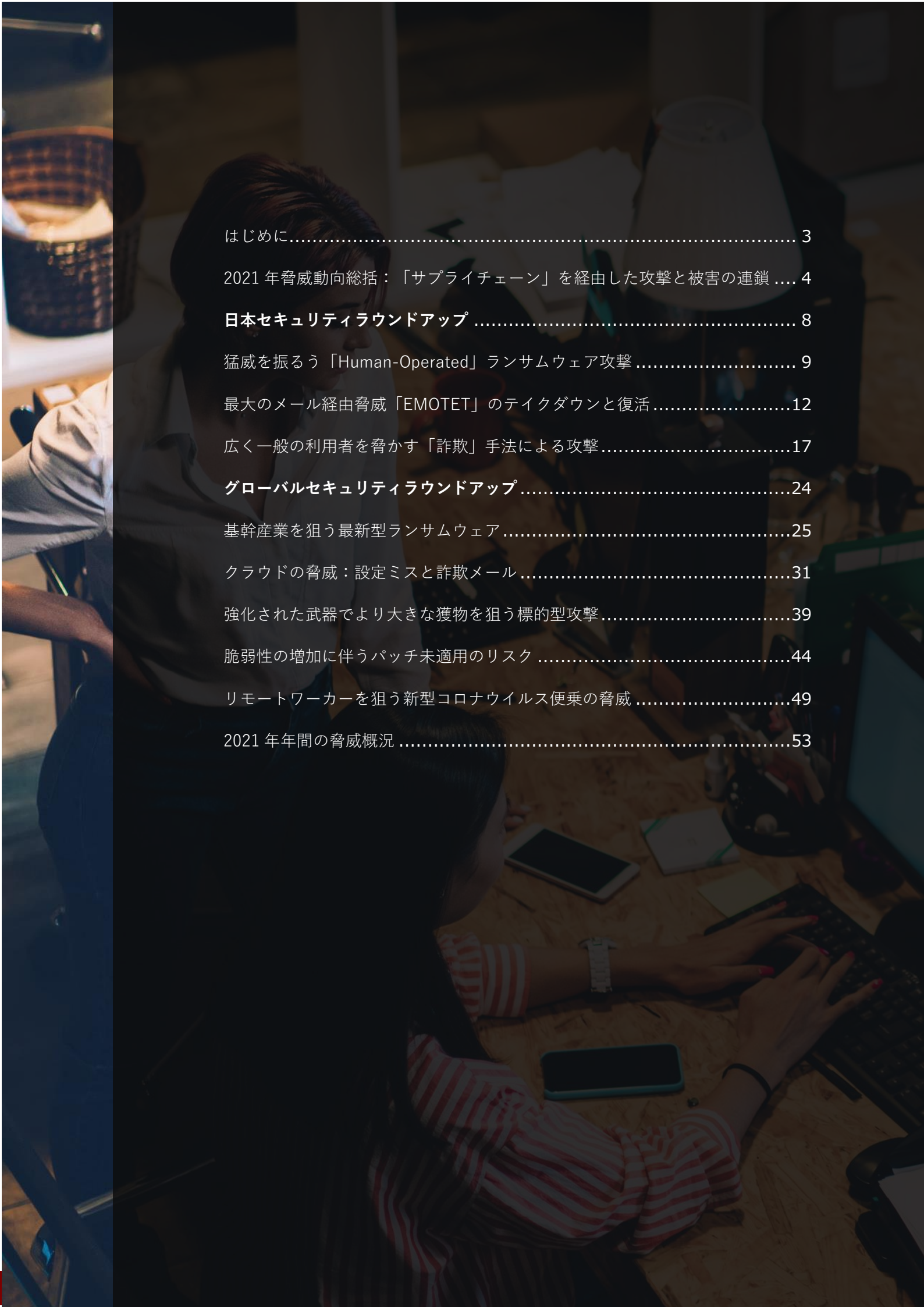
TREND MICRO | research

2021 年年間セキュリティラウンドアップ

「サプライチェーン」を経由した攻撃と被害の連鎖



はじめに

「2021 年年間セキュリティラウンドアップ」は、2021 年 1 年間の世界と日本における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 940 億件以上の脅威から 2021 年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。脅威データは 2021 年 1 年間を基本とし、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 3 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 3 月 14 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。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。

2021 年脅威動向総括：「サプライチェーン」を経由した攻撃と被害の連鎖

世界的な脅威動向の中で、2021 年はここ数年進んでいた「サプライチェーン攻撃」の拡大と共に、法人組織におけるセキュリティリスクの連鎖が顕著になった年と言えます。

◆「境界線の曖昧化」が招いた脅威変化

以前には、組織ネットワークへの侵入を狙う攻撃は、社内の従業員をセキュリティ上の弱点として狙う、標的型メール攻撃に集中していました。しかしここ数年、脆弱性やアカウントハッキングによる外部からの直接侵入が目立ってきています。この変化の背景の 1 つとして、ネットワーク境界線の曖昧化があります。業務のデジタル化とその積極的な活用が進むにつれ、内部リソースの外部クラウドへの移動、従業員が組織ネットワークの外で業務を行う、これまで閉域化されていたシステムがネットワークに繋がる、など、これまでセキュリティの要と考えられていたネットワーク境界線の曖昧化が進みました。この傾向は、2020 年から続くコロナ禍の状況によりさらに加速された一方、攻撃者は曖昧化によって生じた弱点を狙って組織ネットワークに直接侵入する攻撃を拡大させました。

具体的には、テレワークの一般化により在宅勤務の従業員による社外からのアクセスが日常化するにつれ、攻撃者の狙いは VPN など組織ネットワークと外部との接点に集まりました。VPN の脆弱性を狙い認証情報を窃取する攻撃と、その窃取した認証情報を使用した認証突破による侵入は 2019 年から継続して発生し、留まるところを知りません。加えて、2021 年には新たに「ProxyLogon[1]」、「PrintNightmare[2]」、「Log4Shell[3]」など、遠隔攻撃による侵入に使用可能な深刻な脆弱性が相次いで確認されると共に、攻撃に悪用されました。さらに、組織内リソースのクラウド移行に伴って、設定ミスを発端とする侵入の事例や、社内ネットワークに比べ相対的にセキュリティレベルが下がるテレワーク環境で業務を行う従業員を侵入の踏み台とする攻撃も確認されています。

◆「組織間の関係性」の弱点を狙う脅威

このように境界線の曖昧化で分散した弱点を狙う侵入経路の多様化に加え、攻撃者は標的組織が信用する他組織を侵害して踏み台にする、いわゆるサプライチェーン攻撃も拡大させました。標的組織が使用するソフトウェアやサービスの提供者を侵害し踏み台とする攻撃とし

[1] https://proxylogon.com/
[2] https://blog.trendmicro.co.jp/archives/28694
[3] https://blog.trendmicro.co.jp/archives/29518

て、2020 年末に露見した「SolarWinds 事例[4]」はまさに過去最大規模の「ソフトウェアサプライチェーン攻撃」事例となり、2021 年にもその影響は続きました。次いで 2021 年 7 月には、Kaseya 社製管理ソフトのゼロデイ脆弱性を利用した攻撃が確認[5]されました。この攻撃では、最終的に同管理ソフトを使用したサービスの利用者がランサムウェア被害に遭うものでした。この Kaseya 社製管理ソフトの攻撃事例は、サービス経由のサプライチェーン攻撃として、2017 年に報告された「Operation Cloud Hopper[6]」以来の大規模な攻撃事例と言えます。また、「Operation Cloud Hopper」は高度な標的型攻撃だったことと比べ、Kaseya 事例は最終的な被害がランサムウェア攻撃であった点も、サプライチェーン攻撃の拡大を示す特徴的な事項と言えます。

同様に、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」も常套手段化しています。攻撃者は標的組織の関連会社や海外拠点など関係の深い組織を侵害し、標的組織への侵入の踏み台とします。特に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。また、標的組織の取引先など関係のある法人組織を侵害しそこから窃取した情報を利用する、もしくはシステムの乗っ取りによるなりすまし攻撃も、組織間の業務上の関係性を踏み台にする攻撃と言えます。

◆サイバーにおける「サプライチェーンリスク」の顕在化

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一方、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サプライチェーンリスクも顕在化してきました。実際にサプライチェーン上の 1 企業の被害により社会に多大な影響が及んだ事例として、2021 年 5 月に発生した米国コロニアルパイプライン社のランサムウェア被害[7]があげられます。この被害により、同社の石油パイプラインは結果的に約 1 週間の操業停止を余儀なくされました。その間の米国東海岸地域への石油供給量は半減し、18 の州で緊急事態が宣言される事態にまで発展しました。

また、特定の法人組織における被害が業務上の関係性を通じて他の組織にも影響を与えた事例が、日本国内で複数発生しています。2021 年 2 月、自治体向け事業を手掛けているコンサルティング業者がランサムウェア被害に遭う事例[8]が発生しました。被害の影響は実際にランサムウェア被害を受けた 1 社だけに留まらず、少なくとも 10 の自治体において業務委託にあたって貸与していた住民情報などが漏えいした可能性が生じました。別のコンサルティング業者でも 2021 年 8 月にランサムウェア被害が発生[9]。自治体から請け負っていた事業

[4] https://www.solarwinds.com/ja/sa-overview/securityadvisory
[5] https://helpdesk.kaseya.com/hc/en-gb/articles/4403440684689-Important-Notice-July-2nd-2021
[6] https://www.pwc.co.uk/issues/cyber-security-services/insights/operation-cloud-hopper.html
[7] https://www.asahi.com/articles/ASP592PNYP58ULFA008.html
[8] https://www.landbrains.co.jp/hp/doc/210226.pdf
[9] https://www.oriconsul.com/news/post_files/210820_newsrelease.pdf

に関する情報漏えいの可能性と共に、企業から発注を受けていた設計業務に履行遅滞が発生[10]するなどの影響が生じました。

このように、今や１つの組織のサイバー被害はその組織だけに留まらず、より大きい範囲に影響するセキュリティリスクの連鎖が顕著になってきました。個々の組織にとっては、業務のデジタル化と更なる活用が進むことにより大きな恩恵がある半面、攻撃者のつけ入る弱点となり組織ネットワークへの侵入を許す事例が出てきました。そして１つの組織におけるセキュリティ上の弱点は、組織間の繋がりを経由して広がる攻撃、つまりサプライチェーン攻撃として具体化しました。また攻撃の被害は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。

◆「サプライチェーン攻撃」への防御と「サプライチェーンリスク」の緩和

このような状況において組織が業務継続を守るためには、自身の安全を守るだけでなく、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。個々の組織においては「ゼロトラスト」と「多層防御」の２つの概念が、今後のセキュリティの基本になっていくと考えられます。サプライチェーン攻撃は既に信頼している相手からの攻撃であるため、ゼロトラストの概念に基づく多重・多段の認証やコンテキストベースの判定により、侵入した攻撃者を自由にさせない取り組みが必須です。同様にゲートウェイ、内部ネットワーク、エンドポイントなど各階層において行われる不審な活動を多層の技術により警告できるようにすると同時に、注意すべき警告を横串で解析できるシステムによって、多数の警告の中から攻撃者の存在を炙り出せるようにすることが重要です。

次に、サプライチェーン全体のセキュリティを考えた場合には、サプライチェーンに参加するすべての組織がセキュリティに向き合うことが必要です。「ドベネクの桶[11]」の喩えのように、セキュリティレベルの最も低い１社がサプライチェーンの弱点となり、全体のセキュリティレベルに影響を及ぼします。そのため、今後はサプライチェーンを形成する個々の組織が、自組織のセキュリティについての説明責任を負うようになるでしょう。例えば、新たに取引を開始する相手に対しては、経営状態が悪くないかなどの調査と共に、セキュリティ状況を確認する取り組みが求められてくるでしょう。当然、相手に求めるのと同じレベルで自社のセキュリティ状況を説明できるようにしておく必要もあります。逆にセキュリティが行き届いていない組織はサプライチェーンから弾かれ、ビジネスの機会を失う可能性も出てくるでしょう。このようなサプライチェーン全体でのセキュリティレベルの引き上げは個々の組織による取り組みだけでは不十分であり、業界全体、ひいては社会全体で取り組んでいく事が必要です。セキュリティには終わりが無いため、最低限行うべき内容について統一し

[10] https://scan.netsecurity.ne.jp/article/2021/05/21/45699.html
[11] https://kotobank.jp/word/%E3%83%89%E3%83%99%E3%83%8D%E3%82%AF%E3%81%AE%E6%A1%B6-789812

たガイドラインやベストプラクティスを業界団体や監督官庁、政府機関などから示すことが望ましいでしょう。

初期のインターネットは、特定の国や政府のものではなく、あくまでも仮想空間であり、現実社会とは別、というイメージがありました。しかし、今やネットは社会に欠かせないインフラであり、現実社会の一部となりました。デジタル化とその活用が進む今、サイバーセキュリティは事業継続を考える上で不可欠な要素です。事業継続計画（BCP）を策定する際には必ず災害発生時の対応を考えるように、サイバーインシデント発生時の対応も考慮する必要があります。またそれは自組織を守るだけでなく、サプライチェーン全体、ひいては社会を守る取り組みでもあるものと言えます。

日本セキュリティラウンドアップ

猛威を振るう「Human-Operated」ランサムウェア攻撃

最大のメール経由脅威「EMOTET」のテイクダウンと復活

広く一般の利用者を脅かす「詐欺」手法による攻撃

猛威を振るう「Human-Operated」ランサムウェア攻撃

海外では 2018 年頃から見られ始めた所謂「Human-Operated」型のランサムウェア攻撃は、日本国内でも継続して大きな被害を発生させています。トレンドマイクロが国内の法人組織から受けたランサムウェアの被害報告件数は、2020 年の第 4 四半期をピークとして、高止まりの状況が続いています。国内でのランサムウェアの検出台数も 2020 年第 2 四半期以降継続して 4000 件以上を記録しており、同様に高止まりの状況と言えます。

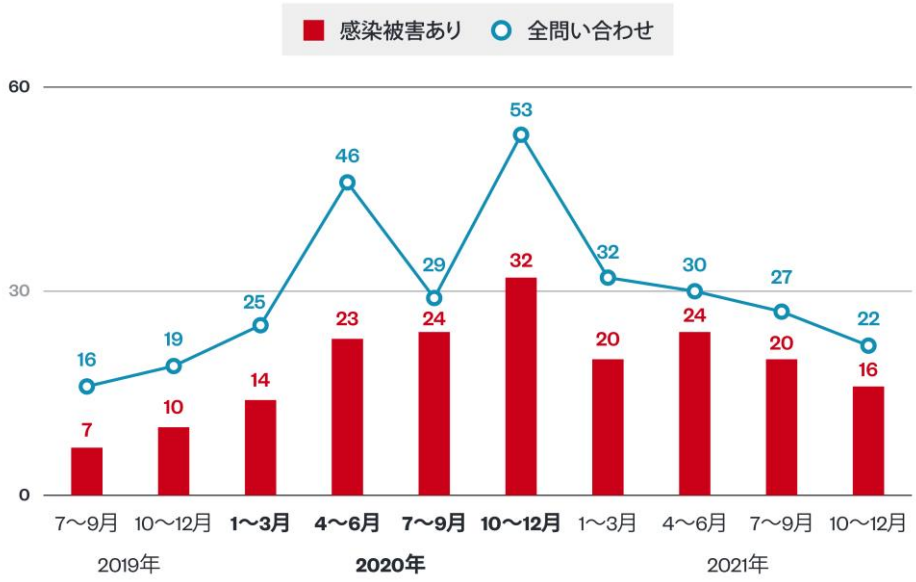


図 1：国内法人からのランサムウェア関連問い合わせ件数とそのうちの被害報告件数の推移（トレンドマイクロ調べ）

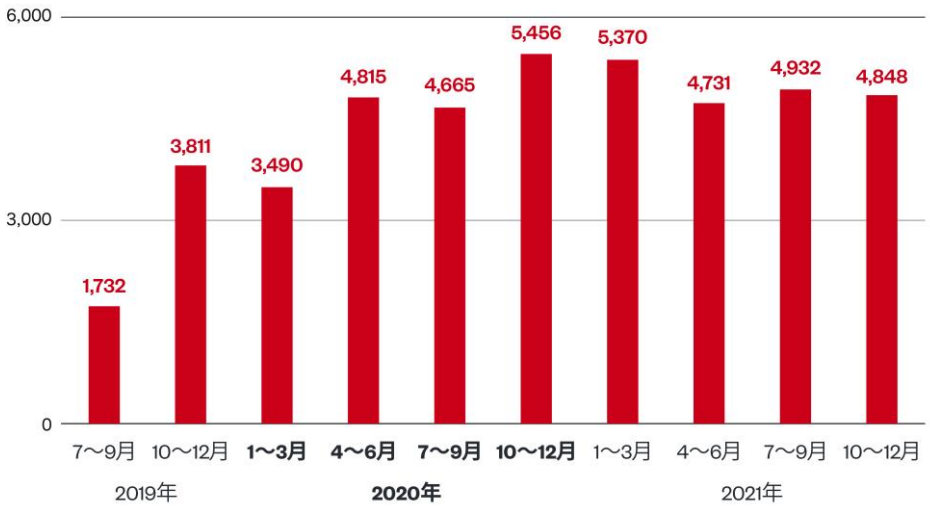


図 2：日本国内でのランサムウェア検出台数推移

2021 年の 1 年間にトレンドマイクロがインシデント対応支援を行ったランサムウェア被害においては、ほぼすべてが「Human-Operated」型のランサムウェア攻撃でした。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[12]」、「侵入型ランサムウェア攻撃[13]」などと呼ばれるこの攻撃手法は、被害組織のネットワークに侵入し、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。このような攻撃手法はこれまで高度な標的型攻撃で見られてきたものであり、高度な攻撃手法の一般化、サイバー犯罪化と言えます。

国内の被害事例で原因として確認できたランサムウェア種類としては「Cring[14]」と「LockBit[15]」が目立ち、2021 年にインシデント対応支援を行ったランサムウェア被害事例のうち 6 割近くを占めました。調査から確認できた主なネットワークへの侵入手法は、VPN、RDP などの外部からのアクセス口に対し、事前に奪取した認証情報の使用もしくは総当たり攻撃などによるアカウントハッキングによるものであり、逆に従来見られていたようなメール経由での侵入が断定できたものはありませんでした。このことから、ランサムウェア攻撃の侵入手法はインターネットからの直接侵入にシフトしているのが実態と言えます。

