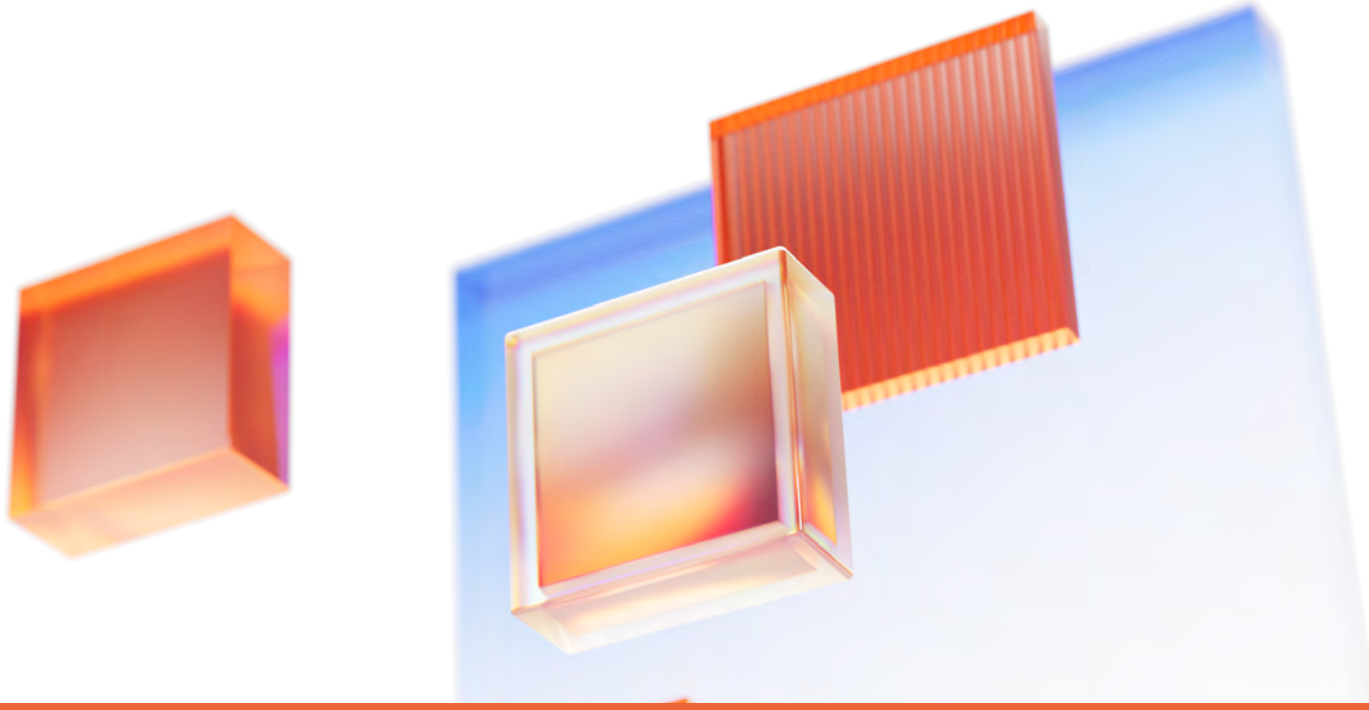
SONICWALL

2024 サイバー脅威レポート 中間アップデート

進化し続ける脅威の実用的なインサイト



はじめに

CEOからのご挨拶

今日のダイナミックな脅威の情勢において、当社のお客様は、巧妙化を続けるサイバー脅威から機密データ、システム、運用を保護するため、これまで以上に当社に信頼を寄せてくださっています。ランサムウェア攻撃からマルウェア、クリプトジャックまで、私たちが直面する攻撃者は絶えず進化しており、私たちは常に警戒を怠らず、積極的であることが求められています。

当社のパートナーシップと協力的な取り組みをさらに強化するために、SonicWall2024年版サイバー脅威レポート中間アップデートを発表いたします。このレポートは、進化を続ける脅威の情勢と、当社のパートナーやお客様のサポートへの絶え間ない注力を示すものです。サイバー犯罪者は、より効率的で洗練された戦術を加えています。マルウェアは前年同期比で30%増加し、IoTマルウェア（+107%）と暗号化された脅威（+92%）が急増しています。これらすべてが世界中のサイバー犯罪者の進化の土台となっています。

このレポートは、パートナー、MSP、MSSP、および顧客に実用的なインサイトを提供し、新旧を問わず、これらの脅威に立ち向かうための防御戦略の策定と導入を支援します。それが、当社がSonicWallサイバー脅威レポートの提供を続ける主要な理由です。そして今年は、当社の脅威データと、あらゆる組織が結び付けることができる必要がある信頼性の高いビジネスの成果を、より密接に関連付けています。

読者の皆様にさらに知識や情報を提供するため、当社は、365日週7日24時間体制のSOCアナリストからのフィードバックや、信頼できるサイバーセキュリティ保険会社が提供する市場に関するインサイト、さらに、一部の当社パートナーの声を含むいくつかの新しい視点を追加しました。

当社のパートナーの皆様には、本レポートを活用して、顧客がブランドやビジネスを守るために必要なサービスや製品について顧客との関わりを深めることをお勧めします。

私は、本レポートが当社のお客様の環境を効果的に保護するための共同の取り組みの基礎となることを確信しています。皆様からのフィードバックとインサイトは、これまでそして今後も、当社のアプローチと方向性を形成する際の助けであり続けています。

当社の信頼できるパートナーのグローバルなセキュリティネットワークと、Capture Labsの脅威研究者を含むSonicWallチーム全体を代表して、2024年版SonicWallサイバー脅威レポート中間アップデートで、サイバー脅威の情勢の最新の進化に関する当社独自の見解を共有できることをうれしく思います。

ボブ・ヴァン・カーク
SonicWall
代表取締役社長兼CEO

エグゼクティブサマリー

脅威の情勢

125%

当社のセンサーは、週40時間の業務時間内に、50時間分に相当する危険な攻撃を検出しました。読み間違いではありません、当社の通常のファイアウォールが、週40時間の業務時間中に125%の攻撃を受けていました。

さまざまな組織が、2024年の最初の5か月で46日分のダウンタイムの可能性を回避しています。

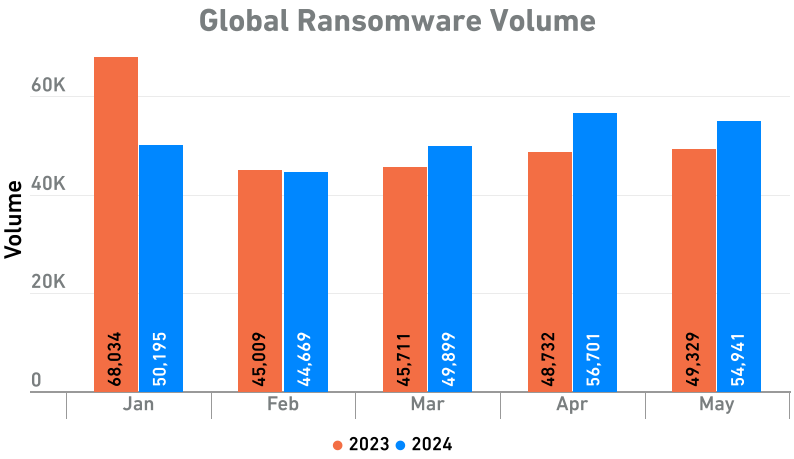
46日

12.6%

少なくとも全収益の12.6%が、適切な保護のない状態でサイバー脅威にさらされています。収益1,000万ドルの企業の場合は120万ドルに相当します。

ランサムウェア

ランサムウェアは南北アメリカで増加しています（北米：15%、ラテンアメリカ：51%）。ただし、EMEA（欧州、中東、アフリカ）地域は世界全体の数値を引き下げています。マイナス49%という検出値は、サイバーセキュリティ対策の向上と法執行機関の介入がプラスの影響をもたらしていることを示しています。



マルウェア

▲30%

マルウェアは3月から5月まで増加傾向であり、5月だけで92%という大幅な増加となっています。

15%

全マルウェアの15%は、ソフトウェアパッキングを主要なMITRE TTPとして利用しています。

IoTマルウェア

攻撃対象となったIoTデバイスは、平均で52.8時間攻撃を受けていました。

▲107%

暗号化された脅威

11001X
10XX11
001XX1
100X11
110X10

▲92%

暗号化された脅威は92%増加しています。サイバー犯罪者がさらに巧妙になっていることや、犯罪者がTLSで暗号化された転送を利用してネットワーク上でマルウェアやその他の脅威を送り込むケースが増え続けていることを示しています。

