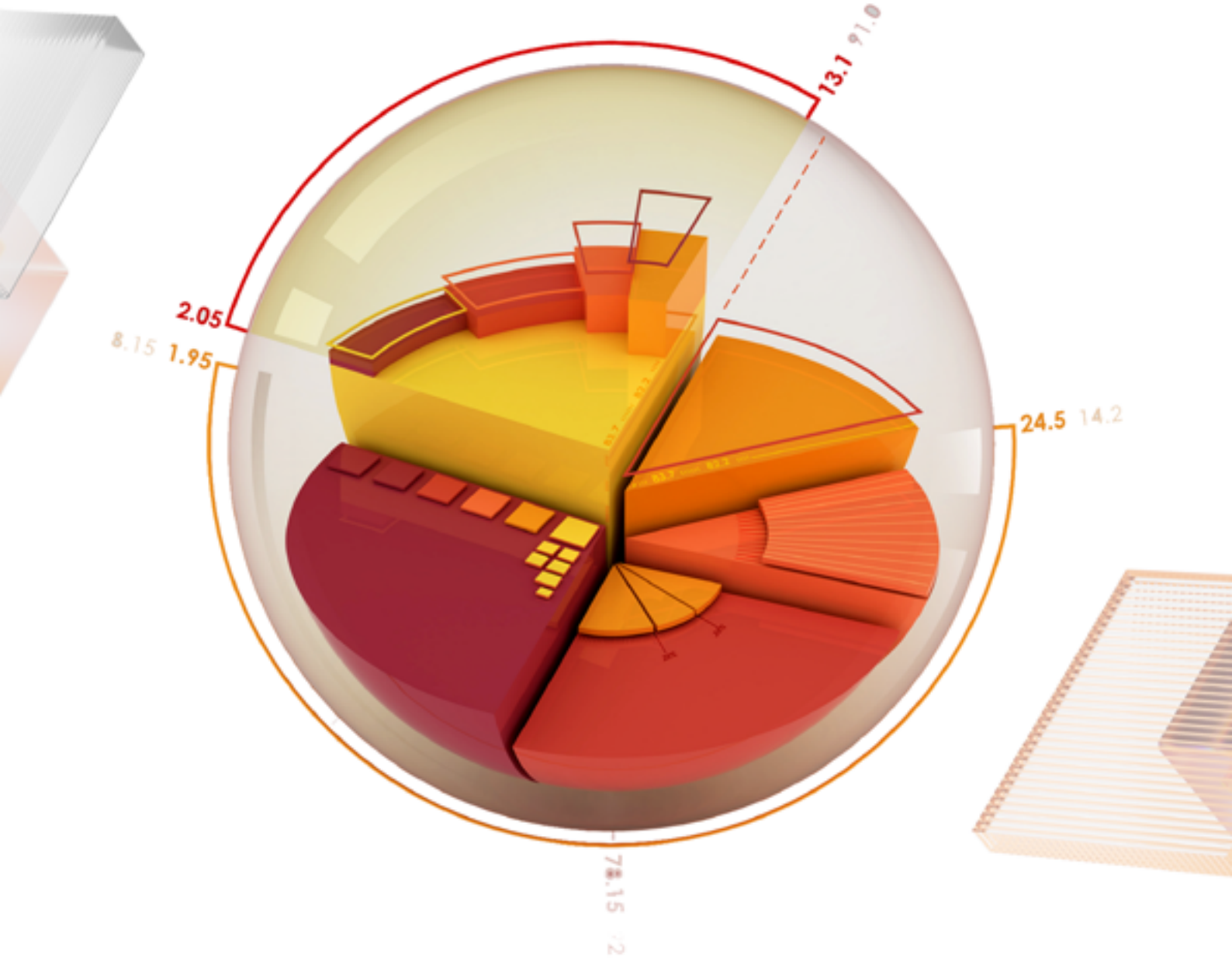
SONICWALL

2025 サイバー脅威レポート

サイバーセキュリティの戦場で勝利するためのスピードと強力な仲間の必要性



CEO、ボブ・ヴァン・カークからのご挨拶

私たちは皆、急速に変化し、ますます複雑化する脅威の情勢に直面しています。私たちが直面している攻撃者は執拗で絶えず進化しており、私たちの顧客は、信頼できる保護を求めてSonicWallを頼りにしています。新年の始まりにあたって、サイバー脅威から防御し、すべての人々の安全な未来を確保するための私たちの協力的な取り組みにおいて大きな助けとなっている重要なパートナーシップに、感謝の意を表したいと思います。システムとネットワークを守ることによって、私たちはコミュニティ全体の安全に貢献し、個人や組織がサイバー脅威を恐れることなくそれぞれの目標を達成できるように努めています。皆様と共にこのような取り組みを行うことができ、この上なく光栄に思っています。

サイバー犯罪者はこれまで以上に巧妙で執拗な戦術を用いており、危険度はかつてないほど高まっています。SonicWall のデータは、サイバー犯罪者の動きがこれまで以上のスピードであることを示しています。私たちは、悪用の実例が公開されてからわずか2日以内に大半のハッカーが脆弱性を悪用していることを確認しています。このような緊急対応の必要性は、あらゆる規模の企業、特に、対応に苦慮する可能性の高い中小企業（SMB）にとって大きなプレッシャーとなります。

2024年には、プロアクティブな防御戦略が急務であることを強調するような警戒すべき傾向が見られました。サイバー攻撃は進化と多様化を続けており、危険なネットワーク攻撃は、68日間以上という驚異的なダウンタイムにつながる可能性もあります。これはリスクにさらされている潜在的な収益の19%に相当します。

米国の医療部門は前例のない問題に直面し、1億9,800万人以上の米国の患者がランサムウェアの影響を受けました。多くの場合、悪用は驚くほど素早く発生しました。私たちのデータでは、21万258件の未知のマルウェア亜種が特定され、毎日平均637件の新しい脅威が確認されています。これは、サイバー犯罪者が成功率を高めるために新しい亜種を継続的に作り出していることを示唆しており、人工知能（AI）ツールの急速な採用と進化に起因している可能性が考えられます。