またネットワーク侵入後に行われる内部活動としては、管理者権限の掌握、Active Directory（AD）サーバの侵害やグループポリシーの悪用、ファイル共有や RDP 機能の悪用による横展開、セキュリティ製品の無効化・アンインストール、バックアップや自動修復機能の無効化といった手口が実事例の中で確認できました。また、「二重脅迫」手法により、窃取された情報を実際に暴露されていた事例も見られました。

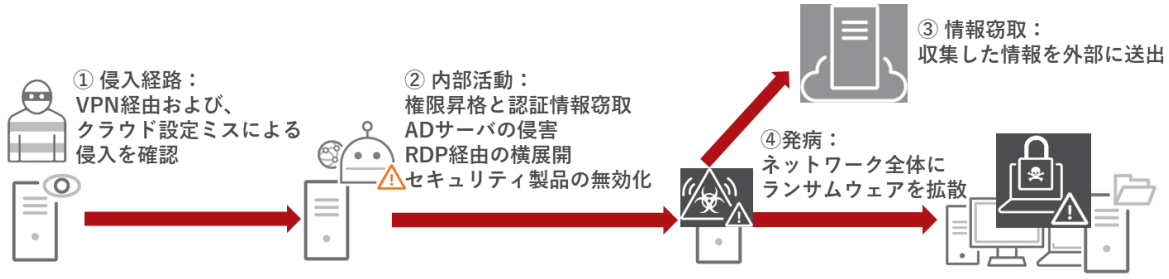


図 3：2021 年に行ったインシデント対応で確認した「ランサムウェア攻撃」の概要図

このようなランサムウェア攻撃は社会生活に影響のある業界に被害を与えています。2021 年にランサムウェア被害が公表・報道された法人組織 53 件についてその業種を確認したところ、官公庁・自治体が全体の 3 割と最も多く、製造業、サービス業、卸・小売業がそれに続く結果となりました。

[12] https://www.ipa.go.jp/security/announce/2020-ransom.html
[13] https://www.jpcert.or.jp/magazine/security/ransom-faq.html
[14] https://blog.trendmicro.co.jp/archives/27830
[15] https://blog.trendmicro.co.jp/archives/28572

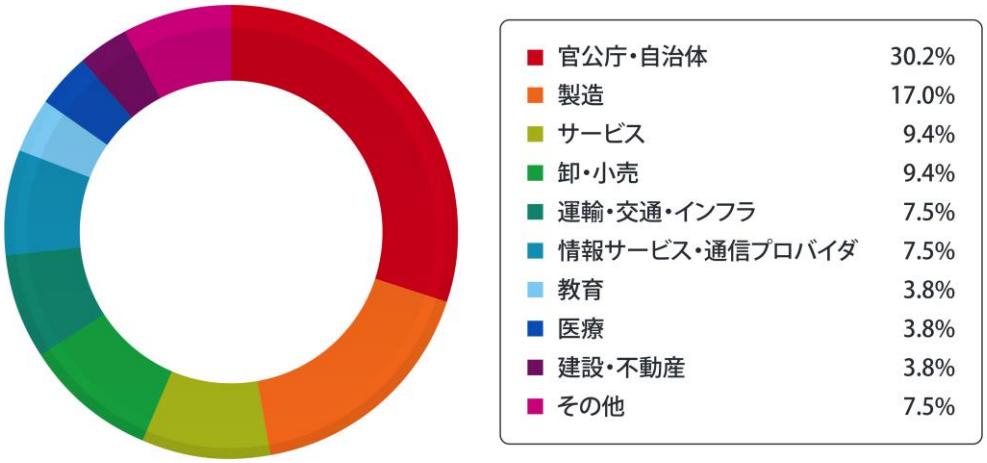
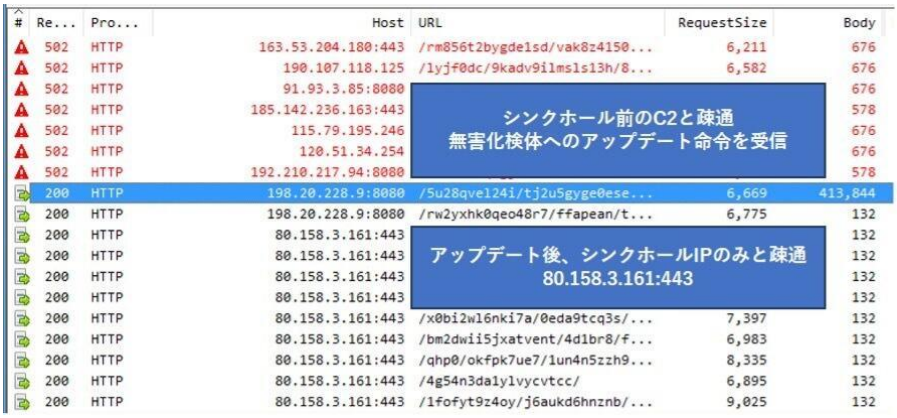


図 4：2021 年に公表・報道された法人組織 53 件における業種割合（公開情報を整理）

これらの事例において公表された被害原因としては、VPN の脆弱性対応が不十分であったり、いわゆる仮想プライベートクラウド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りなど、境界線上の「弱点」が存在していたケースが目立っています。このような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。また侵入を前提とした対策として、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、侵入後の内部活動を自由にさせないゼロトラストに則った対策などが不可欠となりつつあります。

最大のメール経由脅威「EMOTET」のテイクダウンと復活

2021 年 1 月 27 日、「史上最恐のマルウェア」とまで呼ばれた「EMOTET」のテイクダウンが発表[16]されました。このテイクダウンはユーロポール（欧州警察刑事機構）を中心とした各国法執行機関の連携によって行われました。このテイクダウンでは、既に世界中に拡散している EMOTET を一掃するため、掌握した遠隔操作サーバ（C&C サーバ）から EMOTET 自身を無害化検体で置き換える指令を送るようにしました。EMOTET と置き換わった無害化検体は、当局が用意したシンクホールサーバとのみ通信を行い、2021 年 4 月 25 日に自身をアンインストールして消滅しました。



#	Re...	Pro...	Host	URL	RequestSize	Body
	502	HTTP	163.53.204.180:443	/rm856t2bygde1sd/vak8z4150...	6,211	676
	502	HTTP	190.107.118.125	/1yjf0dc/9kadv9ilmsls13h/8...	6,582	676
	502	HTTP	91.93.3.85:8080			676
	502	HTTP	185.142.236.163:443			578
	502	HTTP	115.79.195.246			676
	502	HTTP	120.51.34.254			676
	502	HTTP	192.210.217.94:8080			578
	200	HTTP	198.20.228.9:8080	/5u28qve124i/tj2u5gyge0ese...	6,669	413,844
	200	HTTP	198.20.228.9:8080	/rw2yxhk0qeo48r7/ffapean/t...	6,775	132
	200	HTTP	80.158.3.161:443			132
	200	HTTP	80.158.3.161:443			132
	200	HTTP	80.158.3.161:443			132
	200	HTTP	80.158.3.161:443			132
	200	HTTP	80.158.3.161:443	/x0bi2wl6nki7a/0eda9tcq3s/...	7,397	132
	200	HTTP	80.158.3.161:443	/bm2dwii5jxatvent/4d1br8/f...	6,983	132
	200	HTTP	80.158.3.161:443	/qhp0/okfpk7ue7/1un4n5zzh9...	8,335	132
	200	HTTP	80.158.3.161:443	/4g54n3da1ylvycvtcc/	6,895	132
	200	HTTP	80.158.3.161:443	/1fofyt9z4oy/j6aukd6hnznb/...	9,025	132

図 5：テイクダウン後に確認した EMOTET の通信例：
実行された EMOTET 検体が C&C サーバに接続すると無害化検体に更新され、
その後はシンクホール IP への接続のみが行われるようになることを確認

EMOTET のテイクダウン後、国内では「Lokibot」、「AgentTesla」、「Qakbot（QBOT）」、「BazarLoader（BazarCall）」、「Trickbot」、「FormBook/XLoader」、「WarzoneRat」など、様々なマルウェアに感染させるためのマルウェアスパムが拡散しましたが、いずれも EMOTET ほどの大規模な拡散には至りませんでした。そして、テイクダウンが公表されてから 10 か月に満たない 2021 年 11 月中旬、EMOTET は復活しました。既存の EMOTET のボットネットはすべて無害化されていたため、復活の初期段階では別のボットである Trickbot が EMOTET のダウンロードを行ったことがわかっています。Trickbot は以前、EMOTET からダウンロードされる別のマルウェアの 1 つとして知られていましたが、その逆パターンで Trickbot が EMOTET の復活を助けたことになります。

Trickbot 経由でボットネットを再構築した EMOTET は、すぐに C&C サーバの再稼働と共にマルウェアスパムの送信などが確認されました。トレンドマイクロ SPN の統計によれば、活動再開翌月の 12 月の段階で検出台数が急増しており、特に EMOTET の本体の検出は前月

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

比で 16 倍となりました。統計データの意味として、検出の総数はマルウェアスパムがばらまかれた規模を表しており、本体の検出はばらまかれたマルウェアスパムからダウンローダを開いてしまったことを表すものと言えます。その後の観測では、2022 年に入っても検出台数の増加は続いており、EMOTET は活動再開後すぐに、ほぼテイクダウン前の状況に戻ったと言える状態です。

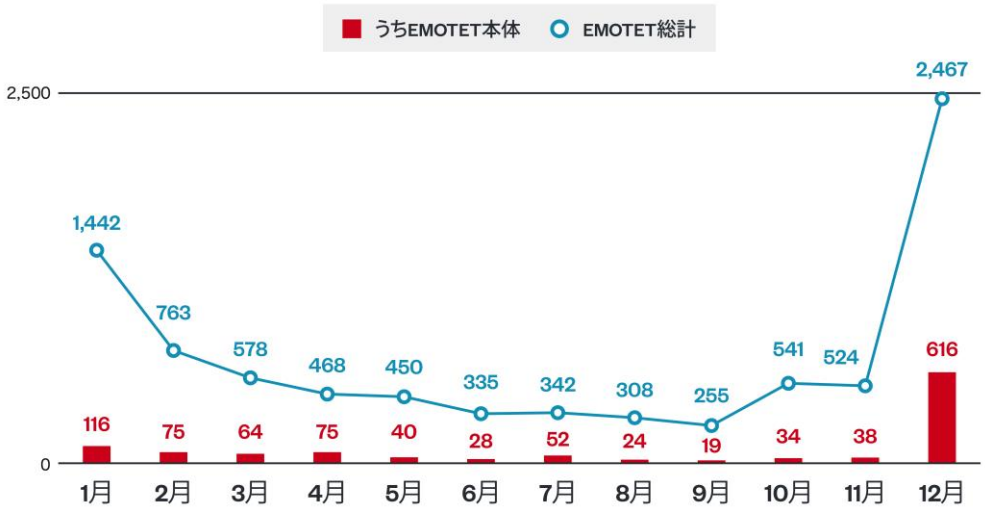


図 6：国内における EMOTET 検出台数推移

テイクダウン前も復活後も、表面上の EMOTET の活動内容はほとんど変っていません。主な拡散経路は EMOTET 自身のボットネットから送信したマルウェアスパムです。

図 7：EMOTET を感染させるマルウェアスパムメールの例（2021 年 12 月確認）
以前のメールへの返信と誤解させるような日本語文章が見られる

マルウェアスパムの宛先、送信元アドレス、本文などとして、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します。このため、受信者にとって以前にやり取りしたことのある送信元情報やメール本文である可能性があり、誤ってメールを開いてしまうことに繋がります。また Web ブラウザに保存されているパスワードなどの情報も窃取するため、ブラウザから利用したクラウドメールや Web サービスに不正アクセスが発生する危険性もあります。マルウェアスパムには主に不正マクロを含む Office 文書ファイルが添付されます。このダウンローダである不正文書ファイルを開き、マクロを有効化すると EMOTET 本体がダウンロードされ、感染します。

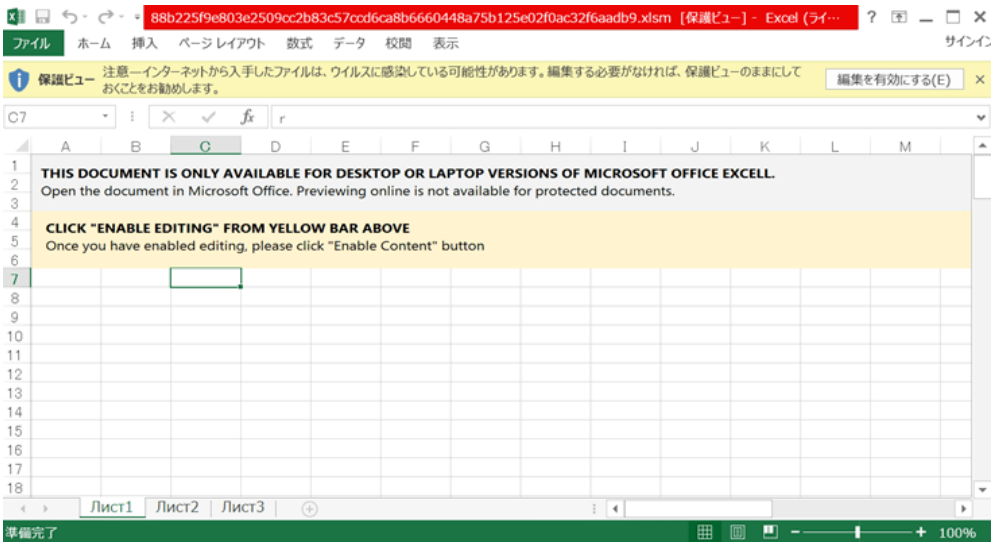


図 9：EMOTET の不正マクロを含んだ Excel 文書ファイル例（2021 年 12 月確認）

図 10：EMOTET の不正マクロを含んだ Word 文書ファイル例（2021 年 11 月確認）

また活動再開後の 12 月に確認された新たな手口として、Microsoft の正規インストーラである Windows App Installer を悪用するケースも確認されました。このケースでは本文中の URL リンクから誘導される不正サイト上で、当時ゼロデイであった Windows App Installer の脆弱性「CVE-2021-43890[17]」により、あたかも Adobe 社正規の PDF コンポーネントであるかのように偽装する手口が使われました。Microsoft は 2021 年 12 月 14 日公開の更新プログラム[18]により一旦この脆弱性に対処したのち、2022 年 2 月に Windows App Installer の MSIX プロトコルを無効化する対応[19]も行っています。

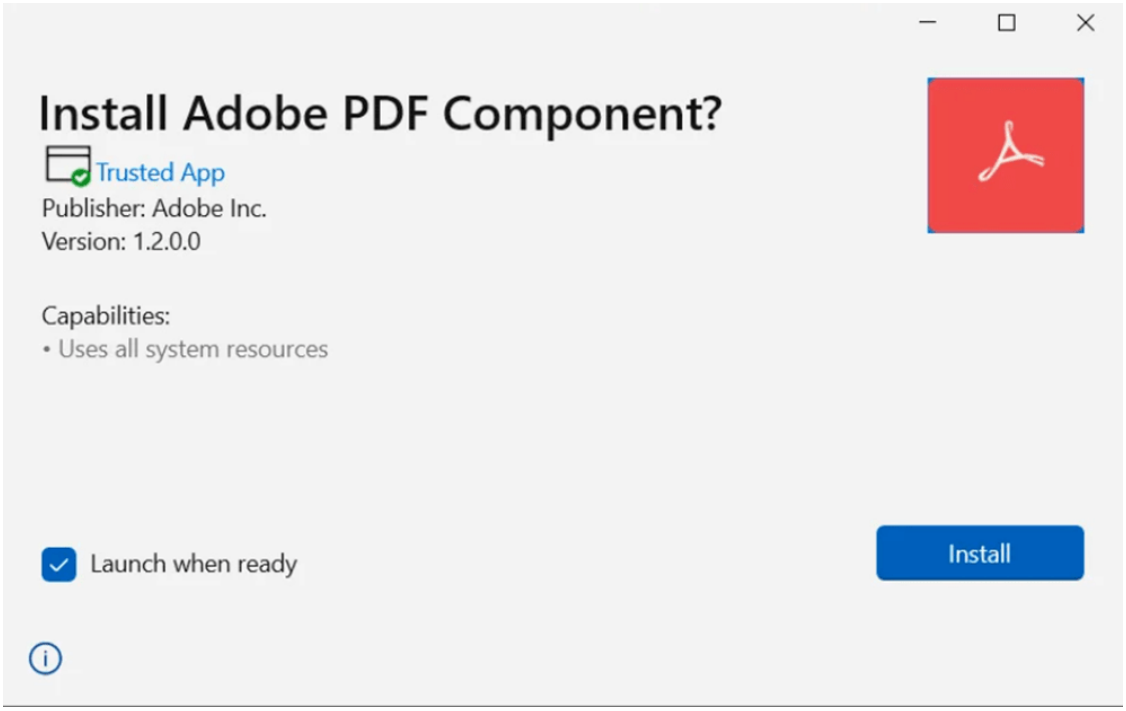


図 8：EMOTET を感染させる Windows App Installer の表示例（2021 年 12 月確認）
脆弱性の利用により、Adobe 社の正規コンポーネントを偽装

このように EMOTET はその時々で使用可能な脆弱性も含めて様々な新たな手口を試行してくる場合があります。常套手段化している不正マクロを含む Office 文書ファイルについても、直接添付、パスワード付き圧縮ファイル、本文内の URL からのダウンロード、PDF 内の URL からのダウンロードなどの手段を変化させながら繰り返し使用しています。本項執筆時点の 2022 年 3 月までの段階では、ダウンローダの不正文書ファイルを添付（直接もしくはパスワード付き圧縮ファイル内に格納）する例が特に多く見られていますが、１つの手

[17] https://jvndb.jvn.jp/ja/contents/2021/JVNDB-2021-006059.html
[18] https://msrc-blog.microsoft.com/2021/12/14/202112-security-updates/
[19] https://techcommunity.microsoft.com/t5/windows-it-pro-blog/disabling-the-msix-ms-appinstaller-protocol-handler/ba-p/3119479