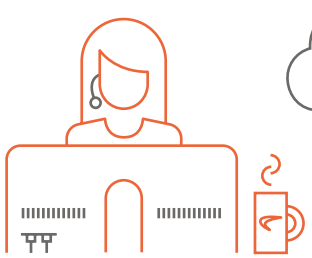
「SonicWall2024年版サイバー脅威レポート中間アップデートは、タイムリーな動向を紹介しています。また、パートナー、MSP、MSSP、および顧客にインサイトに満ちた動向を提供し、新旧を問わず、これらの脅威に立ち向かうための防御戦略の策定と導入を支援します。」

– SONICWALL社長兼CEO、ボブ・ヴァン・カーク

SOC

当社のマネージドサービスチームの顧客からのアラートの83%はクラウドアプリや侵害を受けた認証情報に関連するものです。

83%



RTDMI™

526個

— 新しい亜種 —

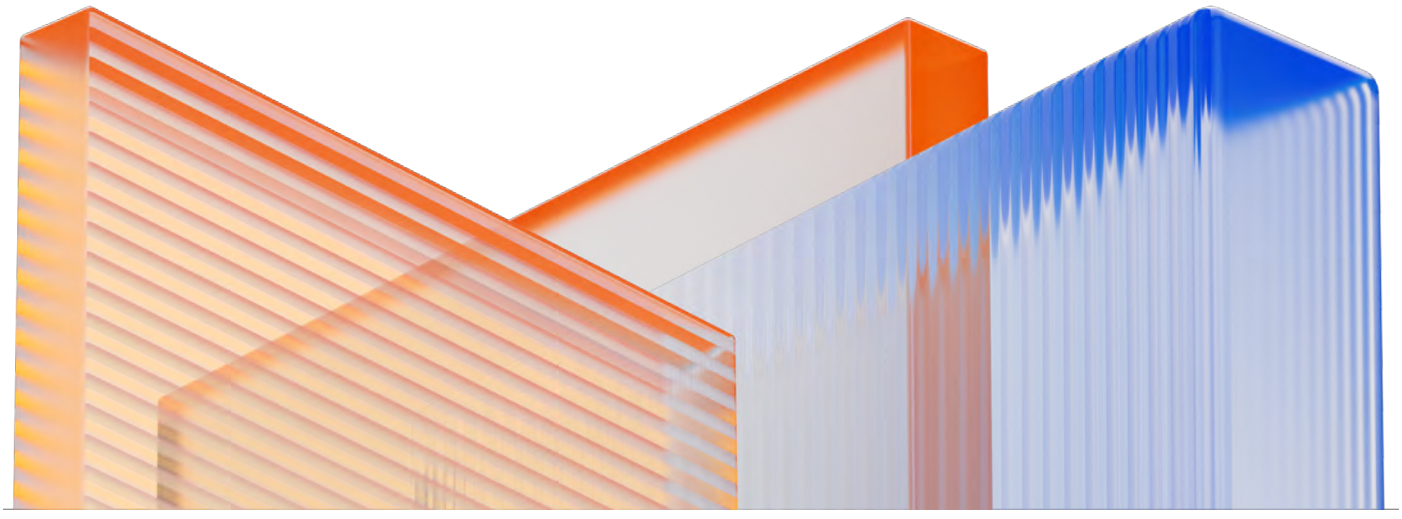
1日あたり

SonicWall Capture Advanced Threat Protection（ATP）およびReal-Time Deep Memory Inspection（RTDMI™）は、7万8,923個の亜種を検出しました。

クリプトジャック

▼60%

過去最高の年の後、クリプトジャックは60%減少しました。世界の大部分で減少しましたが、例外としてインドでは409%という驚異的な増加が確認されました。



指標の進化

SonicWallのサイバー脅威レポートの成熟に応じて、データを測定する方法を常に見直して分析することが重要です。このことは、セキュリティ上の脅威のダイナミックな情勢に適応するために不可欠です。新たな脅威が出現すると、攻撃対象領域が広がり、データの複雑さが増大します。従来の指標では不十分になり、誤った解釈につながる可能性があります。当社は、分析方法を継続的に改良することで、進化する脅威の意味合いをより適切に捉えて、異常の影響を軽減し、より正確なタイムリーで実用的なインサイトを確保することを可能にしています。本日、当社は、これまでHITS指標と呼ばれていたものから新しいTICKS脅威指標への移行により、データを業界に提供する方法が進化したことを発表します。これにより、当社のパートナーや顧客の皆様により有意義なインサイトを提供できると確信しています。

テレメトリデータを報告するためのTICKS指標への移行は、精度、信頼性、そしてファイアウォールのアクティビティの明確な測定方法の向上を求める意識が原動力となっています。TICKSは、1つのファイアウォールが特定の脅威から攻撃を受けた時間数を表すものです。

HITSの絶対数はシグネチャの記述方法によって異なる可能性があります。それは実際の脅威の特性ではなく、脅威を検出する技術の特性です。

TICKSは、デフォルトの時間の単位（1時間）に対する脅威の検出イベントを論理値（trueまたはfalse）に正規化します。

TICKS指標は、イベントの合計数をカウントするのではなく、1時間に少なくとも1回の攻撃を受信することによって、ファイアウォールが攻撃を受けている時間をカウントします。このような方法でデータを正規化して異常値に対する感度を下げ、攻撃の強度ではなく攻撃の期間に注目し、持続的な脅威をより効果的に浮き彫りにします。このアプローチによって、攻撃強度の偶発的な急上昇の影響を軽減し、早急な対応が必要な可能性がある持続的な脅威を強調します。また、サイバーセキュリティの脅威の評価における精度と信頼性を向上させ、ネットワークやシステムに対するより適切な意思決定とより効果的な保護戦略を支援します。

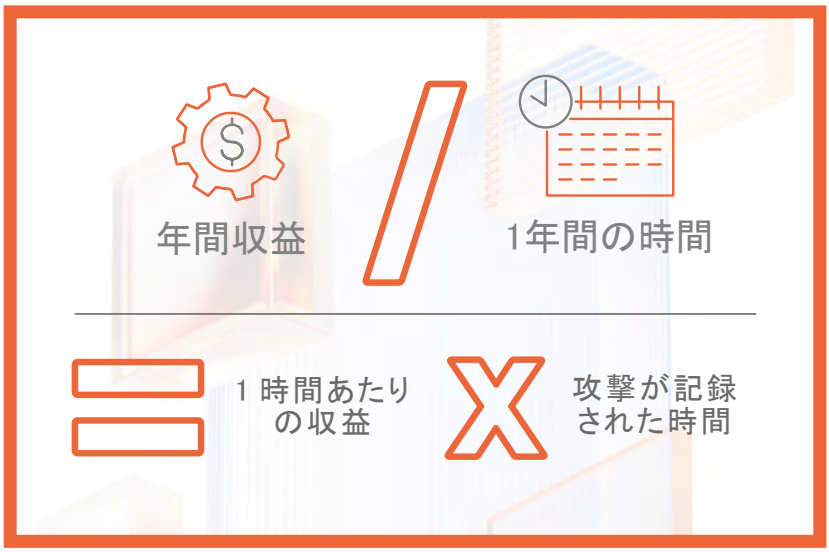
このような継続的な進化によって、当社は、データサイエンスとテクノロジーの進歩を活用して、パターンの検出、動向の予測、情報に基づいた決定を行う能力を向上させることも可能になっています。突き詰めれば、データ分析と測定の実践において最先端でいることが、堅牢なセキュリティ体制の維持、パフォーマンスの最適化、イノベーションの促進に不可欠です。

調査方法

前述のように、当社の指標は、悪意のある攻撃から当社の製品が保護した収益のおおよその金額を割り当てることができるレベルまで進化しています。当社では、1時間に生み出される収益を決定するために、年間収益を1年間の時間数で除算しています。

この式では、年間収益を1年間の時間数で除算して、1時間に生み出される収益を決定します。新たに導入したTICKSデータを活用して、その数値と、センサーが検出した危険な攻撃の時間の乗算を行います。

