された事例が目立っており、主に以下の 3 つの原因を確認しています。

1）VPN や RDP などの外部からアクセスを受ける接点においてセキュリティ対策・脆弱性対応が不十分だった
2）テレワークなどで外部に持ち出した PC が、USB 接続のモバイル Wi-Fi や SIM などグローバル IP が付与された状態でインターネット接続していた
3）仮想プライベートクラウド[6]に移行した内部向けサーバが設定ミスにより外部からもアクセス可能になっていた

[4] https://www.ipa.go.jp/security/announce/2020-ransom.html
[5] https://www.jpcert.or.jp/magazine/security/ransom-faq.html
[6] 仮想プライベートクラウド：VPC、パブリッククラウド上に論理的に構築されたプライベートクラウド
https://techtarget.itmedia.co.jp/tt/news/2103/19/news03.html

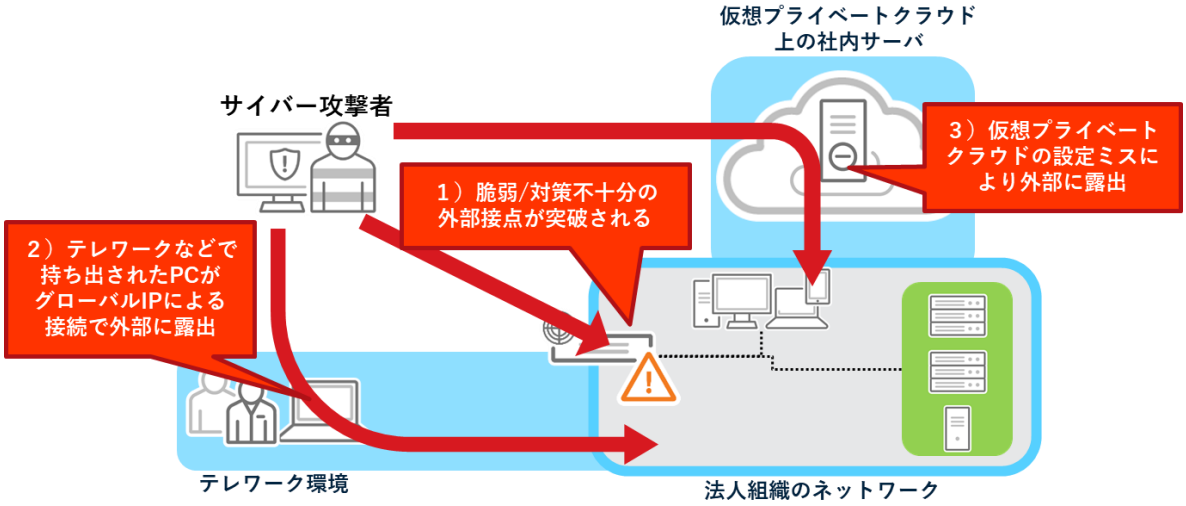

図 1：トレンドマイクロの調査で確認した 3 つの直接侵入原因の概念図

これらはすべて、組織ネットワークにおける境界線防御に迂回可能な「弱点」があったものと言えます。このような弱点が利用され、外部から組織ネットワーク内へ直接侵入される事例は、主要な VPN で悪用可能な脆弱性が出始めた 2019 年頃から顕在化してきました。逆にそれ以前、例えば 5 年前の 2017 年にはこれほど多くの直接侵入事例が問題となっていなかったことを考えると、法人組織のセキュリティ自体が大きく後退している感すらあります。

また、もう 1 つの侵入経路として、「Access-as-a-Service(AaaS)」や「イニシャルアクセスブローカー(IAB)」などと呼ばれるサイバー犯罪の存在も見逃すことができません。これらは事前に侵入した法人組織ネットワークに構築したアクセス経路（バックドア）を、他のサイバー犯罪者に販売したり貸し出したりする闇サービスです。もちろん、AaaS の商品であるアクセス経路を構築するためには、そもそも侵入を成功させている必要があります。その際の侵入経路としては、上述の直接侵入の他、従来からある攻撃メールによるマルウェア感染もあります。特にメール経由で侵入するマルウェアの代表格である EMOTET のサイバー犯罪者は、侵入したネットワークへのアクセス権を販売することが知られています。直接侵入、メール経由侵入のいずれにせよ、組織内ネットワークへのアクセス経路自体が商品となっていることにより、不特定の組織内ネットワークへの侵入自体がビジネス化していることがポイントです。

このように組織内ネットワークへの侵入は既にビジネス化しており、必ずしも標的とされる理由がなかったとしても、侵入される弱点を持った組織が被害に遭う状況と言えます。また、ビジネス化したサイバー犯罪者は、なるべくコストをかけずに攻撃を成功させ金銭利益を得たいため、侵入に手間がかかるネットワークほど攻撃のモチベーションを失います。つまり、セキュリティを漏れなく行っている組織は相対的に攻撃対象から外れていき、セキュリティに弱点を抱えている組織ほど更なる危険に晒されていくのが現在の脅威状況と言えます。

浮き彫りにされたサプライチェーンリスク

このように組織内ネットワークへ侵入する脅威の被害事例の中で、この数年、サプライチェーンに影響を与えるサイバーインシデントが目立つようになりました。その代表的事例としては、2020 年末に発生した管理ソフトの汚染によるソフトウェアサプライチェーン攻撃[7]、2021 年に発生した米国石油パイプラインでのランサムウェア被害事例[8]や米国 Kaseya 社製品の脆弱性を起点とするサービスサプライチェーン攻撃事例[9]などがありました。

ここで前提としてサプライチェーン関連の概念を整理します。サイバーセキュリティの概念としては、まず「サプライチェーン攻撃」があります。この用語は現在ではより広義で使われており、「組織間の業務上の繋がりを悪用して次なる攻撃の踏み台とするサイバー攻撃手法全般」を指す言葉になっています。侵害する対象により大きく、ソフトウェア起点、サービス起点、ビジネス起点の 3 種に分けることができます。

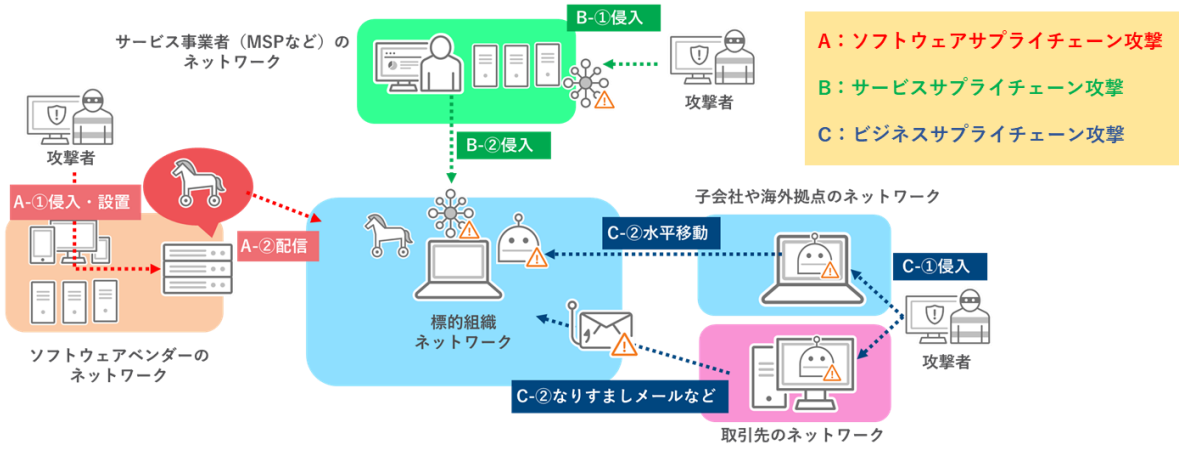

図 2：サプライチェーン攻撃の概念図

これに対し「サプライチェーンリスク」はサプライチェーン上の要因によって負の影響を受けるリスク全般を意味する、より視点が高い用語です。サイバーインシデントの例で言えば、ある企業がサイバー攻撃を受けた（サプライチェーン上の要因）ことにより、自社が委託した顧客情報が漏洩する（負の影響）、というような事態が発生するリスクです。ここでサプライチェーン攻撃は、サプライチェーンリスクでいう「サプライチェーン上の要因」の 1 つであり、サプライチェーンリスクはサプライチェーン攻撃を含むより上位の概念となります。

このようなサプライチェーンに影響を与えた最も大きな国内事例として、2022 年 3 月に公表された製造業・自動車部品メーカーにおけるランサムウェア被害[10]があります。この事例では、自動車部品を製造する企業がランサムウェア攻撃を受けたことにより、製造する部品

[7] https://japan.cnet.com/article/35163843/

[8] https://www.asahi.com/articles/ASP592PNYP58ULFA008.html

[9] https://helpdesk.kaseya.com/hc/en-gb/articles/4403440684689-Important-Notice-July-2nd-2021

[10] https://xtech.nikkei.com/atcl/nxt/news/18/12332/

の納入先である自動車メーカーが、直接のランサムウェア被害を受けていないにも関わらず、全国の工場での操業を停止させる事態となりました。これはまさに、サプライヤーで起こった事故が下流の企業に大きな影響を与えるサプライチェーンリスクが現実になったものと言えます。

またこの事例におけるランサムウェア攻撃の侵入原因としては、直接の被害企業の子会社が取引先企業に接続させるために設置していたリモート接続機器の脆弱性がきっかけとなった、と報告[11]されています。この子会社のネットワークを経由した侵入は、まさに企業間の業務上の繋がりから生まれた弱点を利用した攻撃であり「ビジネスサプライチェーン攻撃」に分類できます。

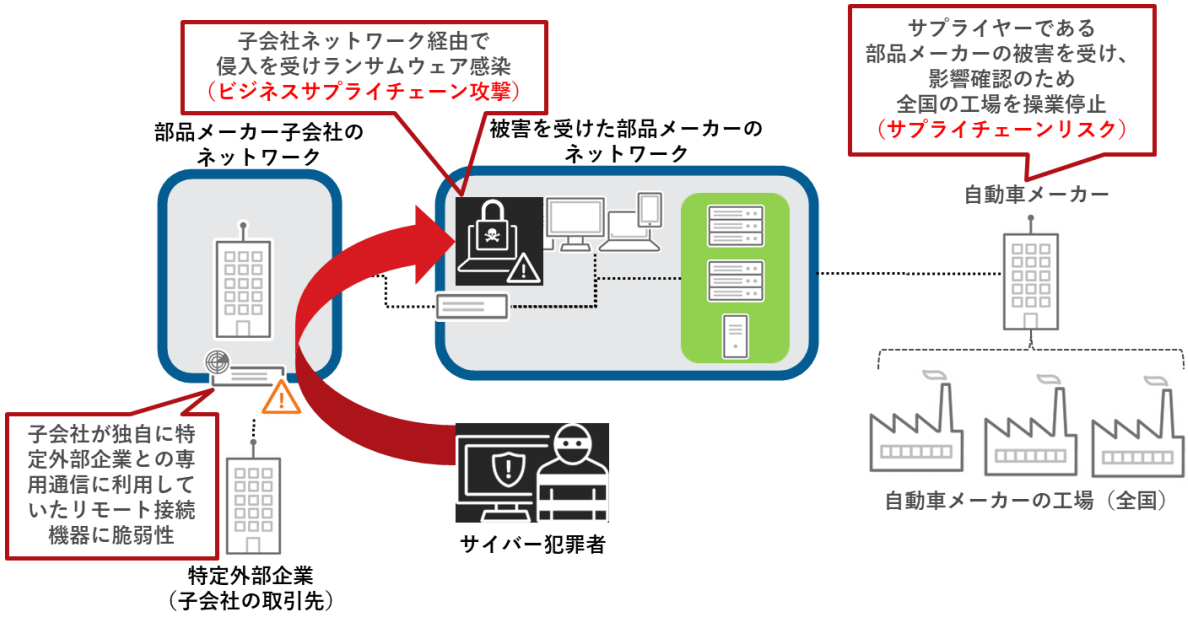

図 3：3 月に公表された自動車部品メーカーのランサムウェア被害の概要図

法人組織間のビジネス上の繋がりを悪用する「ビジネスサプライチェーン攻撃」は既に常套手段化したと言ってよい段階に入っています。標的型攻撃の中では、法人組織の海外拠点を侵害し、接続ネットワークを経由した水平移動により国内拠点へ侵入する攻撃が、継続して観測されています。より一般的なランサムウェア被害事例の中でも、既に 2020 年 11 月に海外拠点への侵入を起点に国内拠点でも被害が発生した日本のゲームソフトウェアメーカーの事例が報告[12]されています。またこの上半期に報道された国内企業のランサムウェア被害 29 件の中でも、実際に被害を受けたのは海外拠点のみである事例が、少なくとも 6 件ありました。これらの事例は単に海外拠点から国内へ攻撃への水平移動が無かっただけであり、ビジネスサプライチェーン攻撃一歩手前の状態だったと見做せます。

[11] https://smbiz.asahi.com/article/14589378

[12] https://www.capcom.co.jp/ir/news/html/210413.html

組織間の関係性の中で自組織のセキュリティを保つには

このように業務上の関係性を経由して攻撃が連鎖していくとともに、一組織の被害が関係する組織や業界、ひいては社会全体にまで影響を与える被害の連鎖も実際に発生していることがわかります。攻撃の被害は 1 組織に留まらず、業務上の関係性により他の組織や社会全体に連鎖します。このような状況において自組織の業務継続を守るためには、自身の安全を守ると共に、自身を取り巻くサプライチェーン全体のセキュリティレベルを高めていく事が必要になっています。

まず自組織の安全を守るには、そもそもの侵入に繋がる弱点を自ら作ってしまわないよう、脆弱性対策と共に、境界線上の設定ミスや意図しない露出のチェックといった基本的対策を徹底する事が重要です。また侵入されたとしてもその後の内部活動を自由にさせず、ネットワーク内の不審な活動を早期に可視化し迅速に適切な対応を行えるような体制が必要です。そのためには、ネットワークやエンドポイントにおける挙動監視など、内部活動を早期に可視化できる対策に加え、ゼロトラストアーキテクチャ（NIST SP800-207）[13]によるゼロトラストコンセプトの実装などが不可欠となりつつあります。

そして同時に、業務上の関連性の観点から自組織を取り巻く他組織が攻撃の踏み台となる可能性を考慮したセキュリティ戦略の立案も必要です。自組織ネットワークに対する他組織のアクセスを受け付ける必要がある際には、より厳しい制限が必要でしょう。この意味でも、ゼロトラストの実装は重要です。また他組織のセキュリティ対応を確認する必要性が高まると共に、すべての組織が自組織のセキュリティに対する説明責任を負うようになるでしょう。

[13] https://csrc.nist.gov/publications/detail/sp/800-207/final

事業継続を脅かすランサムウェア攻撃

組織のネットワークへの侵入を前提とした所謂「Human-Operated」型を中心としたランサムウェア攻撃は、法人における被害の中でも最も深刻なものとなりました。国内における四半期ごとのランサムウェア検出台数はここ数年高止まりの状況と言えましたが、2022 年、第 1 四半期は新たに 5700 件を超え、2019 年以降最多となりました。

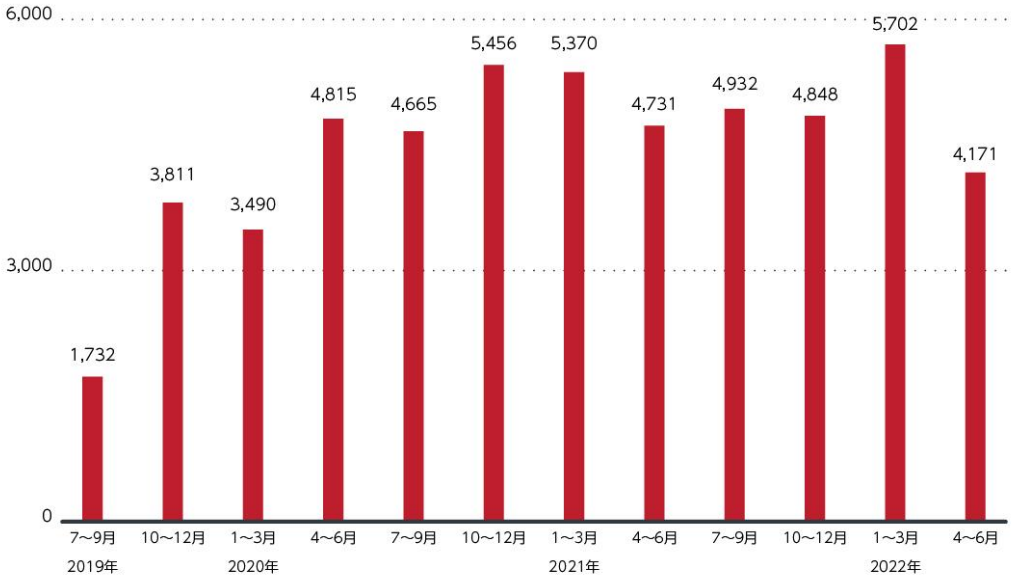

図 4：日本国内でのランサムウェア検出台数推移

国内ランサムウェア被害状況に見る二面性

実害の面から見ても、2022 年上半期の 6 か月間に国内で公表・報道されたランサムウェア被害は、トレンドマイクロが確認しただけでも 29 件を数えました。これは、2021 年 1 年間の 53 件を上回るペースであり、毎週 1 件以上の被害が公表されている状況となっています。

これらの被害を公表した法人の中でも製造業での被害が全体のほぼ半分を占め最多でした。中でも特に注目すべき事例として、3 月に公表された製造業における被害[14]があります。この事例では、被害企業が製造する部品の納入先にあたる自動車メーカーの工場が全国で操業を停止するなどの大きな影響が報じられており、この上半期に国内で最も注目されたインシデントと言えます。

[14] https://xtech.nikkei.com/atcl/nxt/news/18/12332/

図 5：2022 年 1 ～6 月に国内でランサムウェア被害を公表した法人組織 29 件の業種別割合
（公表を元に整理）

ただし、このような国内での被害状況については別の観点もあります。トレンドマイクロが受けた国内法人からのランサムウェア関連問い合わせのうち、実害の発生を示す被害報告件数に関しては減少傾向が見られています。被害報告件数を半年ごとの月平均で比較すると、2021 年上半期の 7.3 件から 2021 年下半期は 6 件、2022 年上半期は 3.2 件と減少の方向で推移しています。

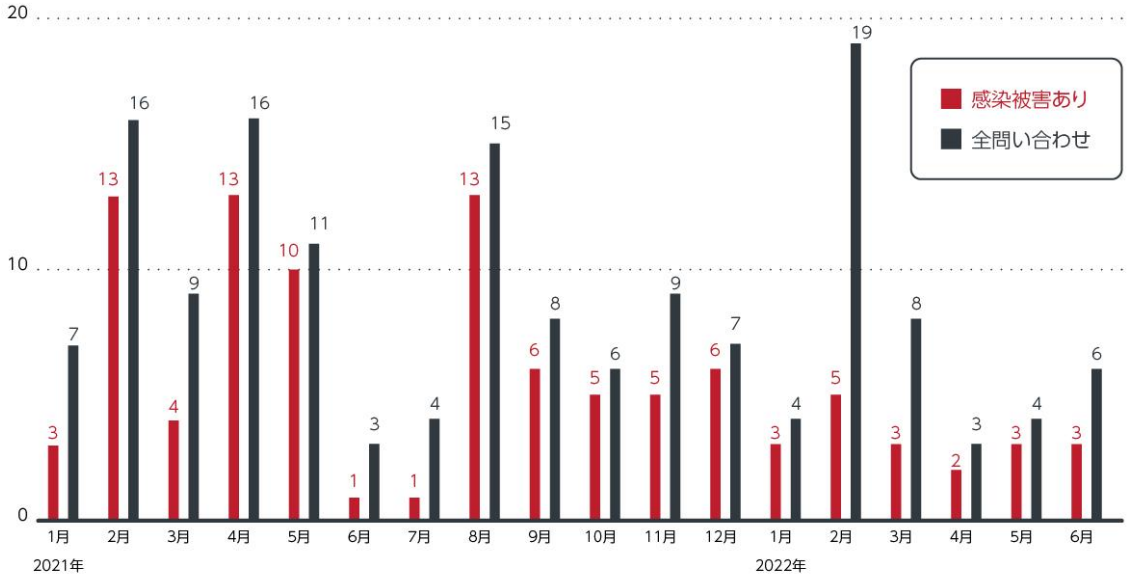

図 6：国内法人からのランサムウェア関連問い合わせ件数及び被害報告件数の推移
（トレンドマイクロ調べ）

2022年にトレンドマイクロが行ったランサムウェア被害の実態調査[15]によれば、日本は他国と比べ、最も身代金を支払わない国であるという結果が出ています。またこの数年、ランサムウェアギャングと呼ばれるサイバー犯罪者の摘発が目立っており、攻撃者側も不安定になっている可能性があります。2022 年に入っても大物ランサムウェアギャングの 1 つである REvil/Sodinokibi の容疑者逮捕[16]が報じられました。またもう 1 つの大物ランサムウェアギャングであった Conti は、内部情報の流出[17]などを経て 5 月には暴露サイトや身代金交渉用サイトが閉鎖されるなど活動休止[18]が観測されました。このようにランサムウェアギャングとそのサービスを利用するアフィリエイトなどのサイバー犯罪者側に不安定要素が多い中で、同じ攻撃を行っても身代金を得られる可能性が低いと考えられる日本企業への攻撃が、敬遠され始めている可能性は十分有り得るものと言えます。前出の被害を公表している国内法人の中でも、実際に被害を受けたのは海外拠点や現地法人のみという事例も目立ちました。サイバー犯罪者の目的は金銭利益であるため、より簡便に利益を得やすいと見做された組織ほど攻撃対象にされる可能性が高くなります。この意味から、そもそも攻撃者を自由にさせない対策を実施すること、及びデータの復旧手段を事前に準備し身代金を払う選択をする状況に追い込まれないようにしておくことは、社会全体のセキュリティにとっても重要な意味を持つことになります。

海外で活発なランサムウェア攻撃が国内でも被害

国内法人からトレンドマイクロに被害が報告されたランサムウェア種別については、世界的に被害が確認されているランサムウェア攻撃が日本にも被害を及ぼしている傾向が確認できました。

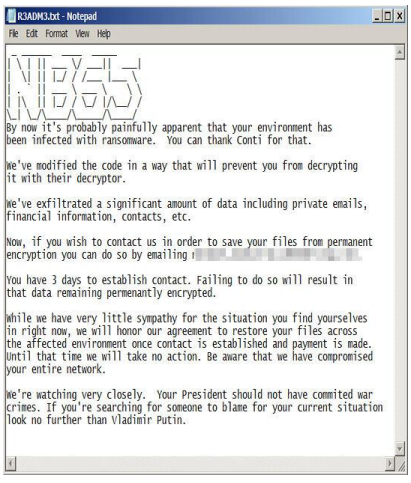

図 7：ランサムウェア「Conti」のランサムノート（脅迫文）例

[15] ※「ランサムウェア攻撃 グローバル実態調査　2022 年版」の公開ページの URL を入れる

[16] https://japan.zdnet.com/article/35182154/

[17] https://techcrunch.com/2022/02/28/conti-ransomware-chats-leaked/

[18] https://news.mynavi.jp/techplus/article/20220525-2351171/

この 2022 年 1~3 月に全世界で活発だったランサムウェア[19]として LockBit、Conti、BlackCat（別名：alphv）の 3 種がありますが、いずれも国内での被害報告を確認[20]しています。また Hive、Pandora についても被害報告が複数件あり、国内のネットワークを侵害する脅威であることを確認しています。特に Pandora は 2022 年 2 月の登場後すぐに被害報告が入っており、新たに登場したランサムウェア攻撃の国内流入が早まっている傾向が見て取れます。