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してください。

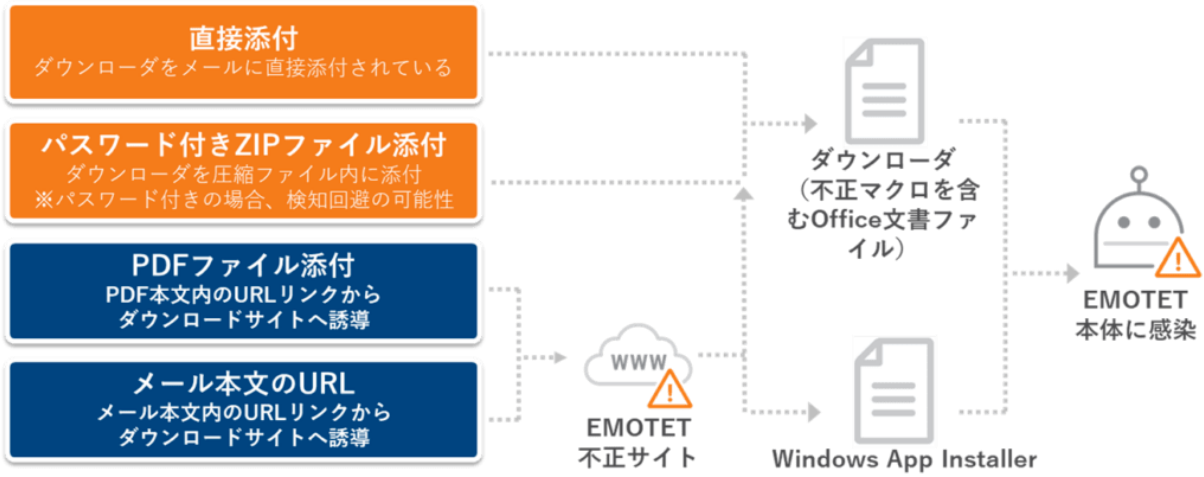


図 11：マルウェアスパムから EMOTET を感染させる手口の概念図

一度は既存のボットネットが壊滅状態となったにも関わらず、EMOTET は復活しました。このことは、背後のサイバー犯罪者の逮捕、拘束が十分でなかったことを示しています。サイバー犯罪の根本解決のためには、C&C サーバなどのインフラのテイクダウンだけでは足りず、中心人物をどれだけ逮捕・拘束できるかが重要です。今回の EMOTET のテイクダウンは、結果的に元に戻ってしまった感はあります。しかし国を越えてテイクダウンを実現したユーロポールはじめとする各国法執行機関の協働については、これまでにない素晴らしい成果と言え、実際、その後には「Netwalker[20]」、「Egregor[21]」、「Clop[22]」、「REvil（別名：Sodinokibi）[23]」といったランサムウェアギャングの逮捕が続いています。トレンドマイクロでは、このようなサイバー犯罪の根本解決を目指す取り組みに協力してまいります。

[20] https://krebsonsecurity.com/2021/01/arrest-seizures-tied-to-netwalker-ransomware/
[21] https://www.zdnet.com/article/egregor-ransomware-operators-arrested-in-ukraine/
[22] https://www.bleepingcomputer.com/news/security/ukraine-arrests-clop-ransomware-gang-members-seizes-servers/
[23] https://www.europol.europa.eu/media-press/newsroom/news/five-affiliates-to-sodinokibi/revil-unplugged

広く一般の利用者を脅かす「詐欺」手法による攻撃

コロナ禍におけるコミュニケーション手段としてインターネットの需要が高まる中、広く一般のインターネット利用者を狙う攻撃の中で、詐欺手法が拡大しています。利用者を騙して操る詐欺手法はこれまでもサイバー犯罪における常套手段であり続けてきましたが、2021年を通じてその傾向が顕著化しているものと言えます。一例として、国内におけるフィッシングを含む各種詐欺サイトへの誘導は 2020 年以降拡大の一途を辿り、2021 年第 1 四半期に初めて 1000 万件を超えて以降、第 2 四半期には 1200 万件を、第 4 四半期には 1400 万件を超えるなど、過去最大を更新し続けています。

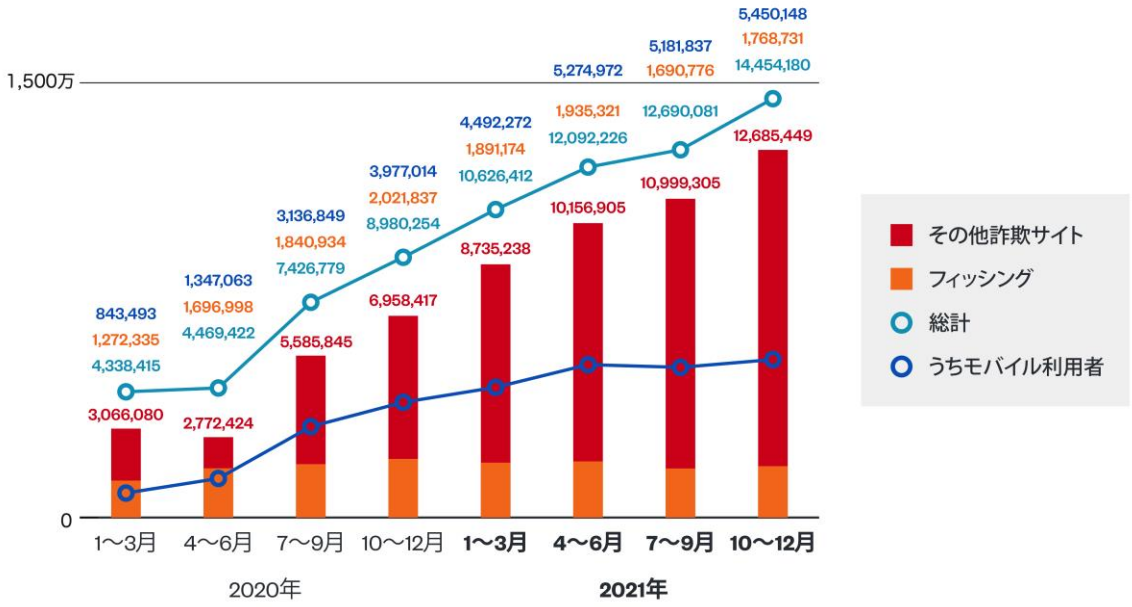


図 12：国内から各種詐欺サイトに誘導された利用者の端末台数[24]推移と内訳

誘導先となるフィッシングを含む詐欺サイトの内容としては、銀行など金融機関やクレジットカード関連の偽サイトの他、モバイル決済、暗号資産取引所、生命保険、携帯電話キャリア、SNS やポータルサイト、ネットショッピング/オークションサイト、給付金・ワクチンなどコロナ禍関連、水道など公共料金支払いなどの偽サイトまで、多岐に及んでいます。

[24] 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

図 13：新型コロナワクチン接種の予約サイトを偽装したフィッシングサイトの例
個人情報と共にクレジットカード情報を詐取する

図 14：定額給付金申請サイトを偽装したフィッシングサイトの例
運転免許所やパスポートなど本人確認書類のスキャン画像をアップロードさせる手口

図 15：生命保険会社を偽装したフィッシングサイトの例（2021 年 12 月確認）

これらの詐欺サイトは、いずれも金銭の詐取を最終的な目的とするものと言えます。多くはクレジットカード情報と、その不正利用に必要な本人確認を突破するための個人情報を詐取するものです。また、ネットバンキングやキャリア決済などの顧客向け Web サービスの認証情報も標的となっており、詐取した認証情報などを使ってサービスにアクセスし、不正な送金や決済を行います。特徴的な事例としては、生命保険会社の顧客専用サイトへの不正アクセスから契約者貸付の手続きを行い、金銭を詐取した被害も確認[25]されています。このようなサービスの不正利用のために必要な認証の突破手法としては、騙された被害者が情報を入力するのと同時にその裏で本物のサービスへの不正アクセスを試行する「リアルタイムフィッシング」の手口も複数確認しています。

図 16：暗号資産取引所を偽装したフィッシングサイトの例（2021 年 3 月確認）
電子メールで送信される確認コードを入力させ突破するリアルタイムフィッシング手口

図 17：銀行を偽装したフィッシングサイトの例（2021 年 2 月確認）
アプリや専用端末上で表示されるワンタイムパスワードを
入力させ突破するリアルタイムフィッシング手口

[25] https://www.meijiyasuda.co.jp/profile/news/topics/attention2.html

各種詐欺サイトへ誘導される利用者の中で、モバイル利用者の割合も増えています。「迷惑メール」や「フィッシングメール」といった言葉があるように、このような各種詐欺サイトへの誘導は不正な電子メールが中心となっていました。これに加え、新たな誘導手段として定着してしまったのが、携帯電話のテキストメッセージ機能である SMS です。SMS 経由での誘導は「スミッシング（SMS＋Phishing）」という用語が定義されていますが、SMS は携帯電話特有の機能であり、スミッシングの増加はサイバー犯罪者がより明確にスマートフォン利用者を攻撃対象としていることを示す傾向と言えます。

図 18：会費支払いの話題を偽装した SMS の例（2021 年 5 月確認）

図 19：宅配便からの通知を偽装した SMS の例（2021 年 2 月確認）

図 20：宅配便業者の通知を偽装した SMS から誘導される不正サイトの例
Android 向け不正アプリをインストールさせる目的

このようなスミッシング事例では、Android 端末からのアクセスの場合は不正アプリのインストール、iPhone からのアクセスの場合はフィッシングサイトへ誘導する事例が多く確認されていました。これに加え、2021 年 9 月には iPhone に対しても不正アプリをインストールさせる事例を確認[26]しています。この事例では、iOS の設定を自動化する機能である構成プロファイル（プロビジョニングプロファイル）の悪用により制限を回避し、不正アプリ「TianySpy」をインストールさせていました。このような構成プロファイルを悪用する手口は 2014 年頃から懸念[27]されていました。海外では 2017 年にリパックアプリをインストール可能にするサードパーティマーケットの事例[28]が確認されていますが、国内で実際の不正アプリの感染に悪用された事例は、これが初めてと言えます。iPhone は標準では正規のアプリマーケットである「App Store」経由でないアプリはインストールできないため、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、今後はその認識を改めていく必要がありそうです。

図 21：iPhone に不正アプリをインストールさせる不正サイトの遷移例
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
（2021 年 9 月確認）

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）」が 2021 年 2 月前後から日本においても見られています。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、正規のセキュリティソフト購入サイトへ誘導されますが、これはアフィリエイトによる金銭利益を狙ったものと考えられます。

[26] https://blog.trendmicro.co.jp/archives/29322
[27] https://blog.trendmicro.co.jp/archives/10497
[28] https://blog.trendmicro.co.jp/archives/16343

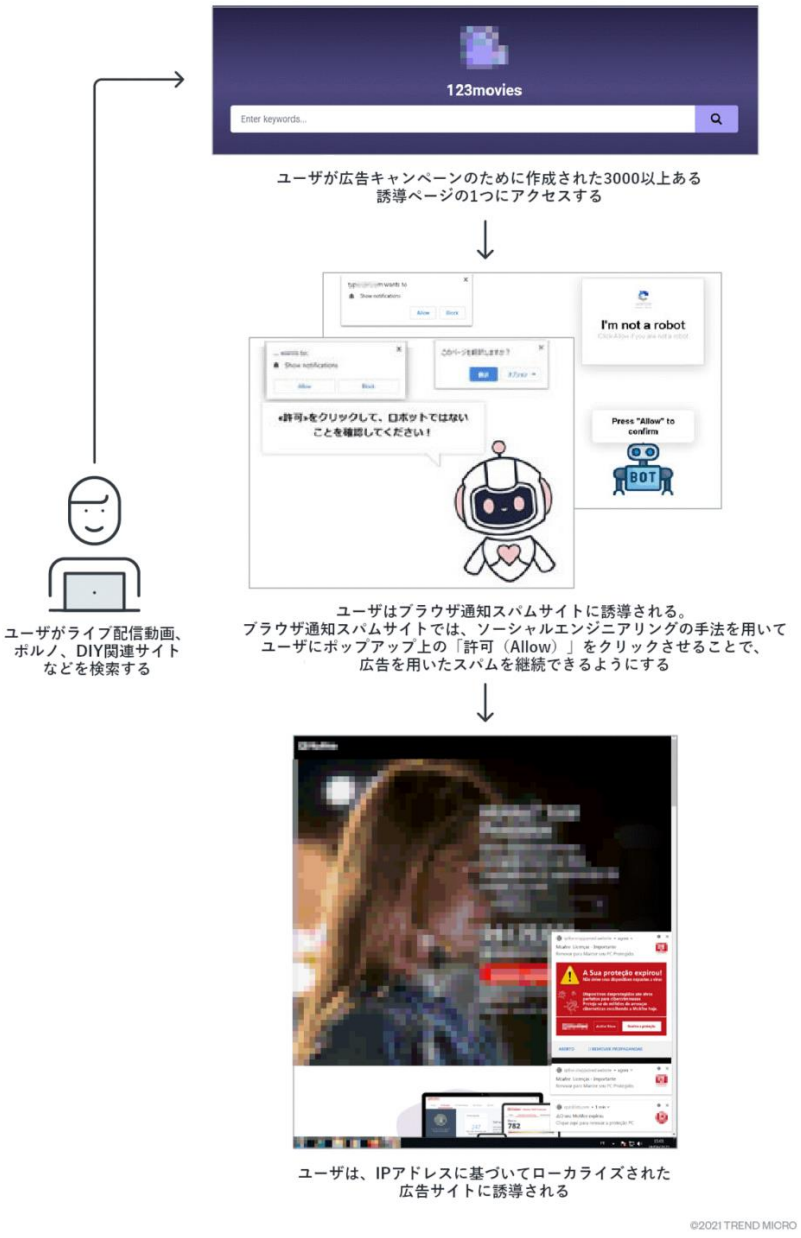


図 22：「ブラウザ通知スパム」手口の概念図

また、いわゆる「サポート詐欺」のサイトへ誘導される事例も確認しています。サポート詐欺は PC のシステム不調やセキュリティ問題、ウイルス感染などの理由で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手口であり、より直接的に利用者に金銭被害を与えるものです。

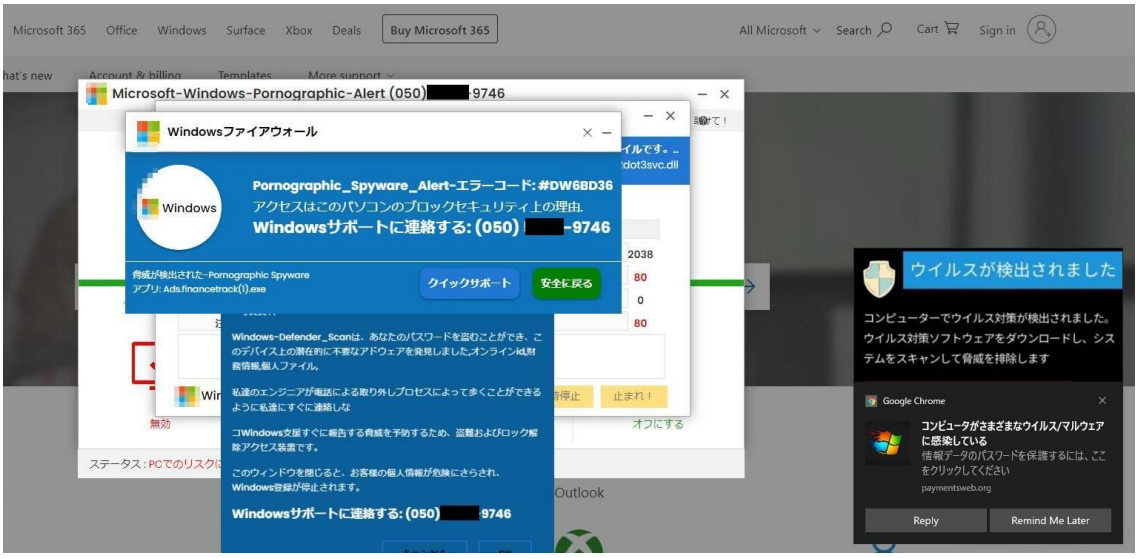


図 23：「ブラウザ通知スパム」からサポート詐欺サイトへ誘導される例

このように、広く一般のインターネット利用者を狙う攻撃はほぼすべてが詐欺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重要となってきています。

グローバルセキュリティラウンドアップ

基幹産業を狙う最新型ランサムウェア

クラウド環境への脅威とクラウド利用者とリモートワーカーへの対応

強化された武器でより大きな獲物を狙う標的型攻撃

脆弱性の増加に伴うパッチ未適用のリスク

リモートワーカーを狙う新型コロナウイルス便乗の脅威

巧妙化する脅威への対策に必要な強固かつ多層的な防御

2021 年年間の脅威概況

基幹産業を狙う最新型ランサムウェア

ここ数年、トレンドマイクロでは、ランサムウェアがどのように大きく進化してきたかを観察してきました。2018 年、攻撃者の間では、できるだけ多くの被害者から利益を得ようとする無差別攻撃的な戦略[29]が主流でした。そうした中、トレンドマイクロのリサーチャーは、ランサムウェア攻撃の傾向が量から質へ移行[30]することを予測していました。特に 2021 年、ランサムウェアの攻撃者は、より収益性の高いターゲットに狙いを定めてきました。これより今後、ランサムウェアの被害は、世界規模での企業や組織へ混乱[31]をもたらすことが予想されます。

世界的な新型コロナウイルスの流行により疲弊していた医療機関は、2021 年、ランサムウェアの攻撃によって大きな打撃を受け、ランサムウェアの検出台数では、銀行や政府機関に迫る件数となっています。ヘルスケア業界の医療機関は、他の業界に比べてデータのバックアップを取ることが少ないため、ランサムウェアの攻撃者からの身代金支払いの要求に応じやすいとも指摘[32]されています。さらにヘルスケア業界は、社会保障番号、病歴、財務情報が記載された患者記録など、アンダーグラウンド市場での販売やランサムウェアの恐喝などに利用可能なデータの宝庫でもあります[33]。

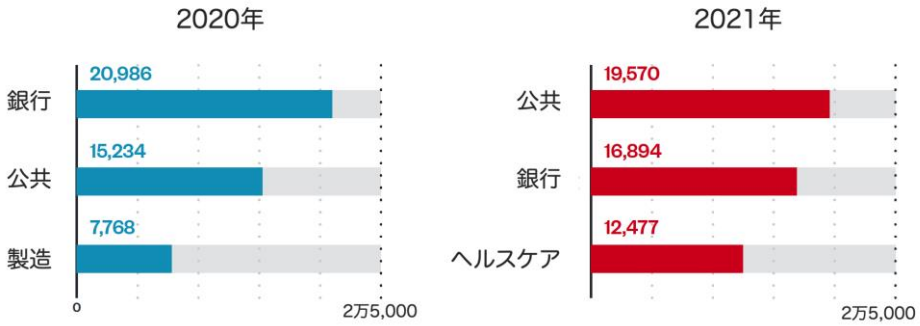


図 1：ランサムウェア検出台数の業界別トップ 3（全世界）

WannaCry の検出台数は、トップ 3 の業界すべてにおいて第 1 位となっており、他のランサムウェアファミリーを大きく引き離しています。WannaCry のような従来型ランサムウェアの場合、無差別攻撃の手法を採用しているため、量的に顕著な傾向を示していますが、一方で注目すべきは、最新のランサムウェアが台頭してきた点です。