最終的な数値は、これらの既知の悪意のある攻撃によるリスクにさらされた最小の総収益を表します。この金額には、感染したシステムの修理や交換、脆弱性の修復、侵害を受けたハードウェアやソフトウェアの隔離など、潜在的な追加費用は含まれていません。



最新の動向の発表

当社のパートナーは、サイバー脅威レポート中間アップデートを活用して今年の上半期から発生している最新のセキュリティ動向を特定することで、サイバー犯罪者の行動をより正確に理解し、各社のセキュリティ戦略を強化することを可能にしています。

サプライチェーン攻撃の激化

サプライチェーン攻撃は、重大なサイバーセキュリティの脅威としての地位を固め、巧妙さや影響力を高めています。これらの攻撃は現代の企業の相互接続性を悪用しており、サードパーティのソフトウェアやサービスの脆弱性を標的にして、より広範なネットワークを侵害します。2024年上半期には、JetBrains　TeamCityの認証バイパスなど、数多くの幅広く報道されたインシデントが見られ、これらの攻撃のまん延する性質や深刻な結果が浮き彫りになりました。

SonicWallの分析では、古い脆弱性は、特にリソースが限られている中小企業（SMB）にとって依然として大きなリスクであることが浮き彫りになっています。以前のレポートのように、2023年末までに最も広範囲に渡った攻撃のトップ5のうち3つはサプライチェーン関連であり、顧客の50%以上がLog4jやHeartbleedなどの古い問題を含む、サプライチェーンの脆弱性の影響を受けています。

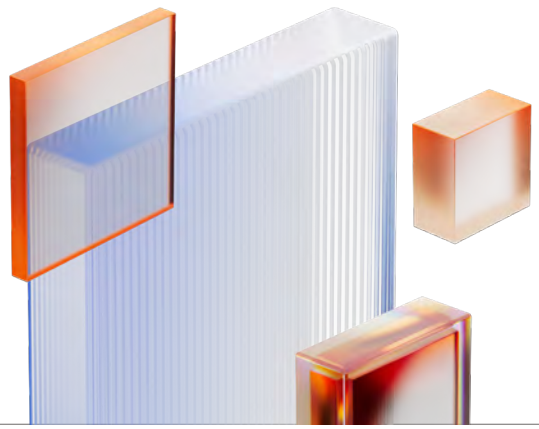
サプライチェーン攻撃の複雑さ

サプライチェーン攻撃は、サードパーティである取引先やパートナーの脆弱性を通じて企業のネットワークに侵入します。サイバー犯罪者は、ソフトウェアアップデート、ライブラリや相互接続されたシステムの弱点を悪用して、機密データやシステムへの不正アクセスを行います。この方法は、直接的な攻撃を注視する従来のセキュリティ対策をバイパスし、検出と防止を困難にするため、特に効果的です。

JetBrains TeamCityのインシデント

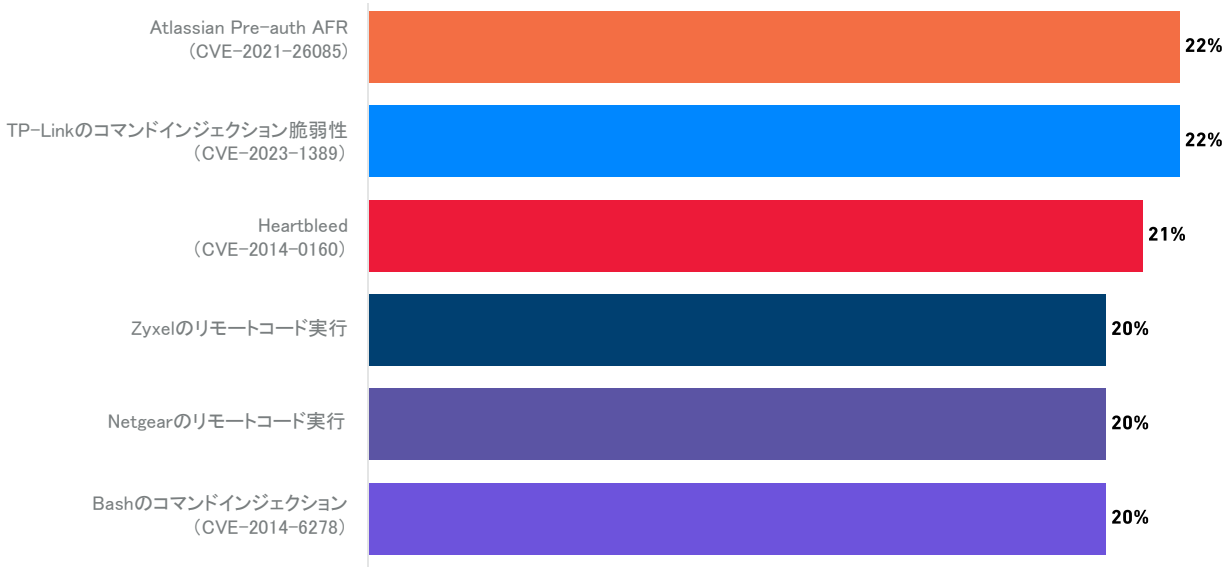
2024年3月に、サイバー犯罪者は、人気の高いCI/CDツールであるJetBrains　TeamCityの脆弱性を悪用しました。当社の調査では、攻撃者は404のレスポンスをレンダリングしてJSPクエリパラメータを操作することによって認証メカニズムをバイパスし、影響を受けるシステムをフル制御できる可能性があることが判明しました。米国サイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA）は、直ちにJetBrainsの脆弱性（CVE-2024-27198）を既知の悪用された脆弱性のカタログに追加しました。

当社のテレメトリデータによると、この脆弱性を悪用したサイバー犯罪者は当社の全顧客の16%を標的にしており、この脆弱性が悪用しやすく、サイバー犯罪者にとって価値があることが明らかになりました。これらの攻撃の83%は3月に発生し、その後数か月で大幅に減少しました。このインシデントは、攻撃者は組織がパッチを実装する必要がある時間帯に頻繁に悪用を行うため、迅速なパッチ適用が非常に重要であることを強調しています。



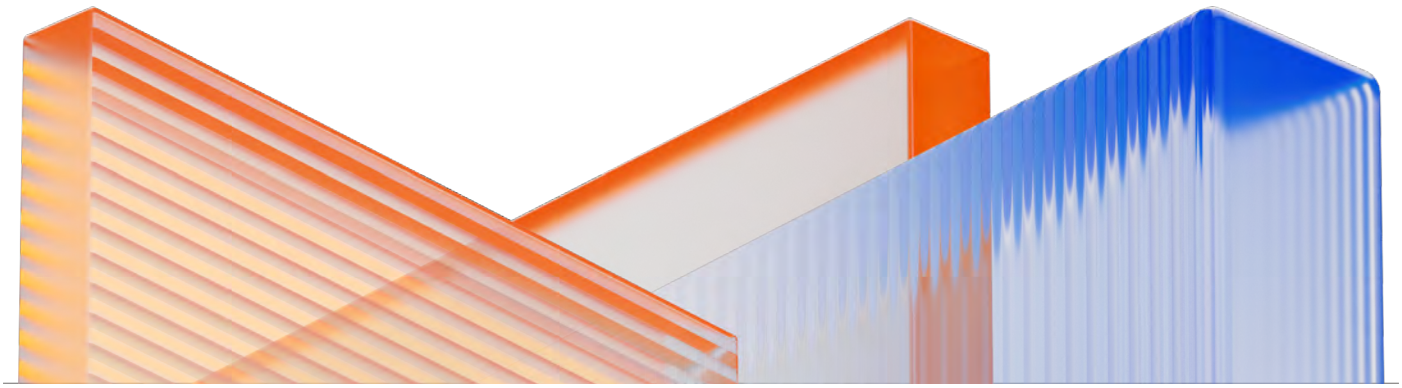
JetBrains TeamCityの脆弱性の悪用が報告されたことで、サイバー犯罪者はJasminランサムウェアやXMRigクリプトマイナーを展開し、深刻なデータ侵害、大量のリソース消費、運用の混乱を引き起こしました。SonicWallは、2024年上半期にクリプトマイナー攻撃が60%減少したことを報告していますが、これらの特定の脆弱性の悪用は、クリプトジャックの脅威が続いていることを示しています。