このような状況を考えると、中小企業やあらゆる規模の企業は、サイバー犯罪との戦いにおいて単独で挑むべきではないことを理解する必要があります。マネージドサービスプロバイダー（MSP）やマネージドセキュリティサービスプロバイダー（MSSP）との提携は、防御を強化するために不可欠です。そして、MSPとMSSPは、包括的な防御を確保するためにセキュリティオペレーションセンター（SOC）サービスと毎日24時間体制の監視を提供するベンダーを探すべきです。

本日は、過去1年間にわたるサイバー脅威の進化の性質を捉えた結果を2025年版 SonicWall サイバー脅威レポートとして紹介できることを誇りに思います。このレポートは、セキュリティの情勢について理解するための私たちの取り組みの証であるだけではなく、私たちのパートナーである皆様やその顧客がそれぞれの組織を防御し、今日の市場におけるセキュリティの重要性について有意義な対話を開始できるように支援するための重要なリソースでもあります。

今年のレポートは、それらの懸念すべき統計について詳しく示しているだけではありません。さらに重要なこととして、効果的な防御戦略を策定して実施できるようにするための実用的なインサイトを提供しています。また、私たちは毎日24時間体制のSOCアナリストからの貴重な視点や、信頼できるサイバーセキュリティ保険会社からの市場に関するインサイトも取り入れました。さらにはAIにもいくつかの見解を生成するように質問しました。

私たちのすべてのパートナーの皆様と顧客には、このレポートをステークホルダーやクライアントとの対話における戦略的なツールとして活用することをお勧めします。提供されたインサイトは、サイバーセキュリティ対策の重要性と、私たちが直面している脅威から皆様の組織を守るために必要なステップを明確にするために役立ちます。私たちは協力して防御を強化し、このダイナミックな脅威の情勢に適応することができます。皆様からのフィードバックは私たちの取り組みを形にする上で非常に貴重であり、私たちは、皆様が環境を効果的に守るために必要なリソースを皆様に提供してサポートすることに継続的に取り組みます。