[29] https://newsroom.trendmicro.com/2018-08-28-Trend-Micro-Report-Reveals-Criminals-Increasingly-Drawn-To-Low-Profile-Attacks
[30] https://www.trendmicro.com/en_us/research/18/a/digital-extortion-forward-looking-view.html
[31] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/modern-ransomwares-double-extortion-tactics-and-how-to-protect-enterprises-against-them
[32] https://news.sophos.com/en-us/2021/05/17/the-state-of-ransomware-in-healthcare-2021
[33] https://www.weforum.org/agenda/2021/11/healthcare-cybersecurity

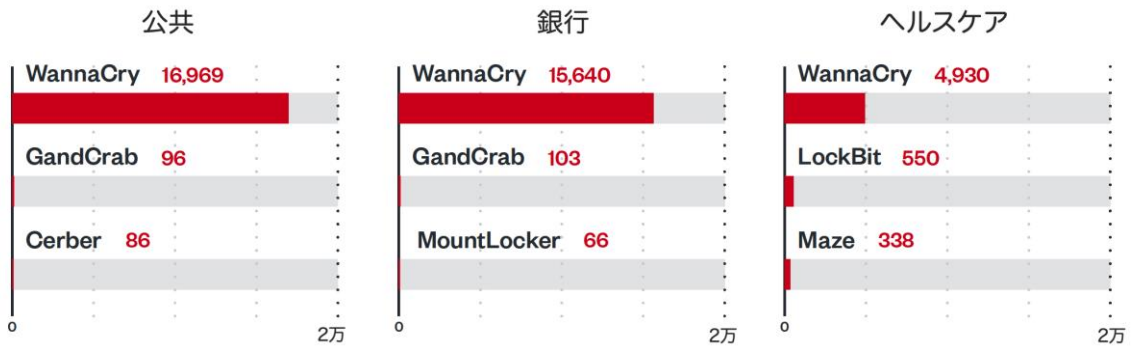


図 2：業界別検出ランサムウェアファミリーのトップ 3（全世界）

従来型のランサムウェアとは異なり、最新型のランサムウェアグループは、広範囲に攻撃を行うのではなく[34]、特定のターゲットに絞った戦略を取るため、一見すると不規則な動きを示す傾向があります。こうした点が、2021 年のランサムウェア攻撃総数における 21%減少の理由とも言えます。そうした中、2021 年、いくつかの最新型ランサムウェアファミリーは検出台数からも活動活発化の傾向が見て取れます。例えば、REvil（別名：Sodinokibi）の検出台数は、前年比 143%増、LockBit の検出台数は 2020 年から 2021 年にかけて 20 倍以上増加し、さらに Conti の検出台数は前年比 9 倍以上と、最新型ランサムウェアファミリーの活発化が顕著となっています。

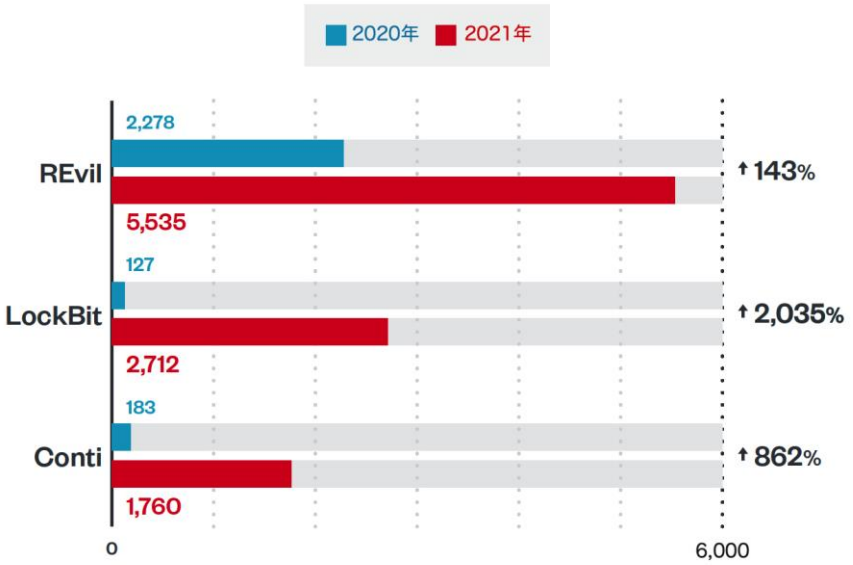


図 3：主な最新型ランサムウェアファミリーの検出台数推移（全世界）

[34] https://www.trendmicro.com/vinfo/us/security/news/ransomware-by-the-numbers/examining-erratic-modern-ransomwareactivities-ransomware-in-q3-2021

また、ランサムウェア攻撃総数が減少した要因として、商用ペネトレーションツール「Cobalt Strike」内のモジュールである「CoBeacon」、ボット型マルウェア「Trickbot」、情報窃取型マルウェア「BazarLoader」など、攻撃ツールの検出とブロックが増加したことも考えられます。これらのツールは、攻撃活動の初期段階で検出されることから、これらの関連ツールが大量にブロックされたことで、ランサムウェアの本格的な攻撃活動を早い段階で阻止した可能性もあります。2021 年、DoppelPaymer、PovIsomware、Ryuk[35]などのランサムウェアファミリーが確認される中、これらの攻撃で悪用された CoBeacon の検出台数も 8 倍増加しました。同様にランサムウェア Ryuk[36]や Conti[37]の感染に繋がるとされる Trickbot の検出台数も前年比 23%増となっていました。中でも顕著な例は、Conti[38]や Ryuk[39]などに攻撃の初期段階で使用された BazarLoader の検出台数が前年比 2,468%増となったことでしょう。

最新型ランサムウェアの場合、より多くの人々が関与するなど、サイバー犯罪者間の共同作業がアンダーグラウンド市場でも人気を集め、この傾向は、サービスとしてのランサムウェア（RaaS）の増加としても表れています。RaaS のアフィリエイトプログラムは、関係するすべてのサイバー犯罪者にとって有益なものとなります。例えば、ランサムウェアの攻撃者は、他のパートナーとの協力によって作業を分担することで、高度な攻撃を展開して効率的に利益を得ることができます。また、RaaS が普及したことで、技術的知識の乏しい攻撃者でもランサムウェアを駆使できるようになっただけでなく、いわゆるサイバー犯罪市場のエコシステムの中で、各担当部門が高い専門性が生み出すことが可能となりました。RaaS を展開する複数の関連企業が、それぞれの専門分野で作業を分担し、スキルを磨き、ネットワークへの侵入やマルウェアの実行など、特定の専門分野に集中することが可能となったのです[40]。

さらに RaaS の普及は、「サービスとしてのサイバー犯罪」を扱う市場全体の継続的な発展の結果でもあり、多くの事業者が、この市場原理の下、攻撃者というユーザのための新しいビジネスモデルを開発し続けています。これらの事業者は、アクセスのサービスを提供し、認証情報をアンダーグラウンド市場で売りさばき、ランサムウェアの攻撃者の中か

[35] https://www.trendmicro.com/en_us/research/21/g/tracking_cobalt_strike_a_vision_one_investigation.html
[36] https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-conti
[37] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ryuk-2020-distributing-ransomware-via-trickbot-and-bazarloader
[38] https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-conti
[39] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ryuk-2020-distributing-ransomware-via-trickbot-and-bazarloader
[40] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-as-a-service-enabler-of-widespread-attacks

らお得意様を見出し、各種の製品やサービスを駆使するなど、さまざまな形で協業し、対象の端末へ感染被害を及ぼすのです[41]。

ランサムウェアの攻撃では、近年、暗号化されたファイルの復号を条件に被害者へ身代金を要求するだけでなく、支払わない場合は機密情報を暴露するという脅迫も合わせた「二重恐喝」の手法が拡大しています。この手法は、2019 年にランサムウェア Maze によって初めて実行され、その後、さらに広く使用されるようになりました。2021 年 6 月の時点でトレンドマイクロでは、35 件のランサムウェアファミリーがこの手法が用いていたことを確認していました。特に REvil や Conti など、RaaS と二重恐喝の双方の手口を駆使して、大手企業を狙った攻撃[42]を展開していました。

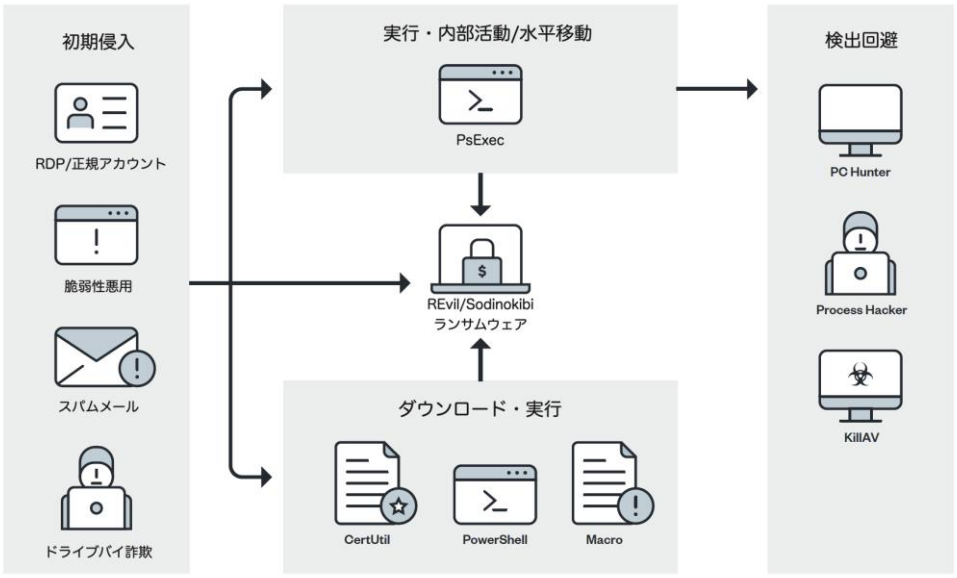


図 4：REvil の感染フロー

2019 年に Cisco 社のリサーチグループ Talos によって確認されて以来、REvil は、最も活発な RaaS 利用のランサムウェアファミリーの 1 つとして知られています[43]。2021 年には、Apple 社[44]、JBS 社[45]、Kaseya 社[46]などの多国籍企業に対して二重恐喝の手口を用いること

[41] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/investigating-the-emerging-access-as-a-service-market
[42] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-double-extortion-and-beyond-revil-clop-and-conti
[43] https://blog.talosintelligence.com/2019/04/sodinokibi-ransomware-exploits-weblogic.html
[44] https://www.crn.com/news/security/apple-menaced-after-revil-ransomware-attack-against-supplier
[45] https://www.npr.org/2021/06/03/1002819883/revil-a-notorious-ransomware-gang-was-behind-jbs-cyberattack-the-fbi-says
[46] https://edition.cnn.com/2021/07/02/tech/ransomware-cybersecurity-attack-kaseya/index.html

で、大きな効果を上げています。REvil の攻撃の大部分は米国で行われましたが、メキシコやドイツなどでも被害事例が報告されています。

トレンドマイクロの観測データによると、REvil は、基幹産業を狙った攻撃を展開していました。その多くは運輸業、次いで金融、石油・ガスなどの業界の企業が攻撃対象となっていました。2021 年上半期のランサムウェアに関するレポートでは、運輸業は、グローバルなサプライチェーンと物流において重要な役割を担っていることから、REvil による攻撃の格好の標的となったと推測しています[47]。

REvil では、巧妙にカスタマイズ化された攻撃も確認され、標的の企業や組織における IT 環境について攻撃者が精通したケースが多かったことも示唆されます。また、REvil の巧妙さは、その多様なツールや脆弱性の悪用にも起因しています。例えば、Qakbot、AdFind、BloodHound といったサードパーティ製同期ツールの使用、Kaseya VSA サーバに影響を与える脆弱性「CVE-2021-30116」、Oracle WebLogic のデシリアライズ脆弱性「CVE-2019-2725」、FortiGate SSL VPN の脆弱性「CVE-2018-13379」、Pulse Secure SSL VPN の脆弱性「CVE-2019-11510」などを突いた手法など、攻撃手法は多岐に及びました[48]。

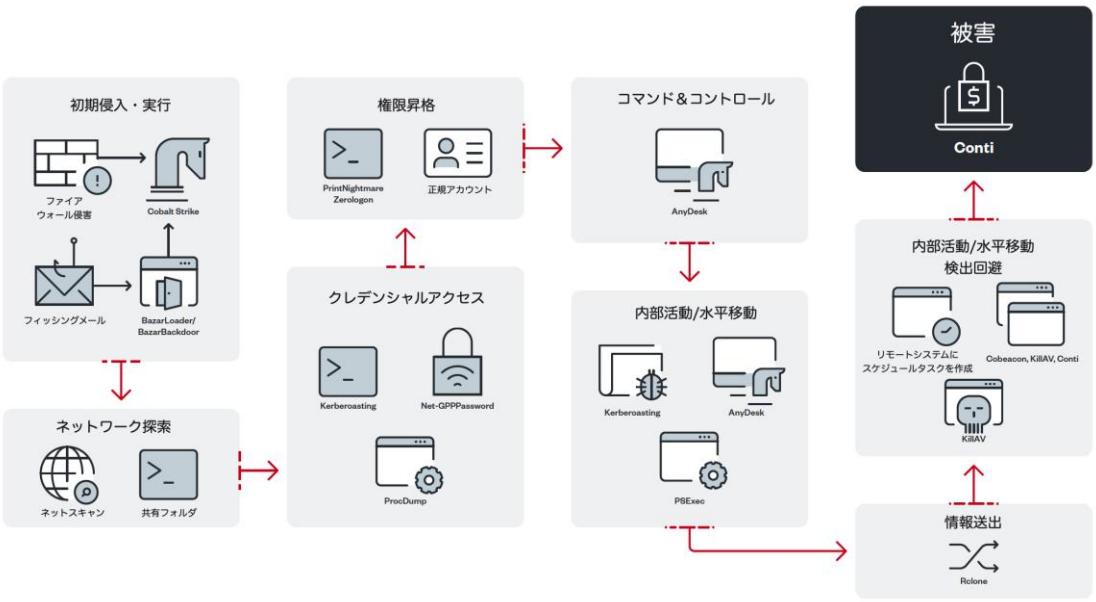


図 5：Conti の感染フロー

また、Ryuk の後継として名高いランサムウェア Conti の場合は、同じく RaaS が駆使され、2021 年に世界中で確認された多数の攻撃に関連したと言われています[49]。米国だけで

[47] https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-revil
[48] https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-revil
[49] https://www.trendmicro.com/en_us/research/21/c/vision-one-tracking-conti-ransomware.html

も、2021 年 1 月 1 日から 11 月 12 日にかけて 100 万件以上の Conti 攻撃数が確認されています[50]。「2021 年上半期セキュリティラウンドアップ」で述べたように、この最新型ランサムウェアファミリーは、2021 年上半期の検出台数のランキングでは第 10 位とランクインしていました[51]。検出台数の大部分は米国で確認され、オランダと台湾がそれに続きました。業界別では、小売業の企業が最も多くの Conti 攻撃を経験しました。保険、製造、通信も大きな被害を受けましたが、特に 2021 年は、医療機関に対する攻撃が大きな話題となりました[52]。

また、Conti の攻撃者は、REvil のケースと同様、被害者が身代金を支払わない場合、窃取した情報を暴露してアクセス権限を売りつけると脅す「二重恐喝」の手口を用いていました。さらに、PrintNightmare や Zerologon といった脆弱性、BazarLoader、Cobalt Strike、Mimikatz、Rclone といったツールなど、さまざまな手法を駆使していました。これらのツールを活用することで、攻撃者は、標的となる端末へのリモートアクセス、セキュリティソフトウェアの無効化、機密情報の送出、身代金要求のためのファイルの暗号化など、さまざまな不正活動が実行できます。

[50] https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-conti
[51] https://www.trendmicro.com/en_us/ciso/21/i/cyberattacks-from-all-angles-2021-midyear-report.html
[52] https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-conti

クラウドの脅威：設定ミスと詐欺メール

2021 年上半期のサイバーリスクインデックスによると、クラウドセキュリティへの脅威は、2021 年、企業や組織にとって最も緊急な IT インフラリスクの 1 つでした[53]。クラウドアーキテクチャを構成する多くの技術は、定期的に新機能が更新されるため、企業や組織にとって保守は困難な課題となっています[54]。こうした複雑さに加え、セキュリティ担当者は攻撃者がクラウドを狙うために使用するツールの変化にも常に対応しなければなりません。例えば、2019 年、ステガノグラフィ（画像内にコードを隠す手法）がクラウドを狙う攻撃のトレンドとなりました[55]。その翌年には、攻撃の展開後にマルウェアを感染端末にダウンロードするクリーンなイメージが使用されるようになりました。そして「2021 年上半期セキュリティラウンドアップ」で詳述されたとおり、2021 年には、不正なコンテンツを含む画像を使用する手法に回帰しました[56]。

クラウドの設定ミスを突く脅威

クラウド技術は、多くの企業や組織におけるデジタルトランスフォーメーションを加速させ、新型コロナウイルスの流行に伴うリモートワーク導入をサポートしました。調査機関「International Data Corporation」[57]によると、クラウドコンピューティングやストレージソリューションを含むクラウドインフラへの支出は、2021 年第 3 四半期には、前年同期比 6.6%増の 186 億米ドルとなり、2021 年を通してクラウド関連の支出が大きく増加しました。

クラウドサービスプロバイダ（CSP）は、クラウドサービスの安全性を高める努力としてすべての顧客に共有責任モデルを説いてきました。しかし、クラウド環境を守るセキュリティ対策が一筋縄ではいかないことから、攻撃者は、こうしたデジタル化推進に伴う弱点をいち早く突いてきました。こうして、クラウド環境に生じる設定ミスは、サイバー犯罪者による攻撃のリスクに直結する大きな弱点であることが明らかになりました[58]。

世界三大 CSP[59]である Amazon Web Services（AWS）、Microsoft Azure、Google Cloud Platform（GCP）などのサービスを利用するクラウド環境のセキュリティ態勢の強化は、クラウド環境と技術を導入する企業や組織にとって、最優先事項であるべきです[60]。設定ミ