2024年に拡大しているネットワーク攻撃トップ5



SOCの視点

サプライチェーンの脆弱性を防ぐには、徹底が必要です。強固なセキュリティ体制を確保するには、サードパーティのソフトウェアやサービスのすべてを把握する必要があります。堅牢なパッチ管理プロトコルは、Log4jやHeartbleedなどの悪用され続けている古い脆弱性にさらされる可能性を低くするために役立ちます。業界のレポートでは、重大な脆弱性の50%であっても、組織はパッチの適用に平均で55日かかっています。MSPは、自動的なパッチ適用と専門家によるセキュリティテストを提供し、高額な費用や社内リソースを必要とすることなく、高度なセキュリティ対策の導入を可能にします。



ビジネスメール詐欺(BEC)攻撃の台頭:サイバー保険の観点から

近年、ビジネスメール詐欺(BEC)攻撃を中心として、サイバー脅威が大きく進化しています。当社の保険パートナーは、ランサムウェアインシデントごとに平均で10件のBECイベントが発生していることを確認しており、すべての兆候が増加傾向を示していると考えています。Microsoft Office 365(O365)の設定ミス、特にActive Directoryレベルでの設定ミスもBECインシデントの増加の要因となっています。

BEC攻撃は主にソーシャルエンジニアリングの手口を用いており、報告されたインシデントの70%は、何らかのタイプのソーシャルエンジニアリングを利用しています。多くの場合、これらの高度な攻撃は、個人を操り、資金の送金や機密情報の送信を引き起こします。一例として、攻撃者は被害者のメールアカウントの一部を管理し、不正な請求を送信したり、返信をRSSフィードにルーティングしたりしていました。この手口では、被害者がメールを管理しているかのように見せかけます。その一方で、攻撃者はメールを介して確認の電話に応答し、クライアントに電信送金を安全に進めることができると偽って安心させます。その結果、数百万ドルが不正な口座に送金されてしまい、回収できる可能性はほとんどありませんでした。

別のインシデントでは、ベンダーが侵害され、中間者(MITM)攻撃につながっています。この攻撃では、ベンダーと顧客との間のやり取りは本当のものでしたが、サイバー犯罪者は送金の指示を変更することができました。その結果、顧客は取引が正当なものであると信用し、多額の金額(時には数百万ドル)を別の不正な口座に送金してしまいました。

これらのインシデントは、保険金の請求に問題を引き起こします。通常、保険契約では電信送金指示の変更を確認する必要があります。しかし、やり取りが本当のものであるように思えると、多くの場合、このステップが見落とされます。堅牢なメールフィルタリングサービスとセキュリティスタックを備えていても、侵害された通信チャネルの信憑性によって、これらの攻撃はすり抜けます。

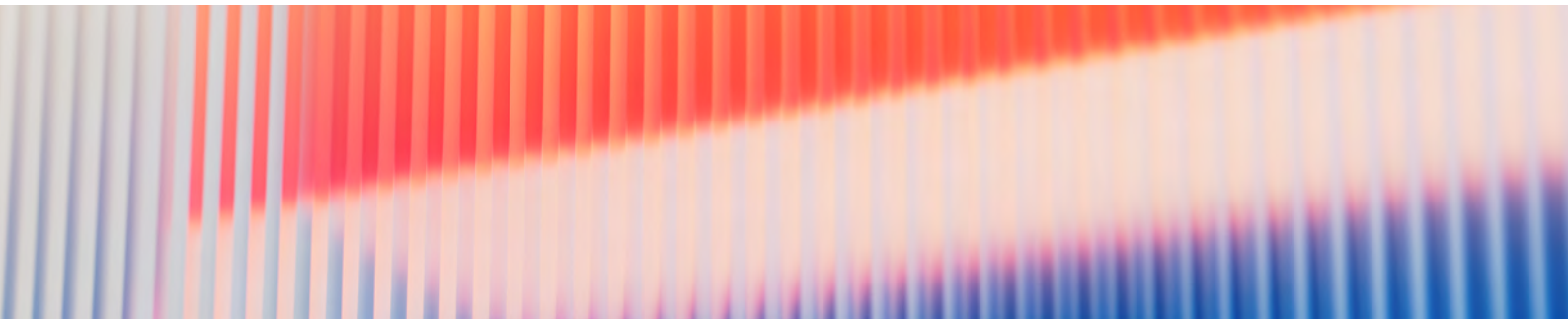
保険の視点

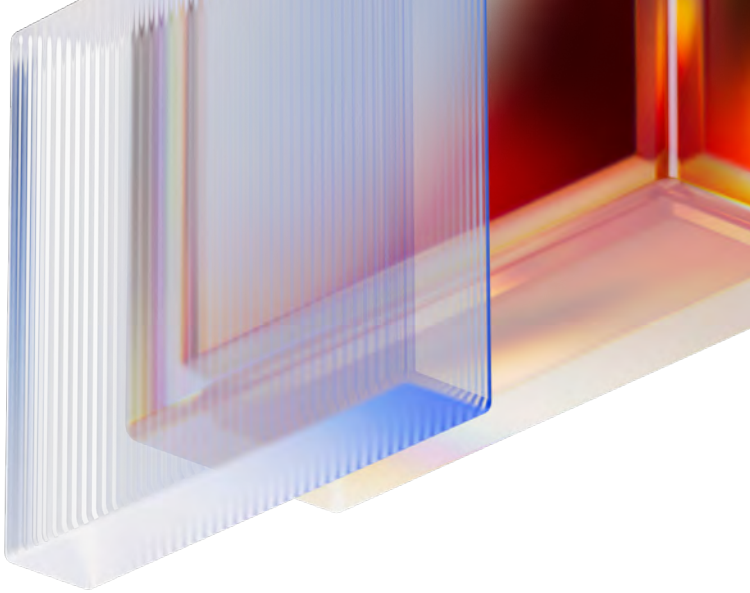
当社の保険パートナーは、ランサムウェアインシデントごとに平均で10件のBECイベントが発生していることを確認しています。

パートナーのインサイト

「脅威の情勢は、組織と組織を守るチームにとって完全に圧倒的な存在です。ほとんどのサイバーセキュリティの侵害には、ある程度のヒューマンエラーが含まれています。突き詰めれば、ヒューマンエラーに対処する方法は2つあります。機会を減らすことと、ユーザーを教育することです。エラーが発生する機会が少なければ少ないほど、検査対象のユーザーも少なくなります。そして、知識が多ければ多いほど、ミスをするような機会に直面しても、ミスを犯す可能性が低くなります。」

STEVEN HUANG氏 – Fornida社COO
SonicWallパートナー





ハッカーは深刻度の低いMicrosoft製品の脆弱性を標的に

今年初めに、SonicWallは、2023年からMicrosoftがリリースしたパッチと脆弱性のレビューを公開しました。この調査では、かなりの数の脆弱性が存在していますが、すべての脆弱性を同等に扱うべきではないことを示しました。Microsoftは2023年に900件以上の脆弱性にパッチを適用しましたが、本当に懸念すべきことは、攻撃者がこれらの弱点をどのように悪用したかです。