献身的な Capture Labs の脅威研究者を含む SonicWall チーム全体を代表して、サイバーセキュリティの最新の進化についての重要な視点と、私たちが協力してこれらの課題を乗り越えられる方法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
社長兼 CEO

エグゼクティブサマリー

脅威の情勢

48時間

61%の確率で、ハッカーは新しいエクスプロイトコードを48時間以内に利用しています。

さまざまな組織が、2024年に68日分のダウンタイムの可能性を回避しています。

68日

60億

当社のセンサーは、3年連続で60億件以上の危険なネットワーク攻撃から防御しました。

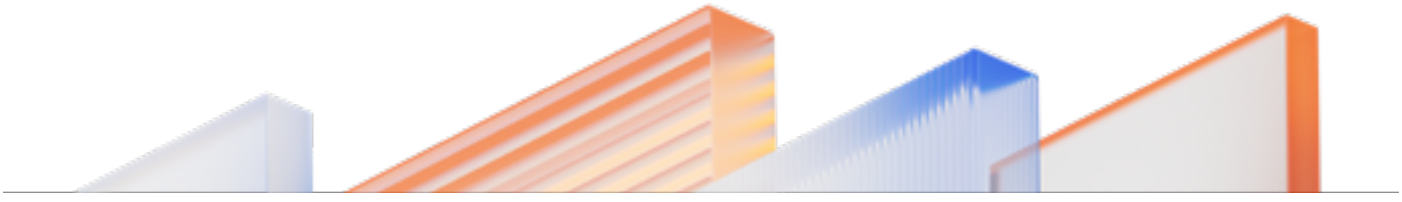
ランサムウェア

ランサムウェアが北米で急増(+8%)し、ラテンアメリカで爆発的増加(+259%)となっています。

▲259%

85万700ドル

ランサムウェアの平均コスト:2024年には、ランサムウェアに対する平均支払金額が85万700ドルに達し、ダウンタイムや復旧のコストを考慮すると、関連する総損失は多くの場合491万ドルを超えています。



マルウェア

▲8%

マルウェアは5月だけで92%の急増を見せ、
前年比8%の増加傾向にあります。

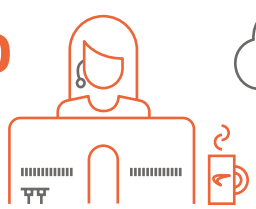
IoTおよび暗号化

IoT攻撃（+124%）および暗号化された脅威（+93%）
は世界的に増加を続けています。

▲124%

セキュリティオペレーションセンター（SOC）

85%



ID、クラウド、認証情報の侵害が、
アクション可能なアラートの85%を占めています。

報告されたサイバー保険の事案の33%はビジネス
メール詐欺のインシデントであり、前年比9%増です。

33%

RTDMI™

637

– 新しい亜種 –
1日あたり

SonicWall は21万258件の「未知の」
マルウェア亜種を特定–1日あたり637件。

2024年のランサムウェア攻撃の深刻化

2024年に、ランサムウェア攻撃は引き続き世界中のさまざまな組織に影響を与え、サイバーセキュリティにおいて最もコストのかかる脅威の1つとしての地位を確立しています。昨年は、サイバー犯罪者が二重の脅迫を戦術として頻繁に利用するという、ランサムウェア攻撃における大きな進化が見られました。南北アメリカで攻撃件数が大幅に増加し、ラテンアメリカでは259%、北米では8%増えました。ランサムウェアは間違いなく全業界に影響を及ぼしましたが、特に医療業界は大きな影響と壊滅的な結果を伴う深刻な被害に遭遇しました。

二重や三重の脅迫がニューノーマル(新常識)