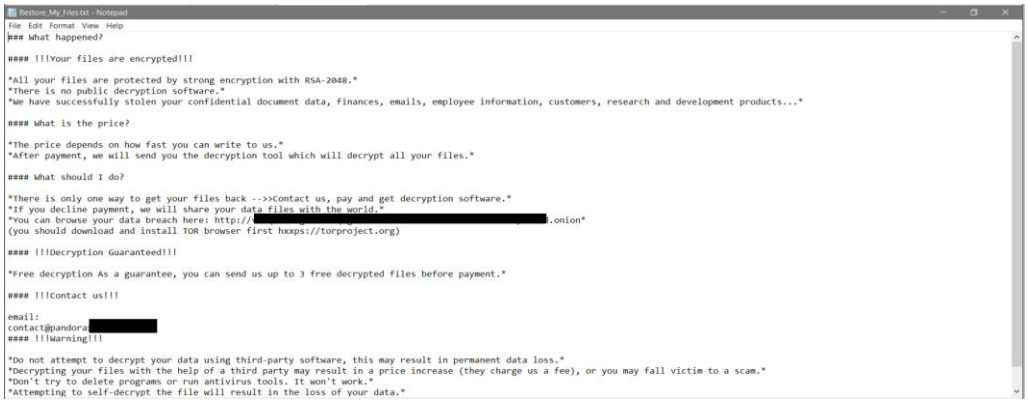

図 8：2022 年 2 月登場のランサムウェア「Pandora」のランサムノート（脅迫文）例

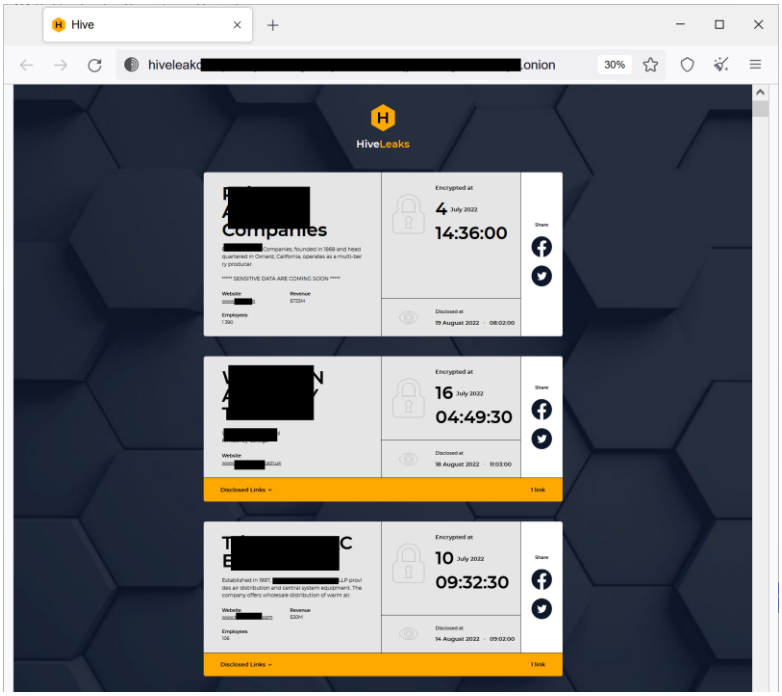

図 9：ランサムウェア「Hive」の暴露サイト例

[19] https://www.trendmicro.com/ja_jp/research/22/f/ransomware-in-q1-2022.html

[20] BlackCat のみ 7 月の報告

復活後さらに拡大する「EMOTET」の脅威

「EMOTET」はテイクダウンによる消滅[21]から一転、2021 年 11 月に活動再開[22]しました。そして 2022 年に入り、「最恐のマルウェア」とまで呼ばれたテイクダウン前を越える状態になっています。トレンドマイクロ SPN の統計によれば、EMOTET のダウンローダなどの関連モジュールと本体の検出を合わせた国内総検出台数で、2022 年第 1 四半期は 6 万件を超え、過去最大となりました。この検出台数は、全世界で国別に見ると日本が最多[23]となっており、この時期に日本が EMOTET の大規模攻撃対象となっていたことは間違いありません。

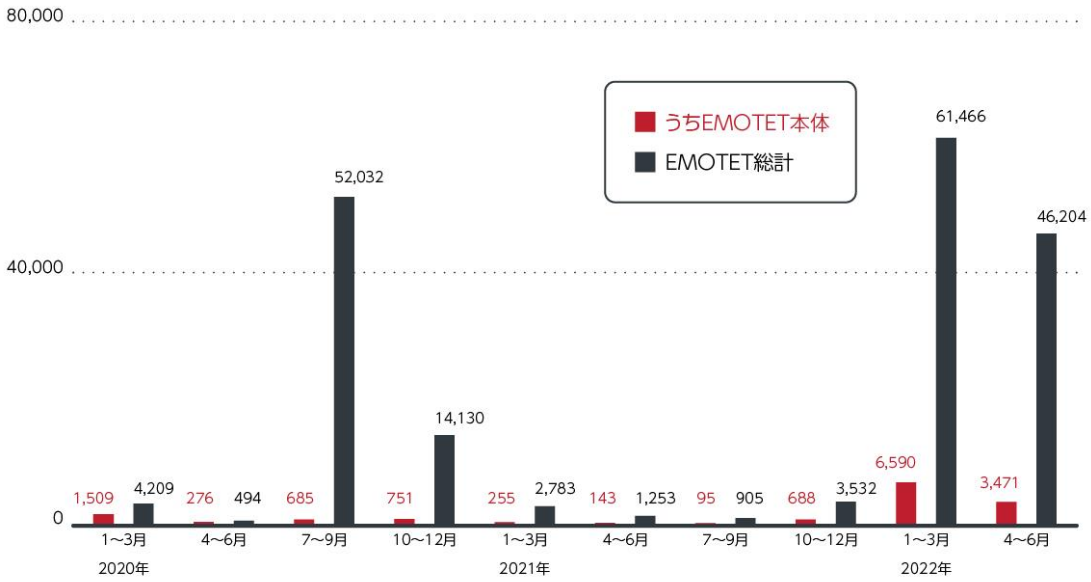

図 10：国内における EMOTET 検出台数推移

また検出を EMOTET 本体に絞っても 6 千件を超えており、国内では過去最大となっています。EMOTET 本体の検出増加は、攻撃メールから添付ファイルのダウンローダを開いてしまった利用者が多くなっていることを示しています。つまり、より感染の危険性の高い状況を示しており、この点に関してはテイクダウン前よりも危険な状態になっていると言えます。実際、EMOTET の感染被害を公表した法人の数は検出台数の動きと連動が見られており、2022 年 2 月、3 月がピークとなっています。

[21] https://www.europol.europa.eu/media-press/newsroom/news/world%e2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

[22] https://www.trendmicro.com/ja_jp/research/21/k/revival-of-emotet.html

[23] https://www.trendmicro.com/ja_jp/research/22/f/bruised-but-not-broken--the-resurgence-of-the-emotet-botnet-malw.html

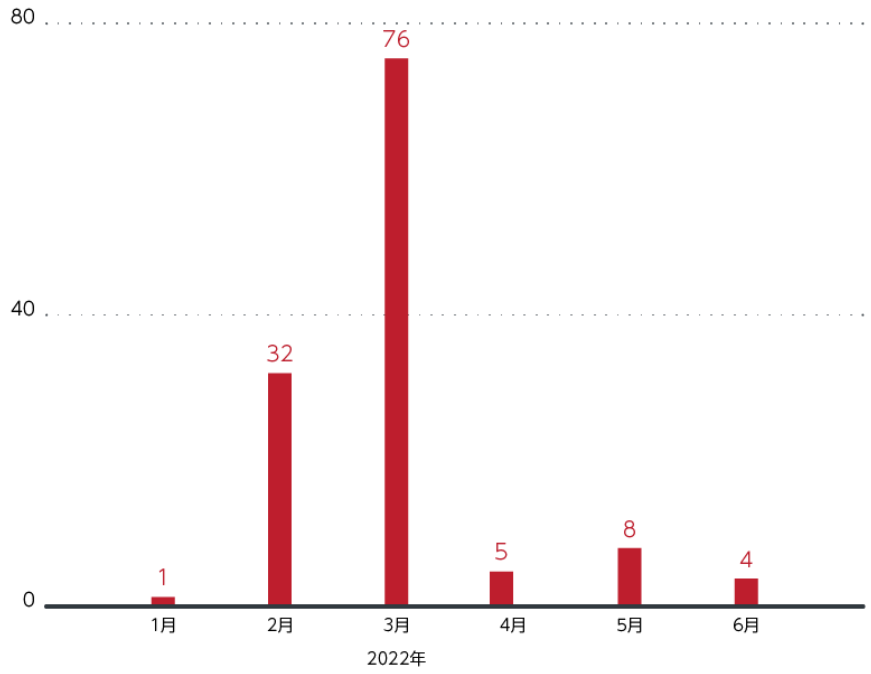

図 11：EMOTET 被害の公表件数推移（公表を元に整理）

復活後も変わらぬメール経由攻撃での拡散

このように EMOTET はメール経由で拡散するマルウェアとして、国内で最大の脅威となっています。ただし、復活後も攻撃内容に大きな変化はなく、不特定多数への攻撃メールと共に、感染端末上で送受信されたメールの情報を窃取して使用する「返信型」の攻撃メールに注意が必要です。

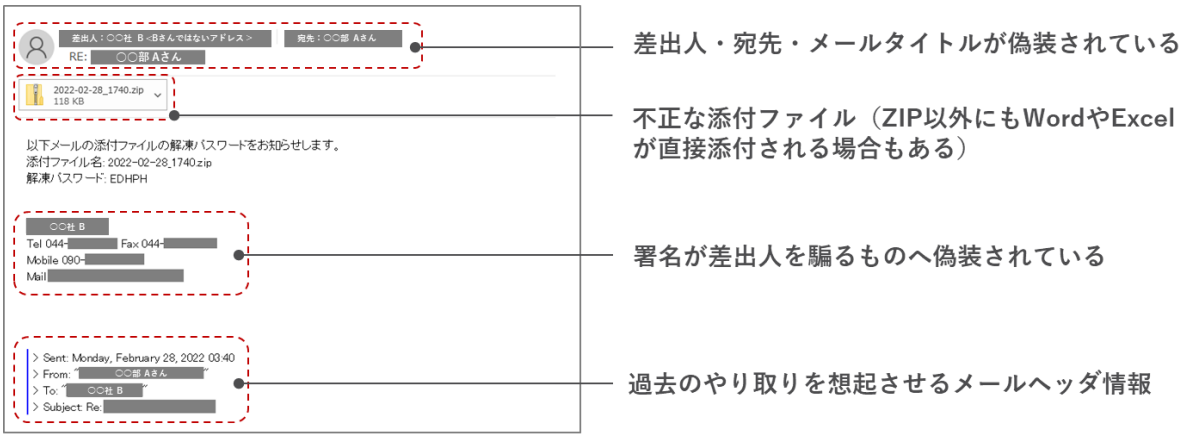

図 12：EMOTET の「返信型」攻撃メールの例（2022 年 2 月確認のサンプルを元に再構成）

そして主に攻撃メールに添付された不正マクロを含む Office 文書ファイルを開くことによって、最終的に EMOTET 本体が感染します。この不正マクロを含む Office 文書ファイルは、EMOTET に限らず、現在のマルウェア感染を目的とした攻撃メールや標的型メールにおけるもっとも主要な手口となっています。

図 13：不正マクロを含む EXCEL 文書ファイルの例（2022 年 2 月確認）
文書ファイルを開きマクロを有効化してしまうことで最終的に EMOTET に感染する

常に変化を見せる不正活動

EMOTET は端末への感染後、不正モジュールを取得して機能を更新することがあります。復活後 2022 年に入り見られた新たな機能として、Chrome ブラウザが保存するクレジットカード情報の窃取機能の追加を 6 月に確認しました。EMOTET に関しては既にブラウザが保存する認証情報を窃取する機能を確認していますが、それに加えてカード情報も窃取対象となったものです。また同じ 6 月には、ネットワークワーム機能が投入されたケースも確認しています。これはネットワーク上の他の端末に対して予め用意した認証情報を使ったいわゆる辞書攻撃による侵入を試行するもので、テイクダウン以前にはよく見られていた機能です。

また、攻撃メールによる感染活動における変化としては、Office 文書ファイルではなく、ショートカットリンク(.LNK)ファイルの悪用を 4 月に確認[24]しました。ショートカットリンクから PowerShell などを呼び出すことにより不正スクリプトを実行させる手口は、これまでも標的型攻撃などでは確認されていた手法ですが、EMOTET の攻撃メールで確認されたのはこれが初めてです。

[24] https://www.trendmicro.com/ja_jp/research/22/e/emotet-new-modus-operandi.html

図 14：2022 年 4 月に確認された EMOTET スパムの例
添付圧縮ファイル内にショートカットリンク（LNK ファイル）が含まれている

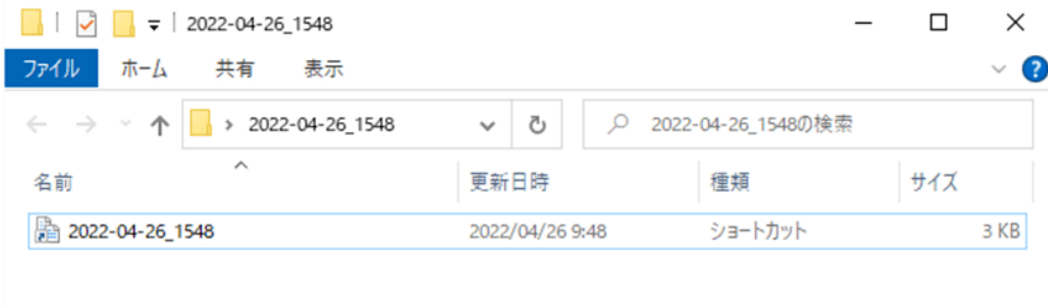

図 15：上図の圧縮ファイルを展開した例
一般の設定ではショートカットリンクを示す「.LNK」の拡張子はエクスプローラ上で表示されないがアイコンとファイル種類でショートカットであるとわかる

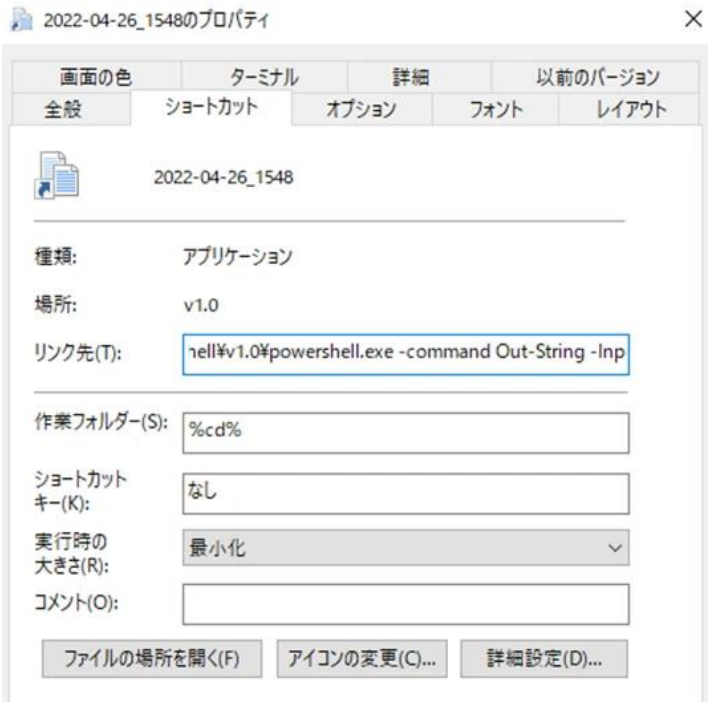

図 16：上記ショートカットファイルのプロパティを確認すると
「リンク先」に powershell.exe を指定し、不正スクリプトを引数として実行させる

この変化の背景として考えられるのは、マイクロソフトが行った不正 Office マクロ対策です。Office マクロの不正利用が常套手段化している現状に対しマイクロソフトは、2022 年 4 月以降にインターネットから入手された Office 文書ファイルについてマクロを無効化する機能変更を行うと発表[25]しました。EMOTET の背後にいるサイバー犯罪者はこの新たな対策に素早く反応し、Office マクロ以外の方法を試行したものと考えられます。

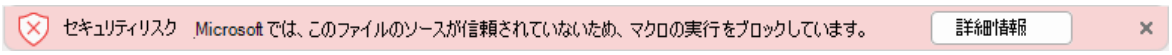

図 17：新たなマクロ無効化時の表示例
（引用：https://docs.microsoft.com/ja-jp/deployoffice/security/internet-macros-blocked）

その後、マイクロソフトはこのマクロ無効の仕様を 7 月に一旦撤回[26]するなど若干の混乱も見られましたが、その後すぐに再開[27]しており、現状としては Office マクロ不正利用への対策が一歩進んだ状態です。マイクロソフトでは、2021 年 12 月に EMOTET などに悪用された Windows App Installer の機能を 2022 年 2 月から当面無効にする[28]など、マルウェア拡散への対策に積極的な姿勢を示しており、EMOTET のサイバー犯罪者も敏感に反応した可能性があります。

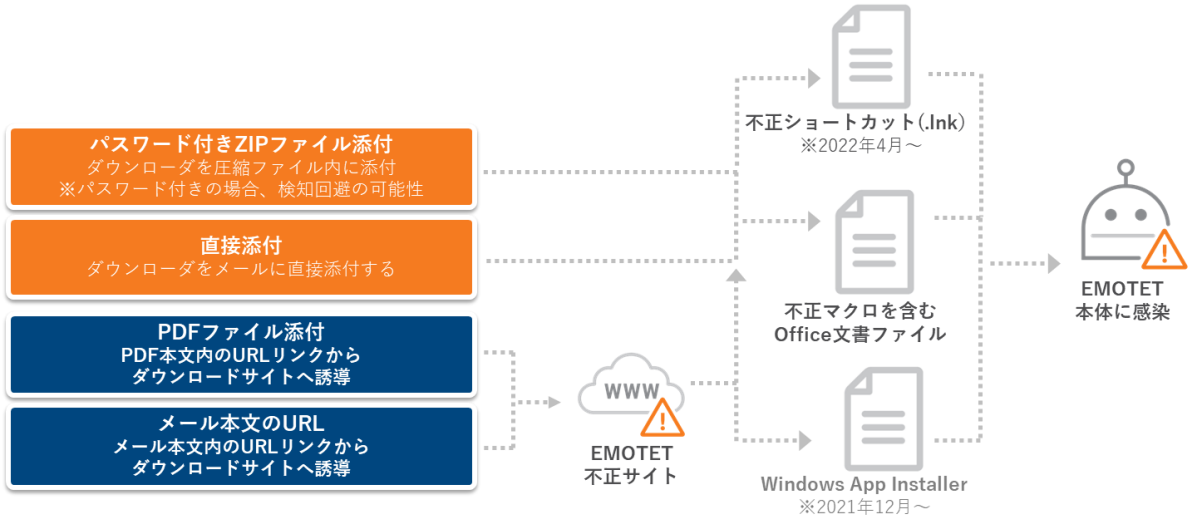

図 18：これまでに確認されたマルウェアスパムから EMOTET を感染させる手口の概念図

EMOTET の攻撃メールについて、本項執筆の 2022 年 7 月現在ではまだ Office 文書ファイルの手口が主流のままとなっているため、なるべく最新の Office を使用することで感染リスクの低減が期待できます。ただし、このような攻撃手法は常に変化するものですので、1 つの手法だけに囚われることなく、メール全般に対する注意を怠らないようにすべきです。EMOTET は不定期的にメール攻撃を停止することがありますが、停止の後には何らかの変

[25] https://docs.microsoft.com/ja-jp/deployoffice/security/internet-macros-blocked
[26] https://gigazine.net/news/20220711-microsoft-rolls-back-block-office-macros
[27] https://news.yahoo.co.jp/articles/191627b20d4e64868ef6d5a3649e100caafb2fa6
[28] https://japan.zdnet.com/article/35183248/

化を見せることが多くなっています。本項内で触れた変化についても、ショートカットリンクの悪用は 4 月下旬に初めて観測されましたが、その直前の 4 月中旬には 2 週間程度の休止がありました。トレンドマイクロの監視によれば、EMOTET は 7 月中旬から本項執筆の 8 月中旬時点まで 1 か月以上攻撃メール送信の休止が見られており、更なる変化と共に攻撃が再開されることが懸念されます。

誰でも手が届く「クラウド」上のリソース侵害

侵入事例の中では、インターネット側から到達可能な VPN などのネットワーク機器が侵入経路として侵害される事例が顕著になっています。同様に、インターネット側から到達可能な公開サーバやクラウド上のリソースも継続して狙われています。サイバー犯罪者は以前から、Web 上の情報を標的の 1 つとしてきましたが、現在はそれに加え、これまでは組織のネットワーク内に保持されていた情報がクラウドに移行する状況を見逃さずに攻撃対象としています。

クラウド上のリソースを危険に晒す「脆弱性」

2022 年上半期に公表された情報漏洩事例をトレンドマイクロで整理、集計したところ、Web やクラウドのシステムからの漏洩は 38 件確認され、公表内容などから漏洩情報の件数を合計すると全体で 430 万件の情報が漏洩した可能性があります。これを昨年同時期にあたる 2021 年上半期と比較してみると、事故件数は半数以下に減少（89 件→39 件）しましたが、漏洩情報件数は約 13 倍に増加（32 万件→430 万件）しており、一件当たりの被害が大規模化していることになります。

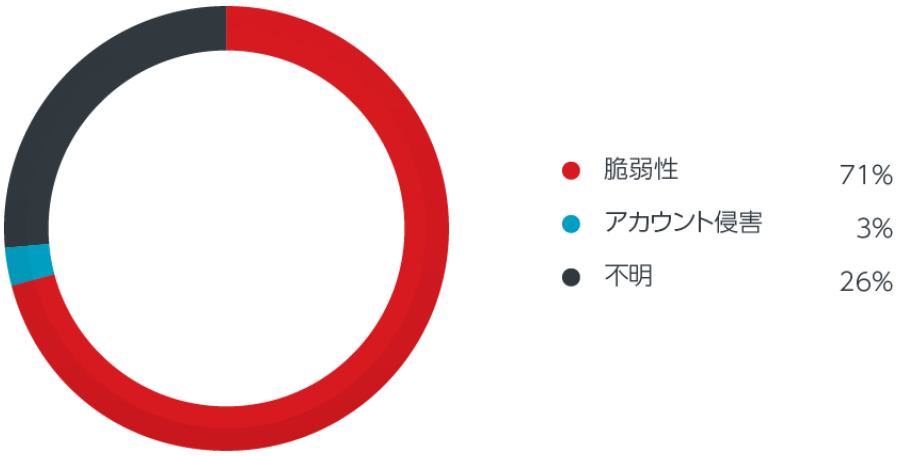

図 19：2022 年 1~6 月に公表された Web/クラウドからの情報漏洩事例
38 件における事故原因割合（公表内容を元に集計）

そしてこれらの事例の発生原因としては、約 7 割が脆弱性となりました。一方、昨年同期には 24%を占め 2021 年を通して大きく増加した設定ミスが原因となる事例は、この上半期には特定した報告がありませんでした。ゼロデイ以外の脆弱性は適切に修正を行っていれば免れていたはずの弱点と言えます。同様に、設定ミスも自ら作り出してしまった弱点による被