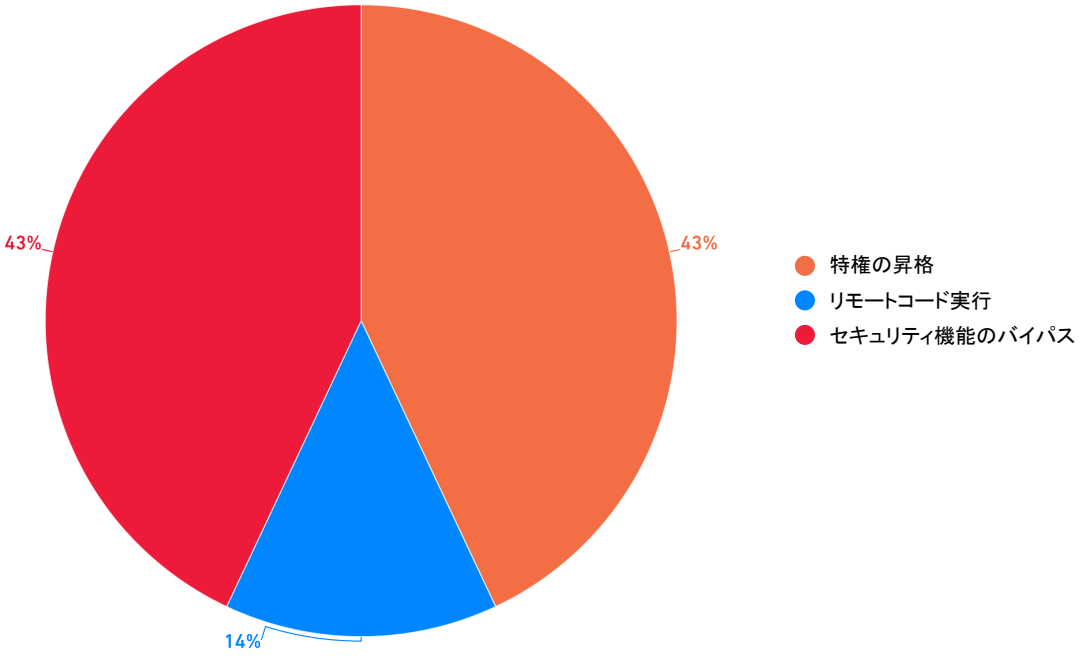
Microsoftがパッチを提供した脆弱性を検討すると、リモートコード実行（RCE）が36%を占めています。RCEの脆弱性が脆弱性全体のかなりの部分を占めているにもかかわらず、RCEの悪用はわずか5%でした。一方、特権の昇格の脆弱性は、2023年に52%の確率で利用されました。

2024年の中間の時点で、434件のMicrosoftの脆弱性が報告され、パッチが提供されています。前年比では同じ件数です。興味深いことに、報告された脆弱性の約40%がリモートコード実行（RCE）に分類されていますが、悪用されたRCEの脆弱性は1つのみです。悪用されたMicrosoftの脆弱性の86%は、セキュリティ機能のバイパスまたは特権の昇格の脆弱性です。このことは、サイバーセキュリティ戦略でこれらのカテゴリを優先する必要性を強調しています。ただし、数値としてはあまり重大ではないように見えるかもしれません。

SOCの視点

組織は、まん延しているRCEと、より頻繁に悪用されている特権の昇格の脆弱性の両方に対処し、バランスの取れたアプローチを維持して、堅牢なセキュリティを確保する必要があります。自動的なパッチ適用は、ユーザーの介入を必要とせずにソフトウェアの更新の適用を可能にします。多くの場合、MSPによって実装されます。このアプローチでは、迅速に脆弱性に対処することによってセキュリティを強化し、潜在的なエクスプロイトにさらされる時間を短くします。重大度の認識は問いません。

悪用されたMicrosoftの脆弱性



脅威の解放

Androidデバイスは、特にRATによって、サイバー犯罪者からますます標的にされています。RATと言っても、チーズを食べるタイプではありません。遠隔操作型トロイの木馬（RAT）のことです。これらのRATは、正当なアプリを偽って権限を取得し、コマンド/コントロールサーバーに接続して認証情報を盗み、多要素認証（MFA）をバイパスします。今年はAnubis、AhMyth、Cerberusなどの著名なRATがサイバー犯罪者によって広く利用されており、MFAをバイパスするように適応しています。4月に、当社のレポートで、人気の高いアプリのアイコンを使ったRATがユーザーを騙して権限を付与させ、アクセシビリティサービスを通じた2要素認証コードの取得や機密情報への不正アクセスを可能にしていた複数の活動について報告しました。

マルウェアのアップグレード

Anubis：バンキング型トロイの木馬です。現在は、ワンタイムパスワード（OTP）を使用してSMSメッセージを取得することによってMFAをバイパスする機能が含まれ、Google Playストアで大きな脅威となっています。

AhMyth：現在も利用されている、2017年から存在するRATです。さまざまなストアで感染したアプリを通じてAndroidデバイスを標的にし、キーロギングの実行、スクリーンショットの取得、MFAのOTPの傍受を行います。

Cerberus：少なくとも2019年から存在しています。SMS制御、キーロギング、音声の録音などの機能を備えたMalware as a Service（MaaS）として動作し、OTPを傍受して不正なトランザクションのためにMFAをバイパスすることが可能です。

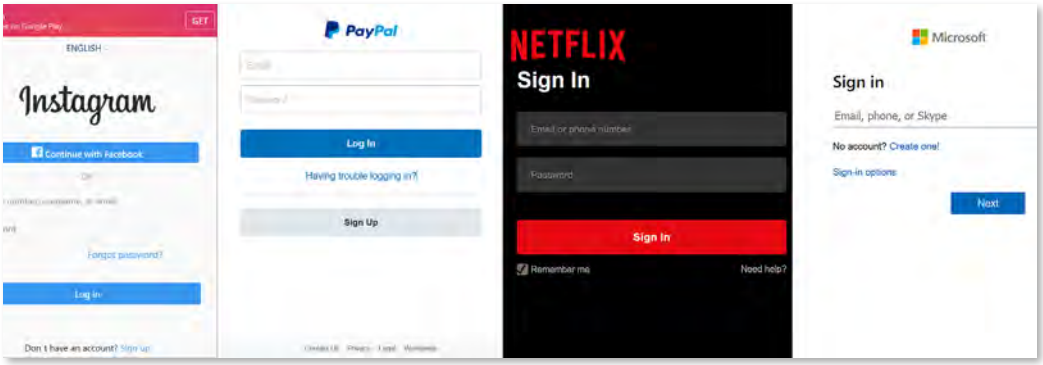


図1：不正なモバイルログインページの実際の例

SOCの視点

セキュリティオペレーションセンター（SOC）の視点では、ロケーションベースのアラートは、地理的に異なる場所からのアクセスの試みによってトリガーされ、セキュリティの脅威の可能性を示します。たとえば、ユーザーが通常はニューヨークからログインしている場合、ロシアからログインしようとするとアラートがトリガーされます。これらのアラートは、MFAセキュリティを強化するために不可欠であり、SOCアナリストが不正アクセスの試み、特に侵害された認証情報や位置情報を操作するマルウェアに関連するアクセスの試みを特定して軽減するために役立ちます。当社のマネージドサービスチームはすでに7,400件以上のロケーションベースのアラートを確認しています。2023年のアラートを10%上回るペースです。

保険の視点

攻撃者は常にMFAをバイパスする方法に注目していますが、MFAを展開していない組織も依然として見られます。その場合、攻撃の難易度が大幅に低下します。多くの場合、影響を受ける電子メール、電子メールシステム、またはサーバーでMFAが有効になっていない場合、ほとんどの保険会社は保険金を支払いません。 MFAの使用は「サイバーシートベルト」を着用するようなものです。自動車衝突事故を防ぐわけではありませんが、自身の組織を保護し、保険会社で可能な限り良い立場を確保するために重要な要素です。

PowerShell:諸刃の剣 – マルウェアファミリーの90%以上に悪用されています

PowerShellは、強力なスクリプティング機能、オブジェクト指向の性質、Windowsオペレーティングシステムと通信するための豊富なインターフェイスによって、開発者やシステム管理者の間で人気があります。Windowsとの緊密な統合によってユーザーはさまざまなタスクを自動化でき、正当な用途の場合は価値のあるツールになります。