二重脅迫が年間を通じて頻繁に行われ、三重脅迫も増加しました。特に、医療業界が標的になっています。この特殊な戦術では、組織の最も重要なデータを暗号化することと、要求に応じなければ機密情報を公開すると脅迫することが同時に行われます。この戦術は、基本的にサイバー犯罪者がデータをさまざまな方法で人質に取り、身代金を支払うようにランサムウェアの被害者に対してさらなるプレッシャーをかけるために使用されます。そして、医療業界における三重脅迫の場合は、サイバー犯罪者は患者に対しても、身代金を支払わないと患者のデータを公開すると脅迫します。AIや「サービスとしてのランサムウェア(RaaS)」などのランサムウェアツールの進化によって、これらの多面的な攻撃は小規模のサイバー犯罪者にとってもさらに使用しやすくなっています。

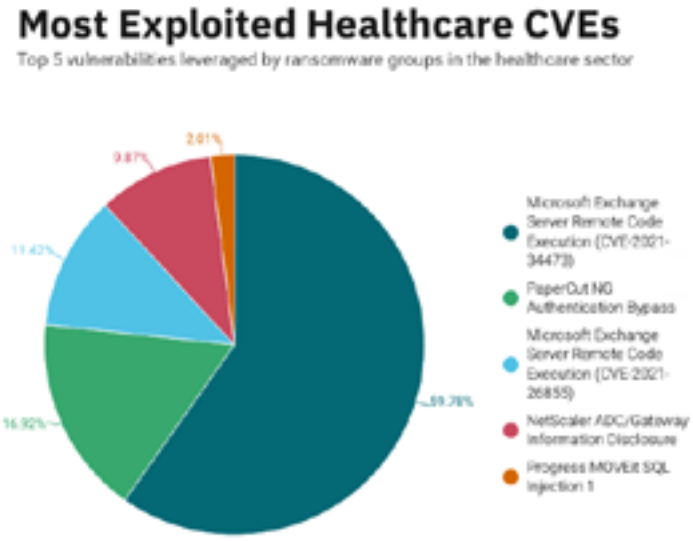
医療とランサムウェア:健康的ではない関係

2024年に医療業界はかつてないランサムウェア攻撃の急増に見舞われ、1億9,800万人以上の米国人が侵害の影響を受けました。特に、Change Healthcare における侵害は、1億人以上が影響を受けた史上最大の侵害の1つでした。

ランサムウェアは医療業界にとってこのうえない最大の脅威であり、この業界におけるすべての侵害の95%に利用されました。LockBit や BlackCat(旧称:ALPHV)のようなよく知られているランサムウェアグループは、「サービスとしてのランサムウェア(RaaS)」のモデルを利用して広範囲にわたって攻撃を実行し、重大な脆弱性を悪用してシステム内に侵入しました。

RaaSモデルによって、小規模で技術レベルが高くない脅威グループであっても、より確実性の高いランサムウェアソフトウェアを利用できるようになりました。最もよく悪用されている脆弱性として、以下のようなものがあります。

- ProxyShell や ProxyLogon のような Microsoft Exchange Server の脆弱性は、医療業界で悪用された脆弱性の60%を占めています。
- MOVEit のSQLインジェクションの脆弱性(CVE-2023-34362)は、300万人以上の患者に影響を与えた CareSource への攻撃など、多くの侵害の原因となりました。