害と言えます。つまり、どちらも運用側の対策で減らせる性格を持つ事故原因と言えますが、結果として脆弱性と設定ミスは正反対の状況になりました。

また、被害を認識した理由として、自組織で気づけた割合は 18%でした。この割合は数年前から 2 割前後で推移しているため、自組織が運用しているシステムの把握、監視が不十分な組織が被害に遭う状況が継続している、と言えます。

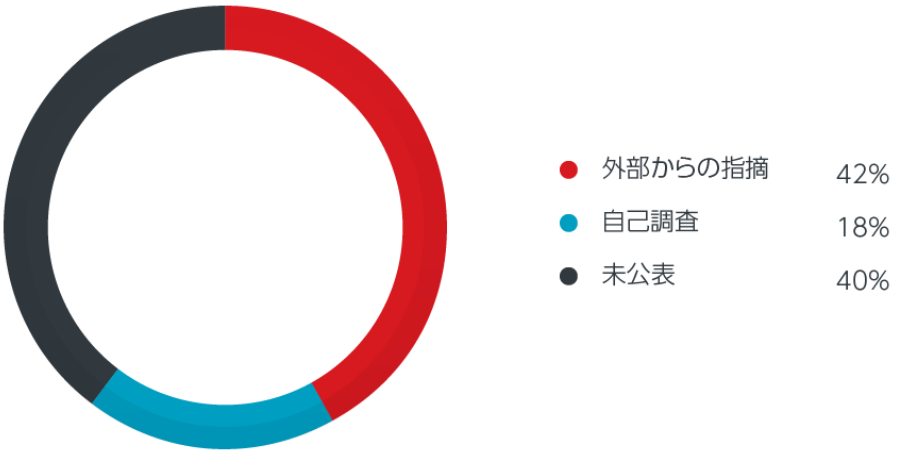

図 20：2022 年 1~6 月に公表された Web/クラウドからの情報漏洩事例 38 件における被害発覚事由割合（公表内容を元に集計）

個人利用者にとっての危険は「ネット詐欺」に集約

不特定多数に対するばらまき型のマルウェアスパムによる EMOTET などのマルウェア感染を例外として、個人のインターネット利用者を狙うサイバー犯罪の手法はほぼ「ネット詐欺」に集約されつつあります。フィッシングに代表される各種詐欺サイトへの誘導件数は、2020 年以降過去最大を更新し続けてきました。2022 年に入り詐欺サイトへの誘導はいったん落ち着いたように見えますが、2022 年上半期（約 2245 万件）は前年同期の 2022 年上半期（約 2272 万件）とほぼ同数となっており、高止まりの状況と言えます。また、全体の誘導に対するモバイル利用者の割合は 2020 年上半期には全体の 25%でしたが、2020 年下半期以降は 4 割前後で推移しています。これは携帯電話のテキストメッセージ機能である SMS を悪用する、所謂「スミッシング」の存在が要因の 1 つと言えます。

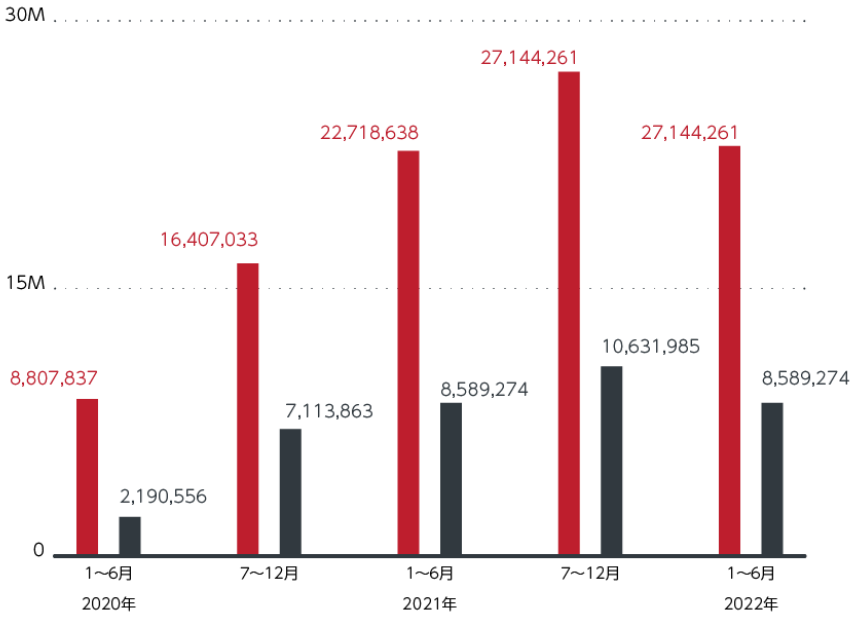

図 21：国内から各種詐欺サイトに誘導された利用者の端末台数[29]の推移と内訳

フィッシング詐欺と不正アプリ

詐欺サイトの中でも情報詐取を狙うフィッシングについては、特に個人情報と共にキャリア決済など金銭にも直結するサービスとして携帯電話キャリアのサービスを狙うものが目立っています。その他にも、詐欺サイトの内容として以前から多い銀行など金融機関やクレジットカードの関連サイトや、モバイル/スマートフォン決済サービス、暗号資産取引所、SNS、ポータルサイト、ネットショッピング/オークションサイト、交通系サービスや生命保険な

[29] ここでは 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しています

ど、多岐に及んでいます。誘導手段としてはフィッシングメールと共に携帯電話のテキストメッセージである SMS によるフィッシング、いわゆるスミッシングが常套手段となっています。

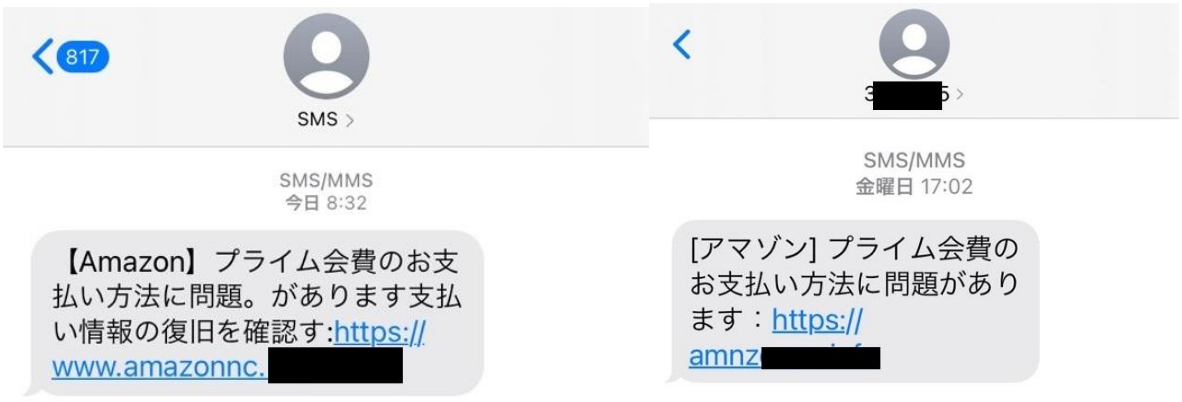

図 22：会費支払いの話題を偽装した「スミッシング」SMS の例
左：2021 年 5 月確認、右：2022 年 6 月確認だがほぼ同じ内容

狙われる情報としてはサービスや決済を利用するための認証情報に加え、クレジットカードなどの番号とセキュリティ番号から、本人確認に利用可能な個人情報を入力させるものの他、電子マネーやプリペイドを悪用して金銭の詐取を狙う詐欺サイトも目立っています。

図 23：携帯電話キャリアを偽装したフィッシングサイトの例
認証情報詐取の後、2 段階認証の突破も試みるリアルタイムフィッシング手口

図 24：鉄道会社の Web サービスを偽装したフィッシングサイトの例
本人確認に利用可能な個人情報とクレジットカード情報の詐取を狙う

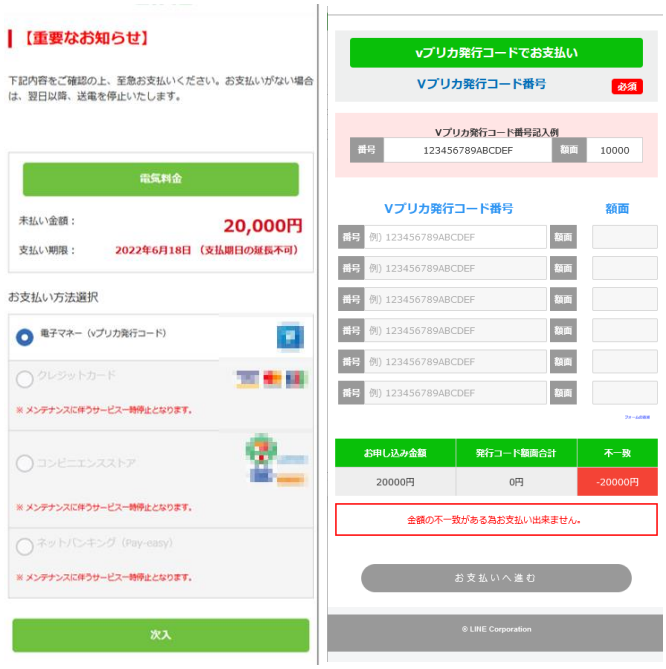

図 25：料金未納の理由で電子マネー経由での金銭詐取を狙うフィッシングサイトの例
コードの連絡だけで受け渡しが可能な電子マネーの仕組みを悪用

モバイル利用者を狙う詐欺サイトでは、スミッシングによる誘導から Android 端末の場合は不正アプリのインストール、iPhone の場合はフィッシングサイトへ誘導する手口が常套化しています。

図 26：不正サイトから Android 向け不正アプリをインストール させる例
セキュリティアプリを偽装し、SMS へのアクセスを要求している

図 27：iPhone でアクセスした場合に誘導される
携帯電話キャリアを偽装したフィッシングサイトの例（2022 年 2 月確認）

ただし、iPhone についても不正アプリの危険が無視できなくなってきています。2021 年に国内で初めて確認[30]された確認された構成プロファイル（プロビジョニングプロファイル）の悪用により iPhone に不正アプリをインストールさせる手口が、2022 年に入って再び確認されました[31]。iPhone は標準では正規のアプリマーケット経由でのみアプリのインストールが許されています。このため、不正アプリのリスクはほとんどないものと認識されてきました。しかし、このように継続して iPhone を狙う不正アプリの事例が確認された今、iPhone 利用者においても不正アプリをインストールされる手口を認識し、注意を怠らないようにしてください。

[30] https://www.trendmicro.com/ja_jp/research/21/k/tianyspy-via-SMS.html
[31] https://www.trendmicro.com/ja_jp/research/22/c/malicious-app-disguised-dating-app.html

図 28：iPhone に不正アプリをインストールさせる手口例（2022 年 1 月確認）
構成プロファイルのダウンロードを許可してしまうと不正アプリがインストールされる

図 29：iPhone にインストールされた不正アプリの画面例
マッチングアプリを偽装し、電話番号、SMS、連絡先、位置情報などの情報を窃取する

サポート詐欺とブラウザ通知スパム

ネット詐欺の中でも常套手段的に継続して確認されているものの 1 つとして、「サポート詐欺」があります。海外では「Tech Support Scam（TSS）」とも呼ばれるこの詐欺手口は、PC のシステム不調やセキュリティ問題、ウイルス感染などを偽装したブラウザ上の表示から、利用者にサポートセンターを偽装した電話番号に電話をかけさせ、実体のないサポートサービスなどの契約を結ばせることで被害者から金銭を詐取するものです。以前からブラウザ上で偽の警告表示を行って利用者を騙す「偽警告（Fake Warning）」などと呼ばれる手口がありましたが、それらの延長線上にある詐欺手口と言えます。サポート詐欺は国内では 2016 年頃から問題になっているネット詐欺手法であり、他のフィッシング詐欺などと同様に増減を繰り返しながら被害の継続が見られています。国内個人利用者からのトレンドマイクロへの問い合わせでは、2021 年末から 2022 年に入り報告の増加が見られており、ここ数年間におけるピークとなっています。

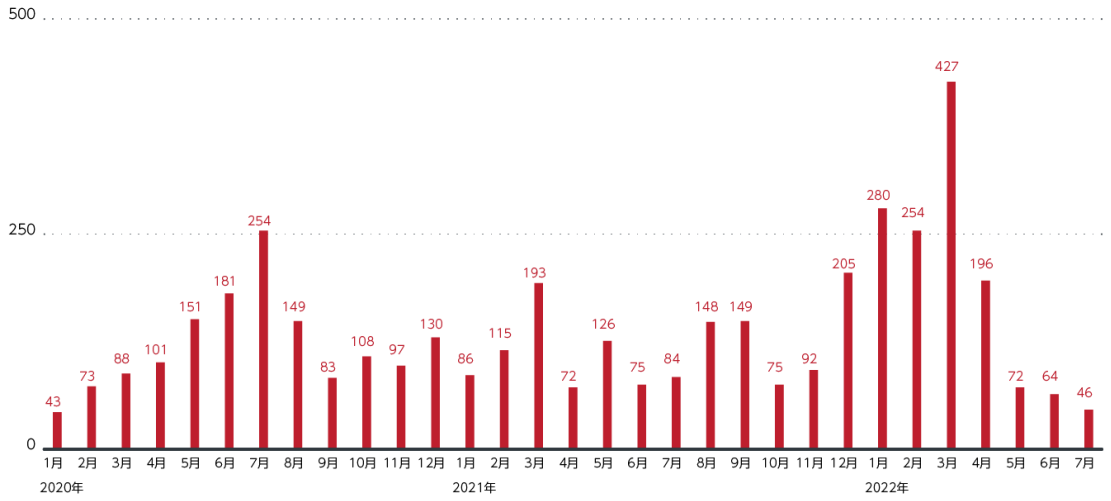

図 30：国内個人利用者からのサポート詐欺関連問い合わせ件数推移
（トレンドマイクロ調べ）

また Web 上での不正広告と連動する誘導経路として「ブラウザ通知スパム（BNS）」も継続して見られています。これは各種ブラウザの正規機能である「Web ブラウザのプッシュ通知」を悪用する手口です。利用者が Web 上で表示されるプッシュ通知の許諾を OK してしまうことにより、ウイルス感染やシステムの異常を訴える不正なプッシュ通知が表示され、不審サイトへ誘導されます。誘導先の不審サイトとして確認されている事例としては、アフィリエイト利益が目的とされる正規セキュリティソフト購入サイトや、上述のサポート詐欺サイトが確認されています。

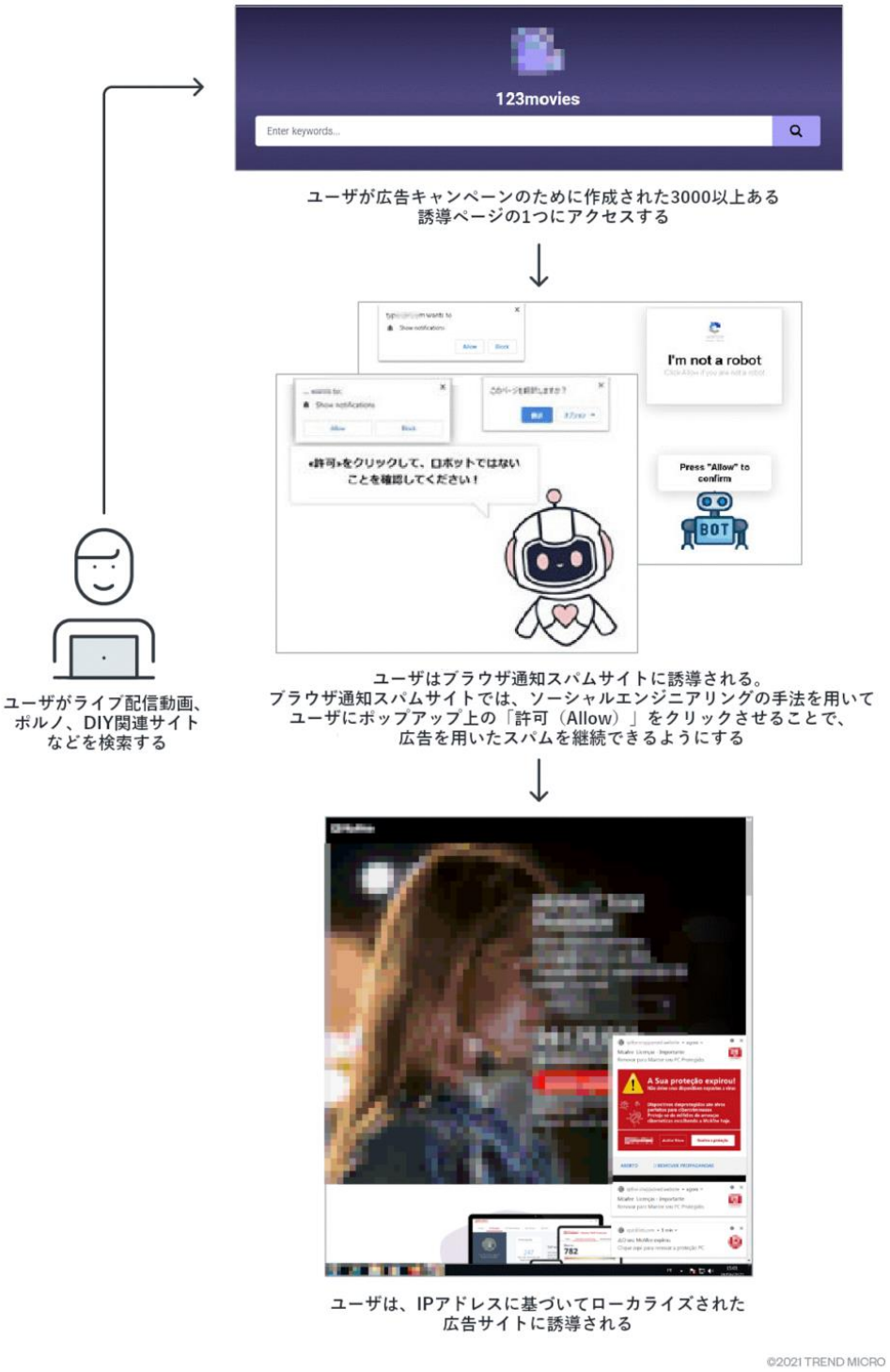

図 31：「ブラウザ通知スパム」手口の概念図

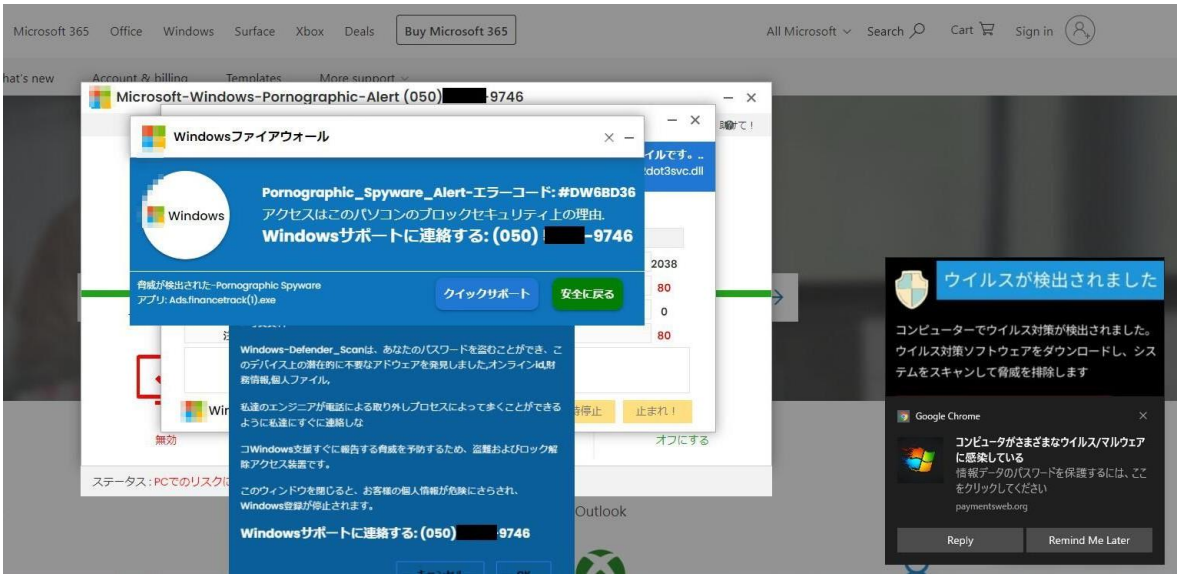

図 32：「ブラウザ通知スパム」から「サポート詐欺サイト」への誘導例
（2022 年 3 月確認）

BNS は各種ブラウザに通知機能が導入された 2015 年前後から既に見られていた手法ですが、最近では 2021 年 2 月前後から世界的な増加が見られました。その後、日本でも問い合わせが急増し、ピークとなった 2021 年 11 月には 700 件を超える問い合わせがありました。しかし 2022 年に入ってからは毎月 200 件未満で推移しており、2021 年と比較して減少が見られています。

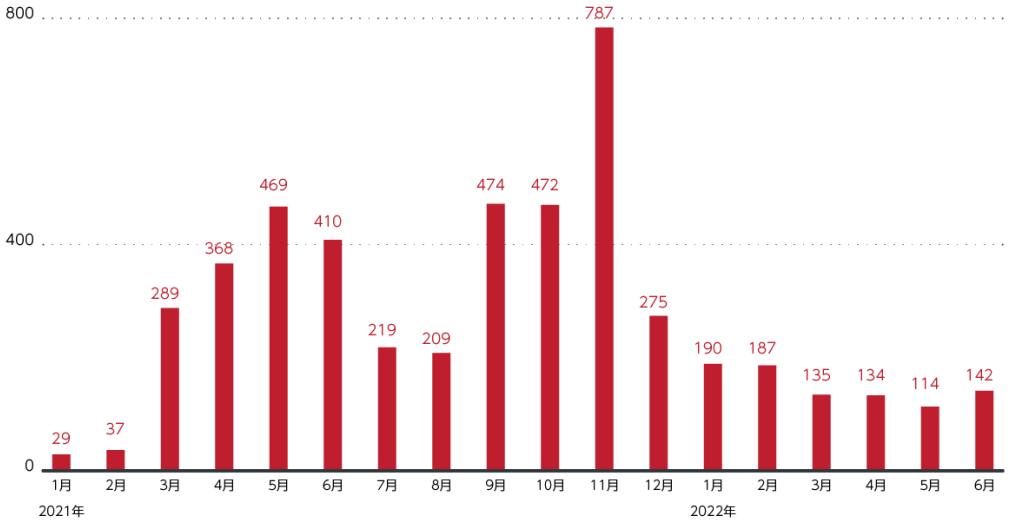

図 33：国内個人利用者からの BNS 関連問い合わせ件数推移
（トレンドマイクロ調べ）

これは、利用者への BNS の脅威周知の浸透と共に、各社の技術的対策の効果があるものと考えられます。例えば Google の Chrome ブラウザでは、2020 年のバージョン 86 の段階か

らセーフブラウジング機能を利用した不正な通知のブロック機能[32]を持っていましたが、2022 年 6 月のバージョン 103 では利用者が望まない通知を判断して表示しない機能[33]も追加されました。また、トレンドマイクロ製品では BNS 対策機能を 2022 年 2 月から徐々に導入し、4 月から個人利用者向けエンドポイント製品で本格展開しました。この結果、開始の 2 月から 6 月の全世界の合計ではのべ 41 万 7 千件（うち国内で 29 万 2 千件）の利用者が BNS サイトへのアクセスから守られました。