[53] https://www.trendmicro.com/en_us/security-intelligence/breaking-news/cyber-risk-index.html
[54] https://www.trendmicro.com/en_us/research/21/i/1h-2021-security-review-shows-active-cloud-attacks.html
[55] https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/trend-micro-cloud-app-security-report-2019
[56] https://www.trendmicro.com/en_us/ciso/21/i/cyberattacks-from-all-angles-2021-midyear-report.html
[57] https://www.businesswire.com/news/home/20220113005919/en/Cloud-Infrastructure-Spending-Increased-in-Third-Quarter-of-2021-with-Overall-Growth-Expected-for-2021-According-to-IDC
[58] https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/the-most-common-cloud-misconfigurations-that-could-lead-to-security-breaches
[59] https://www.zdnet.com/article/the-top-cloud-providers-of-2021-aws-microsoft-azure-google-cloud-hybrid-saas
[60] https://www.trendmicro.com/en_us/research/21/k/what-can-you-do-to-mitigate-cloud-misconfigurations.html

スは、深刻な情報漏洩を招くだけでなく、アイドル状態のインスタンスや未使用のストレージの費用増大を回避する上でも重要です。

クラウド環境のリスク可視化を行うトレンドマイクロのセキュリティサービス「Trend Micro Cloud One™ - Conformity」では、様々なリスクを含んだ設定の状態を「設定ミス[61]」として検出し警告可能です。以下は 2021 年の統計データから、設定ミス検出数の多いものについて検索回数と検出数の割合、つまり検出率を算出したものです。

図 6： AWS サービス設定ミス検出数トップ 3 における検出率（2021 年）

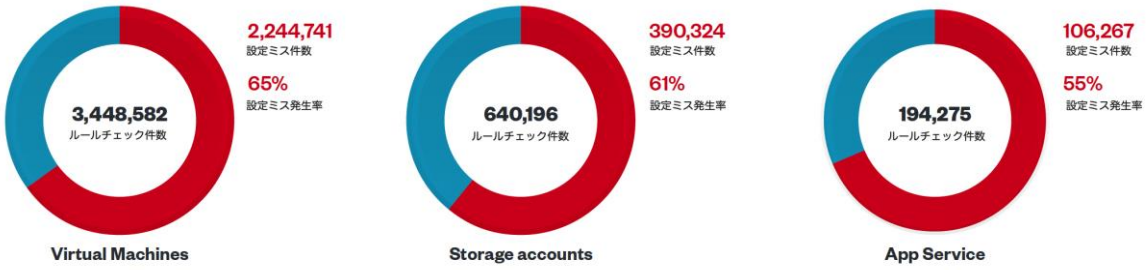


図 7：Microsoft Azure サービス設定ミス検出数トップ 3 における検出率（2021 年）

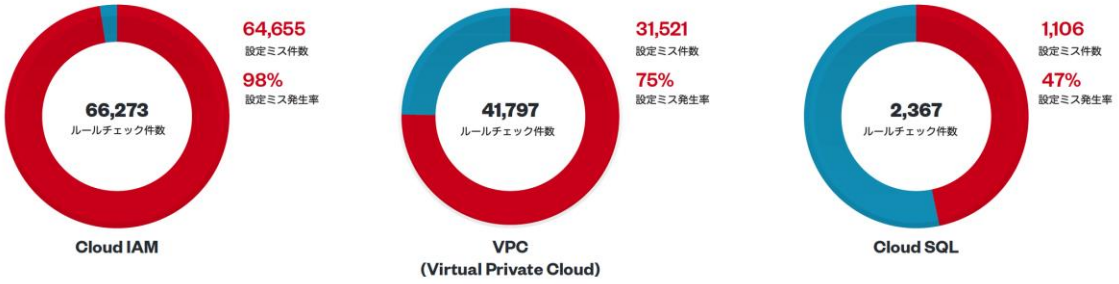


図 8：GCP サービス設定ミス検出数トップ 3 における検出率（2021 年）

[61] なんらかのセキュリティリスクがあると判断される設定を「設定ミス」としています。これには、運用上利用者が意図して設定している場合なども含まれます

この統計によると、ブロックストレージサービスの「Amazon Elastic Block Store」は、AWS サービスの中で最も検出が多く、チェック回数に対する検出率は 29%でした。Azure サービスの中で最も検出数が多かったのは「Virtual Machines」で検出率は 65%、さらに GCP サービスの中で最も検出数が多かったのは「Identity and Access Management（IAM）」で検出率は 98%となっていました。ただしこれらの「設定ミス」の検出には、直ちに侵害を受けてもおかしくないレベルのリスクから、必ずしも危険に直結しない場合までが含まれていることに留意が必要です。例えば、利用者の運用上の都合により、他の緩和策を講じた上で、敢えてベストプラクティスに準拠しない設定にしている場合などもこの検出の中に含まれています。

2021 年、攻撃者によって頻繁に狙われた設定ミスは、ソフトウェアアプリケーションの構築、テスト、デプロイに使用されるソフトウェアプラットフォーム Docker の REST API でのものでした。設定ミスを伴う Docker REST API のサーバは、サイバー犯罪者グループ TeamTNT の格好の標的となり、そして攻撃により侵害した Docker Hub アカウントを使用してコインマイナーなどのマルウェアが展開されました[62]。

クラウドベースのソフトウェアやサービスの普及に伴い、TeamTNT のようなサイバー犯罪者グループは、クラウドを標的にした攻撃キャンペーンを展開し、主に CSP の環境メタデータの窃取など、いち早く CSP をターゲットにしていました。TeamTNT による最近の攻撃キャンペーンを分析したところ、同グループはツールのレパートリーを増やし、特定の被害者に対してモジュール化された攻撃を仕掛けていたことも判明しました[63]。

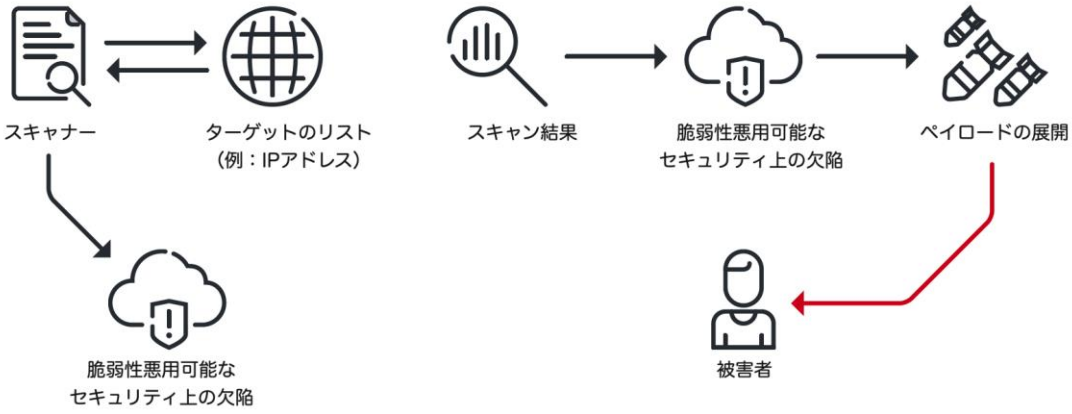


図 9：TeamTNT の攻撃フロー

[62] https://www.trendmicro.com/en_us/research/21/k/compromised-docker-hub-accounts-abused-for-cryptomining-linked-t.html
[63] https://www.trendmicro.com/en_us/research/21/k/teamtnt-upgrades-arsenal-refines-focus-on-kubernetes-and-gpu-env.html

このサイバー犯罪者グループは、2021 年 3 月から 5 月にかけて、コンテナ管理プラットフォームとして広く利用されている Kubernetes を標的とした暗号資産マイニングおよび認証情報窃盗を行う攻撃キャンペーンの実行犯でもありました。TeamTNT は、ロールベースのアクセス制御に関する設定ミスを攻撃経路とすることで、複数の Kubernetes クラスタを乗っ取ることに成功しました。この結果、約 5 万件の IP アドレスが侵害され、そのほとんどが中国と米国に存在していました[64]。

リモートワークの導入が進む中、電子メールを狙う脅威が増加

新型コロナウイルス発生以降、インターネットや電子メールの利用は、企業の事業継続やリモートワークのためにさらに不可欠な要素となっています。電子メールが在宅勤務をする世界中の人々にとって便利なツールとなるにつれ、攻撃者は、在宅勤務者のオンラインでのコミュニケーション依存に便乗した攻撃を、よりいっそう仕掛けるようになってきました。個人ユーザと企業の双方をクラウドベースのアプリやサービスへの脅威から保護する API ベースのソリューション「Trend Micro Cloud App Security」は、2021 年、2,570 万件以上のメール関連脅威を検知・ブロックし、前年の 1,670 万件以上から著しく増加しました。

電子メールは、今なおサイバー犯罪者の攻撃でよく使われる手段となっています。実際、2021 年にはマルウェアの 92%が電子メール経由で感染しました[65]。特にフィッシングメールは、2021 年の情報窃取事例の 90%に関与しています[66]。フィッシング攻撃キャンペーンは、マルウェア、特にランサムウェアを拡散する効果的な手段として 2021 年も存続しており、この傾向は、悪名高いボットネット型マルウェアから RaaS となった EMOTET の長年の成功からも明らかです。EMOTET は、2021 年 11 月に法執行機関によって関連サーバが閉鎖されましたが、しばらくの潜伏期間後、同年末に再び登場しました[67]。EMOTET は、ランサムウェア Ryuk やマルウェア Trickbot とも、数年にわたり連携を繰り返す中、アンダーグラウンド市場で大きく発展し、最終的には独自のサプライチェーンを構築するまでに進化しました[68]。

2021 年に Trend Micro Cloud App Security が検知・ブロックしたフィッシング攻撃の件数は、2020 年の約 2 倍に増加しました。このうち、62%はスパムメールであり、前年比約 7 倍となっています。残りの 38%はクレデンシャルフィッシングであり、前年比 14%増となっています。クレデンシャルフィッシングとは、サイバー犯罪者が偽のログインページでユーザをだまし、アカウントの認識情報（クレデンシャル）を引き渡させるフィッシングの手法です。一方、スパムメールによるフィッシングの手法は、ユーザの情報窃取を目的とした

[64] https://www.trendmicro.com/en_us/research/21/e/teamtnt-targets-kubernetes--nearly-50-000-ips-compromised.html
[65] https://purplesec.us/resources/cyber-security-statistics
[66] https://umbrella.cisco.com/info/2021-cyber-security-threat-trends-phishing-crypto-top-the-list
[67] https://success.trendmicro.com/solution/1118391-malware-awareness-emotet-resurgence
[68] https://www.trendmicro.com/en_us/research/21/c/emotet-one-month-after-the-takedown.html

より広いカテゴリーを意味します。フィッシング攻撃の被害が最も多かった業界は、金融であり、次いで医療、教育と続いていました。

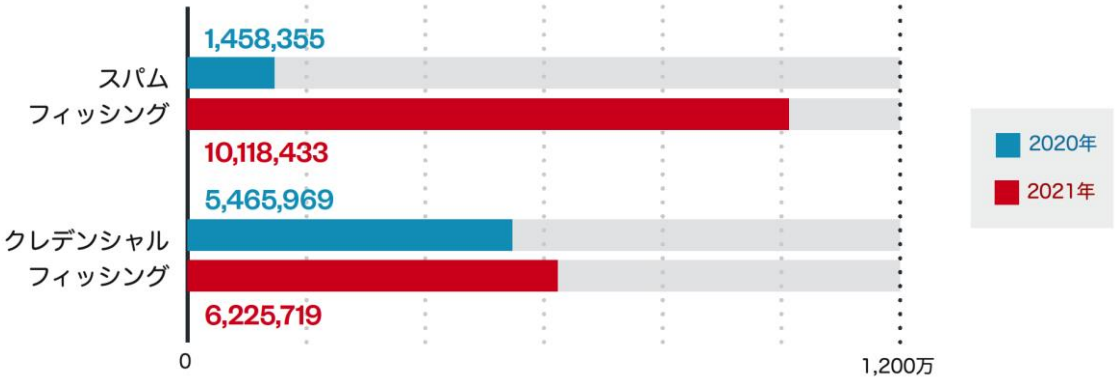


図 10：フィッシングメール検出数の年間推移（全世界）

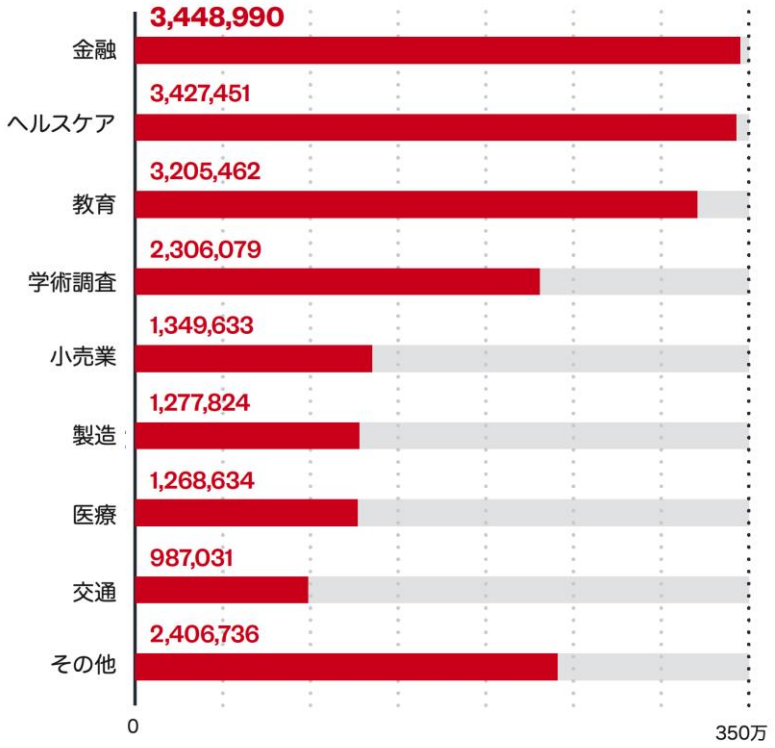


図 11：2021 年全世界における業界別フィッシングメール検出数

受信者を騙す詐欺メールの中でも高度なビジネスメール詐欺（BEC）の検出数は、2021 年には 28 万 2,775 件であり、前年比 11%減となっています。実際には、ワクチン製造に関連

する企業やサプライチェーンへの攻撃が増えた[69]ためか、2021年上半期にはやや増加が見られていましたが、年間の総計では減少となっています。背景として、BEC の攻撃者は、大量に送信する無差別な手口を減らしており、詐欺行為を念頭にメールコンテンツの質向上に重点を置いてきているようです。Trend Micro Cloud App Security は、「Writing Style DNA」を用いることで 13 万 3,541 通の BEC メール、さらに挙動分析により 14 万 9,234 通の不審なメールを検出・ブロックしました。なお、前者の分析手法は、なりすましメールの送信者と推測される「メール本文の書き方の癖」を比較検討するものであり、2021 年、BEC の 47%がこの手法で検出されました。2020 年は、この手法による検出数は 73,210 件であり、その年の BEC の 23%にとどまっていました。

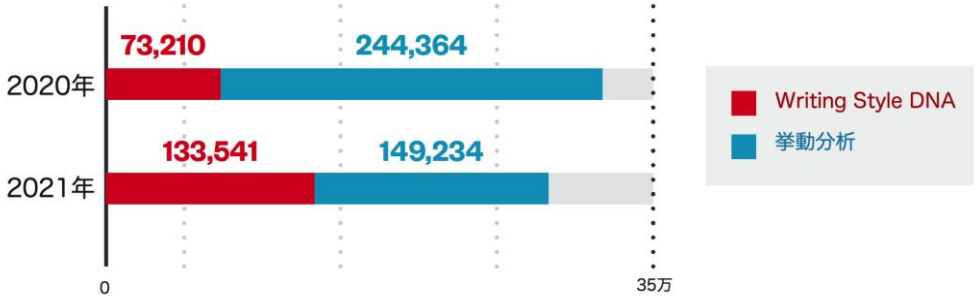


図 12：全世界における筆跡や挙動の分析に基づく BEC 件数数の年間比較

BEC の被害は、小売およびコンサルティングの業界で最も多くなっています。小売業は、顧客の決済データ、クレデンシャル、その他の個人情報を豊富に保有しているため、金銭的な動機をもつサイバー犯罪者、特にフィッシングの攻撃者にとって魅力的なターゲットであることは現在も変わりはありません[70]。

2021 年、マルウェアが仕込まれたメールの標的として最も多く狙われた業界は情報通信でした。新型コロナウイルス流行時に多くの企業が苦戦する中、この業界は成長を続け、2025 年には収益が 11 兆 9 千億米ドルを超えると予想されており、攻撃者のターゲットになっていた理由もこうした理由によるのかもしれません[71]。小売業の企業もマルウェアを含む多くのメールを受信していました。この場合も、新型コロナウイルス流行の影響でオンライン販売が急増し[72]、収益が増したことで、より多くの攻撃者の目に留まったと言えるでしょ

[69] https://newsroom.trendmicro.com/2021-09-14-Attacks-Surge-in-1H-2021-as-Trend-Micro-Blocks-41-Billion-Cyber-Threats
[70] https://www.darkreading.com/vulnerabilities-threats/don-t-help-cybercriminals-dash-with-your-customers-cash-this-black-friday
[71] https://www.businesswire.com/news/home/20210909006056/en/Information-Technology-Global-Market-Report-2021-IT-Services-Computer-Hardware-Telecom-Software-Products---Forecast-to-2025-2030---ResearchAndMarkets.com
[72] https://partnernews.sophos.com/en-us/2021/08/resources/the-state-of-ransomware-in-retail-2021