業務における課題

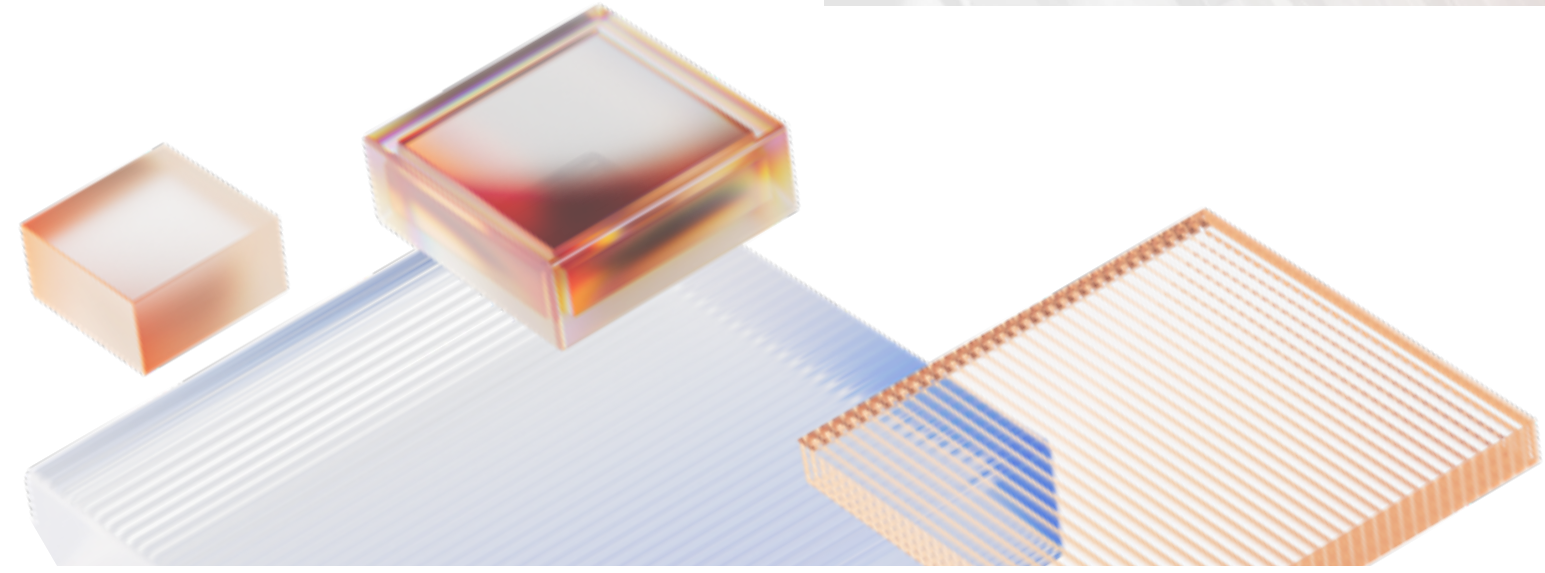
医療機関は、ランサムウェアを用いる攻撃者の大きな標的であっただけではなく、攻撃による影響に対処する準備が最もできていない組織の1つでもありました。復旧に要する時間は、全体的にランサムウェアのインシデントが複雑さを増していることを反映しています。特に、医療業界では多くの組織が現在もレガシーシステムを使用しています。また、パッチの適用が非常に長い間遅れているところも多く、重大な脆弱性に対して無防備な状態です。このような最悪の状況の組み合わせによって、医療サービスの提供者は高度な脅威に対抗するための準備が不足し、復旧するための準備も整っていないため、平均的な攻撃の総コストは平均支払額の5倍以上、つまり491万ドルに達しています。

SOCの視点

当社のマネージドセキュリティサービス（MSS）チームは、2024年末から2025年にかけての30日間でランサムウェアが25%増加したことを確認しており、Fog Ransomware、Akira、SafePay を最も活発なグループとして挙げています。

サイバー保険の視点

2024年には、サイバー犯罪者に支払われたランサムウェアに対する平均支払額は85万700ドルでしたが、その数字は、全体について説明するには不十分です。復旧コストも急増しており、平均的な攻撃の総コストは平均支払額の5倍以上、つまり491万ドルに達しています。



ビジネスメール詐欺（BEC）攻撃の驚異的な急増

今年はビジネスメール詐欺（BEC）攻撃が大幅に増加し、最も広範囲にわたるサイバー脅威の1つとしての位置づけをさらに強調しました。通常、BEC攻撃は騙すこととなりすましを利用しており、これらの2つの要素は、正確に実行された場合、識別することが非常に困難な場合があります。報告されたサイバー犯罪事案の3分の1近くがBEC攻撃であり、2023年にはわずか9%でしたが、そこから大幅に増加しました。