また 6 月にはネット詐欺のインフラとなり得る、不審な「Web プロキシサイト」の事例[34]が注目されました。Web プロキシサイトとは「プロキシ回避システム（Proxy Avoidance Websites）」などとも呼ばれ、指定サイトを中継表示するサービスですが、特定のサイトが本来とは異なる URL で表示されるため、偽サイトと認識されることがあり、これまでも度々騒ぎになってきました。また、中継時に本来の表示を変更する、不正なコンテンツを追加するなどが可能なため、悪用も懸念されてきました。この 6 月の事例では、中継するサイトの表示に本来は存在しない広告を追加するグレーな動きが確認され、不正な目的へ転用される可能性が高まったことを示す事例と言えます。

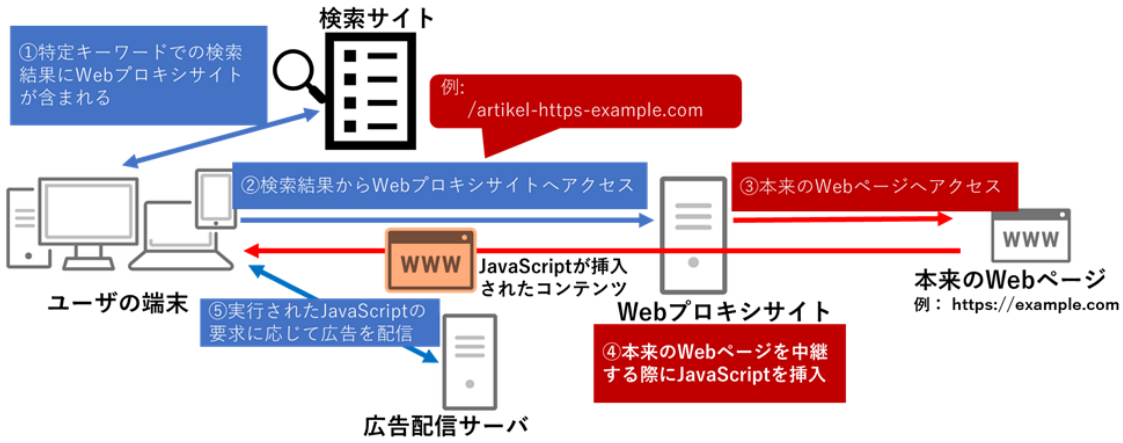

図 34：6 月に確認された事例の Web プロキシサイトによる「不審な行為」の概念図

このように、不特定多数の個人インターネット利用者を狙う攻撃は、ほぼすべてが詐欺的な手口へシフトしています。現実社会のいわゆる振り込め詐欺（特殊詐欺）などと同様に、ネット詐欺に対しても騙す側の手口を知り、騙されないように注意する心がけが自身を守るための第一歩となります。またネット詐欺の場合には、詐欺手口の判断が難しい場合にはスパムメール対策や不正サイト対策などの技術的対策を利用することで危険を避けることが可能です。

[32] https://forest.watch.impress.co.jp/docs/news/1285706.html

[33] https://japan.cnet.com/article/35188755/

[34]

グローバルセキュリティラウンドアップ

アタックサーフェス拡大と時事問題で巧妙化する攻撃手口

「RaaS」と「多重脅迫」で進化するランサムウェア

企業の業務に影響するソフトウェアの脆弱性

クラウド環境における旧態依然の問題と従来とは異なる攻撃

2022 年上半期の脅威概況

アタックサーフェス拡大と時事問題で巧妙化する攻撃手口

アタックサーフェス拡大への懸念を表明する企業

ここ数年、多くの企業がデジタル技術を導入し、既存のビジネスモデルやプロセス、企業文化に手を加えることで、デジタルトランスフォーメーションに挑戦しています。この変革により、電子メールのインボックス、IoT（Internet of Things）デバイス、モバイルアプリケーション、ウェブサイト、パブリッククラウドサービス、さらにはサプライチェーンのインフラなど、より広い範囲を網羅するデジタル上のアタックサーフェス（攻撃対象領域）が生じることとなりました。

トレンドマイクロでは、調査機関 Sapio Research と共同で、29 カ国の IT セキュリティの意思決定者 6,297 人を対象に、アタックサーフェスの拡大がもたらすリスクについての考えを調べました[35]。その結果、相当数（73%）の企業がそうしたアタックサーフェスの大きさを懸念していることが判明しました。また、37%が「状況は常に進化しており、混乱している」とし、さらに 43%が「アタックサーフェスは制御不能になりつつある」と主張しました。

こうした懸念の中、回答者の 62%が、セキュリティ態勢を弱める盲点があることを認めています。また、37%の企業は、クラウド資産に対する知見が最も乏しいと主張しています。さらに 35%は、ネットワークに対する知見も同様であると回答し、そして 32%は、エンドユーザの資産に対する知見が最も低いと回答しています。

また、これらの企業の多くは、直面するリスクに対してどのように対処すればよいのかがわからないということも明らかになりました。回答者の 38%は、サイバーリスクの定量化を主要な課題としており、33%は、これらのリスクを理解し管理するためのリソースが単に不足していると述べています。さらに 32%は、リスクにさらされている領域の可視性が限られていると述べています。

図 1：IT セキュリティの意思決定者 6,297 人を対象とした調査により、
相当数の意思決定者がデジタル攻撃表面を懸念していることが明らかになった

[35] https://www.trendmicro.com/explore/trend_global_risk_research_2/the-challenge-of-man

図 2：IT セキュリティの意思決定者は、セキュリティに関する知見が最も低い分野として、クラウド資産、ネットワーク、エンドユーザ資産の 3 つを挙げている。

ツールやインフラを駆使する Earth Lusca や Earth Berberoka

2022 年上半期、大規模なインフラを採用してさまざまな種類のマルウェアやその他のツールを統合して長期的な攻撃を展開する APT グループの標的型攻撃キャンペーンが継続的に実行されました。

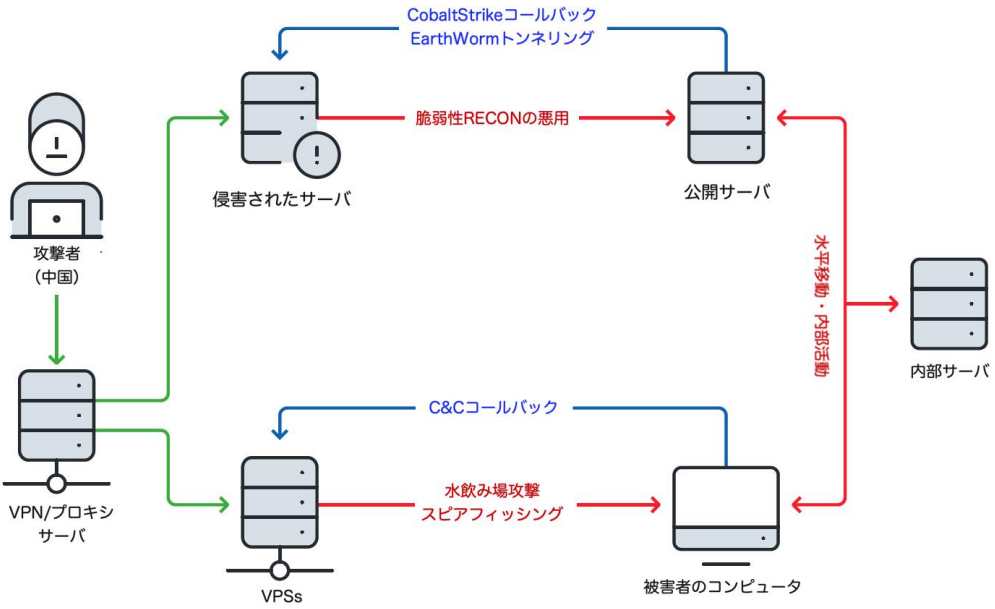

図 3：Earth Lusca の感染フロー。攻撃グループが用いる 2 つのインフラ

Earth Lusca ：2022 年上半期に注目された APT グループの 1 つ Earth Lusca は、2021 年半ばから活動しており[36]、スピアフィッシングや水飲み場攻撃を利用して、世界中の企業や組織を狙って諜報活動や金銭目的の攻撃動機キャンペーンを展開しています。被害を受けた組織の大部分は、政府機関や教育機関、政治団体、報道機関、さらには Covid-19 関連の

[36] https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/a/earth-lusca-employs-sophisticated-infrastructure-varied-tools-and-techniques/technical-brief-delving-deep-an-analysis-of-earth-lusca-operations.pdf

研究機関といった付加価値の高いターゲットでした。この攻撃グループは、2 種類のインフラを利用しています。
1 つ目は、ソーシャルエンジニアリング攻撃に使用されるレンタル仮想プライベートサーバ（VPS）で、コマンド＆コントロール（C&C）サーバとしても使用されています。特にこの C&C サーバを使用して、Cobalt Strike、ShadowPad、Funny Switch、Winnti などの多くのマルウェアや攻撃ツールを展開しています。
もう 1 つのインフラは、古いオープンソースバージョンの Oracle GlassFish Server で構成されたサーバであり、一般公開されているサーバの脆弱性スキャンやネットワーク内のトラフィックトンネルの構築に使用されています。また、Cobalt Strike の C&C サーバとしても使用されていました。

Earth Berberoka ：2022 年 4 月、トレンドマイクロは、中国のギャンブルサイトを主な標的する APT グループの活動記録の調査結果を発表しました[37]。この攻撃グループを「Earth Berberoka」と名付けました。この攻撃グループは、少なくとも 2020 年から活動しており、異なる OS（Windows、Linux、macOS）をターゲットにする中、同一のバックエンドインフラを共有して数多くの種類のマルウェアファミリーを使用していました。
さらにこの攻撃グループは、これらのマルウェアファミリーに加え、複数の異なる感染経路を採用していました。それらは、安全とされるチャットアプリ「MiMi」、偽の暗号資産アプリ、不正な Adobe Flash Player インストーラをホストする Web サイトなど多岐に及んでいました。
そうした中、2022 年上半期に確認された注目すべき感染経路は、ペイ・パー・インストール（PPI）サービスを通じて配布されるマルチコンポーネント型のマルウェア「NetDooka」を利用した手法です[38]。この場合、ローダ、ドロッパ、保護ドライバ、リモートアクセスツール（RAT）などが駆使され、拡散には、マルウェア「PrivateLoader」が使用されていました。セキュリティ機関 Intel471 のレポートによると、PrivateLoader は、ダウンロードした海賊版ソフトウェアを通じてユーザの端末に感染します[39]。
感染後、まずマルウェア NetDooka がインストールされ、その後、ローダを解読して実行するドロッパのコンポーネントがインストールされます。このローダにより、感染端末の環境がスキャンされた後、別のドロッパのコンポーネントがダウンロードされ、実行されます。そしてこのドロッパは、リモートシェルの起動、ブラウザデータやスクリーンショットの取得などの機能を備えた RAT の復号と実行に使用されます。
NetDooka が使用するインフラは、攻撃者にとっては、PPI の手口を利用する際の格好の選択肢であり、マルウェアを容易に拡散できる点でも有効といえます。

[37] https://documents.trendmicro.com/assets/white_papers/wp-operation-earth-berberoka.pdf
[38] https://www.trendmicro.com/en_us/research/22/e/netdooka-framework-distributed-via-privateloader-ppi.html
[39] https://intel471.com/blog/privateloader-malware

EMOTET 復活の原動力となった攻撃活動

新しく登場したマルウェアファミリーは、セキュリティ業界や一般の人々から注目されることが多い一方、旧来のマルウェアファミリー、特に効果が実証されているものも、依然として企業や組織にとっての脅威となっています。トレンドマイクロの「2022 年セキュリティ脅威予測」[40]では、攻撃者がより効果的な攻撃のために、コモディティ化したマルウェアやその他のツールを継続的に利用し、攻撃がより一層深刻化すると予測していました。この予測は、サービスとしてのマルウェア（MaaS）の手口で利用された悪名高いボットネット型マルウェア EMOTET を巡る状況から、現実に証明されました。

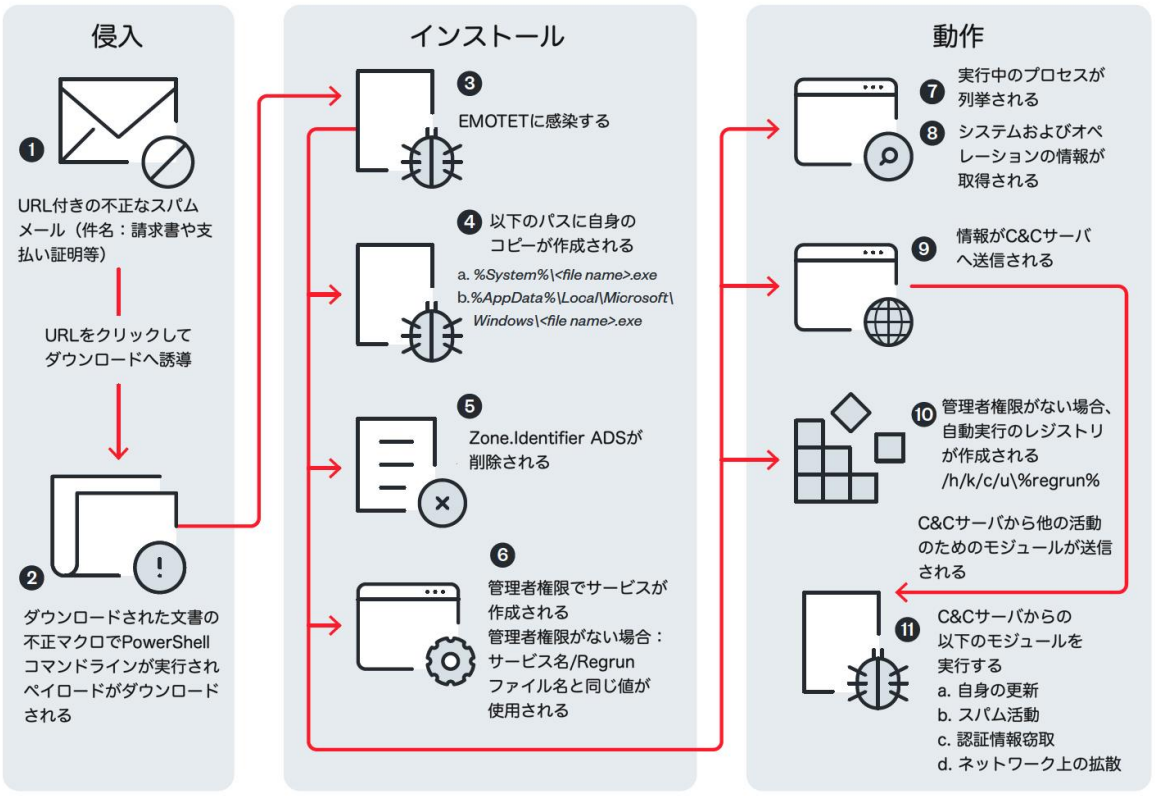

図 4：2022 年 5 月の解析で明らかになった EMOTET 感染フロー

EMOTET は 2014 年の登場以来、Conti や Ryuk といったマルウェアの攻撃に使用されてきたことが知られています。2021 年には、各国の法執行機関の協力により、そのインフラが閉鎖されました[41]。

しかし、インフラが解体されても EMOTET の活動が完全に終息したわけではありませんでした。それから 1 年も経たないうちに、Trickbot の攻撃キャンペーンで EMOTET の使用が

[40] https://resources.trendmicro.com/jp-docdownload-form-m426-web-prediction2022.html
[41] https://www.europol.europa.eu/media-press/newsroom/news/world%e2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

確認され、EMOTET は復活を遂げました[42]。2022 年上半期には、2021 年上半期と比較して EMOTET の検出台数が大幅に増加しました。これは、攻撃者が攻撃キャンペーンにボットネット型マルウェアの利用を選択した結果として復活したことを証明するものです。実際、セキュリティ機関 Advintel のリサーチャーは、EMOTET が最近復活した理由の 1 つとして、ランサムウェア Conti の攻撃キャンペーンを挙げています[43]。

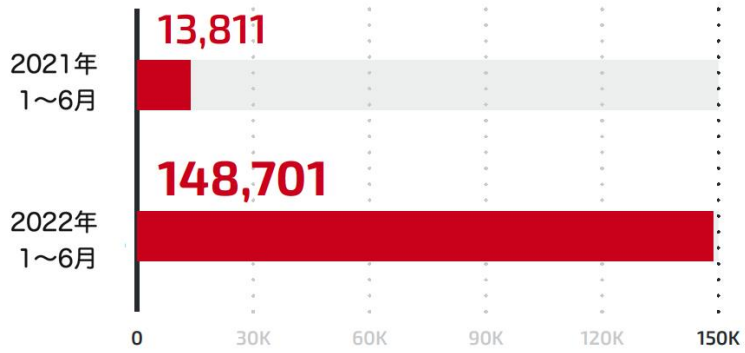

図 5：EMOTET の検出台数は 2022 年上半期に 2021 年上半期の 10 倍以上増加しており、攻撃活動で頻繁に利用されたことが推測される

SPN のデータによると、EMOTET の検出台数の大部分は日本からであり、米国、インド、イタリア、ブラジルと合わせて上位 5 位を占めています。この国別の検出台数は、各国のセンサー数の割合も異なるため単純には比較できませんが、それでもなお、日本国内で EMOTET の活動レベルが高いことは確かと言えます。

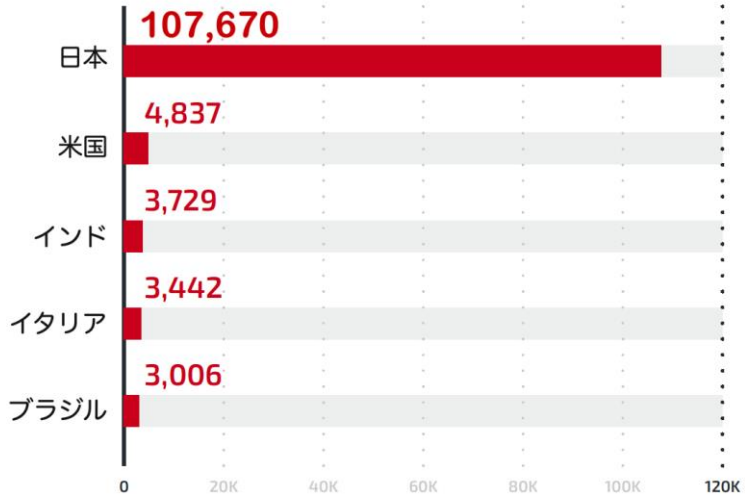

図 6：EMOTET の国別検出台数（2022 年 1~6 月）

[42] https://success.trendmicro.com/dcx/s/solution/1118391-malware-awareness-emotet-resurgence?language=en_US&

[43] https://www.advintel.io/post/corporate-loader-emotet-history-of-x-project-return-for-ransomware

2022 年 5 月、トレンドマイクロは、各地域の EMOTET 感染事例を調査しました。その結果、感染経路は依然スパム攻撃の手口に依存している中、ダウンロードの手順として VBA（Visual Basic for Applications）の代わりに Excel 4.0 のマクロを使用するなど、小さな変化が見られることを確認しました[44]。最近の EMOTET 感染事例でのその他の変更としては、合理化されたペイロードおよび難読化の手法も挙げられます。中でも特筆すべきは、ボットネット型マルウェアとしては初めて EMOTET の攻撃において Cobalt Strike が使用された点であり、これにより新たな EMOTET 関連の攻撃キャンペーンがより危険なものとなってきています。

ロシアとウクライナの対立がサイバー犯罪の領域にも拡大

2022 年 2 月 24 日、ロシアによるウクライナ侵攻が勃発し、地上での物理的な戦闘が注目される一方、その混乱の中で、双方を標的としたサイバー攻撃も行われたことは特筆に値します[45]。

早くからこうしたサイバー攻撃に関与していたのがランサムウェア Conti を駆使する攻撃グループであり、勃発後わずか 1 日でロシア政府への支援を表明していました。同グループは、自分たちのリークサイト上で、ロシアにサイバー攻撃を仕掛けたグループや個人に対して反撃すると発表しましたが、その後、後続の投稿でその姿勢を軟化させています。

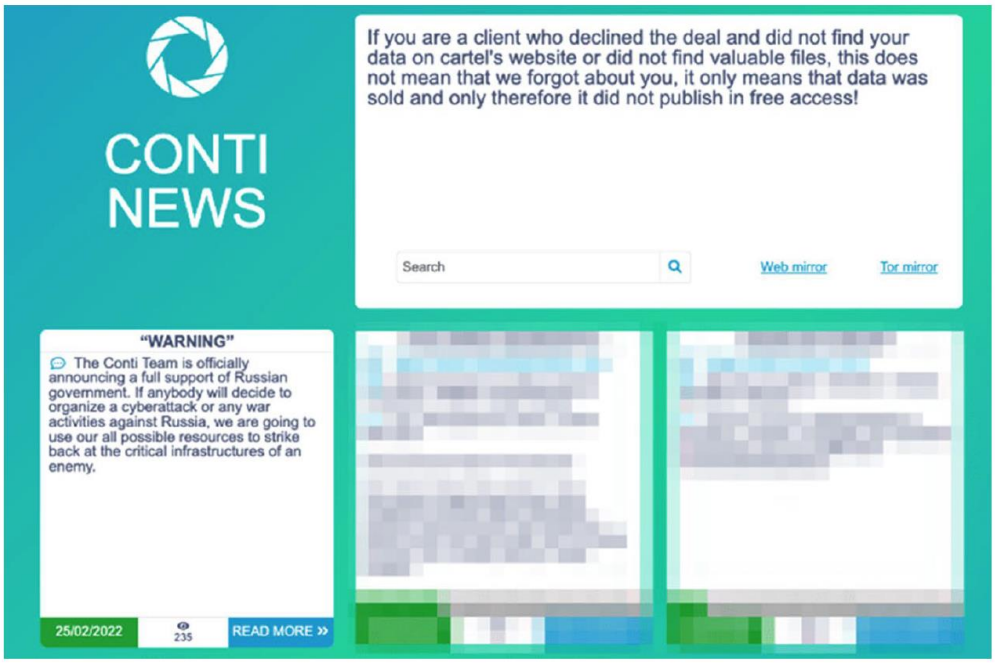

図 7：ロシアのインフラを標的としたサイバー攻撃への報復を警告する Conti の攻撃グループの最初の声明文

[44] https://www.trendmicro.com/en_us/research/22/e/bruised-but-not-broken--the-resurgence-of-the-emotet-botnet-malw.html

[45] https://www.trendmicro.com/en_us/research/22/c/cyberattacks-are-prominent-in-the-russia-ukraine-conflict.html

SPN のデータによると、2022 年上半期のマルウェア BazarLoader の検出数は、前年上半期と比較して急増しています。このマルウェアは、Conti の攻撃キャンペーンで重要な役割を果たしているため、注目すべき変化といえます。

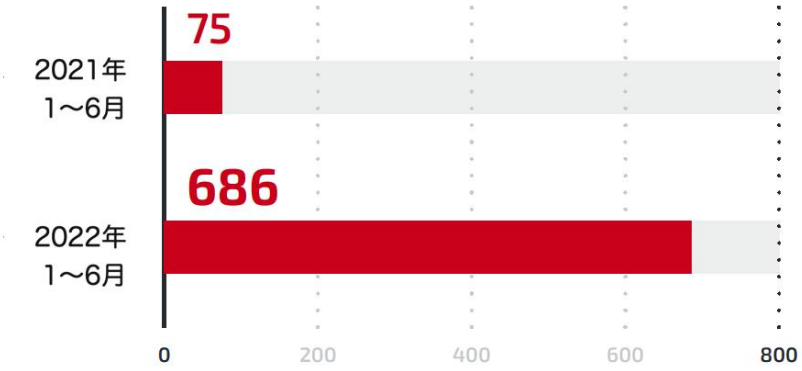

図 8：2022 年上半期における BazarLoader の検出台数は、2021 年上半期と比較して約 10 倍となっている

また、アラビア語を話すランサムウェア攻撃グループ「Stormous」は、ロシアへの支援を表明し[46]、その計画の一環としてウクライナの政府機関を標的にすることを宣言していました。Stormous が使用するランサムウェアをトレンドマイクロで解析したところ、同グループは、リモートアップロードや Pastebin などのリソースを通じて、さまざまな種類のカスタマイズされたペイロードを展開していることが分かりました。