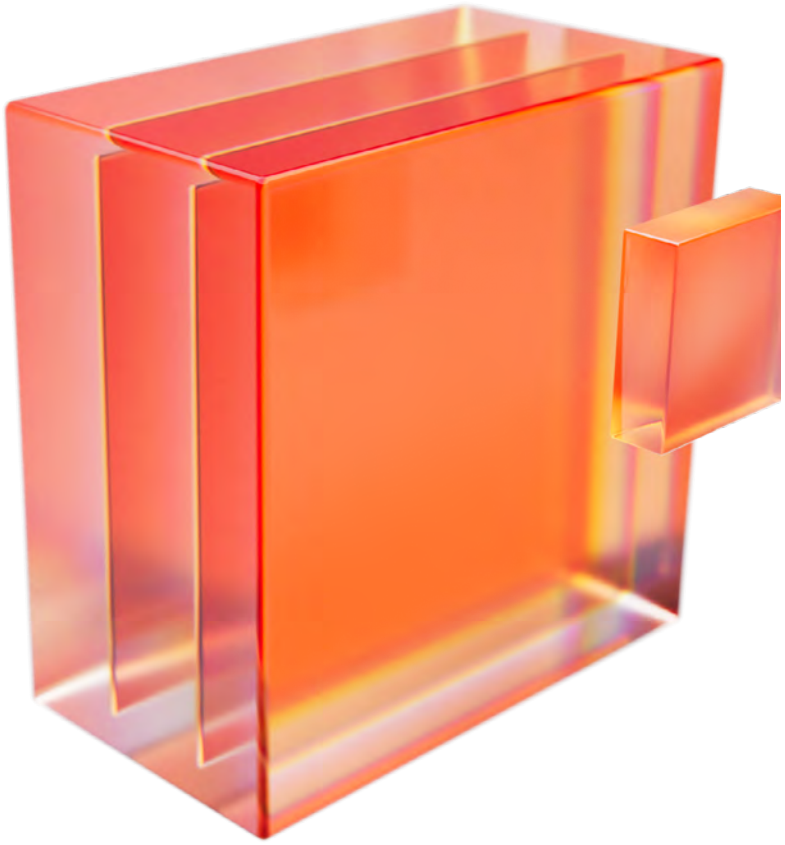
しかし残念なことに、これらの同じユーザーフレンドリーな機能が、PowerShellをサイバー犯罪者にとって魅力的なツールに変えてしまっています。まん延しているマルウェアファミリーの90%以上がPowerShellを利用しており、73%がPowerShellを使ってマルウェアを追加的にダウンロードしたり、検出をバイパスしたりしています。基本的に、PowerShellはマルウェアファミリーにとっての「主食」です。AgentTesla、GuLoader、AsyncRAT、DBatLoader、LokiBotなどの著名なマルウェアファミリーは、さまざまな悪意のあるタスクでPowerShellスクリプトを幅広く利用しています。

PowerShell は、実行ポリシーの制限を用いて、ダウンロードされたスクリプトの実行を防ぐための幅広い取り組みを行っています。不幸にも、攻撃者はスクリプトをローカルで呼び出したり、コマンドライン引数を使用して悪意のあるコードを実行したりすることによって、これらの制限をバイパスする方法を発見しました。

最近のレポートは、PowerShellベースの攻撃が大幅に増えていることを示しています。PowerShellを利用する脅威の数は2020年後半に208%増加し、ほぼすべてのマルウェアファミリーによる利用が最大レベルまで増えています。この急増は、プロセスインジェクションや特権昇格の技術など、さまざまな種類の攻撃でPowerShellの利用が増加していることによるものです。ファイルレスマルウェア攻撃でのPowerShellの利用も増えています。スパムメールやOfficeドキュメントマクロに埋め込まれたPowerShellスクリプトを介してペイロードを配信する多数の活動で確認されています。

SOCの視点

当社のマネージドサービスは、PowerShellに関連するリスクを熟知しています。2024年のインシデントでは、サイバー犯罪者が認証情報を盗むために広く使用しているMimikatzツールによって、複数のマシンが侵害されました。調査の結果、エンコードされたPowerShellスクリプトが複数のマシンで実行されていることが判明しました。このスクリプトは、Mimikatzをダウンロードして、悪意のあるPowerShellコマンドをさらに実行する役割を果たしていました。残念なことに、当時のセキュリティポリシーは、このようなスクリプトをブロックするのではなく警告を発するように策定されていたため、悪意のあるアクティビティが拡散して問題を引き起こす可能性がありました。攻撃者は、ネットワーク内の侵害された保護されていないマシンを悪用して、内部でこれらの有害なスクリプトの展開や拡散を行いました。このインシデントは、サイバー攻撃におけるPowerShellの悪用を抑制するためには、堅牢なセキュリティ構成とセキュリティアラートへの積極的な対応が重要であることを浮き彫りにしました。



IoT攻撃のリスクの高まり

2024年に、IoTセキュリティの情勢は拡大を続けており、IoT（モノのインターネット）デバイスを標的とした攻撃が大きく増加しています。当社のデータでは、2024年上半期のIoT攻撃は前年比で107%というきわめて大幅な増加を記録しています。この増加は、攻撃者がIoTデバイスを標的にする頻度が高くなっていることを浮き彫りにしています。これは、IoTデバイスが標的になりやすい傾向があるという事実によるものでしょう。Microsoft　Windowsなどの主要なシステムの攻撃対象領域は堅牢化が続けられていますが、これらのデバイスは、多くの場合、堅牢なセキュリティ対策が欠けています。

TP-Linkのコマンドインジェクションの脆弱性（CVE-2023-1389）は、サイバー犯罪者によって悪用される数多くの脆弱性の中で重大な脅威となっています。この脆弱性は、2024年に攻撃が激増している主な要因の1つであり、5月には顕著な急増が確認されました。2番目に広範囲にわたる攻撃として順位づけられており、中小企業（SMB）の21.25%が影響を受けています。この不具合の悪用は、悪名高いMiraiマルウェアの拡散の原動力であり、IoTデバイスを乗っ取り、大規模な分散型サービス拒否（DDoS）攻撃を実行できるボットネットを形成します。当社のチームのレポートでは、サイバー犯罪者によって悪用される脆弱性の活動の増加と共通の特徴について報告しています。この脆弱性は2023年から存在していましたが、攻撃者が大量に利用し始めたのはつい最近のことであり、古い脆弱性を悪用するという広範囲にわたる動向と一致しています。

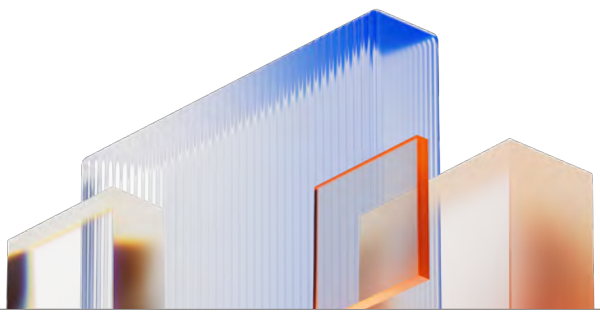
もうひとつの悪用されている重大な脆弱性は、2024年に4番目に広範な攻撃として順位付けされているZyxel Remote Code Executionの不具合です。この脆弱性は中小企業の20.5%に影響を及ぼしています。Miraiの拡散の手助けにもなっており、このマルウェアのまん延性をさらに強調しています。

IoT攻撃の影響

IoT攻撃の増加は、世界中のサイバーセキュリティリーダーにとって大きな懸念事項となっており、Volt　Typhoonボットネット攻撃やデンマークのエネルギーセクターへの組織的な攻撃などのインシデントは、脅威が拡大していることを示しています。Volt　Typhoon攻撃では、中国の国家的な支援を受けたハッキンググループが米国内の数百台のSOHOルーターを侵害し、重要なインフラストラクチャを標的とするさらなるハッキング活動を隠すために使用されるボットネットを形成しました。これらの侵害されたルーターは、主にCiscoとNetgearのもので、旧型でサポート対象外であったため、特に悪用に対して脆弱でした。

同様に、2023年5月に、デンマークのエネルギー関連企業22社を標的とした組織的なサイバー攻撃が発生しました。ハッカーは、Zyxelファイアウォールの複数の脆弱性を悪用し、システムの制御権を取得してコマンドを実行しました。この攻撃は、デンマークの重要なインフラストラクチャに対する攻撃として過去最大規模のものであり、攻撃者がエネルギーの運用を妨害したり、侵害されたデバイスをDDoS攻撃に使用したりできることを浮き彫りにしました。

これらのインシデントは、2024年上半期に観測された傾向と一致しており、IoTデバイスを標的にして活用する攻撃者は大幅に増えています。IoTデバイスは重要なインフラストラクチャに不可欠であることが多いため、攻撃が成功すると、サイバー犯罪者にとって利益率が高くなる可能性があります。



フィッシングの手口:HTML、AI、QRコードによるサイバーセキュリティの再定義

フィッシングの手口は、長い歴史があるため、より巧妙になり、高度なテクノロジーを活用するようになりました。HTMLフィッシングは、依然として認証情報を盗むために普及している有効な方法です。当社のデータでは、2023年の第4四半期から2024年上半期にかけて、月平均で1,200件以上の新たな脅威が確認されています。通常、攻撃者は警告の文面を使用して被害者を怖がらせ、重要なドキュメントを表示するための認証情報を入力させます。場合によっては、メールアドレスを事前に入力してパスワードのみを要求します。入力してしまうと、認証情報は悪意のあるサーバーに送信されます。ユーザーは、疑いを避けるために正規のウェブサイトにリダイレクトされます。これらのHTMLファイルは、多くの場合、検出を回避するため、iframeリダイレクトやJavaScriptなどの手法を使用して難読化されています。