中間者攻撃と認証情報の盗用：主な要因

中間者攻撃（MitM）はBEC攻撃において重要な役割を果たしており、サイバー犯罪者は侵害されたメール（通常、認証情報の盗用によって獲得）や他の侵害された通信チャネルを利用してメッセージを傍受したり、内部通信の操作まで行ったりします。その結果、これらの攻撃は非常に狡猾で危険なものになり、攻撃によって現状の認識が変えられてしまいます。従業員は自分が一緒に仕事をしている親しい相手と連絡を取り合っていると信じているかもしれません。しかし実際には関連情報をサイバー犯罪者に渡してしまっている可能性があります。

ベンダーメール詐欺（VEC）の増加

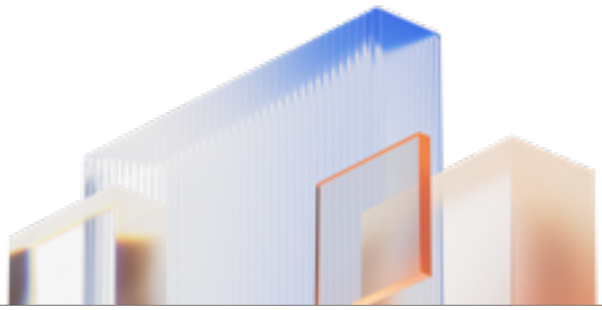
Abnormal Security によると、2024年上半期にVEC攻撃は建設・エンジニアリング業界で68%、小売・消費財製造業界で70%の急増となりました。 VEC 攻撃はBEC攻撃に非常に似ています。VEC攻撃では、サイバー犯罪者がベンダーの認証情報を偽装または盗むことによって、ベンダーとその多くの顧客との間の信頼関係を悪用し、1社だけでなく複数の企業から情報を盗みます。攻撃者は、ベンダーのシステムに侵入することで、支払いのスケジュール、意思決定者のID、財務処理などの重要な情報を入手できます。攻撃者は、十分な情報を手に入れると、請求を装ったり、大口顧客からの緊急の支払を要求するために話を捏造造したり、手に入れた情報をその他の悪質な方法で使用したりするような形で攻撃を行います。

サイバー保険の視点

BEC攻撃による損失はCISAの予算を上回る – 2024年のBEC攻撃による世界の損失は、29億5,000万ドルを超えました。視点を変えると、米国サイバーセキュリティ・社会基盤安全保障庁（CISA）の2024年の予算は28億ドルでしたが、これよりも1億5,000万ドル多いということです。

SOCの視点

先ごろ、大手コンサルティング会社が、自社の上級役員の1人を標的にしたBEC攻撃を発見しました。被害者は、信頼性は高いが、侵害されていたアカウントからのメールを受け取りました。そのメールには OneDrive のリンクが含まれており、従業員の認証情報を盗むために設計された偽の Microsoft のログインページにリダイレクトされました。攻撃者は侵入に成功すると、その役員のメールへのアクセス権を手に入れて、外部のファイル共有を通じて連絡先リストを共有することにより詐欺を拡散しました。



サイバー犯罪者のスピード

野放しの状態で悪用されている主な脆弱性に関する分析では、ほとんどの攻撃が概念実証（PoC）の公開から48時間以内に開始されていることが明らかになっています。この傾向は Google の脅威分析グループによって裏付けられており、多くの脆弱性は公開されてからわずか数日後には悪用されていると報告されています。

これらの攻撃は、Microsoft Exchange 、IoTデバイス、MOVEit のようなサードパーティのソフトウェアの脆弱性を定期的に標的にしています。高度な「サービスとしてのランサムウェア（RaaS）」のオペレーションがこれらの脆弱性の悪用を効率化しています。LockBit や BlackCat のようなグループは、新しいセキュリティの脆弱性に対する素早い動きによって知られています。