これらランサムウェア攻撃グループの関与の他、複数のセキュリティリサーチャーは、進行中の対立とは直接関係しないものの、その前からウクライナの企業や組織、ウェブサイト、インフラに対して攻撃が行われていたことを確認しています。2022 年 1 月から 2 月にかけて、ウクライナのいくつかの標的に向けてスピアフィッシングメールが相次いで送信されていました。送信元としては表向き国民医療サービスや警察など、ウクライナの正規の組織を装っていましたが、実際は、マルウェア OutSteel および SaintBot をダウンロードして実行する添付ファイルが含まれていました[47]。これらの攻撃キャンペーンは、侵攻の前段階としての情報収集を目的に実施された可能性があります。また 2022 年 1 月 13 日と 14 日には、ウクライナ政府の約 70 のウェブサイトに対して直接攻撃が行使され、マルウェア WhisperGate を介してウェブサイトのコンテンツの改ざんやシステムの破損が引き起こされました[48]。これらの攻撃は、コンテンツ管理システム OctoberCMS、サプライチェーン攻撃、Log4j の脆弱性の悪用などによって実現されたと推測されています[49]。

[46] https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/stormous-the-pro-russian-clout-hungry-ransomware-gang-targets-the-us-and-ukraine/

[47] https://unit42.paloaltonetworks.com/ukraine-targeted-outsteel-saintbot/

[48] https://www.trendmicro.com/en_us/research/22/c/cyberattacks-are-prominent-in-the-russia-ukraine-conflict.html

[49] https://www.trendmicro.com/en_us/apache-log4j-vulnerability.html

一見すると、これらのサイバー攻撃は一方通行ではなく、ロシアとウクライナの双方に対して仕掛けられた点で事態の複雑さを物語っています。例えばトレンドマイクロが解析した 2022 年 3 月の攻撃キャンペーンでは、ロシアの標的を感染させるために設計されたマルウェア「RuRansom」が使用されていました。このマルウェアは、その名称に反して、実際はランサムウェアの一種ではなく、標的のデータやバックアップファイルを破壊するために設計されたワイパー型マルウェアの一種です。また、多数のバージョンが確認されており、このマルウェアがまだ開発中である可能性も示唆されています。

ロシア、ウクライナ双方への攻撃でランサムウェアを駆使する攻撃グループの関与が指摘されると共に、他のグループの関与も確認されています。例えば、ハクティビスト集団「アノニマス」は、ロシア中央銀行の機密ファイルの公開、国営テレビの乗っ取り、ロシア軍関係者の個人情報の流出など、ロシアの資産や情報を標的とした攻撃でサイバー紛争に参加していました[50]。

その他、どちらの側にも直接狙いを定めることなく、この状況に便乗しようとした活動も確認されていました。トレンドマイクロのハニーポットは、紛争に関連するスパムメールとして、寄付を求めるという名目でこの状況を利用し、偽の寄付先を作り出そうとした詐欺を行うケースを確認しています。これらのスパムメールの中には、添付ファイルとしてマルウェア「Ave Maria」などを感染させるものも含まれていました[51]。

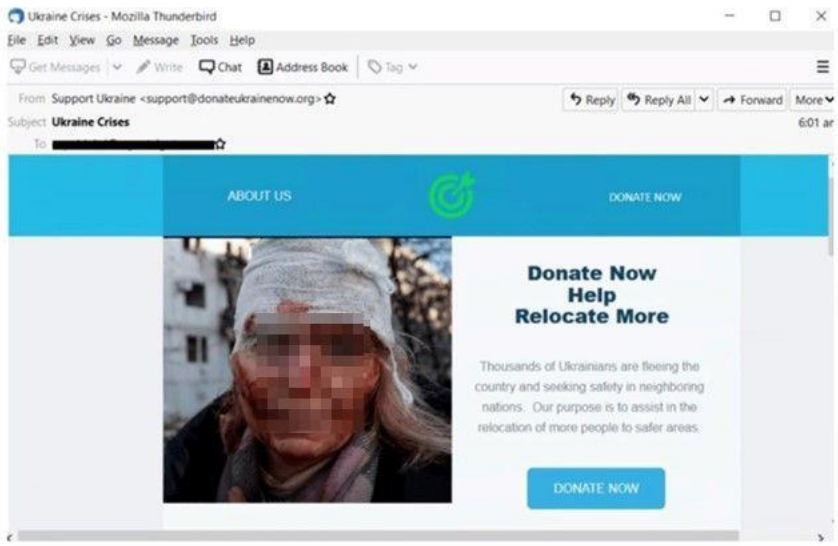

図 9：ウクライナ人の移住を支援するために寄付を募る詐欺メール

[50] https://fortune.com/2022/04/11/anonymous-cyber-war-russia-ukraine/

[51] https://www.trendmicro.com/en_us/research/19/j/autoit-compiled-negasteal-agent-tesla-ave-maria-delivered-via-malspam.html

「RaaS」と「多重脅迫」で進化するランサムウェア

収益性の高い RaaS を採用し続ける LockBit、Conti、BlackCat

RaaS の登場により、サイバー犯罪者は、専門性を持ち合わせていなくとも、本来であれば利用できなかったツールやインフラにもアクセスできるようになりました[52]。RaaS モデルのユニークな点の 1 つは、ランサムウェアの開発者と利用者双方の仲介役を務める事業者という関係です。この仲介により、RaaS の利用者は、ランサムウェア攻撃を実行する中、身代金の支払いで得た利益は、RaaS 事業者と決められた割合で山分けにします。このような仕組みにより、開発者は、ランサムウェア本体や攻撃で使用するツールを改良する時間を確保でき、なおかつセキュリティリサーチャーや法執行機関の追求からも比較的自由でいられます。一方、利用者側は、大規模なランサムウェアの攻撃キャンペーンを開始する際、大規模な開発やインフラ確保等の作業に煩わされることなくランサムウェア攻撃を実行し、利益を得ることができます。トレンドマイクロでは、ランサムウェアの攻撃者は現代的で洗練された手口を導入し、より著名な標的を狙うだろうと予測[53]していましたが、実際にランサムウェアの脅威は RaaS という仕組みにより深刻化しているものと言えます。

トレンドマイクロの調査では、2022 年上半期に 50 以上の攻撃グループが運営する暴露サイトを確認しました。これらの多くは RaaS モデルのランサムウェア攻撃に紐つくものでした。これらの暴露サイト上の主張によれば、1,200 以上の企業や組織がランサムウェアの被害に遭ったと考えられます。

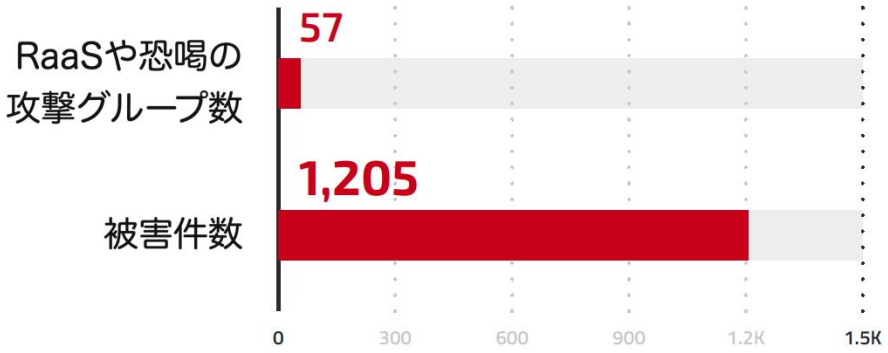

図 10：RaaS などに紐つく暴露サイトに掲載された被害組織の件数
（2022 年 1～6 月）

[52] https://www.trendmicro.com/vinfo/us/security/definition/ransomware-as-a-service-raas
[53] https://resources.trendmicro.com/jp-docdownload-form-m426-web-prediction2022.html

2022 年上半期、RaaS の活用では、LockBit、Conti、BlackCat が主要プレイヤーでした[54]。SPN データによると、同年上半期にこれらのマルウェアファミリーの検出数がそれぞれ急激に増加していることが確認されました。LockBit や Conti といった以前から活動しているランサムウェアの 2022 年上半期の検出数は、前年上半期と比較すると、LockBit は 5 倍以上、Conti は 2 倍近くになっています。BlackCat は、2021 年末に初めて報告された比較的新しいランサムウェアであるため、2021 年の検出台数はゼロでしたが 2021 年上半期には LockBit や Conti 同様、1000 件を超える検出を確認しました。

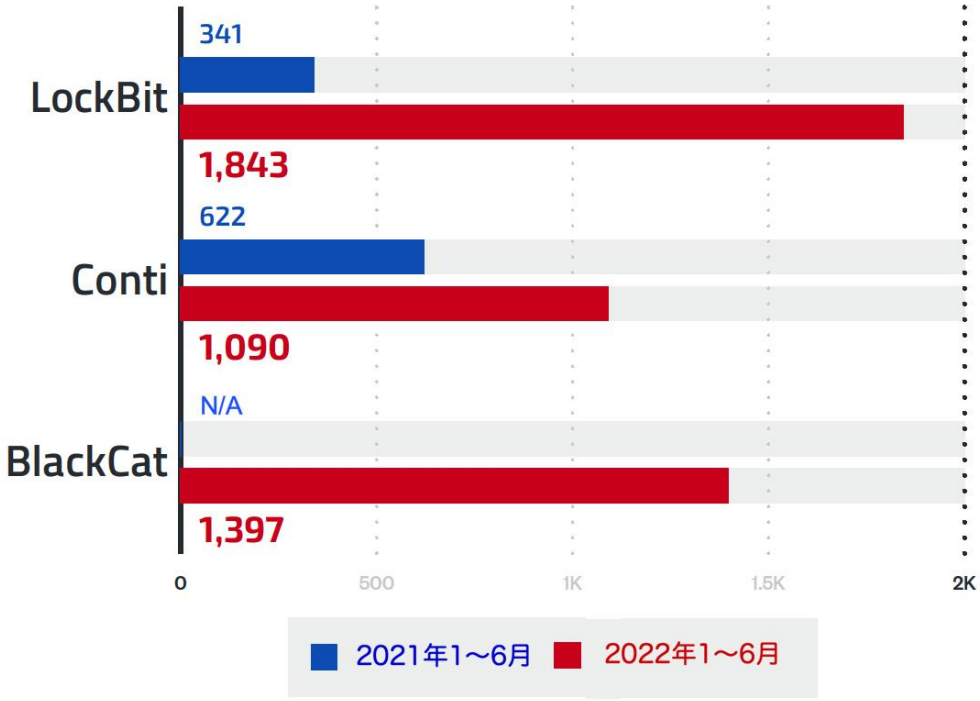

図 11：LockBit、Conti、BlackCat は、2022 年上半期の検出台数が軒並み 1000 件を超え、大幅に増加

LockBit：2019 年の活動開始当初は ABCD ランサムウェアとして知られていた LockBit は、2022 年には最も検出台数の多いランサムウェアファミリーとなりました[55]。2020 年、LockBit にリブランドすると共に RaaS のアフィリエイトプログラムを開始、その数ヶ月後には、ファイルの暗号化に加え、リークサイトを利用して窃取情報を暴露すると脅す二重恐喝の手口を利用し始めました。2021 年「LockBit 2.0」にモデルチェンジすると、このランサムウェアファミリーが関与するとされる最も著名な事例の 1 つである、アクセンチュア社への攻撃においてリークサイト上に同社の窃取情報を暴露しました[56]。
LockBit は、特に 2021 年のモデルチェンジ以降、最もよく知られたランサムウェアとなり

[54] https://www.trendmicro.com/vinfo/ph/security/news/ransomware-by-the-numbers/lockbit-conti-and-blackcat-lead-pack-amid-rise-in-active-raas-and-extortion-groups-ransomware-in-q1-2022
[55] https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-lockbit
[56] https://threatpost.com/accenture-lockbit-ransomware-attack/168594/

ました。攻撃グループは、常にその機能を進化させ、特に RaaS は、そのスピードと効率から同攻撃グループのセールスポイントの 1 つとなっています。また、LockBit が利用するネットワークは、その機能性と信頼性で人気を集めています。
LockBit の RaaS は、利用者の状況、目的、標的となるシステムへのアクセス方法に応じて、感染フローについて複数のオプションを提供しています。例えば、利用者がブルートフォース方式で仮想プライベートネットワーク（VPN）サーバへのアクセスを用いる場合、LockBit の RaaS は、リモートアクセスサービス（RAS）に基づいた感染フローを提供するという具合です。さらには、侵害された IIS の Web サーバにアクセスする利用者向けに PowerShell スクリプトを提供することもあります。その他、ファイル暗号化の動作に加えて、追加の認証情報を収集するポストエクスプロイトツール「Mimikatz」を導入しているケースも確認されています。

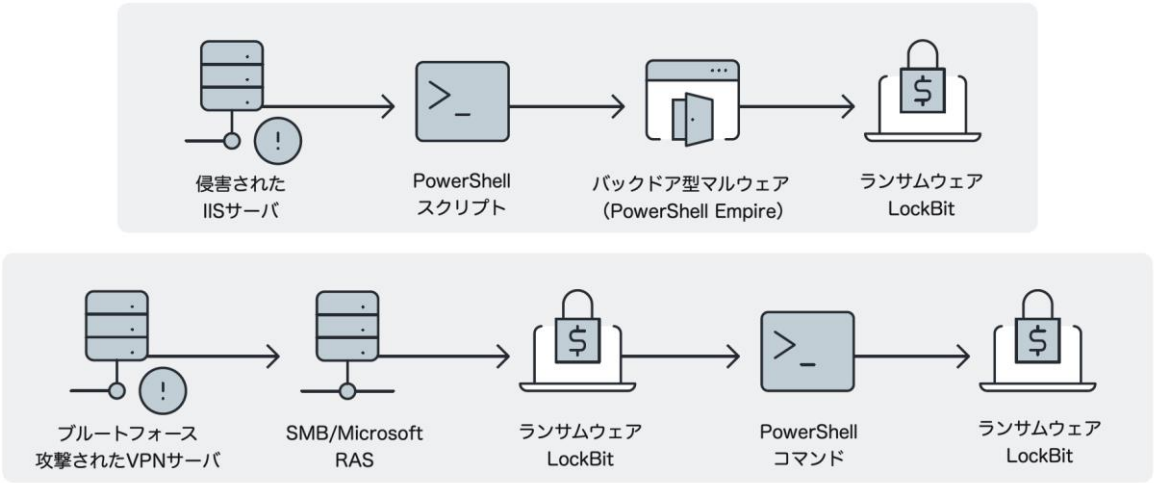

図 12：LockBit の攻撃で確認された 2 つの感染フロー：
1 つは IIS サーバの侵害に成功したケース、
もう 1 つはブルートフォース攻撃で VPN サーバの侵害に成功したケース

Conti ：悪名高いランサムウェア Ryuk の後継として注目されてきた Conti[57]は、2021 年 5 月に医療機関を狙った事例など、同年に多くの著名な攻撃を成功させ、本格的な普及を遂げました[58]。
最近の多くのランサムウェアファミリーと同様、Conti は、標的となるシステムに侵入するために複数の手法を採用しています。フィッシングメールは依然として一般的な侵入手法です。Conti の事例では、攻撃メール本文内の Google Drive のリンクを介してマルウェア BazarLoader を送り込まれ、最終的にランサムウェア感染に至った事例があります。ま

[57] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/addressing-threats-like-ryuk-via-trend-micro-xdr
[58] https://www.rnz.co.nz/news/national/442795/waikato-hospitals-hit-by-cyber-security-incident

た、FortiGate ファイアウォールに存在[59]した脆弱性 CVE-2018-13379[60]や CVE-2018-13374、または Microsoft Exchange の ProxyShell 脆弱性[61]など、様々な脆弱性を悪用して、標的ネットワークに侵入したケースもありました。

Conti の攻撃者は、端末内に侵入すると、Whoami、Nltest、Net などのツールを使用し、感染端末を介して得た権利や権限など、いくつかのシステム情報を収集します。同時に、二重恐喝のために暴露させる情報に関連したファイルを探索します。また、より大きな特権を得る必要があると判断した場合、Zerologon のような脆弱性[62]を悪用して特権昇格を行う可能性もあります。

2022 年 2 月、あるセキュリティリサーチャーが、Conti ランサムウェア攻撃グループのファイルや文書の一部を流出させ、同グループの規模やリーダーなどの情報を明らかにしました[63]。ここで特筆すべきは、明らかにされた情報の中には、管理者パネル、復号ツール、Conti Locker v2 など、Conti の攻撃者がコンポーネントやインフラに使用しているコードが含まれていたことです。

とはいえ、こうした情報の暴露は諸刃の剣ともなります。リサーチャーが Conti の活動を把握し、知見を深めることは有益ですが、他の攻撃者がこれら流出したソースコードを利用して、独自の新興ランサムウェアを構築することも可能だからです。

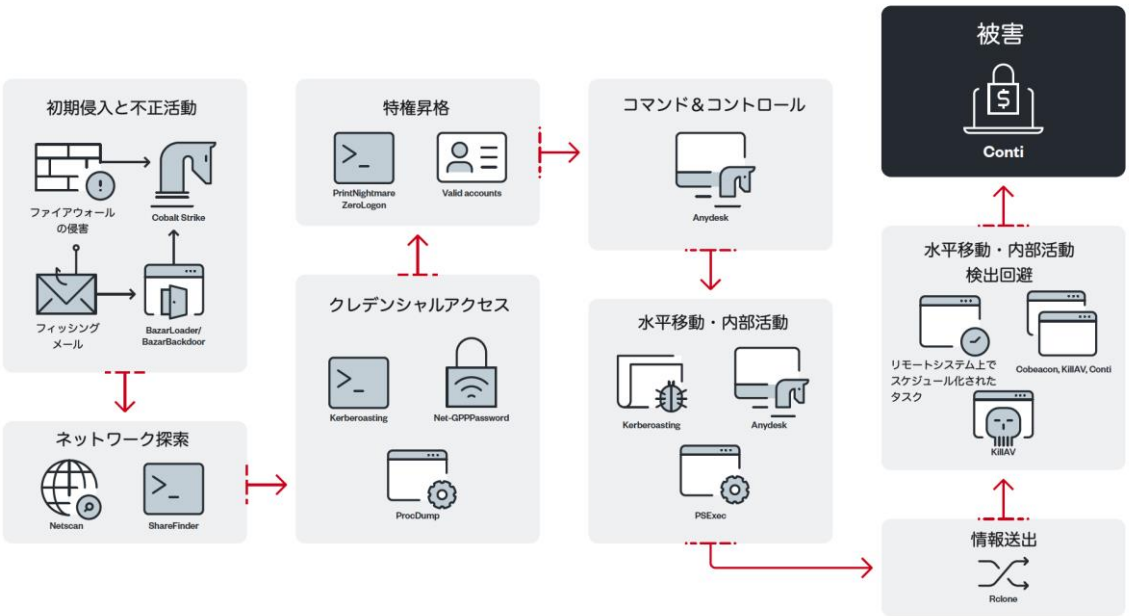

図 13：Conti 攻撃で使用される典型的な感染フロー

[59] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13379

[60] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13374

[61] https://www.bleepingcomputer.com/news/security/conti-ransomware-now-hacking-exchange-servers-with-proxyshell-exploits/

[62] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1472

[63] https://www.cnbc.com/2022/04/14/conti-ransomware-leak-shows-group-operates-like-normal-tech-company.html

BlackCat：LockBit や Conti に比べると比較的新しいランサムウェアである BlackCat（別名：alphv）ですが、最近のランサムウェア攻撃グループが使用する典型的な二重恐喝以外の手口も駆使し、数ヶ月間に渡って活動を広げることに成功しています。BlackCat は、ファイルを暗号化し、機密情報を暴露すると脅すだけでなく、攻撃グループの要求が満たされない場合は、被害者のインフラに分散型サービス妨害（DDoS）攻撃を仕掛けると警告する多重恐喝[64]の手口を採用していました[65]。

BlackCat の攻撃者は、通常、露出した脆弱なアプリケーションを悪用して、標的のシステムに侵入します。そして、Cobalt Strike のようなサードパーティのフレームワークやツールセットを使用してランサムウェアを拡散させます。

2022 年 4 月、トレンドマイクロでは「Trend Micro Vision One™」プラットフォームを通じて BlackCat の調査を開始し、その動作に関する情報を収集しました。その結果、攻撃者が Microsoft Exchange Server の脆弱性 CVE-2021-31207[66]を積極的に悪用して、被害者のサーバに Web シェルを挿入してリモートアクセスを行っていることがわかりました。これにより、攻撃者は、情報窃取や不正ツールの投下など、さまざまな作業をリモートで実行できるようになります。攻撃者は、これらのツールを使用して、標的のシステム内で水平移動・内部活動を行ない、システム環境をスキャンし、最終的に BlackCat に感染させる準備をします。

BlackCat は、並行処理機能を持つ安全なプログラミング言語 Rust で書かれた初の本格的なランサムウェアファミリーであり、また、独自のマネタイズ手法、広範なインフラ、攻撃における幅広い補助ツールなどにより、今後、RaaS 利用の攻撃活動での定番となる可能性を秘めていると言えます。

これらのランサムウェアファミリーは、トレンドマイクロのデータおよび彼らのリークサイトで主張している情報から、主に従業員 200 人までの小規模企業や従業員 1000 人までの中規模企業での被害が多いことが判明しています。このような企業ではサイバー攻撃に適切に対処するためのリソースや従業員数が少なく、より規模の大きい企業と比べて相対的にセキュリティに弱点を抱えている可能性が多いことが、攻撃の標的となりやすい理由と推測されます[67]。

---

[64] https://securityaffairs.co/wordpress/125459/cyber-crime/blackcat-ransomware.html

[65] https://unit42.paloaltonetworks.com/blackcat-ransomware/

[66] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31207

[67] https://www.trendmicro.com/vinfo/ph/security/news/ransomware-by-the-numbers/lockbit-conti-and-blackcat-lead-pack-amid-rise-in-active-raas-and-extortion-groups-ransomware-in-q1-2022

ランサムウェアの主要な標的となる Linux システム

Linux システムはその使用範囲が広がるにつれ、攻撃者にとって魅力的な標的となってきています。特に今後数年間で Linux の成長が見込まれるサーバや組み込みシステムなど、特定の種類のインフラでの攻撃が拡大する可能性があります[68]。「2022 年セキュリティ脅威予測」[69]でも、ランサムウェア攻撃が Linux 使用のサーバ、サーバコンポーネント、それらの関連サービスをターゲットとして拡大する可能性を示唆しました。

2021 年上半期と比較すると、2022 年上半期は、Linux ベースの端末を標的としたランサムウェア攻撃は 75%増加しており、攻撃者がより多くの努力を Linux に注ぐとした予測がより現実のものとなっています。