最近では、QRコードフィッシング(または「クイッシング」)の台頭という動向が確認されています。クイッシングでは、攻撃者はフィッシングメールにQRコードを埋め込み、受信者にスマートフォンでスキャンするように促します。通常、これらのコードによって、Microsoftなどの正規のログインページを模倣したフィッシングURLにつながり、認証情報を収集します。業界レポートによると、クイッシング攻撃は大幅に増えており、2021年の0.8%から、2024年には全フィッシング攻撃の10.8%まで増加しています。この方法は、スマートフォンやQRコードの利用の拡大を悪用するため、特に効果的です。QRコードはかつては比較的ニッチな存在でしたが、現在ではデパートやレストランのテーブルで見つけることができ、メニューやクーポンなどにつながります。このようなタイプの攻撃の増加は、一般的なQRコードの使用の増加と一致している可能性があります。

また、フィッシング攻撃も多角的になり、さまざまな通信チャネルを利用して成功率が高くなっています。人工知能(AI)は、フィッシング攻撃の効果を高めるために使用が増えています。AIツールによって、攻撃者は、より説得力があり、検出が困難な、高度にパーソナライズされたフィッシングメッセージを作成できます。攻撃者は、メールから始めてMicrosoft Teams、Slack、またはSMSに広げていき、フィッシングの試みの信頼性を高める可能性があります。このようなマルチチャネルのアプローチは、悪意のある攻撃者にとって利益率が高く、Microsoft Teamsのようなプラットフォームがこれらの二次的な攻撃の大部分を占めています。

フィッシングの手口は、人間の行動をより効果的に悪用するように進化してきました。2024年のフィッシングの情勢は、高度な検出と防止の対策を必要とする複雑な課題を示しています。

図1:クイッシングメール

SOCの視点

SOCは、MFAが無効になっている場合やパスワードに不適切にアクセスされた場合など、認証情報の侵害を助長する構成を積極的に監視します。2023年に、当社のSOCは、MFAの無効化に関連する800件以上のアラートに対処しました。驚くべきことに、2024年上半期だけで、同じ問題に対してすでに650件以上のアラートに対処しており、2024年はMFA関連のアラートの数が前年の約2倍のペースであることを示しています。この動向は、フィッシング攻撃の進化中の情勢と密接に関連しており、多くの場合、MFAの展開の弱点を標的としています。MFA関連のアラートの大幅な増加は、これらのフィッシング戦略の成功が増えていることを示しています。これらすべての動向を合わせて考えると、認証情報の侵害から保護するための、堅牢な監視の重要性が浮き彫りになります。

保険の視点

保険に関して報告されたランサムウェア攻撃のほとんどは、フィッシング型の攻撃が成功していることが原因です。

今日の進化し続ける脅威の実用的なインサイト

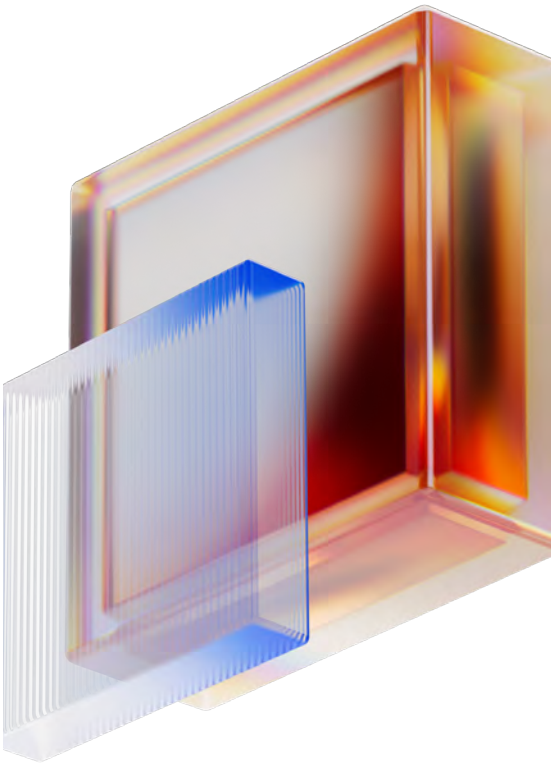
堅実なセキュリティ体制を構築する際に克服すべき課題

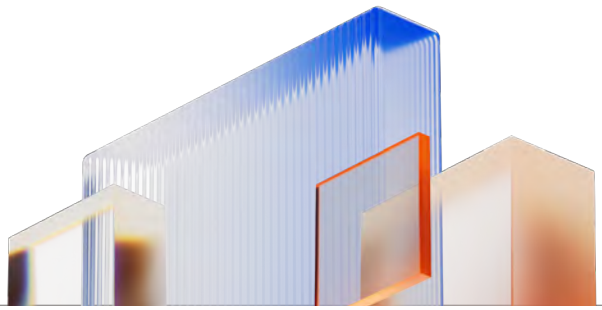
良好なサイバーセキュリティハイジーンを構築する際の課題について理解することは、非常に重要です。障害を特定することが、効果的なセキュリティ対策の導入を妨げる可能性がある障壁に対処するための最初のステップです。一般的な課題として、次のようなものがあります。

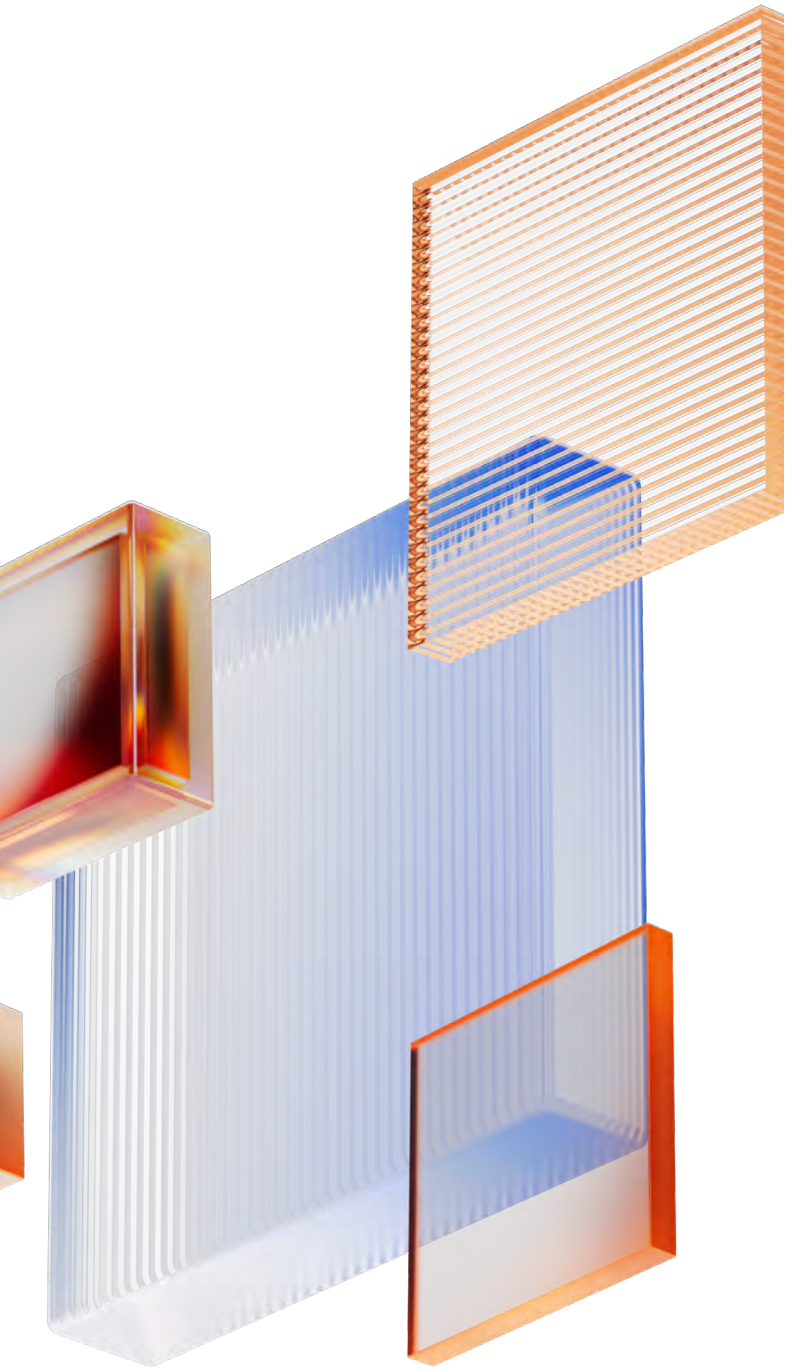
1. ヒューマンエラー：ヒューマンエラーは、誤って脆弱性を露呈したり、機密情報の処理をを誤ったりすることで、データ侵害や不正アクセスのリスクを高める可能性があるため、大きなサイバーセキュリティの課題をもたらします。
2. セキュリティソリューションの設定ミス：セキュリティソリューションの設定を誤ると、特にクラウド環境の場合、防御メカニズムの重大なギャップにつながり、システムやネットワークがサイバー脅威や不正アクセスにさらされるおそれがあります。
3. ブロックvsアラート：サイバーセキュリティでは、ブロック戦略とアラート戦略の選択がきわめて重要です。アラートに過度に依存すると、脅威がブロックされない可能性があります。また、過剰なアラートはアナリストの負担を増やし、アラート疲れを引き起こして重大なセキュリティインシデントが見落とされる可能性があります。
4. パッチ適用の先延ばし：多くの場合、脆弱性や類似するマルウェアは過去に公開済みであるにもかかわらず、更新が遅れたり、更新されなかったりすることにより、ソフトウェアやハードウェアはパッチが適用されていないままです。これでは、修正が可能になっても、デバイスは悪用に対して脆弱なままです。
5. デフォルト構成：多くの場合、ソフトウェアとハードウェアは初期設定の状態で最適に動作するようには設計されていません。時間をかけてハードウェアやデバイスを微調整することで、より高いレベルのセキュリティを確保できます。