う。その他、設計図などの貴重な知的財産を保有し、建物関連のセキュリティにも精通すると見なされがちな建設業界も、サイバー犯罪者の攻撃対象となっていました[73]。

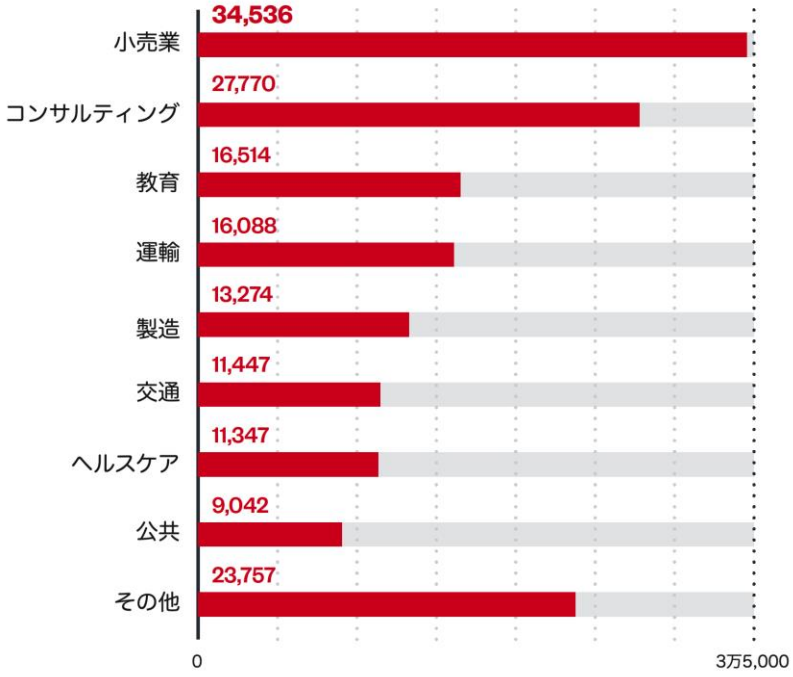


図 13：2021 年全世界における BEC 件数の業界別ランキング

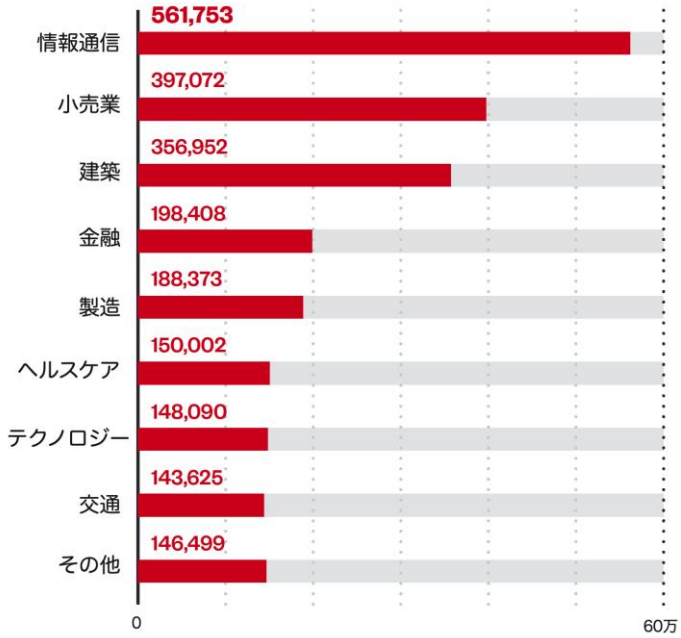


図 14：2021 年全世界におけるマルウェアを含むメール件数の業界別ランキング

[73] https://www.constructormagazine.com/site-security

強化された武器でより大きな獲物を狙う標的型攻撃

2021 年、マルウェアを無差別に拡散させる攻撃者が増える中、特定の業界を狙う標的型攻撃のケースも確認されました。標的型攻撃は、2012 年以来[74]、企業や組織を悩ませている脅威です。攻撃者は、標的にした被害者のシステムに合わせてツールやテクニックを調整する必要があるため、高度な技術的専門知識と豊富なリソースを必要とします[75]。

2021 年上半期には、より多くのサイバー犯罪者が標的型攻撃の高度なツールやテクニックに頼るようになり、量的な攻撃から、より収益性の高い標的に絞って獲物へ最新型ランサムウェアを駆使する方向へのシフトが観察されました[76]。この種の攻撃は、標的となった企業や組織に直接的な被害を与えるだけでなく、その結果生じるビジネスの混乱や顧客情報の流出など、被害を受けた企業や組織の顧客にも影響が及ぶ可能性があります[77]。標的型攻撃の攻撃者としては、金銭利益を目的とするサイバー犯罪者と「State-Sponsored」と呼ばれる国家背景による機密情報窃取と目的とするものがありますが、いずれにおいてもまずは侵入した環境からの情報窃取を行います[78]。

政府機関などをターゲットに攻撃を仕掛ける攻撃者グループ Void Balaur

Void Balaur は、Rockethack とも呼ばれるサイバー犯罪の傭兵グループであり、情報窃取とサイバースパイを中止に活動しており、ロシア語圏のサイバー犯罪アンダーグラウンド市場では、Darkmoney や Probiv といったフォーラムや Web サイトを通じて自分たちが提供できるサービスや活動などを宣伝しています。実際、過去数年、電気通信、小売、金融、医療、バイオテクノロジー業界に対して、彼らからの攻撃が仕掛けられたのを確認しています。2021 年には、電気通信関連業界に狙いを定め、ロシアやイギリスのさまざまな電気通信関連の企業のエンジニアや管理職を標的にしていたことが判明しました[79]。

このグループの背後の傭兵、つまり雇われハッカーは、金銭目的の活動と同時に、ジャーナリストや人権活動家、政府高官を狙った攻撃も頻繁に実行しています。例えば、2021 年 9 月には、東欧のある国の情報機関の元長官、国会議員 2 名、現役の政府閣僚 5 名を標的とした攻撃事例が確認されました。このことは、広範囲な混乱を引き起こすための多面的な大規

[74] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/historical-overview-of-proactive-incident-response-strategies-and-what-they-mean-to-enterprises
[75] https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/targeted-attacks-six-components
[76] https://www.trendmicro.com/en_us/ciso/21/i/cyberattacks-from-all-angles-2021-midyear-report.html
[77] https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/the-impact-of-targeted-attacks
[78] https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/understanding-targeted-attacks-what-is-a-targeted-attack
[79] https://www.trendmicro.com/en_us/research/21/k/void-balaur-and-the-rise-of-the-cybermercenary-industry.html

模キャンペーンにも、多くの場合、彼らが関与している可能性を示唆しています。彼らの活動は、東欧の他、各ヨーロッパ諸国、米国、日本、イスラエルでも確認されています。

Void Balaur が提供する主なサービスは、メールやソーシャルメディアのアカウントへのハッキングです。高い料金を支払えば、同グループはユーザに気づかれずに盗取したメールボックスの完全なコピーを提供することもできます。2019 年には、犯罪歴、クレジット履歴、銀行明細、テキストメッセージ、パスポートやフライトデータなど、ロシア人個人の機密情報の販売を開始しました。彼らは、Z*Stealer や DroidWatcher などの特殊なマルウェアを使用しており、これらを駆使して遠隔追跡、位置情報へのアクセス、さまざまなアプリやデジタル通貨ウォレットのユーザ認証情報などの窃取も可能です[80]。

運輸・官公庁を攻撃する攻撃者グループ Tropic Trooper の再来

現在は Earth Centaur と名乗るサイバー犯罪諜報グループ Tropic Trooper は、2011 年からすでに活動していました。そして 2020 年 7 月に改良型リモートアクセスツール（RAT）など、新たなツールを駆使する形で再来してきました。特に 2020 年末から 2021 年にかけては、これら新たなツールを駆使し、運輸事業者や運輸関連の政府機関[81]を標的にしていました。その攻撃は、侵入したシステムから財務書類、検索履歴、フライトスケジュールなどの情報を窃取することが一般的でした。トレンドマイクロの解析によれば、Tropic Trooper は今後も機密情報を収集しながら、その情報を活用するタイミングを伺っている様子が確認されました。

Tropic Trooper は、通常、Microsoft Internet Information Services や Exchange サーバの脆弱性を突いて攻撃対象の端末に侵入し、ChiserClient や SmileSvr といったバックドアを実行する Webshell をインストールします。そして、カスタマイズされたツール Gh0st RAT を使用して、感染端末上のアクティブなセッションを検出することで情報を収集します。その上で感染端末上のイントラネットを使用して窃取した情報を送出します。

Tropic Trooper の背後にいる脅威者は、卓越したチームワークを備えていることが分かります。彼らは、オープンソースのフレームワークを駆使することで、さまざまなプロトコルのバックドアを開発し、攻撃対象のセキュリティ回避に使用します。また、ネットワークセキュリティシステムによる検出を回避するためにリバースプロキシも使用しています。

[80] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-far-reaching-attacks-of-the-void-balaur-cybermercenary-group
[81] https://www.trendmicro.com/en_us/research/21/l/collecting-in-the-dark-tropic-trooper-targets-transportation-and-government-organizations.html

BazarLoader を侵入手段として利用する攻撃者の増加

2021 年第 3 四半期は、以下の検出名の情報窃取型ローダ BazarLoader 使用の増加が確認されました。特にアメリカ大陸地域で多数の検出台数が確認されました[82]。

- TrojanSpy.Win64.BAZARLOADER
- Backdoor.Win64.BAZARLOADER

2020 年に初めて観測されて以来[83]、BazarLoader は、サイバー犯罪者が情報窃取に際しての初期アクセス、またはランサムウェア攻撃に際しての第 1 段階のマルウェア侵入などに使用されてきました。2021 年 1 月から 10 月にかけて、スパムメールによる侵入手段としても駆使された BazarLoader の攻撃キャンペーンは、主に米国を標的とし、次いでヨーロッパやアジアの一部の国々をターゲットとしていました。この場合、スパムメールのほとんどは、注文の請求書やサービスプランの解約通知などになりすましていました。一方、同時期に JavaScript ドロッパーを使用して BazarLoader を配信した攻撃キャンペーンは、米国とオーストラリアのユーザを中心に狙っていました。

さらに注目すべきは、BazarLoader の感染に際して複数の異なる侵入手段が用いられていたことです。第一の手段は、BazarLoader が正規のプログラムにバンドルされ、VLC や TeamViewer のようなソフトウェアインストーラを使用して展開される手口です。この場合、侵入に際してユーザを騙して危険なインストーラをダウンロードさせるため、ソーシャルエンジニアリングの手法が含まれている可能性があります。そして、インストーラのロード中に BazarLoader の実行ファイルがドロップされます。このインストーラは、BazarLoader の EXE ファイルを実行するプロセスを作成し、その上で Microsoft Edge を使用してコマンド＆コントロール（C&C）サーバとの接続を確立します。

また別の手段としては、Windows の LNK（リンク）ファイルを含む ISO ファイルによって侵入する方法も挙げられます。LNK ファイルは、フォルダのアイコンとして偽装されており、ユーザが誤ってクリックすると、BazarLoader ダイナミックリンクライブラリ（DLL）によるペイロードが実行されます。

Qakbot が改良型として再登場

2007 年に発見され[84]、トレンドマイクロのソリューションで「TrojanSpy.Win32.QAKBOT」として検出対応した情報窃取型マルウェア Qakbot は、ランサムウェアの攻撃者の間で、攻撃キャンペーンに際してマルウェア配布させるボットネット側マルウェアとして重宝されて

[82] https://www.trendmicro.com/en_us/research/21/k/bazarloader-adds-compromised-installers-iso-to-arrival-delivery-vectors.html
[83] https://www.trendmicro.com/en_us/research/21/d/a-spike-in-bazarcall-and-icedid-activity.html
[84] https://www.fbiic.gov/public/2010/dec/FS_Nov_2010_PDF.PDF

きました。2019 年に入ると、MegaCortex、PwndLocker、Egregor、ProLock、最近では REvil/Sodinokibi といったランサムウェアファミリーの攻撃活動に使用されていました[85]。

その後、約 3 ヶ月の休止期間を経て、2021 年 9 月、Qakbot の攻撃者は、スパムメールを介して活動を再開しました。攻撃キャンペーンで Excel 4.0 や、Visual Basic for Applications（VBA）マクロを駆使する新たなバージョンとして戻ってきました。また、過去数年間、Qakbot のスパム攻撃キャンペーンでは、主に通信、テクノロジー、教育などの業界が標的にされており、国別ランキングでは、米国、日本、ドイツが上位にランクインしていました。

検出回避を向上させた Buer Loader

Buer Loader は、競争力のある価格設定のため、2019 年にアンダーグラウンド市場に登場した際、多くの攻撃者が選択したローダ型マルウェアとなりました。現在も活発な活動を続けており、標的型ランサムウェア攻撃の一環として、Ryuk、Wizard Spider、Cobalt Strike Beacon などによる有名な攻撃に際して使用されてきました[86]。国別ランキングでは、インドでの検出が最も活発で、次いでイスラエルとなっています。業界別ランキングでは、医療、銀行、通信などの企業や組織で最も多く検出されていました。

2021 年、プログラミング言語 Rust で書かれた Buer Loader の新たな亜種が、他のローダ型マルウェアを添付ファイルとするスパムメールに使用されました。ある攻撃キャンペーンでは、DHL の出荷通知を装ったメールが使用され、その他の攻撃キャンペーンでは、誘い文句としてメール内で Covid-19 に言及するなど、主に DHL と Covid-19 の両方を便乗していました。これらのスパムメールで使用された Buer Loader の新亜種は、以前の亜種と同じコードのほとんどを保持していた一方で、検出回避のために新たなプログラミング言語で書き直された可能性が高いと言えます。この新亜種は、攻撃対象の IT 部門に気づかれない方法として、署名された XLL（Excel アドイン）ファイルも使用していました。

新たな暗号化ツールで RAT を感染端末上に氾濫させる Water Basilisk

2021 年 8 月、Water Basilisk と呼ばれるファイルレス攻撃キャンペーンが活発化しました。この攻撃キャンペーンは、新たな HCrypt[87]というツールを用いて、BitRat、NjRat、LimeRat、Warzone、QuasarRat、Nanocore RAT などの RAT を感染端末へ展開します。Water Basilisk の攻撃者は、いわゆる「サービスとしての暗号化（CaaS、cryptter-as-a-

[85] https://www.trendmicro.com/en_us/research/21/k/qakbot-loader-returns-with-new-techniques-and-tools.html
[86] https://www.trendmicro.com/en_us/research/21/k/a-review-and-analysis-of-2021-buer-loader-campaigns.html
[87] https://www.trendmicro.com/en_us/research/21/i/Water-Basilisk-Uses-New-HCrypt-Variant-to-Flood-Victims-with-RAT-Payloads.html

service）」のアプローチでペイロードを展開し、難読化された VBScript や PowerShell スクリプトを作成していると言えます。トレンドマイクロでは、すでに合計 7 つの RAT が関わる PowerShell スクリプトを駆使した Water Basilisk 事例を確認しています[88]。

Water Basilisk の攻撃者は、これらのマルウェアやフィッシングキットなどを一般からアクセス可能なファイルホスティングサービスや WordPress のサイト上で提供しています。この場合、これらの WordPress ウェブサイトやフィッシングメールを介して偽装した ISO イメージを展開しています。このイメージには、難読化された VBScript Stager が含まれており、これにより感染端末上で次の攻撃段階の VBScript がダウンロード・実行されます。そして最後に、PowerShell スクリプトが難読化を解除した上で、所定のプロセスでペイロードの RAT が展開されます。

Water Basilisk がマルウェアの拡散に用いる暗号化ツール HCrypt のバージョンは、アンダーグラウンド市場では 199 米ドルで販売されています。トレンドマイクロの解析によると、こうした暗号化ツールは、開発者によって更新され続けており、今後さらに新たなバージョンが登場し、よりいっそう多くの RAT を巻き込んで、なおかつ効果的な検出回避策を備えた難読化アルゴリズムが登場してくる可能性があります。

[88] https://www.trendmicro.com/en_us/research/21/i/Water-Basilisk-Uses-New-HCrypt-Variant-to-Flood-Victims-with-RAT-Payloads.html

脆弱性の増加に伴うパッチ未適用のリスク

現代の IT インフラは複雑に入り組んでいるため、修正パッチの適切な運営は、企業や組織がビジネスを円滑に進める上で不可欠です。しかし実行に際しては多くの困難が伴います。脆弱性の修正には平均 200 日、重大な欠陥の場合は 256 日かかると言われています[89]。対応としては、日々の業務で使用するソフトウェアやセキュリティポリシーを速やかに更新できれば理想的です。しかし、さまざまな更新情報を追跡して対応することは、業務に忙殺されがちな IT 部門にとって、簡単なことではありません[90]。

旧来の脆弱性が招く無防備な IT 環境

2021 年、トレンドマイクロ傘下の脆弱性調査機関 Zero Day Initiative™（ZDI）は、1,604 件の脆弱性に関するアドバイザリを公開し、前年の対応件数より 10%増加しました。このうち、深刻度が「重要」と評価されたものは 54 件で、2020 年の 173 件から大きく減少しています。一方で、深刻度が「緊急」と評価されたものは増加し、前年の 983 件から 1,138 件に増加しました。

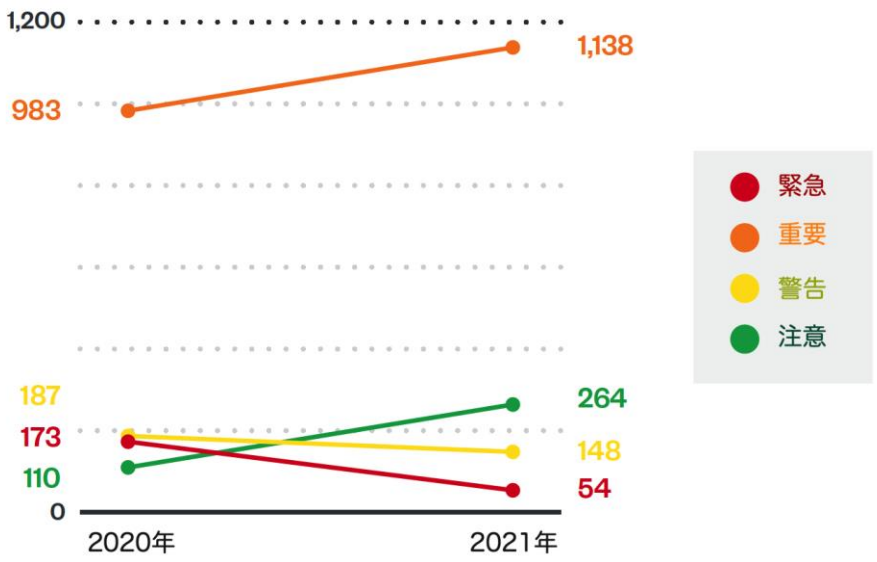


図 15：CVSS 評価別公開済み脆弱性の件数推移（ZDI の集計による）

旧来からのレガシー脆弱性の多くは、現在もサイバー犯罪アンダーグラウンド市場の脆弱性悪用ツール（エクスプロイト）向けとして需要があり、使用され続けています。実際、2021 年の調査では、アンダーグラウンド市場で販売されているエクスプロイトの 22%が 3