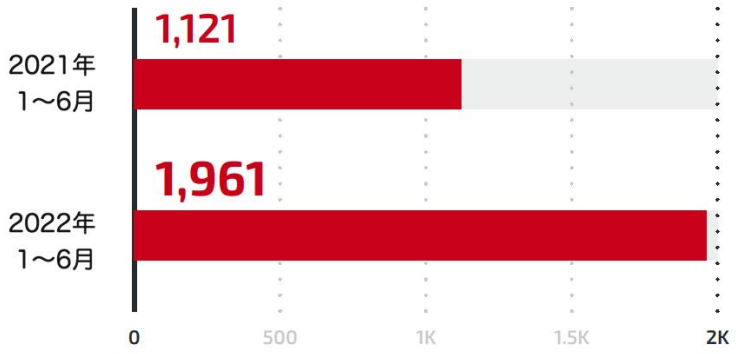

図 14：Linux 向けランサムウェアの検出台数は、2021 年上半期と比較して 2022 年上半期は大幅に増加した

2022 年上半期、VMware のハイパーバイザーESXi は激しい攻撃にさらされました。ただしサイバー犯罪者が ESXi を標的にすることは新しいことはありません。例えば、RansomEXX [70]は、少なくとも 2021 年[71]から ESXi の脆弱性を悪用した攻撃キャンペーンを行っています。そして、他の攻撃者もこれに追随しているようです。

2021 年 10 月、LockBit の攻撃グループは、Linux 向けランサムウェアの亜種「LockBit Linux-ESXi Locker version 1.0」をアンダーグラウンドのフォーラムで発表しました。この亜種は、Advanced Encryption Standard（AES）と楕円曲線暗号（ECC）のアルゴリズムを組み合わせてデータを暗号化し、ESXi サーバをターゲットにしています。以降、この亜種は野放し状態となっています。

[68] https://www.fortunebusinessinsights.com/linux-operating-system-market-103037
[69] https://resources.trendmicro.com/jp-docdownload-form-m426-web-prediction2022.html
[70] https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-ransomexx
[71] https://www.kaspersky.com/blog/ransomware-in-virtual-environment/39150/

2022 年 5 月には、Cheerscrypt と名付けられた新しいランサムウェアの亜種が、ESXi を使用する機器を標的としていることも確認されています[72]。この亜種は、2021 年 9 月に流出した Babuk ランサムウェアのソースコード[73]に基づき、二重恐喝の手法でログファイルやその他の VMware 関連ファイルを暗号化します。

LockBit Linux-ESXi Locker version 1.0 および Cheerscrypt の双方とも、他の多くのランサムウェア攻撃で行われている二重恐喝の手口を用いています。そして ESXi サーバがサーバ仮想化のために企業で広く使用されている点も、感染被害の潜在的影響として注意すべきでしょう。ESXi サーバは、サーバの仮想化に広く利用されており、重要なデータを保存する複数の仮想マシン（VM）をホストするために利用されることもあります。このように、ESXi サーバは、企業や組織の重要なインフラの一部であることが多く、これらのコンポーネントへの攻撃が成功すると、大きな損害につながる恐れがあります。

Black Basta や Nokoyawa など世界各地の企業を襲うランサムウェアファミリー

ランサムウェアは、多額の身代金を支払う能力を持つ企業に狙いを定めています。そうした中、ランサムウェア Black Basta[74]の攻撃者は、2022 年初めの数カ月の間に 50 近くの企業や組織を襲って猛烈な勢いで攻撃しています[75]。このランサムウェアファミリーの名称は、2022 年 4 月に Black Basta と名乗るユーザが、米国、カナダ、英国、オーストラリア、ニュージーランドの企業ネットワークへのアクセス認証情報を探していると、いくつかの大手アンダーグラウンドフォーラムに投稿したことが発端となっています。また、このユーザは、潜在的なパートナーにはランサムウェア攻撃で得た利益の一部を提供するとも述べています。

現状、これら攻撃者の活動範囲や体制に関する情報は限られています。しかし、Black Basta の最初の広告を見ると、この攻撃グループは窃取した認証情報を使って被害者のシステムにアクセスしている可能性が推測されます。そして、初めに vssadmin.exe を使用してシャドウコピーを削除し、デバイスをセーフモードで起動した後、暗号化を実行します。その後、Fax というサービスを削除し、自身のパスを介して新しいサービスを作成してレジストリに追加し、活動の永続化を図ります。そして最後に、侵害したサービスを使用してファイルを暗号化するため、感染端末をネットワーク有効のセーフモードの状態でシャットダウンしてリブートします。Black Basta の顕著な特徴の 1 つは、身代金要求の動作が自

[72] https://www.trendmicro.com/en_us/research/22/e/new-linux-based-ransomware-cheerscrypt-targets-exsi-devices.html
[73] https://www.bleepingcomputer.com/news/security/babuk-ransomwares-full-source-code-leaked-on-hacker-forum/
[74] https://www.trendmicro.com/en_us/research/22/e/examining-the-black-basta-ransomwares-infection-routine.html
[75] https://www.cybereason.com/blog/cybereason-vs.-black-basta-ransomware

身にハードコードされていることです。この点から、攻撃者は、それぞれの標的に固有のバイナリを使用している可能性も推測されます。

図 15：%temp%フォルダに作成した.jpg ファイルを使って表示される Black Basta ランサムウェアの壁紙

また、何人かのセキュリティリサーチャーは、Black Basta と他のランサムウェアや APT グループとの関連性も指摘しています。セキュリティ機関「MalwareHunterTeam」のツイートでは、Black Basta と Conti の間に多くの類似点があることが述べられており[76]、トレンドマイクロのリサーチャーも、Black Basta と QakBot の間に相関関係を見つけることに成功しました[77]。

2021 年下半期、ランサムウェア「Hive」が米国のヘルスケア分野への攻撃を開始し、ランサムウェアの運用開始から 100 日間で 300 以上の企業や組織が被害に遭ったとする報告もありました[78]。そして 2022 年には、Hive といくつかの類似性を持つランサムウェア「Nokoyawa」が確認されました[79]。例えば、これらのランサムウェアファミリーは、攻撃の開始段階で Cobalt Strike を使用し、防御回避作戦の一環としてアンチルートキットスキャナーGMER や PC Hunter などのツールを統合するなど、共通のツールやテクニックを有しています。

他方、Hive と Nokoyawa は、特にコード（バイナリのコンパイルの使用言語）やパッキング方法において異なる特徴も持っています。Hive は UPX でパッキングされる一方、Nokoyawa はパケットを一切使用しないといった差異です。

なお、Nokoyawa のターゲットは、アルゼンチンを中心とした南米地域で多く確認されました。

[76] https://twitter.com/malwrhunterteam/status/1519301421958578177

[77] https://www.trendmicro.com/en_us/research/22/e/examining-the-black-basta-ransomwares-infection-routine.html

[78] https://www.hhs.gov/sites/default/files/hive-ransomware-analyst-note-tlpwhite.pdf

[79] https://www.trendmicro.com/en_us/research/22/c/nokoyawa-ransomware-possibly-related-to-hive-.html

企業の業務に影響するソフトウェアの脆弱性

2022 年上半期に深刻度の高い脆弱性の件数が増加

2022 年上半期、CVE.org が公表した脆弱性の件数は大幅に増加しました。2021 年上半期に公表された 9,420 件から大幅に増加し、12,380 件となりました[80]。トレンドマイクロが運営する ZDI プログラムによる脆弱性の公開件数も同様の傾向を示し、2021 年上半期の 770 件から約 23%増加し、944 件の脆弱性関連アドバイザリが公開されています。

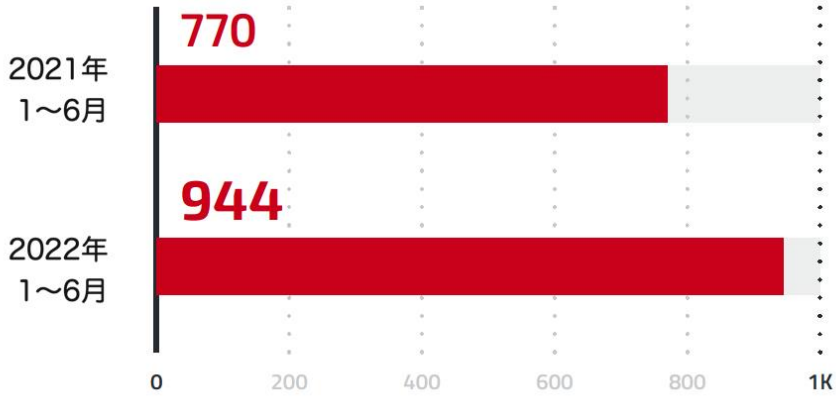

図 16：2022 年上半期の脆弱性アドバイザリ件数は前年同期比で約 23%増加している

公表された脆弱性のうち、深刻度が高い脆弱性が 68%と最も多くなっています。「緊急」および「重要」ともに大きく増加し、「警告」だけが 2021 年同時期より減少を示していました。

このような傾向を踏まえ、企業は、自社の環境に影響を及ぼす脆弱性に着目し、米国サイバーセキュリティインフラストラクチャセキュリティ局（CISA）による「Known Exploited Vulnerabilities Catalog」[81]などのリソースを利用して、これらの脆弱性が概念実証されているかどうか、実際に悪用されているかどうかを検証し、リスクベースのアプローチを効率的に採用することをお勧めします。

通信アプリケーションの構築に使用されるオープンソースソフトウェア「Asterisk」の一部バージョンに影響し、悪用されるとシェルコマンドの注入が可能となる脆弱性「CVE-2017-14100」[82]は、トレンドマイクロ™ TippingPoint® Threat Protection System センサーに基づく 2022 年上半期の悪用の検出数が最も多くなっています。次いで OpenSSL のメモリリークの脆弱性「CVE-2014-3567」、IIS の Web サーバのフォルダトラバーサルの脆弱

[80] https://www.cve.org/About/Metrics#PublishedCVERecords

[81] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

[82] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14100

性「CVE-2000-0884」が、それぞれ 900 万件以上、400 万件以上の検出数を記録しています。今年上半期に最も悪用された脆弱性の中にこれら古い脆弱性（検出数が数百万に及ぶケースもある）が含まれていることは、多くの企業や組織が依然としてソフトウェアの重要な更新を実施することが困難であることの証拠でもあると言えます。さらに悪いことには、多くの企業や組織がいまだにこれらの更新を完全に無視している可能性もあります。

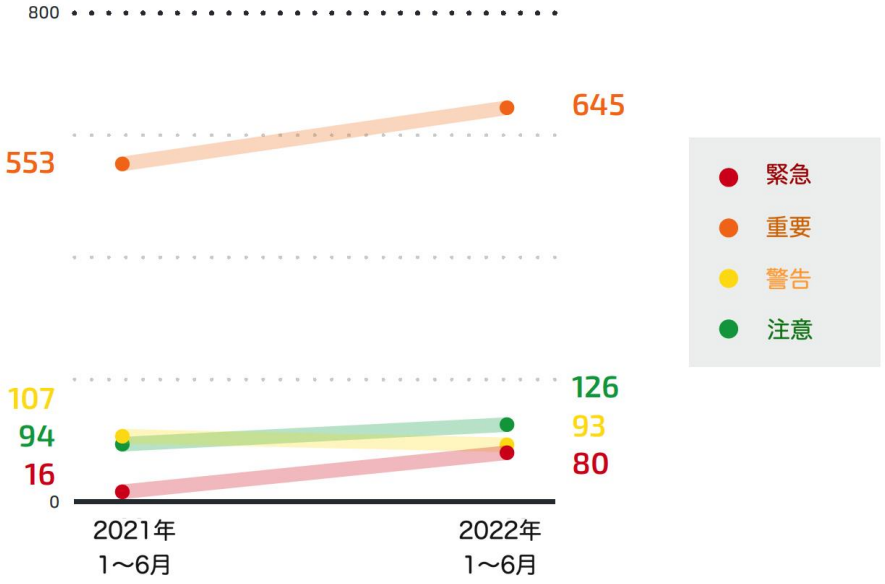

図 17：2021 年上半期と 2022 年上半期に公表された脆弱性の CVSS に基づく深刻度別内訳
2022 年前半、深刻度が「緊急」「重要」「注意」の深度脆弱性が増加し、「警告」はやや減少した

ルール ID	CVE番号	ヒット数	影響を受けた製品
29739	CVE-2017-14100	15,200,809	Asterisk 11.x before 11.25.2, 13.x before 13.17.1, and 14.x before 14.6.1 and Certified Asterisk 11.x before 11.6-cert17, and 13.x before 13.13-cert5
17056	CVE-2014-3567	9,107,139	OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j
1095	CVE-2000-0884	4,447,190	IIS 4.0 and 5.0
3886	CVE-2010-0817	2,597,362	Microsoft SharePoint Server 2007 12.0.0.6421 and possibly earlier and SharePoint Services 3.0 SP1 and SP2.
	CVE-2011-1264		Microsoft Windows Server 2003 SP2 and Server 2008 Gold, SP2, R2, and R2 SP1
40693	CVE-2021-35394	1,166,969	Realtek Jungle SDK version v2.x up to v3.4.14B
2023	CVE-2005-1380	711,159	BEA Admin Console 8.1
	CVE-2010-0817		Microsoft SharePoint Server 2007 12.0.0.6421 and possibly earlier and SharePoint Services 3.0 SP1 and SP2
	CVE-2010-3936		Microsoft Forefront Unified Access Gateway (UAG) 2010 Gold, 2010 Update 1, and 2010 Update 2
	CVE-2017-0068		Microsoft Edge
10146	CVE-2010-2861	648,690	Adobe ColdFusion 9.0.1 and earlier
	CVE-2013-3336		Adobe ColdFusion 9.0, 9.0.1, 9.0.2, and 10
31852	CVE-2014-0224	597,386	OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
6161	CVE-2008-1451	580,030	Microsoft Windows 2000 SP4 and Server 2003 SP1 and SP2
31936	CVE-2018-10562	518,502	Dasan GPON home routers

表 1：2022 年上半期の脆弱性検出数上位一覧

一方、Microsoft Windows Support Diagnostic Tool（MSDT）に影響を及ぼすリモートコード実行（RCE）脆弱性「CVE-2022-30190（別名 Follina）」[83]は、欧州諸国や米国の著名な企業を狙った攻撃に使用されていると報告されています[84]。その後、マイクロソフトは、2022年6月のセキュリティアップデートでこの脆弱性への修正パッチを適用しています[85]。

重要なビジネスツールやソフトウェアに影響を及ぼす主な脆弱性

重要なソフトウェア、ツール、コンポーネントに関わる脆弱性は、その影響範囲の広さから、最も危険なタイプの脅威といえます。さらに、トレンドマイクロ Vision One のデータによると、このサービスで把握している全企業の約 85%において、悪用されやすい脆弱性を検出したことが判明しています。

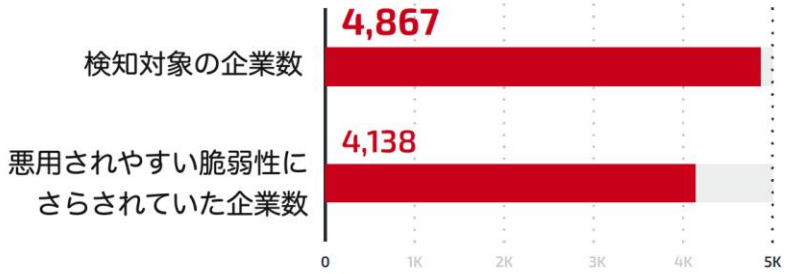

図 18：2022 年 8 月第 1 週に Vision One の検出機能を有効化していた企業 4,867 社のうち 4,138 社（85%）において悪用されやすい脆弱性の検出を確認

2021 年には、Java ベースのログ記録ライブラリである Apache Log4j が影響を受ける脆弱性「CVE-2021-44228（別名：Log4Shell）」[86]が登場しました。この脆弱性は、影響を受けるソフトウェアの広範囲に及び、異なるシステムとも統合しており、企業や組織で影響範囲を判断することが困難であったため、サイバーセキュリティの状況を揺るがすものとなりました[87]。2022 年上半期には、重要な企業向けソフトウェアに影響を与える脆弱性が増加しており、その中で最も注目すべきものとして Spring4Shell があげられます。

2022 年 3 月 31 日、企業向けアプリケーションとして広く使われているオープンソースの Java フレームワーク Spring Framework の制作者は、多くの依存関係に影響を及ぼす重大なゼロデイ脆弱性（Log4Shell と類似しているため Spring4Shell と俗称される）CVE-2022-22965[88]に関する情報を公開しました。このアプリケーションの依存関係は、Spring

[83] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30190
[84] https://techcrunch.com/2022/06/01/china-backed-hackers-are-exploiting-unpatched-microsoft-zero-day/
[85] https://www.zerodayinitiative.com/blog/2022/6/14/the-june-2022-security-update-review
[86] https://www.trendmicro.com/en_us/apache-log4j-vulnerability.html
[87] https://www.wired.com/story/log4j-log4shell-vulnerability-ransomware-second-wave/
[88] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22965

Framework 5.2.20 および 5.3.18 以前のバージョン、さらに Java Development Kit (JDK) 9 以降で動作するセットアップに及びます。

脆弱性 Spring4Shell は、通常、特殊なオブジェクトやクラスが特定の条件下で公開されている場合に発生します。このため、オブジェクトに直接アクセスしたい攻撃者は、リクエストにクラス変数を指定することで目的のアプリケーションにアクセスできます。また、クラスオブジェクトを介してオブジェクトの子プロパティにアクセスすることで、攻撃者は、プロパティの連鎖を辿って、システム内の重要なオブジェクトへのアクセスが可能になります[89]。

2022 年 4 月の時点で、Spring4Shell が実際の攻撃で悪用されたことが確認されています。確認された攻撃の 1 つは、脆弱性を悪用することで、暗号資産をマイニングするマルウェアを展開するものでした。この場合、攻撃者はまず、文字列チェックを用いて標的となる端末のオペレーティングシステムを判断します。オペレーティングシステムが特定されると、暗号化されたペイロード（復号されると Spring4Shell の Web シェルになる）が実行、その後に PowerShell コマンドも実行されます。このコマンドにより、感染端末上にコインマイナーをダウンロードして実行するように設計されたスクリプトが取得されます[90]。「2022 年セキュリティ脅威予測」[91]で我々は、攻撃者は極めて短期間に脆弱性を武器化するようになることを指摘していましたが、Spring4Shell の悪用はまさにその指摘の通りの状況と言えました。

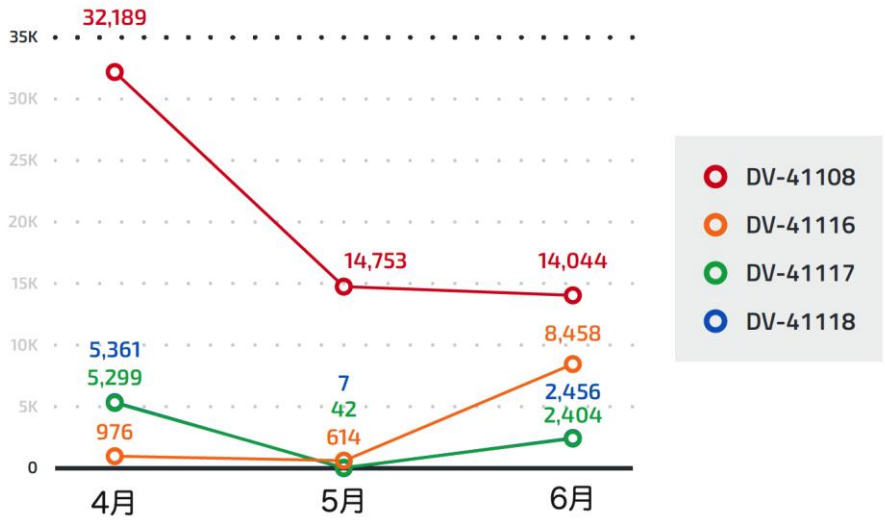

図 19：Spring4Shell 関連脆弱性悪用通信の検出数推移（全世界）
2022 年 3 月 31 日に Spring4Shell が確認された直後の 4 月に検出数がピークに

[89] https://www.trendmicro.com/en_ph/research/22/d/cve-2022-22965-analyzing-the-exploitation-of-spring4shell-vulner.html

[90] https://www.trendmicro.com/en_us/research/22/d/spring4shell-exploited-to-deploy-cryptocurrency-miners.html

[91] https://resources.trendmicro.com/jp-docdownload-form-m426-web-prediction2022.html

2022 年 2 月、トレンドマイクロが運営する脆弱性発見コミュニティ ZDI は、Linux および Unix 向けの Windows 標準相互運用プログラム群である Samba に存在する脆弱性 CVE-2021-44142 [92]、特に 4.13.17 以前の Samba のバージョン[93]について詳述したブログ記事を公開しました。CVE-2021-44142 は、Samba サーバーデーモン（smbd）において、ファイルを開く際の EA メタデータの解析に存在します。この脆弱性を悪用されると、認証なしでもルート権限でコードが実行される可能性があります。

セキュリティイベント「Pwn2Own Austin 2021」で Samba ソフトウェアに存在する境界外（OOB）脆弱性の初期バージョンが公開された後、ZDI ではさらに調査を進め、この脆弱性のさらなる亜種を発見し、Samba の開発者に報告しました。その後、2022 年 1 月 31 日に CVE-2021-44142 などの脆弱性に対応した修正パッチがリリースされました[94]。Samba は、ほぼすべての Linux ディストリビューションに標準搭載されているシステムサービスとして広く利用されています。そのため、CVE-2021-44142 への修正パッチの適用は、Linux や Unix ベースのシステムを使用する企業や組織にとって必須となります。

Trend Micro Deep Security のデータから顧客環境に関するいくつかの重要な知見が明らかになりました。脆弱性 Log4j（CVE-2021-44228 [95]と CVE-2021-45046 [96]）は、2022 年上半期に高い活動レベルを示し、DS によって検出およびフィルタリングされた合計イベント数は 50 億を超えました。CVE-2017-14495 [97]は、主に dnsmasq へ影響を与える脆弱性です。dnsmasq は、DNS、DHCP（Dynamic Host Configuration Protocol）、TFTP（Trivial File Transfer Protocol）サーバとして構成できるフリーソフトウェアです。このソフトウェアから検出されたイベント数が最も多く、ルータや IoT ゲートウェイでの普及状況からもこの数値は当然ともいえるでしょう[98]。

これらの脆弱性に関連するイベントが数多く検出された状況は、広く普及して必要不可欠なソフトウェアに影響を及ぼす脆弱性は攻撃者によって悪用される人気の選択肢であり続ける。というトレンドマイクロの予測をさらに裏付けるものといえます。

---

[92] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44142

[93] https://www.zerodayinitiative.com/blog/2022/2/1/cve-2021-44142-details-on-a-samba-code-execution-bug-demonstrated-at-pwn2own-austin

[94] https://www.samba.org/samba/history/security.html

[95] https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2021-44228

[96] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45046

[97] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14495

[98] https://www.trendmicro.com/en_ph/research/17/j/dnsmasq-reality-check-remediation-practices.html

検出関連CVE番号	脆弱性対象ソフトウェア	検出製品	検出されたイベント数
CVE-2017-14495	Dnsmasq	Deep Security	114,995,958,044
CVE-2006-4154	Apache HTTP Server	Deep Security	5,665,473,527
CVE-2021-44228	Apache Log4j	Deep Security	4,794,466,414
CVE-2009-2524	Microsoft Windows （LSASS）	Apex One	995,700,958
CVE-2010-2730	Microsoft Internet Information Services (IIS)	Deep Security	967,669,441
CVE-2021-29441	Nacos	Deep Security	846,824,548
CVE-2014-0098	Apache HTTP Server	Deep Security	417,996,287
CVE-2022-26134	Atlassian Confluence ServerおよびData Center	Deep Security	381,361,877
CVE-2017-8543	Microsoft Windows （Search handles objects）	Apex One	266,267,487
CVE-2017-11815	Microsoft Windows （SMB）	Apex One	188,900,588

表 2：2022 年上半期の脆弱性関連イベントの検出数
（Trend Micro Deep Security および Trend Micro Apex One のデータに基づく）