SOCの視点

2024年に、当社のMSPの1社は、RDPが外部からアクセス可能なままであったために侵害され、ランサムウェアに感染した金融系の顧客に対処しました。このような既知の設定ミスは依然として見られ、組織にとって非常に大きなコストとなる可能性があります。







サイバーセキュリティ体制を強化するための積極的な手順

現代の脅威の情勢は、特にAIの台頭によって信じられないほど急速に変化しています。影響を受けない組織はありません。しかし、このレポートで概説されている攻撃や脅威の多くは適切なサイバーセキュリティハイジーンによって回避できるということには、変わりはありません。サイバーセキュリティ体制の大幅な強化を可能にする積極的な手順として、次のようなものがあります。

- 迅速なパッチ適用を優先する：定期的なパッチ適用は、脆弱性を減らし、驚異的なスピードで攻撃する悪意のある犯罪者による悪用のリスクを軽減するために不可欠です。
- 多要素認証（MFA）を追加：MFAは、パスワード以外の追加的な検証ステップを要求し、アクセス制御を大幅に強化して不正な侵入の試みを阻止することによってサイバーセキュリティを強化します。
- クラウドセキュリティを強化：企業は定期的にデータと運用をクラウドにプッシュするため、セキュリティサービスエッジ（SSE）やゼロトラストネットワークアーキテクチャ（ZTNA）などの堅牢な対策を導入してデータとアプリケーションを保護し、クラウド環境で、進化を続けるサイバー脅威に対する包括的な防御を確保する必要があります。
- 継続的な監視とインシデント対応：リアルタイムの脅威検出のためのツールを導入し、堅牢なインシデント対応計画を策定することによって、サイバー攻撃を迅速に抑制して封じ込めることができます。セキュリティオペレーションセンター（SOC）を利用して、人的レイヤーと週7日24時間体制の脅威検出の追加を検討します。
- ネットワークセグメンテーション：ネットワークをより小さく安全なセグメントに分割して、侵害や不正アクセスの影響を制限します。
- 継続的なトレーニング：進化を続けている脅威、防御戦略や規制について専門家から最新情報を入手し、脅威を迅速に認識して対応し、データ侵害や金銭的損失を防ぐには、継続的なサイバーセキュリティトレーニングが不可欠です。積極的なサイバーセキュリティ文化を育み、新たな脅威に対する組織の回復力を強化します。

重要なポイント

SOCの重要なポイント

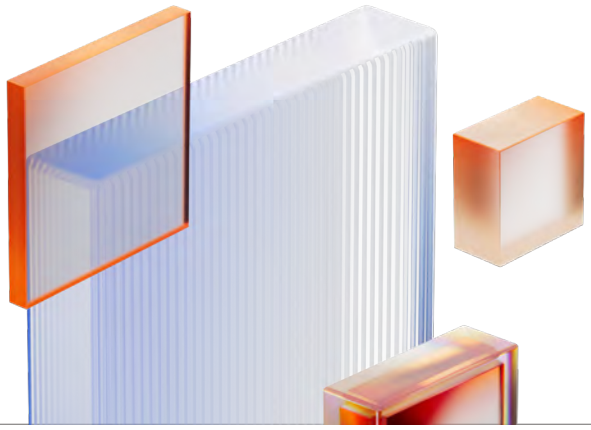
- 効果的なパッチ管理プロトコルは、古い脆弱性にさらされる可能性を低くするために役立ちます。
- 自動的なパッチ適用を導入することによってセキュリティを強化し、迅速に脆弱性に対処して、潜在的なエクスプロイトにさらされる時間を短くします。
- 火曜日の午前3時から午前6時の間は、多くの危険な攻撃のが発生する時間帯です。これは一般的に業務時間外です。
- ロケーションベースのアラートは、MFAによるセキュリティを強化し、SOCアナリストが不正アクセスの試みを特定して軽減するために不可欠です。
- セキュリティポリシーを単純なアラートではなくブロックに設定することで、悪意のあるアクティビティが拡大して問題が発生することを回避できます。
- SOCは、MFAが無効になっている場合やパスワードに不適切にアクセスされた場合など、認証情報の侵害を助長する構成を積極的に監視します。

保険会社の重要なポイント

- ランサムウェアがメディアの見出しの大部分を占めているにもかかわらず、ビジネスメール詐欺（BEC）攻撃はまだ存続しています。1件のランサムウェアイベントの発生に対して、BEC攻撃は10件発生しています。
- MFAを導入していない組織はまだ多いため、攻撃の難易度は大幅に低いレベルです。
- ほとんどのケースで、影響を受ける電子メール、電子メールシステム、またはサーバーでMFAが有効になっていない場合、保険会社は保険金を支払いません。
- 保険に関して報告されたランサムウェア攻撃のほとんどは、フィッシング型の攻撃が成功していることが原因です。

パートナーの重要なポイント

- ほとんどのサイバーセキュリティの侵害には、ある程度のヒューマンエラーが含まれています。
- これらのエラーに対処する最も良い方法は、機会を減らすことと、教育を強化することです。
- エラーが発生する機会を制限することは、よくあるミスの防止に役立ちます。



SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035 USA

www.sonicwall.com

SonicWall脅威レポートは、Capture Labsチームの不断の努力がなければ発行できませんでした。

SonicWallについて

SonicWallは、30年以上の実績を誇るサイバーセキュリティの先駆者であり、パートナーを通じてビジネスを展開するトップ企業です。クラウド、ハイブリッド、従来型ネットワークが混在する環境にリアルタイムでセキュリティを構築、拡張、管理するSonicWallは、無数の攻撃ポイントにわたってシームレスな保護対策を提供し、リモート、モバイル、クラウド化の進むユーザーを巧妙なサイバー攻撃から守ります。独自の脅威研究センターを持つSonicWallは、専用のセキュリティソリューションを短時間で経済的に提供し、企業、行政機関、中小企業など、世界中のあらゆる組織をサポートします。詳細は、www.sonicwall.comをご覧いただくか、Twitter、LinkedIn、Facebook、Instagramで当社をフォローしてください。

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035 USA

SonicWallでは、ベストプラクティスとして、データ収集、分析、レポート作成の方法を日常的に最適化しています。こうした業務として、データクレンジングの改善、データソースの変更、脅威フィードの統合といった方法を取り入れています。以前のレポートで発表された数値は、様々な期間、地域または業界にわたって調整されている場合があります。