[89] https://www.kaseya.com/blog/2022/02/22/patch-management-policy
[90] https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/the-nightmares-of-patch-management-the-status-quo-and-beyond

年以上前の脆弱性に対応するものであることが判明しています[91]。こうしたエクスプロイトは、攻撃者にとって確実な収入源となっており、アンダーグラウンド市場のフォーラムでは、1,000 米ドルからの価格で販売されています[92]。

各国の企業で導入されているネットワークセキュリティプラットフォーム「Trend Micro™ TippingPoint® Threat Protection System」のデータによると、攻撃者は、旧来の脆弱性とともに比較的新しい脆弱性も悪用されていることが分かります。また旧来の脆弱性は修正パッチが提供されている一方、古いものでは 2005 年発見の脆弱性がいまも悪用対象になっています。2021 年に検出されたランキングには、よく知られた脆弱性が並んでいます。これらのうち 7 つは、2017 年以降から広く悪用されたものとしてランクインしています。

2021 年のエクスプロイト検出数で圧倒的に多かった脆弱性は CVE-2019-1225 であり、その件数は 7,500 万超にのぼります。CVE-2019-1225 は、2019 年 8 月に公開された Microsoft の Remote Desktop Services におけるメモリ漏洩に関する脆弱性です[93]。この脆弱性が悪用されると、感染端末から情報窃取が可能になります。第 2 位は、深刻度「重要」な脆弱性「CVE-2017-14100」となります。Digium 社の構内交換機のソフトウェア実装である Asterisk で発見されたこの脆弱性は、2021 年、2,000 万件以上の検出件数に達しました。2017 年 9 月に公開されたこの脆弱性は、悪用されると、権限のないユーザがリモートで任意のシェルコマンドを注入することが可能になります[94]。

CVE番号	影響を受けた製品	ルールID	ヒット件数
CVE-2019-1225	Windows RDP server	DV-36042	75,267,406
CVE-2017-14100	Asterisk 11	DV-29739	20,846,194
CVE-2011-1264	Microsoft Windows Server	DV-3886	4,831,951
CVE-2010-0817	Microsoft SharePoint server		
CVE-2014-6271	GNU Bash	DV-16798	1,860,228
CVE-2014-6277			
CVE-2014-6278			
CVE-2014-3567	OpenSSL	DV-17056	1,622,083
CVE-2005-1380	BEA Admin Console	DV-2023	1,054,890
CVE-2010-3936	Microsoft Forefront Unified Access Gateway		
CVE-2010-0817	Microsoft SharePoint server		
CVE-2017-0068	Microsoft Edge		
CVE-2003-1138	Apache	DV-11984	1,032,998
CVE-2017-5638	Apache Struts	DV-27410	784,031
CVE-2018-13379	Fortinet FortiOS	DV-36087	631,799
CVE-2018-10562	Dasan GPON home router	DV-31936	588,763

表 1：2021 年全世界で検出された脆弱性ランキング

[91] https://newsroom.trendmicro.com/2021-07-13-Nearly-a-Quarter-of-Exploits-Sold-on-Cybercriminal-Underground-Are-More-Than-Three-Years-Old
[92] https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/trends-and-shifts-in-the-underground-n-day-exploit-market
[93] https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2019-1225
[94] https://cve.report/CVE-2017-14100

Log4j の脆弱性 Log4Shell が引き起こしたさまざまな攻撃事例

2021 年は、深刻度の高い脆弱性 CVE-2021-44228 など、パッチ未適用のセキュリティギャップに起因する注目事例が散見された年でした。この脆弱性は、2021 年 11 月に Apache 上で初めて非公開で報告され[95]、Log4Shell と呼ばれ、Java ベースのログ記録ツール Apache Log4j に影響を与えます[96]。オープンソースの Apache コミュニティは 2021 年 12 月に修正パッチをリリースしていましたが、それでもなお、この脆弱性により、情報窃取、マルウェア感染、暗号資産のマイニングや、クリプトジャッキングなど、さまざまな脆弱性悪用事例が引き起こされました。特に注目すべきは、ランサムウェア Khonsari の攻撃者が 2021 年 12 月、この脆弱性を攻撃に使用し始めたことでしょう[97]。

Log4j は、企業の社内アプリケーションおよびサードパーティアプリケーションとして広く使用されているユーティリティです。Log4j は、Java に依存しているため、企業の環境全体でツールが実行されていることを検出することが困難です。これが、修正パッチが提供されていても、脆弱性 Log4Shell を簡単に対処できなかった理由となっています。この脆弱性が悪用されると、任意のコードを実行するようにする細工したログメッセージを送信することが可能になります。こうして感染端末を踏み台にして、さまざまな種類の攻撃を仕掛けることができるようにします。

2021 年 12 月現在、Log4Shell はトレンドマイクロのお客様の 7%にしか影響を与えておらず、アメリカ、AMEA（アジア、中東、アフリカ）地域、ヨーロッパ、日本に分散した状況の中、最も多くの事例はアメリカで確認されました[98]。業界別では、主に政府機関、小売業、製造業が影響を受けました。

ProxyLogon と ProxyShell の脆弱性を悪用する攻撃者

2021 年に確認されたその他の注目すべき脆弱性としては、2020 年末に発見された Microsoft Exchange Server の脆弱性 ProxyLogon と ProxyShell が挙げられます。これを受けて、Microsoft 社は、2021 年 3 月に ProxyLogon（CVE-2021-26855）、2021 年 5 月と 7 月に ProxyShell（CVE-2021-34473、CVE-2021-34523）に対する修正パッチをリリースしました[99]。しかし修正パッチ提供にもかかわらず、トレンドマイクロの観測データからは、ProxyLogon が、コインマイナーLemonDuck、ランサムウェア BlackKingdom、ボットネッ

[95] https://www.trendmicro.com/en_us/research/21/l/patch-now-apache-log4j-vulnerability-called-log4shell-being-acti.html
[96] https://www.trendmicro.com/en_us/research/21/l/the-log4j-story-and-how-it-has-impacted-our-customers.html
[97] https://www.trendmicro.com/en_us/research/21/l/patch-now-apache-log4j-vulnerability-called-log4shell-being-acti.html
[98] https://www.trendmicro.com/en_us/research/21/l/the-log4j-story-and-how-it-has-impacted-our-customers.html
[99] https://threatpost.com/attackers-hijack-email-threads-proxylogon-proxyshell/176496

トマルウェア Prometei など、多くの異なるマルウェアファミリーによる 2021 年発生の攻撃の一部となっていることが確認されました[100]。

2021 年 9 月、セキュリティリサーチャーは新たなローダ型マルウェア「Squirrelwaffle」を駆使する複数のスパム攻撃キャンペーンについて報告しました[101]。これらの攻撃キャンペーンでは、ProxyLogon や ProxyShell を悪用するエクスプロイトも使用されており、これにより、既存のメールスレッドへの返信を装った不正メールが送信されていたことが分かりました[102]。2021 年 11 月、中東で発生したマルウェア Squirrelwaffle の事例を調査したところ、ProxyLogon が、攻撃対象のメールメッセージへのアクセス、検索、ダウンロードに悪用されていることが判明しました。また、ProxyShell の場合は、Squirrelwaffle の攻撃者が感染端末のローカル管理者になりすまして PowerShell コマンドを実行し、不正な Excel ファイルが添付されたメールの返信を配信することが可能となっていました[103]。

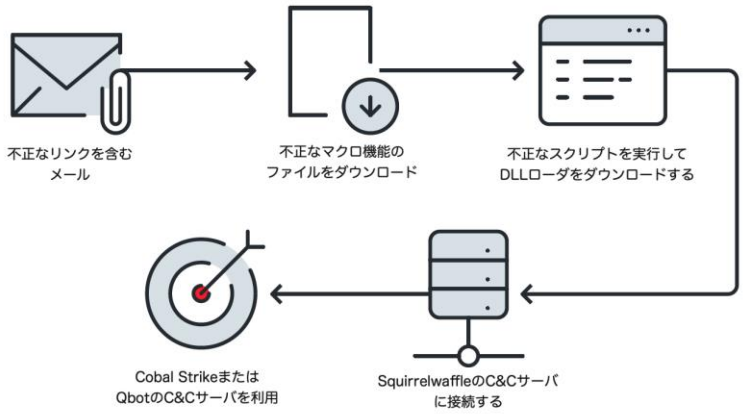


図 16：Squirrelwaffle 関連のスパムメールに添付された不正な Excel ファイルの感染フロー

修正パッチ未適用の VPN 脆弱性が在宅勤務を脅かす

新型コロナウイルス流行を契機にして、地理的に分散した従業員の在宅勤務では、安全な企業ネットワーク接続の必要性から仮想プライベートネットワーク（VPN）の利用が促進されています。リモートワークを導入している企業にとって、拡張性の高い企業内 VPN と、VPN を介してアクセス可能な社内アプリケーションは、喫緊の課題となっています[104]。世界的に見ると、2021 年に VPN の利用が急増し、その間に VPN のダウンロード数は 7 億 8,500 万件に達しました[105]。

[100] https://www.trendmicro.com/en_us/research/21/e/proxylogon-a-coinminer--a-ransomware--and-a-botnet-join-the-part.html
[101] https://blog.talosintelligence.com/2021/10/squirrelwaffle-emerges.html.
[102] https://www.trendmicro.com/en_us/research/21/l/this-week-in-security-news-dec-3-2021.html
[103] https://www.trendmicro.com/en_us/research/21/k/Squirrelwaffle-Exploits-ProxyShell-and-ProxyLogon-to-Hijack-Email-Chains.html
[104] https://www.trendmicro.com/en_us/devops/21/k/cybersecurity-trends-from-the-global-pandemic.html
[105] https://atlasvpn.com/vpn-adoption-index

しかし、他のセキュリティ技術と同様、VPN も攻撃者に悪用される可能性があります。2021 年、VPN 製品で最も悪用された脆弱性の 1 つが CVE-2018-13379 で、修正パッチが 2019 年 5 月から提供されていたにもかかわらず、検出数は、63 万 1,000 件以上に達しました[106]。この脆弱性は、Fortinet FortiOS のパストラバーサルの欠陥であり、悪用されると、脆弱な FortiGate SSL VPN のエンドポイントへのカスタム HTTP リソース要求を作成し、これにより、感染端末からファイルを読み取りやダウンロードが可能になります[107]。2021 年初頭、ランサムウェア Sodinokibi[108]や Conti[109]の攻撃でも、CVE-2018-13379 が悪用され、他の脆弱性と組み合わせて感染端末を踏み台にしていたことが判明しています。この脆弱性は、日本情報処理推進機構（IPA）および JPCERT コーディネーションセンターによると、2021 年に注目すべき VPN の脆弱性の 1 つとされています。

製品・CVE番号		1月	2月	3月	4月	5月	6月
合計		198,777	139,165	158,372	138,181	114,727	98,577
Fortinet	CVE-2018-13379	113,330	77,853	75,785	68,651	70,083	61,467
Pulse Secure	CVE-2019-11510	45,937	15,627	27,876	21,440	15,230	9,558
		787	488	566	956	508	301
	CVE-2019-11539	0	0	1	0	0	11
	CVE-2021-22893	0	0	0	107	27	0
Citrix Systems	CVE-2019-19781	1,388	579	713	988	650	418
		3	761	158	5	5	15
Palo Alto	CVE-2019-1579	0	0	0	0	0	0
F5	CVE-2020-5902	37,332	43,857	53,038	36,493	24,493	24,378
		0	0	0	0	0	1
	CVE-2021-22986	0	0	2	12	66	19
		0	0	12	12	29	39
		0	0	221	9,517	3,636	2,370

製品・CVE番号		7月	8月	9月	10月	11月	12月
合計		61,950	43,963	185,374	103,444	34,139	59,124
Fortinet	CVE-2018-13379	24,735	16,668	53,467	31,496	15,545	22,719
Pulse Secure	CVE-2019-11510	9,146	7,717	29,343	13,719	5,266	8,296
		274	451	3,629	4,919	487	951
	CVE-2019-11539	35	1	0	5	0	12
	CVE-2021-22893	0	0	17	3	0	0
Citrix Systems	CVE-2019-19781	631	695	9,265	5,347	472	1,268
		17	63	24	32	16	11
Palo Alto	CVE-2019-1579	0	0	0	10	0	12
F5	CVE-2020-5902	23,333	15,899	79,272	41,841	10,863	21,671
		6	0	0	0	0	5
	CVE-2021-22986	160	0	0	0	0	970
		251	151	223	309	30	86
		3,362	2,318	10,134	5,763	1,460	3,123

表 2：2021 年の主な VPN 関連脆弱性の検出数推移（全世界）

[106] https://www.fortinet.com/blog/psirt-blogs/fortios-ssl-vulnerability
[107] https://nvd.nist.gov/vuln/detail/CVE-2018-13379
[108] https://www.trendmicro.com/en_us/research/21/a/sodinokibi-ransomware.html
[109] https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-conti

リモートワーカーを狙う新型コロナウイルス便乗の脅威

新型コロウイルスの流行により、企業や組織は自らの業務を見直す必要に迫られています。その中で、多くはリモート接続とクラウドコンピューティングに依存するハイブリッドワークモデルを採用し、これらの激変への適応に追われている状況が続いているようです[110]。こうした中、サーベイ調査によると、2021 年になっても、米国では 72%の企業や組織が、従業員の在宅勤務を介した社内のネットワークへの攻撃に対する防御に苦慮していることが明らかになりました[111]。

トレンドマイクロ傘下の ZDI プログラム[112]が主催したハッキングコンテスト「Pwn2Own Austin 2021」で実証されたように、在宅勤務に伴うホームオフィスは、企業や組織の攻撃対象を拡大する事態を招いてしまったとも言えます。イベントでは、在宅勤務者の多くが依存している定番の機器がいかに攻撃対象になり得るかが浮き彫りになりました。例えば、参加者のセキュリティリサーチャーは、プリンタ、ルータ、ネットワーク接続ストレージ（NAS）などのデバイスに対して、公開済みの脆弱性を利用したり、新たな脆弱性を発見したりして、攻撃手法を実証しました。そしてこのイベントだけで合計で 61 件の新たな脆弱性が確認されました[113]。

攻撃者は、通常、フィッシング攻撃において最新の出来事やニュース記事に便乗しますが、こういった便乗メールは短期的しか利用できません。一方、新型コロナウイルスの話題は、フィッシングメールに長期間便乗可能なテーマや情報を豊富に提供しています。新型コロナウイルスが毎日報道・更新される度に、攻撃者はその時点で適合する攻撃対象に合わせ、より巧妙なソーシャルエンジニアリングを展開することが可能になります[114]。

2021 年、攻撃対象から個人情報を窃取するため、ソーシャルエンジニアリングの手法によるさまざまな詐欺やマルウェア攻撃が確認されました。その 1 つの傾向として、ワクチン供給に特化したサプライチェーンといえる「コールドチェーン」に対するフィッシング攻撃の増加が挙げられます。こうしたコールドチェーンに関わるあらゆる領域から貴重な機密情報へのアクセスが可能となるためです。また、政府機関、非政府組織、ワクチンの流通に携わる企業を装った偽のモバイルアプリやウェブサイトも急増し、悪徳業者が、援助や就労機会、ワクチンの入手方法[115]に関する詳細情報を求める人々を狙って不正活動を展開しました。

---

[110] https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/addressing-cloud-related-threats-to-the-iot
[111] https://resources.trendmicro.com/Osterman-Email-Security-WP.html
[112] https://www.zerodayinitiative.com/blog/2021/11/1/pwn2ownaustin
[113] https://www.securityweek.com/device-exploits-earn-hackers-over-1-million-pwn2own-austin-2021
[114] https://www.trendmicro.com/en_us/research/21/g/reduce-instances-of-covid-19-phishing-email-attacks.html
[115] https://www.trendmicro.com/en_us/research/21/g/threats-ride-on-the-covid-19-vaccination-wave.html

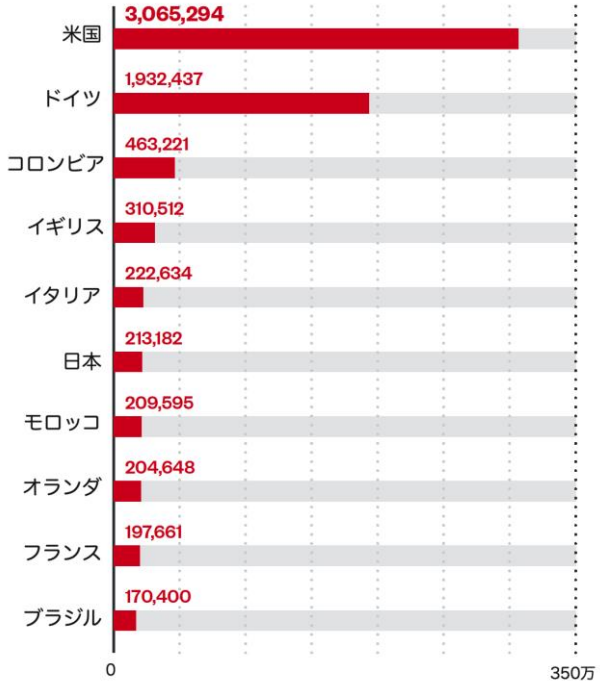


図 17：新型コロナウイルス便乗脅威の国別検出数トップ 10（2021 年）

2021 年、新型コロナウイルスに便乗した脅威を 800 万件以上検出しましたが、これは前年の約半数でした。2020 年と同様、脅威の多くは米国やドイツからのものであり、主要なワクチン研究者やメーカーの拠点国としてこれらの国々がコールドチェーンにおいて重要な役割を担っているために標的とされたと推測されます。

新型コロナウイルスに便乗した脅威は、主にメールを感染経路としたものが検出数全体の 94%を占めている一方、2020 年と比較して前年比 45%減少しています。また、不正 URL 経由の脅威も 2020 年から 2021 年にかけて 82%減少しています。一方、不正なファイルとして検出されたものは 2020 年から 2021 年にかけて 4 倍以上に増加しており、その多くはインドネシアとブラジルで検出されました。