DDS 規格を脅かす新たな脆弱性が発見される

DDS（Data Distribution Service）規格は、IIoT（Industrial Internet of Things）の安全なリアルタイム情報交換、モジュラーアプリケーション開発、迅速な統合を可能にする接続規格として機能するミドルウェア技術の一例です[99]。DDS は、交通、ロボット、通信、ヘルスケア、防衛などの分野で、センサー、コントローラー、アクチュエーター間の信頼性の高い通信層を実装するために使用されており、一般に広く知られていないにもかかわらず、重要なミドルウェア技術の一種となっています。

ソフトウェアサプライチェーンにおける DDS の重要性に加え、サプライチェーンの最初に位置するため、状況を把握しづらい点も特筆されます。その結果、攻撃者は、DDS を魅力的なターゲットと見なすことになります。また、システムのセキュリティ上重要な構成要素として機能しているため、その中の 1 つの脆弱性が悪用されると、ソフトウェアスタックの残りの部分に影響を残す可能性があります。

2022 年 1 月、トレンドマイクロリサーチ、TXOne Networks、ZDI は、ADLINK Labs、Alias Robotics と共同で、サイバーセキュリティの観点から DDS を論じたリサーチペーパーを発表しました。このリサーチペーパーには、最も一般的な 6 つの DDS 実装に対する 13 の新たな脆弱性についての情報が含まれています[100]。これらの新たな脆弱性は、DDS をミドルウェアとして使用するロボティクスおよびオートメーション用のデフォルトの OS である Robot Operating System 2（ROS 2）にも影響するため、それぞれの脆弱性の影響は DDS そのものだけでなく、それ以上の範囲に及ぶ可能性があります。

[99] https://www.rti.com/products/dds-standard#:~:text=DDS%3A%20An%20Open%20Standard%20for,meet%20real-time%20system%20requirements

[100] https://documents.trendmicro.com/assets/white_papers/wp-a-security-analysis-of-the-data-distribution-service-dds-protocol.pdf

ATT&CK ICS	攻撃対象領域	攻撃経路	CVE	適用範囲	CVSS	共通脆弱性タイプ（CWE）
T0804 – ブルートフォースI/O T0814 – DoS T0827 – 制御喪失 T0880 – 安全性喪失 T0802 –収集自動化 T0846 – リモートシステムの探索 T0856 – レポートメッセージのスプーフィング	ネットワーク	RTPSディスカバリパケット	CVE-2021-38425*	Fast-DDS, ROS 2	7.5	CWE-406 – ネットワーク増幅
			CVE-2021-38429*	OpenDDS, ROS 2	7.5	
			CVE-2021-38487*	Connext DDS, ROS 2	7.5	
			CVE-2021-43547*	CoreDX DDS, ROS 2	7.5	
		不正RTPSパケット	CVE-2021-38447	OpenDDS, ROS 2	8.6	CWE-405 – ネットワーク増幅
			CVE-2021-38445	OpenDDS, ROS 2	7.0	CWE-130 –不適切な長さ処理
			CVE-2021-38423	GurumDDS, ROS 2	8.6	CWE-131 – 不正確なバッファサイズ計算
			CVE-2021-38435	Connext DDS, ROS 2	8.6	
			CVE-2021-38439	GurumDDS, ROS 2	8.6	CWE-122 – ヒープベースバッファオーバーフロー
T0862 – サプライチェーン侵害 T0839 – モジュールファームウェア T0873 – プロジェクトファイルの感染	設定	XMLファイル	CVE-2021-38427	Connext DDS, ROS 2	6.6	CWE-121 – スタックベースバッファオーバーフロー
			CVE-2021-38433	Connext DDS, ROS 2	6.6	
			CVE-2021-38443	CycloneDDS, ROS 2	6.6	CWE-228 –無効な構文構造の不適切な処理
			CVE-2021-38441	CycloneDDS, ROS 2	6.6	CWE-123 – 任意の場所に任意の内容の書き込みが可能な状態

図 20：新たな DDS の脆弱性 13 件の概要
（トレンドマイクロリサーチ、TXOne Networks、ZDI、ADLINK Labs、Alias Robotics が共同で発見）

DDS の脆弱性は、ネットワークレベルに影響するものと、コンフィギュレーション（環境設定）レベルに影響するものとに分けられます。前者はサービス妨害（DoS）攻撃、スプーフィング、自動の情報収集などさまざまな不正な手法に利用され、後者は DDS のシステム開発者やインテグレーターをターゲットにした攻撃で利用される可能性があります。

実際の攻撃がどのように行われるかを検証するため、リサーチャーは、Gazebo シミュレーターの物理エンジンを使って実世界のシナリオを模倣した環境を作り出しました。この設定により、自律走行プラットフォームへの攻撃をシミュレートし、攻撃者が CVE-2021-38447 [101]および CVE-2021-38445 を悪用できるようなシナリオ[102]を作成することができました。悪用された場合、ROS 2 ノードはクラッシュするか、攻撃者がシステム内で任意のコードを実行できるようになります。

CVE番号	詳細	スコープ	CVSS	根本原因
CVE-2021-38447	3.18.1 以前の OCI OpenDDS は、関連データの実際の長さと一致する長さパラメータを処理できないため、攻撃者はリモートで任意のコードを実行できる	OpenDDS, ROS 2	8.6	リソース枯渇
CVE-2021-38445	3.18.1 以前の OCI OpenDDS は、関連データの実際の長さと一致する長さパラメータを処理できないため、攻撃者はリモートで任意のコードを実行できる	OpenDDS, ROS 2	7.0	アサーションエラー

図 21：CVE-2021-38447 と CVE-2021-38445 を悪用し、
自律走行プラットフォームへの攻撃を開始する方法の概要

[101] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38447#:~:text=OCI%20OpenDDS%20versions%20prior%20to,denial%2Dof%2Dservice%20condition
[102] https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-38445

Windows 以外のオペレーティングシステム関連の注目すべき脆弱性

2022 年上半期に発見・分析した注目すべき脆弱性の中には、Windows 以外のプラットフォームにも影響を及ぼすものがありました。2022 年 4 月、トレンドマイクロでは、SUHelper クラスを含む macOS ソフトウェアアップデートのヘルパーデーモンプロセスである suhelperd の脆弱性 CVE-2022-22639 [103]の発見と解析についてブログ記事を公開しました。このクラスは、プロセス間通信（IPC）機構を介した重要なシステムサービスを担っています。この脆弱性が悪用されると、ルート権限が取得されて攻撃に利用される可能性があります[104]。Apple 社は、2022 年 3 月にリリースされた macOS Monterey 12.3 のアップデートを通じてこの脆弱性を修正しました[105]。

また、Linux や Unix 系の OS に影響を与える脆弱性も確認されました。CVE-2022- 0847 は、Dirty Pipe とも呼ばれ [106]、バージョン 5.8 以降の Linux カーネルに影響を与える脆弱性です。この脆弱性は、Linux カーネルのメモリ管理、特にパイプページキャッシュのマージと他のページキャッシュの上書きの方法に関する不具合に関連しています[107]。脆弱性 Dirty Pipe が悪用されると、ホストの端末上での ルート権限取得による権限昇格が可能となり、比較的容易に脆弱性悪用の攻撃につながる可能性があります。したがって、企業や組織は、脆弱なバージョンの Linux カーネルを使用しているかどうかを確認することが不可欠となります。脆弱性が発見された場合は、Linux カーネルバージョン 5.16.11、5.15.25、5.10.102 以降にアップデートする必要があります[108]。

一方、CVE-2022-29464[109]は、アプリケーションプログラミングインターフェース（API）、アプリケーション、ウェブサービスを統合するためのオープンソースプラットフォームを提供するプロバイダ WSO2 社の複数の製品に影響を与える重要なリモートコード実行（RCE）の脆弱性として確認されました。

- WSO2 API Manager 2.2.0 およびそれ以降
- Identity Server 5.2.0 以降
- Identity Server Analytics 5.4.0 から 5.6.0 まで
- Identity Server as Key Manager 5.3.0 以降
- Open Banking AM 1.4.0 およびそれ以降
- Enterprise Integrator 6.2.0 以降

---

[103] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22639

[104] https://www.trendmicro.com/en_us/research/22/d/macos-suhelper-root-privilege-escalation-vulnerability-a-deep-di.html

[105] https://support.apple.com/en-us/HT213183

[106] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0847

[107] https://www.trendmicro.com/en_us/research/22/d/detecting-exploitation-of-local-vulnerabilities-through-trend-mi.html

[108] https://www.cisa.gov/uscert/ncas/current-activity/2022/03/10/dirty-pipe-privilege-escalation-vulnerability-linux

[109] https://cve.mitre.org/cgi-bin/cvename.cgi?name=2022-29464

この脆弱性により、ユーザ操作や管理者権限が必要となくなるため、悪用されると、攻撃者は、対象となるシステムのネットワークに侵入することが可能になります。

2022 年 4 月以降、CVE-2022-29464 悪用の試みは放置された状態となっています。これらの試みは、脆弱性悪用の概念実証が GitHub で公開された後に発生しました[110]。その直後、影響を受ける環境向けの Metasploit モジュールが公開されました[111]。これら脆弱性悪用の試みでは、攻撃フローの一部として、Cobalt Strike ビーコンやその他のマルウェアのインストールも含まれています[112]。

その他、脆弱性の影響を受けた WSO2 製品を使用している企業や組織も、システムを更新するか、それぞれのセキュリティアドバイサリで提案されている一時的な緩和策を適用することをお勧めします[113]。WSO2 でも、その後、該当する脆弱性に対応する修正パッチをリリースしました[114]。

[110] https://github.com/hakivvi/CVE-2022-29464/blob/main/exploit.py

[111] https://packetstormsecurity.com/files/166921/WSO-Arbitrary-File-Upload-Remote-Code-Execution.html

[112] https://www.trendmicro.com/en_us/research/22/e/patch-your-wso2-cve-2022-29464-exploited-to-install-linux-compatible-cobalt-strike-beacons-other-malware.html

[113] https://docs.wso2.com/display/Security/Security+Advisory+WSO2-2021-1738

[114] https://docs.wso2.com/display/Security/Security+Advisory+WSO2-2021-1738

クラウド環境における旧態依然の問題と従来とは異なる攻撃

TeamTNT や Kinsing などの攻撃グループによるクラウドベースの暗号資産マイニング活動が増加中

クラウド技術は過去 10 年間で爆発的な成長を遂げ[115]、多くの企業や組織が、コスト削減、運用の回復力、ビジネスの俊敏性、自動化などの利点から、インフラの少なくとも一部をクラウドに移行しています。この傾向は今後数年間も続くと予想され、調査機関 Gartner は、パブリッククラウドへの支出だけでも 2022 年には 5000 億米ドル近くに達すると予測しています[116]。このようなクラウドの普及により、多くの企業が効率的に業務を遂行できるようになった一方で、クラウドベースのシステムは、これまでよりも攻撃範囲を拡大しようとする攻撃者にとって魅力的なターゲットにもなっています。トレンドマイクロの「2022 年セキュリティ脅威予測」[117]でも、クラウドの攻撃者は技術動向を追いながらも、クラウド利用者に対して従来型の攻撃を続けるだろうと予測しています。

暗号資産の価格は 2022 年上半期に急落したものの[118]、暗号資産を狙った攻撃は、マイニング活動のインフラとリソースは感染端末に利用できるため、高い投資コストを必要としません。もとより暗号資産のマイニングには、強力な GPU を搭載した高価な端末を利用するのが最も効率的な方法でした。CPU ベースのマイニングなど、他のタイプの暗号資産マイニングでも利益を上げることができますが、この場合は、多数の端末が利用できる状況下に限定されてしまいます。そしてほとんどのユーザは高価なグラフィカルのパワーハウス仕様の端末を自由に使える状況にもありません。こうした中、一部の攻撃グループは、暗号資産マイニングのオペレーションに際してクラウドインスタンスに狙いを定めることで、質より量でカバーする戦略を採り始めています[119]。

クラウドベースの暗号資産マイニングに関する調査では、こうした戦略を採り始めた主要な攻撃グループを注目し、最も顕著な 5 つの攻撃グループとその活動方法を特定しました。

---

[115] https://pages.awscloud.com/rs/112-TZM-766/images/cloud-value-benchmarking-study-quantifies-cloud-adoption-benefits.pdf

[116] https://www.gartner.com/en/newsroom/press-releases/2022-04-19-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-500-billion-in-2022

[117] https://resources.trendmicro.com/jp-docdownload-form-m426-web-prediction2022.html

[118] https://fortune.com/2022/06/18/bitcoin-has-extended-its-record-breaking-decline-to-below-19000-although-painful-removing-the-sectors-froth-is-likely-healthy-one-expert-contends

[119] https://documents.trendmicro.com/assets/white_papers/wp-navigating-the-landscape-of-cloud-based-cryptocurrency-mining.pdf

Outlaw：この攻撃グループは、自分たちが精通しているツールや手法に固執することを好む傾向があり、その活動内容は、長年にわたって大きな変化は見られていません[120]。IoT デバイスや Linux クラウドサーバなどを好んでターゲットとし、既知の脆弱性の悪用や、ブルートフォース Secure Shell（SSH）攻撃などを駆使して、これらのデバイスを侵害します。

TeamTNT：ここ数年、トレンドマイクロで注目している攻撃グループであり[121]、ソーシャルメディア（SNS）に積極的に参加することで知られており、攻撃を解析したリサーチャーに SNS 経由で返信するまでに至っています。短期間で急速に進化し、暗号資産マイニング活動を重視し、技術的に巧妙な手法を駆使します。また、この攻撃グループの場合、まず脆弱なソフトウェアを悪用し、その上で、感染端末での水平移動・内部活動や設定ミス悪用などの本格的な攻撃の前段階としてクレデンシャル情報を窃取します。

Kinsing：ネット上での存在感という点では、TeamTNT とは逆の攻撃グループといえます。ソーシャルメディアやアンダーグラウンドのフォーラムにおいてさえ、目立った存在感を示していないからです。他方、迅速に適応し、攻撃用のツールキットを進化させる能力という点では、TeamTNT と似ているともいえます[122]。また、この攻撃グループは、Log4Shell の脆弱性が最初に公開されてからわずか数日後に利用するなど、新たに確認された脆弱性を素早く採用することでも知られています[123]。

8220：主に Oracle WebLogic Server に影響を与える脆弱性を頻繁に悪用している攻撃グループです。比較的静かだった 2020 年を経て、2021 年には前年の約 10 倍の活動レベルにまで活発化したことが確認されています。また、この攻撃グループは、Kinsing と同じリソースを奪い合うことが知られており、両者は、しばしば侵害された端末からお互いを追い出し、自分たちのコインマイナーをインストールすることがあります。

Kek Security：比較的新しい攻撃グループですが、手口の巧妙さと新しい脆弱性悪用の手法を攻撃に組み込む傾向があることから注目を集めています。また、継続的に自前のマルウェアを開発しており、最近追加されたマルウェアの中には、検知を回避し、リサーチャーの解析を阻止するために、より優れた難読化機能を駆使するものもあります。

これらの攻撃グループは、共通の限られたリソースをターゲットにしているため、グループ同士で同じ端末をめぐって争い、しばしばキルスクリプトを使用して相手に対処するケースなども複数目撃されています。このような熾烈な競争によって、さまざまな脅威が革

[120] https://www.trendmicro.com/en_us/research/18/k/outlaw-group-distributes-botnet-for-cryptocurrency-mining-scanning-and-brute-force.html

[121] https://documents.trendmicro.com/assets/white_papers/wp-tracking-the-activities-of-teamTNT.pdf

[122] https://www.trendmicro.com/en_us/research/20/k/analysis-of-kinsing-malwares-use-of-rootkit.html

[123] https://www.bleepingcomputer.com/news/security/hackers-start-pushing-malware-in-worldwide-log4shell-attacks/

新的な技術が生み出されてもいます。例えば、相手が攻撃できないシステムを自分たちは狙えるようになるといった機能の追加なども試みられています。

図 22：クラウドベースの暗号資産マイニングを狙う各攻撃者の概要
（活動期間、巧妙化レベル、脆弱性悪用、ソーシャルメディアでの存在感）

クラウドのトンネルサービスを悪用した攻撃

クラウド技術が提供する利点の中には、企業や組織にとってセキュリティ上の課題をもたらすものもあります。例えば、クラウド技術を利用すれば、資産やサービスを迅速に展開することができるため、業務効率化に役立ちます。しかし、その反面、導入された資産を完全に把握することができなくなるリスクもあります。攻撃者は、こうした状況を突いて、企業の IT 部門やセキュリティ担当者が監視しにくい場所を狙い、従来とは異なる手法で攻撃を仕掛けてくる可能性があります。

トレンドマイクロでは、最近、クラウドのトンネルサービスを悪用して攻撃の事例を確認しました。このサービスは、個人と企業の両方が、クラウドベースのインフラを通じてトラフィックを中継することにより、内部システムをインターネットに公開するために使用するものです。通常、この種のサービスは、開発者がコードのテストや展開に使用したり、特定のサービスをインターネット上の特定のユーザに利用させたりするものです。つまり、ユーザがネットワークファイアウォールを設定したりドメイン名を登録したりする必要なく、ローカル開発サービスを展開できる便利なツールといえます。

こうした人気の高まりから、攻撃範囲の拡大を目指す攻撃者にとっての格好の標的になっています。通常、恒久的なインフラを維持する必要がない一時的な用途で利用され、また、実際の所在地が隠ぺいできるため、機密性を高める目的で用いられたりもしています[124]。

クラウドのトンネルサービスを狙う脅威は、内部を狙うもの外部を狙うものの 2 種類に分類されます。内部を狙う脅威とは、SMB（Server Message Block）、FTP、HTTP などの内部サービスを公開する際に（意図的または無自覚に）利用されるサービスが狙われる攻撃を指します。一方、外部からの脅威とは、フィッシング攻撃や、クラウドトンネルを介した C&C 通信など、従来型の攻撃活動のことを指します。

2020 年 9 月のブログ記事では、内部からの脅威として、正規ツールやサービスが悪用された事例を紹介しています。この場合、攻撃者が ngrok を使用して SMB ポートを公開し、最終的にキーロガーのダウンロードと実行につながりました[125]。一方、外部からの脅威は、一般的には、マルウェアのトラフィックのルーティングやフィッシングサイトのホスティングのため、クラウドのトンネルサービスの操作が狙われます。

[124] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/how-cybercriminals-abuse-cloud-tunneling-services

[125] https://www.trendmicro.com/en_us/research/20/i/analysis-of-a-convoluted-attack-chain-involving-ngrok.html

企業にとってのセキュリティ課題であり続けるクラウドの設定ミス

2025 年までに 82 億米ドルに達すると推定されるコンテナ市場の成長は、クラウドに特化した攻撃者にとって魅力的なターゲットとなっています[126]。コンテナを利用することで、企業や組織は、自社の開発サイクルのスピードや効率を向上させることができますが、この際、適切なセキュリティ管理が行われないと、リポジトリの乗っ取りからコンテナソフトウェアの特定のコンポーネントの脆弱性悪用に至るまで、パイプライン上のさまざまな段階で危険にさらされることになります[127]。

コンテナソフトウェアの設定ミスは、多くの企業や組織にとって依然として重要な問題です。DevOps、エンジニアリング、セキュリティの専門家 300 人以上を対象とした IT 企業 Red Hat の調査によると、回答者の 53%がコンテナや Kubernetes の導入において設定ミスを発見いたといいます[128]。

トレンドマイクロでは、Kubernetes の展開における主要な設定ミスの問題の 1 つであり、特に 10250 番ポートを介して一般に公開されている Kubernetes クラスタについて調査しました[129]。その中で kubelet は、Kubernetes の不可欠な部分であり、すべてのコンテナがポッド内で実行されていることを確認します。特にノードの Kubernetes クラスタへの参加、コンテナ状況の管理、ノード情報の更新や制御といった機能を実行する役割を担っています。この kubelet API が使用する 10250 番ポートは、内部で公開されているため、通常、外部サービスからはアクセスできなくなっています。

しかし、Shodan のデータに基づき、IP アドレス情報と簡単なスクリプトを使用して kubelet API にリクエストを送信することで、インターネットに露出した 24 万を超える Kubernetes クラスタノードを特定することができました。これらのノードのうち、かなりの数が HTTP の「401 Status Code - Unauthorized」を返しており、これは匿名のリクエストをブロックしていることを意味します。しかし、熟練した攻撃者であれば、kubelet 認証トークンを侵害したり、他のエクスプロイトを使用したりして、これらのクラスタを侵害しようと試みます。そして約 600 のノードが「200 - OK」通知を返しています。これは kubelet を実行している一部のノードは、特定のノード内のポッドに関する情報を提供することを示しています。これら公開されたノードに対して、攻撃者は、kubelet API を介してプログラムをインストールして実行することができます。

---

[126] https://www.globenewswire.com/news-release/2020/05/06/2028585/0/en/Application-Container-Market-is-Expected-to-Reach-8-20-Billion-by-2025-Says-Allied-Market-Research.html

[127] https://www.trendmicro.com/vinfo/us/security/news/security-technology/container-security-examining-potential-threats-to-the-container-environment

[128] https://www.redhat.com/en/resources/kubernetes-adoption-security-market-trends-overview

[129] https://www.trendmicro.com/en_us/research/22/e/the-fault-in-our-kubelets-analyzing-the-security-of-publicly-exposed-kubernetes-clusters.html

一方、Trend Micro Cloud One™ Conformity のデータでは、Amazon Web Services（AWS）、Microsoft Azure、Google Cloud Platform（GCP）のサービスで、総チェックを行った際に設定ミスが検出された率が高いツールやサービスは下図のとおりとなります。検出した「設定ミス」にはリスクレベル評価で高リスクのものから中～低リスクのものまで様々なレベルの検出を確認しています。また利用者によっては一定の検出に対し、リスクレベルの検討から緩和策を講じるなど、認識の上で設定を選択している場合も含まれているものと推測されます。

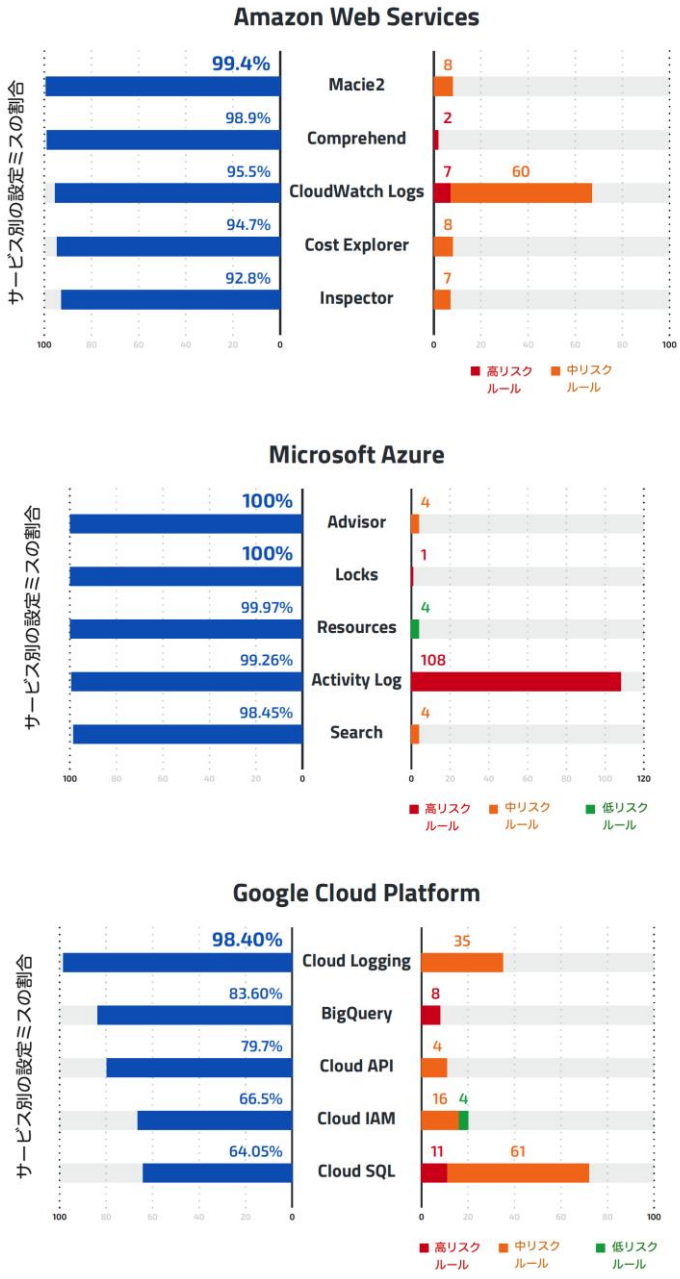

図 23：Amazon Web Services (AWS)、Microsoft Azure、Google Cloud Platform (GCP)における設定ミス検出率