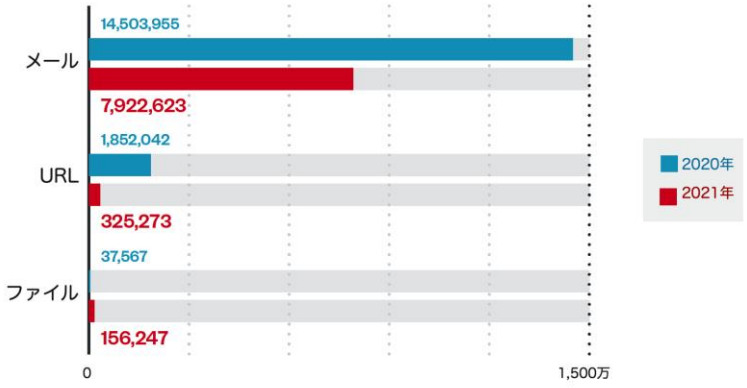


図 18：新型コロナウイルス便乗脅威のレイヤー別検出数推移

2021 年、新型コロナウイルスに便乗した脅威は 5 月にピークを迎え、医療業界に対するサイバー犯罪が多発した時期でした。同月、アイルランドの公的医療システム「Health Service Executive」がランサムウェア Conti による攻撃に見舞われ、医療サービスのコンピュータシステムに対する既知のサイバー攻撃としては最大規模となりました[116]。別の報道では、2021 年 3 月から 7 月まで連続 5 か月、医療業界において 1 日 2 件以上の情報侵害の事例が発生したと伝えており、2021 年 5 月に脅威が急増した状況とも一致しています[117]。

2021 年、新型コロナウイルスに便乗した脅威は前年比 49%減となりましたが、これはさまざまな要因で説明できます。攻撃者は、新型コロナウイルスに関する悪用可能な新たな関連のトレンドやニュースを待ち構えていたのかもしれません。もしくは脅威が一部の国に集中していたため、ソーシャルエンジニアリングに利用するというサイバー犯罪者の関心は、全体的には薄れていた可能性も否定できません。西ヨーロッパ諸国などの特定の国々では盛んにメディアで報道されていますが、報道がそれほどでもない国については、同じことは言えないでしょう[118]。さらに、大規模なロックダウンのために失われた労働時間は、2020 年には 2 億 5,500 万人の正規雇用に相当しましたが[119]、2021 年には、集団予防接種の実施や感染者の減少により職場に復帰する人が増え、規模が 1 億 2,500 万人相当に後退したことも理由かもしれません[120]。また、こうした脅威に対する認識が高まったことで、多くの企業や個人ユーザが、セキュリティ体制を改善するソフトウェアソリューションを採用するようになった可能性も挙げられるでしょう。

[116] https://www.hhs.gov/sites/default/files/lessons-learned-hse-attack.pdf
[117] https://wow.intsights.com/rs/071-ZWD-900/images/Building%20Immunity-Healthcare-Pharma%20Report-2021.pdf
[118] https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2021/dnr-executive-summary
[119] https://www.weforum.org/agenda/2021/02/covid-employment-global-job-loss
[120] https://www.ilo.org/global/about-the-ilo/newsroom/news/WCMS_824098/lang--en/index.htm

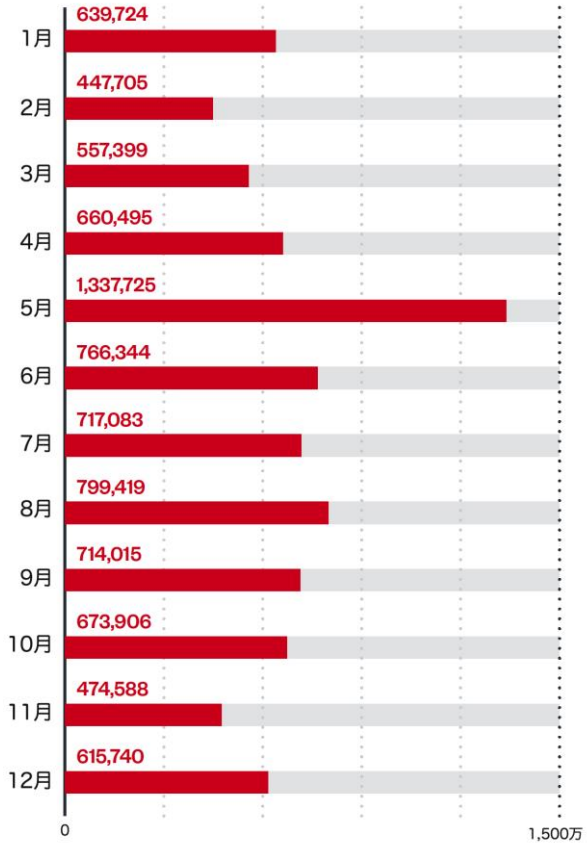


図 19：新型コロナウイルス便乗脅威の検出数推移（2021 年）

いずれにしても、新型コロナウイルスにまつわる詐欺に常に注意を払うことは、すべての企業や組織にとって損失を避けるために必要なことです。世界経済フォーラムの報告によると、新型コロナウイルスの流行以来、サイバー犯罪は、世界のデジタル経済の成長に伴って進化していると言います。2021 年だけで、企業や組織は、平均して一社につき 270 件の攻撃を回避する必要があったと報告されています。しかも 1 件の攻撃が成功すると、360 万米ドルの損失を被る可能性があると言います[121]。

[121] https://www.weforum.org/press/2022/01/closing-the-cyber-gap-business-and-security-leaders-at-crossroads-as-cybercrime-spikes

2021 年年間の脅威概況

エンドポイント、メール、ネットワーク、クラウド環境のさまざまなニーズを同時に監視し、対処できる統合的なサイバーセキュリティのプラットフォームを採用すれば、企業や組織は、拡大する攻撃対象に対してより有利な立場に立つことができます。これにより、デジタルエコシステム全体の状況を把握し、新たな脅威を予測し、適切なセキュリティ対策を講じることができます。

なお、2020 年、「Trend Micro Apex One™」をはじめとするトレンドマイクロ製品は、SPN フィードバック機能の自動運用を開始しました。このアップデートの結果、トレンドマイクロのお客様への恩恵として検出機能が向上し、2021 年における脅威検出数の増加の理由となったとも考えられます。

94,289,585,240

2021 年にブロックされた脅威の総検出数

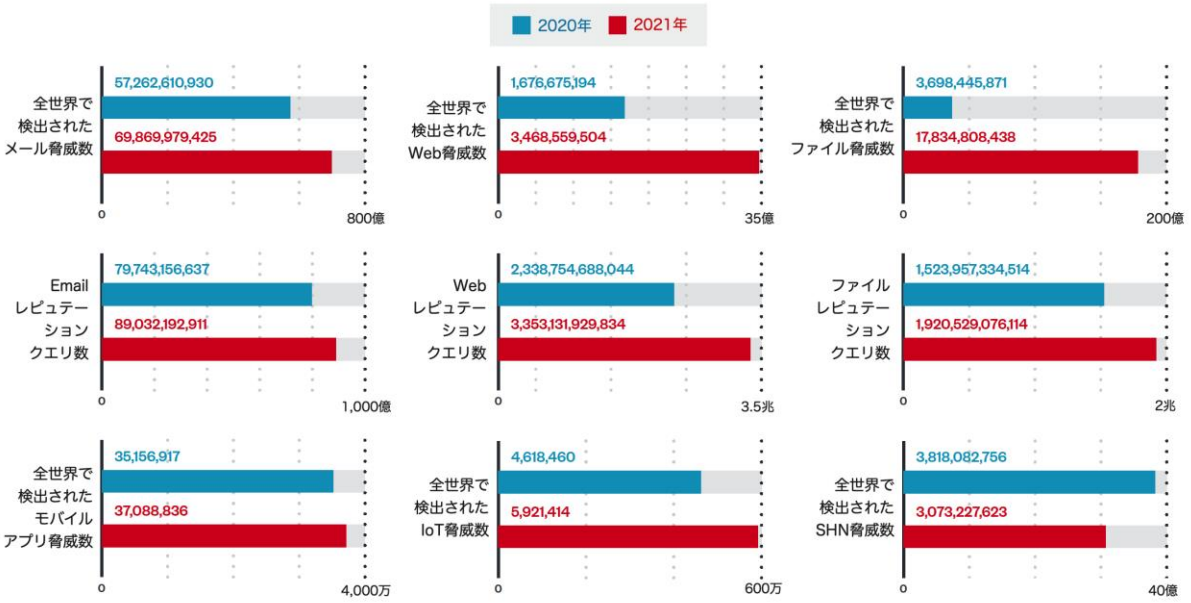


図 20：全世界で検出された脅威数およびクエリ数の推移

2021 年の脅威の状況を支配したマルウェアファミリーは、コインマイナーが筆頭で、Webshell および Ulise が僅差で続いています。2020 年のトップ WannaCry は、引き続きその中で唯一のランサムウェアとなりました。

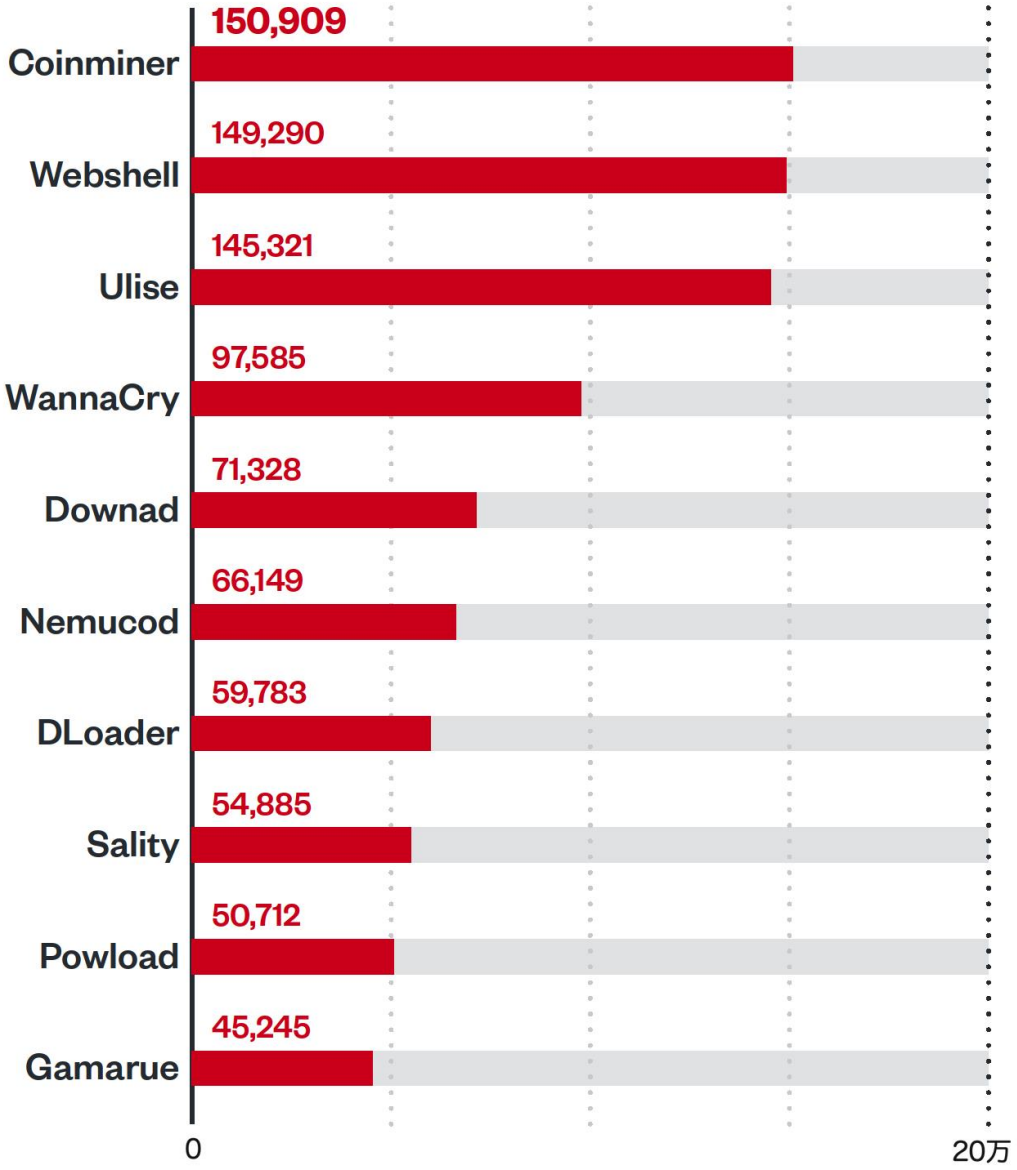


図 21：マルウェアファミリーの検台出トップ 10（2021 年）

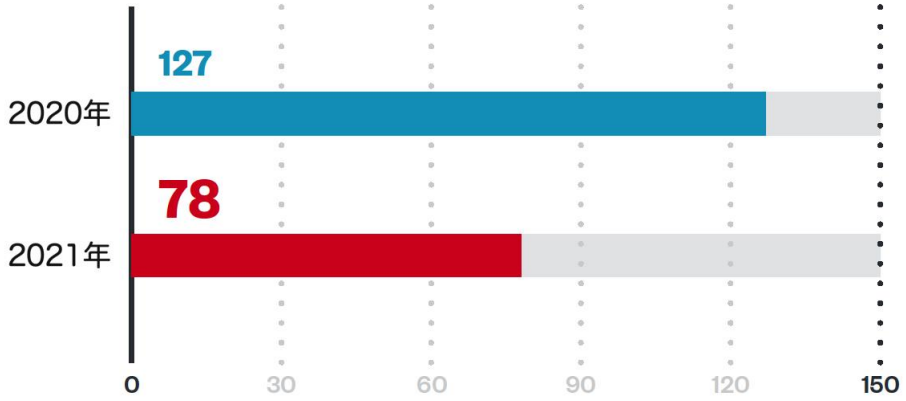


図 22：新たに発見されたランサムウェアファミリーの年間比較

2021 年に新たに発見されたランサムウェアファミリーは 78 件で、前年比 39%減となりました。

1月	2月	3月	4月	5月	6月
Amjixius	IziCrypt	TrojanLock	BlackHole	Apostrius	DarkRadiation
SophCrypt	Cryng	VoidCrypt	Nitro	Venus	Babuk
SharpCrypter	HDLocker	HogLocker	AstroLocker	Hades	FakeRyuk
Cicada	SickRansom	OnCrypt	Hanta	QLocker	LegionLocker
Crysis.Tibggh	Lucifer	DadiCrypt	WhiteBlackCrypt	FiveHands	GonnaCrypt
BlueCrab	Butwo	Assist		Taihenchan	
Judge	Flamingo	HelpYou		Networm	
Mijnal	CNHCrypt	ThunderCrypt		NoCry	
Namaste		GangBang			
Gunshot		DarkWorld			
GaryTest					
Moloch					
Psixtin					

7月	8月	9月	10月	11月	12月
Grief	Hive	Ransomart	KCry	Polaris	Splinjok
GoFive	Cyrat	Diavol	LokiLocker	QuantumLocker	BlackCat
RedDot	CalCrypt	Sanwai	TimeCrypt		Rook
HKitty	AvosLocker	AtomSilo	HQCrypt		
Epsired	BlackMatter	MorrisCrypt	Colossus		
	LockFile				
	Rantu				
	ChaosBuilder				
	Chaos				

表 3：新たに発見されたランサムウェアファミリー一覧（2021 年）

2021 年、モバイル端末の不正サンプルは前年比 14%増となりました。また、ブロックされた Android モバイルアプリの数も増加し、前年比 5%増となりました。

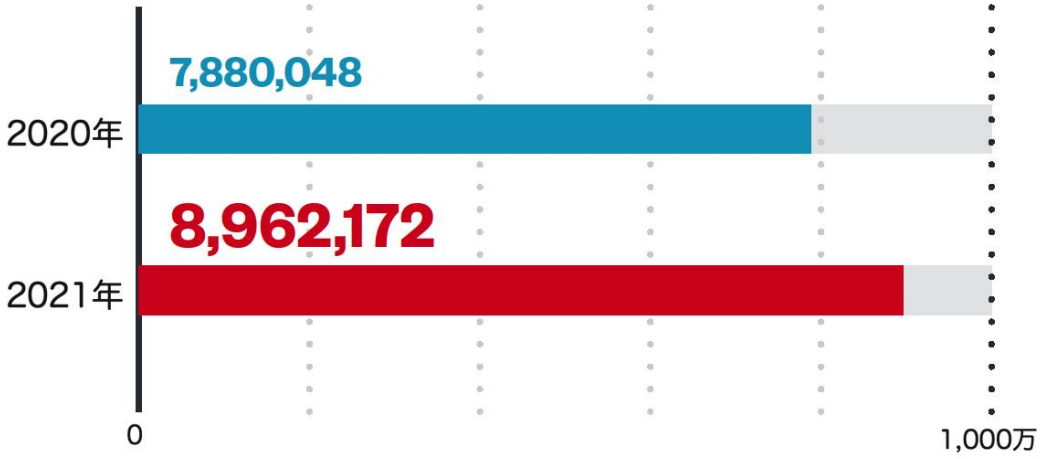


図 23：モバイル端末の不正サンプル検出数の年間比較

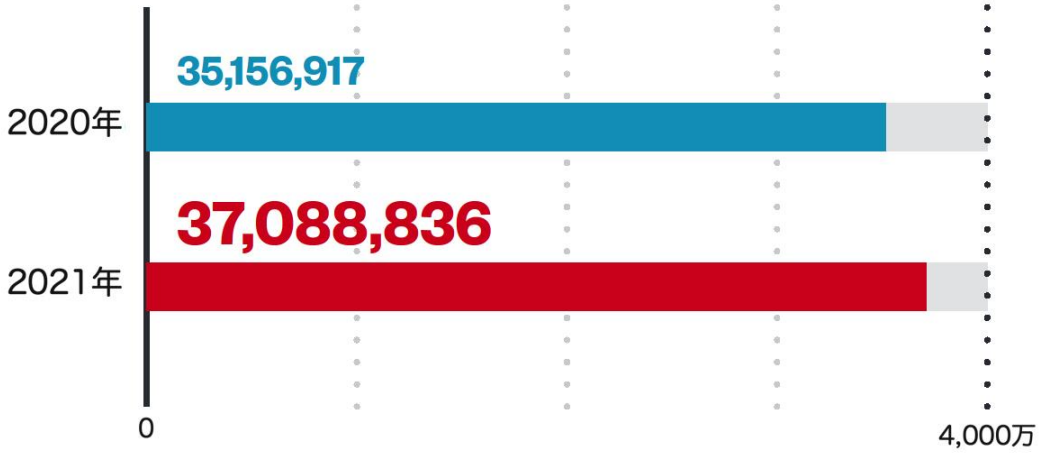


図 24：不正な Android アプリの検出台数の年間比較

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
http://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。