2022 年上半期の脅威概況

2022 年上半期、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）」は、メールの脅威、不正なファイル、不正な URL からなる約 620 億以上の脅威をブロックし、ユーザを保護しました。

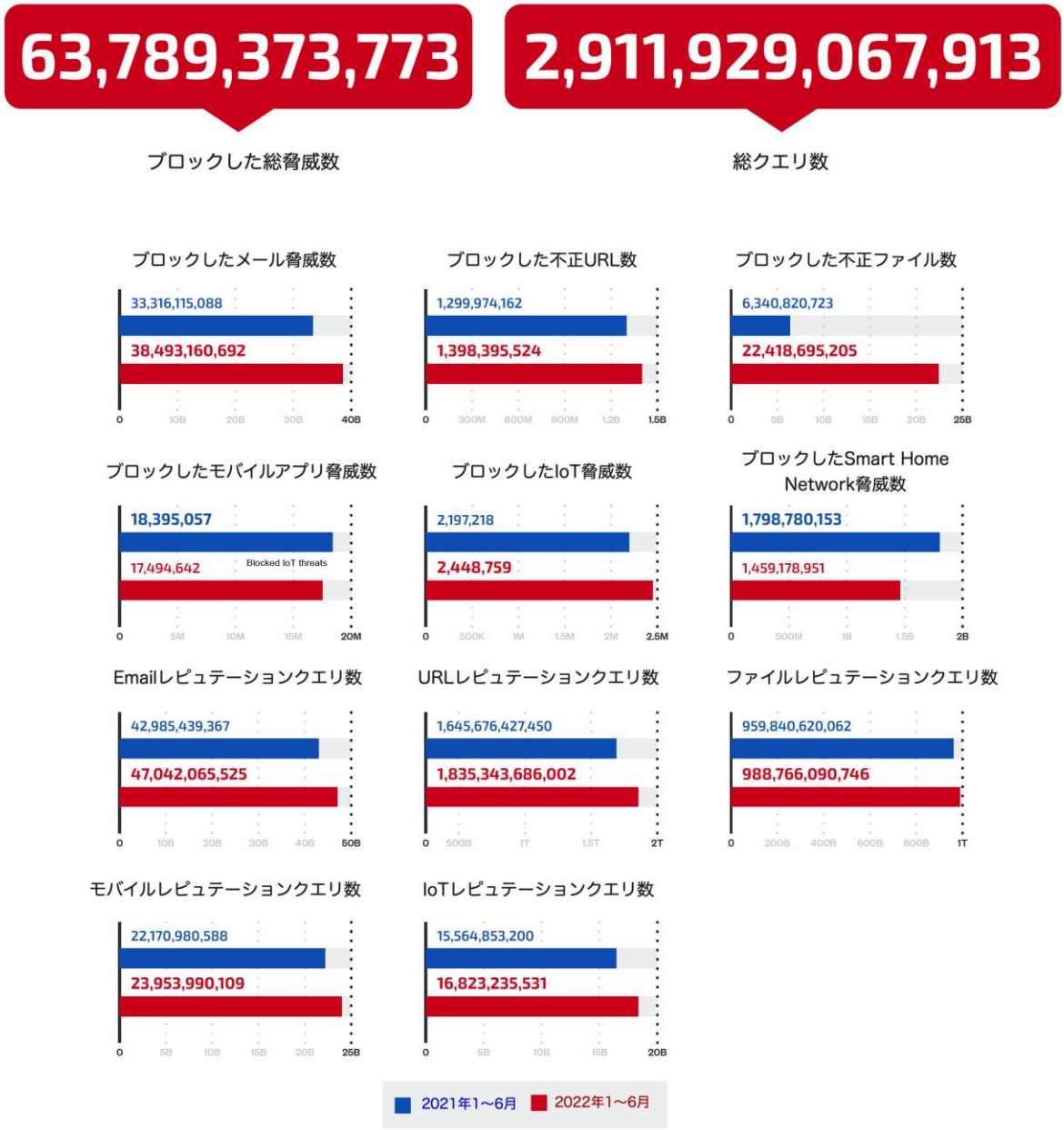

図 24：トレンドマイクロ製品によるメール、ファイル、URL の脅威検出数とクエリ数の推移
2022 年上半期は、2021 年上半期と比較しすべてにおいて増加がみられた

マルウェア関連の脅威状況

マルウェアなどのブロックされた不正なファイルは、2020 年以降、増加傾向を示しています。2020 年上半期には 10 億強程度だった不正ファイルの検出件数は、2022 半ばには 220 億強に増加しました。この間 SPN のフィードバック機構が改善されたことに加え、コロナ禍におけるリモートワークやハイブリッドワークといった業務体制への移行も、この検出数の増加に影響していると推測しています。

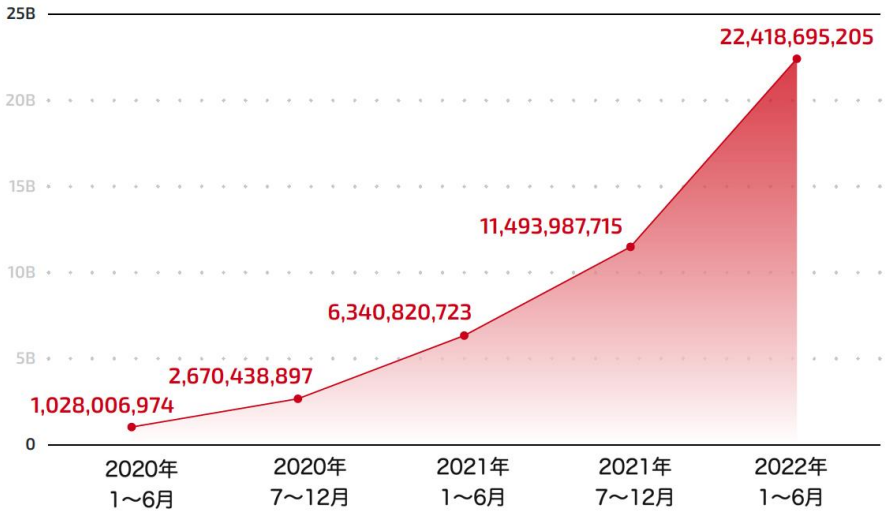

図 25：ファイルの脅威検出数推移

2020 年に入ってからブロックされたファイル数は着実に増加しており、その後約半年ごとに倍増している

2022 年上半期の検出数では、Webshell がマルウェアファミリーのトップで、2022 年復活を遂げた EMOTET がそれに続きました。コインマイナーが 3 番目に検出台数が多く、Ulise および Powload と合わせてトップ 5 を占めています。

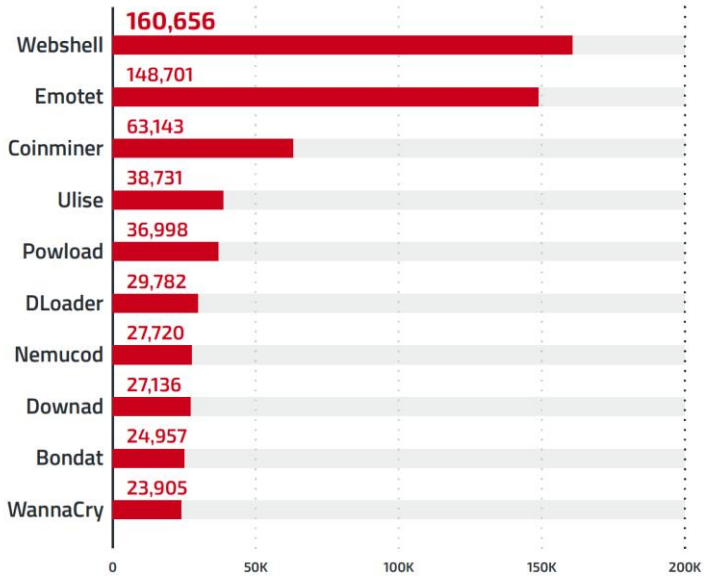

図 26：2022 年上半期のマルウェアファミリー別検出台数トップ 10

SPN のデータによると、2022 年上半期にマルウェアの検出台数が最も多かった業界は、引き続き公共、製造、ヘルスケアであることが明らかになりました。それでも上位には若干の変化があり、公共が製造を抜き、テクノロジー分野が銀行に代わって上位 5 位に入っています。

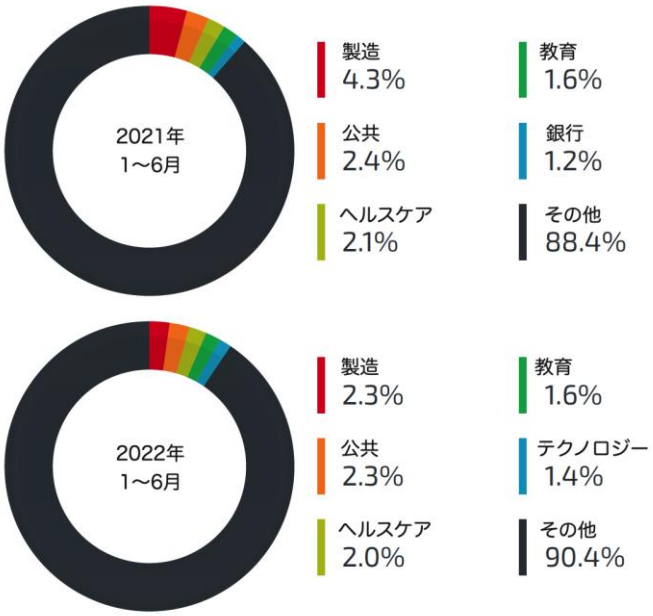

図 27：2021 年上半期と 2022 年上半期の業界別マルウェア検出数トップ 5 の比較

2022 年上半期に登場した新しいランサムウェアファミリーは、前年上半期と比較して大幅に減少しました。しかし、Cheerscrypt など、注目すべきランサムウェアファミリーも存在します。また、攻撃者は独自のファミリーを自身で新たに開発するのではなく、既存の RaaS の利用などに目を向け始めていることも理由の 1 つと推測されます。

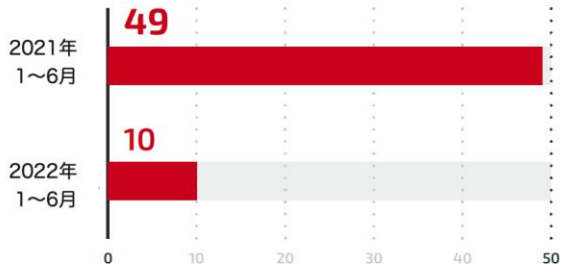

図 28：新たに確認されたランサムウェアファミリー数の比較

1月	2月	3月	4月	5月	6月
新規ファミリーは確認されなかった	新規ファミリーは確認されなかった	Explus	Cheerscrypt	Keversen	ZagreuS
		NoEscape		StorageCrypt	Lorenz
				Palang	EvilNominatus
				Blaze	

表 3：2022 年上半期に確認された新たなランサムウェアファミリーは 10 件にとどまり、1 月と 2 月には新たなランサムウェアファミリーは確認されなかった

狙われる VPN 脆弱性

ランサムウェア攻撃をはじめとする様々なサイバー犯罪者が、組織ネットワークへの侵入口として、VPN の脆弱性を狙い続けています。特に、Fortinet の FortiGate SSL で発生するパストラバーサルの脆弱性「CVE-2018-13379」[130]は、2022 年上半期に VPN で確認された不具合として 2022 年 6 月には 9 万件超の検出数となり、ピークを迎えました。一方、F5 のソフトウェアである iControl REST Interface に影響を及ぼす脆弱性「CVE-2021-22986」[131]は、2022 年 6 月に 10 万件以上の検出数に達し、月別では最高値となりました。

製品名	CVE番号	DVフィルタ (Digital Vaccine)	1月	2月	3月	4月	5月	6月	合計
Fortinet	CVE-2018-13379	DV-36087	21,710	21,733	26,405	25,077	32,590	90,700	218,215
Pulse Secure	CVE-2019-11510	DV-36089	8,708	8,204	10,110	14,950	16,226	48,098	106,296
		DV-36241	506	775	1,940	1,483	1,800	1,765	8,269
	CVE-2019-11539	DV-36095	0	0	0	0	30	0	30
	CVE-2021-22893	DV-39636	0	0	0	3	1	2	6
Citrix Systems	CVE-2019-19781	DV-36876	1,120	684	2,068	1,134	1,770	3,361	10,137
		DV-36927	27	15	60	67	76	43	288
Palo Alto	CVE-2019-1579	DV-38230	0	0	0	0	0	0	0
F5	CVE-2020-5902	DV-37841	19,339	17,581	34,507	24,881	36,079	62,302	194,689
		DV-38276 (Malware)	0	0	0	0	0	0	0
	CVE-2021-22986	DV-39360	1,320	2,503	1,481	91	12	39	5,446
		DV-39352	173	446	313	303	394	241	1,870
		DV-39364	3,126	3,419	3,418	3,884	54,692	105,075	173,614
SonicWall	CVE-2021-20016	DV-39727 (Malware)	0	0	0	0	0	0	0
		DV-41488	0	0	0	0	0	0	0
Cisco	CVE-2021-1609	None	0	0	0	0	0	0	0
	CVE-2021-1610	None	0	0	0	0	0	0	0

表 4：Trend Micro TippingPoint Threat Protection System による
2022 年上半期の主要 VPN 関連脆弱性[132]の検出件数の月別比較

[130] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13379

[131] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22986

[132] 独立行政法人情報処理推進機構（IPA）および JPCERT コーディネーションセンターによる注意喚起から抽出

IoT 関連の脅威状況

2022 年上半期にブロックされた IoT 関連の脅威件数は、前年上半期と比較して 11.4%増加しており、この期間に IoT を狙った攻撃者がより活発に攻撃キャンペーンを実施していたことが分かります。

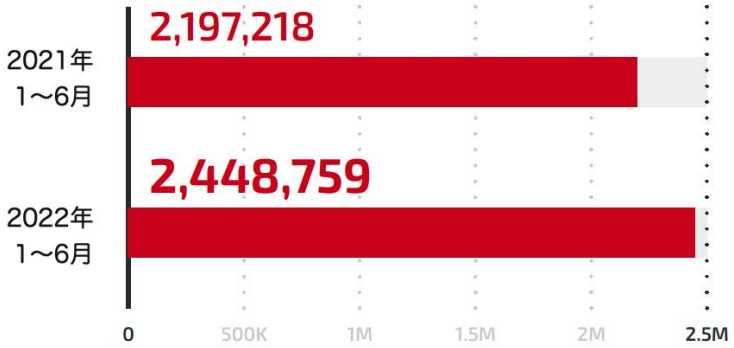

図 29：ブロックされた IoT 脅威の数は 11.4%増加（2022 年上半期および 2021 年上半期との比較）

このような IoT のプラットフォームに関連する注目すべき事件の 1 つとしては、以前に APT グループ「Sandworm」[133]に関連したモジュラー型ボットネット Cyclops Blink の亜種が、感染デバイスのフラッシュメモリにアクセスできる特殊なモジュールを用いて、新たに Asus 社製ルータを狙い、情報を窃取し、システムリセットにも耐えられる攻撃を実行していた点が挙げられます[134]。Cyclops Blink は、以前、WatchGuard Firebox への攻撃を試みたこともあり、国家支援型のボットネットと見なされていました[135]。ただし今回の調査では、標的となったデバイスは必ずしも重要なインフラや産業に属しているわけではないことが明らかになりました。したがって、今回の Asus 社製ルータへの攻撃は、将来的により価値の高いターゲットへの攻撃に備えて、攻撃者がインフラを拡大しようとした活動の一環であった可能性が高いと考えられます。その後、Asus 社はセキュリティ情報を公開し、影響を受けるデバイスのファームウェアのアップデートを提供しています[136]。

[133] https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/faq-blackenergy

[134] https://www.trendmicro.com/en_us/research/22/c/cyclops-blink-sets-sights-on-asus-routers--.html

[135] https://www.watchguard.com/wgrd-news/blog/important-detection-and-remediation-actions-cyclops-blink-state-sponsored-botnet

[136] https://www.asus.com/content/ASUS-Product-Security-Advisory/

暗号通貨を狙うコインマイナーの状況

近年の動向を見ると、2018 年をピークにコインマイナーの検出台数が着実に減少していることが確認されています。例えば、2022 年上半期は、前々半期から顕著に減少しています。この落ち込みの原因として考えられるのは、さまざまな外的問題により、暗号資産の価格が暴落したことです[137]。これにより、サイバー犯罪者の中で暗号資産マイニングの手口への関心が低下したものと推測されます。

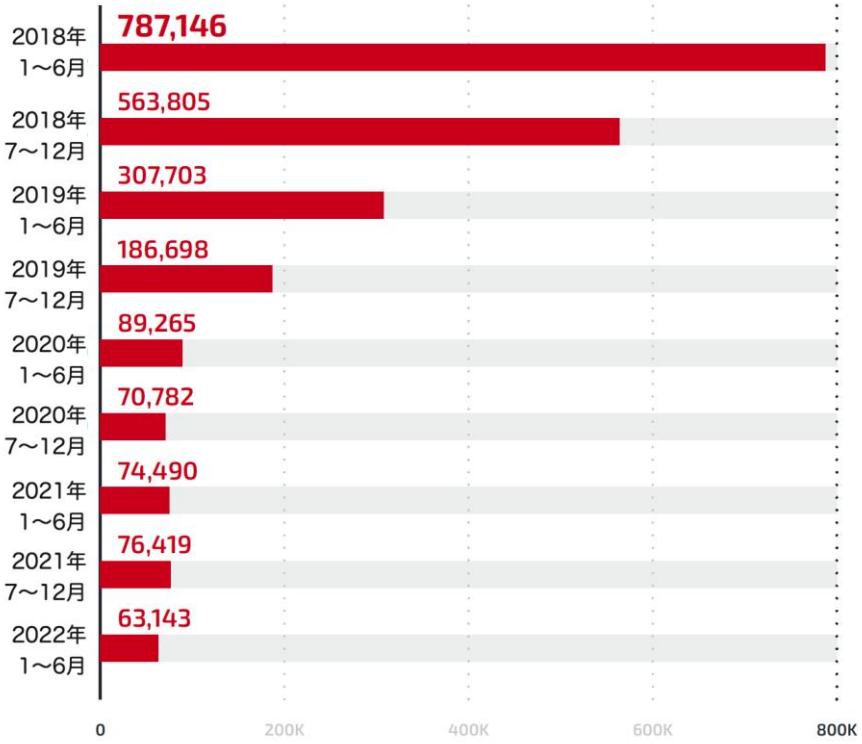

図 30：コインマイナーの検出台数推移

他方でコインマイナーは、Linux のオペレーティングシステムを狙う脅威としては増加しています。2022 年上半期は、2021 年の同時期と比較して、Linux ベースのコインマイナーの検出台数は約 145%増加していました。

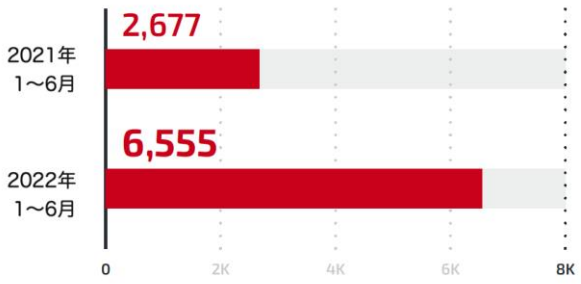

図 31：Linux ベースのコインマイナーの検出台数の半期比較では 145%増加している

[137] https://www.bbc.com/news/technology-61796155

2022 年上半期、トレンドマイクロでは、特定のコインマイナー関連の動向を確認[138]しました。特に非可溶性トークン（NFT）などの新技術は、攻撃者にとって格好のターゲットとなっています。例えば、トレンドマイクロが確認した NFT 関連の攻撃の中には、ユーザを騙して不正なサイトにウォレットを接続させ、さらなる攻撃の道を開くよう設計された偽の NFT トレーダードメインを使用するものがありました。また、説明文にフィッシングリンクが記載された NFT が、不用心なユーザに対してエアドロップされる例も確認され、この場合も、ウォレットを接続させる手口となっていました。

その他、最近では、暗号資産を狙う攻撃の手法としてアプリケーションの Telegram が利用されるケースも確認されています。この事例では、攻撃者がチャットグループでテクニカルサポートの担当者になりすまし、暗号資産に関するユーザの悩みを解決するよう持ちかけました。この偽の担当者は、次に、ニーモニックシードフレーズ（暗号通貨のウォレットを作成する際に生成される一連の無関係な単語）や秘密鍵を窃取するために設計されたフィッシングサイトにアクセスするように被害者を説得していました。また、Telegram のチャットグループでも、グループのオーナーが正規のチャットグループ管理者のふりをして、暗号資産に関心を持つユーザを騙して偽の Web ページにアクセスさせるという類似の攻撃シナリオも確認されました。

[138] https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/c/an-investigation-of-cryptocurrency-scams-and-schemes/03Technical%20Brief%20Keeping%20Assets%20Safe%20From%20Cryptocurrency%20Scams%20and%20Schemes.pdf

モバイル関連の脅威状況

トレンドマイクロのデータによると、2022 年上半期のモバイル機器関連の不正な検体数は、2021 年上半期と比較して若干（4.9%）減少しています。

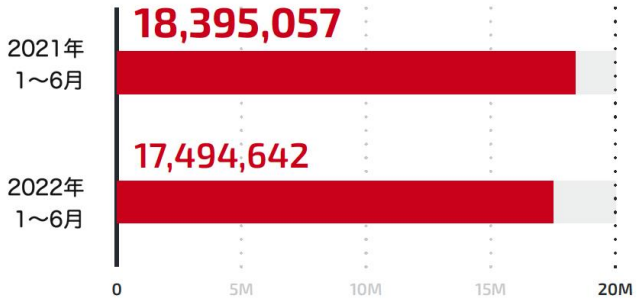

図 32：モバイル端末関連の不正な検体の検出数の比較

モバイル端末向け不正プログラム関連で注目すべきは、暗号資産マイニング用ソフトウェアを装った偽モバイルアプリが公開され、ユーザを有料サービスに加入させたり、偽の暗号資産収入を宣伝する広告を表示させたりする悪質業者が存在したことです[139]。さらに調査したところ、これらの偽モバイルアプリの１つが、ユーザに秘密鍵やニーモニックフレーズを入力させ、将来の使用に備えてこれらの収集を促す偽の Web サイトを読み込ませていることも判明しました。

[139] https://www.trendmicro.com/en_us/research/22/e/fake-mobile-apps-steal-facebook-credentials--crypto-related-keys.html

TREND MICRO

〒151-0053

東京都渋谷区代々木 2-1-1　新宿マインズタワー

大代表 TEL：03-5334-3600 FAX：03-5334-4008

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。