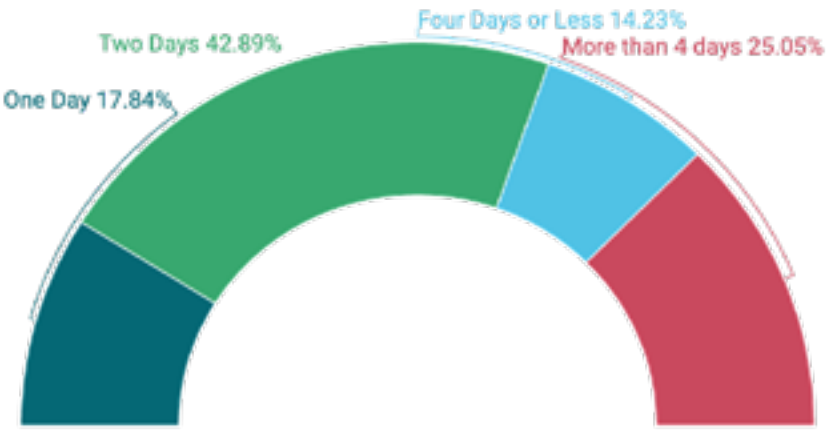
一例を挙げると、LockBit はCVE-2024-27198（JetBrains TeamCity の認証バイパス）を素早く悪用し、脆弱性の公表から24時間以内にランサムウェア攻撃を開始しました。同様に、ランサムウェア攻撃集団であるCl0pも、他のファイル転送製品の重大な欠陥を利用して66社に侵入し、PoCの公開からわずか48時間以内に身代金を要求しました。

「当社はMSPとしてサイバー脅威がどれほど急速に進化しているかを体験しています。公開されている武器化されたコードをサイバー犯罪者が利用するスピードは通常1日から4日以内であることから、積極的なセキュリティ対策の重要性が非常に高まっています。脆弱性にパッチを適用するために数週間待つ時代は終わりました。攻撃者は反応時間を数時間まで短縮しています。これは、企業は多額のコストが必要になる侵害につながる前に新たな脅威を積極的に監視、検出、対応できるMSPが必要であることを示しています。」

—パートナーの視点
FARZAD VAHID氏
（FORNIDA社）

サイバー犯罪者が悪用を開始するまでの時間

ハッカーがエクスプロイトコードを利用する速さ



Living Off the Landバイナリ(LOLBin):笑ってはいられない問題

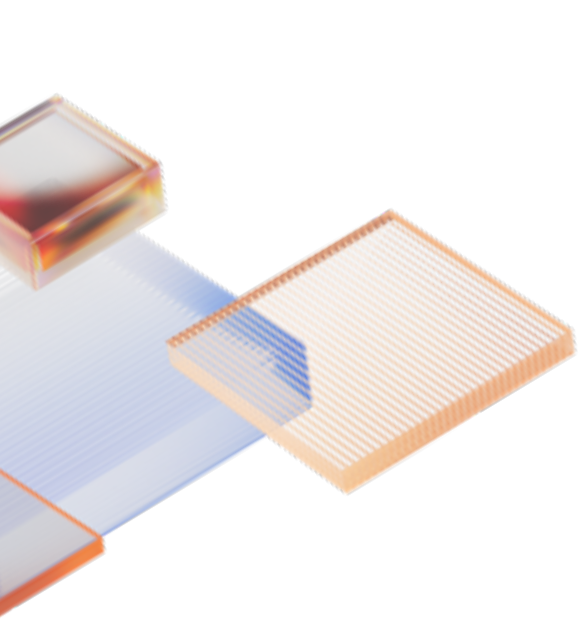
Living Off the Land バイナリ(LOLBin)とは、コンピューターを動作させるための正当で有益な用途を持つ、オペレーティングシステムに含まれているプログラムを指します。皆さんが自宅にいて、新しい工具を買わずにすでに持っている工具を使って何かを修理したい場合を想像してみてください。サイバー犯罪者は、コンピューターを攻撃するときに皆さんの例と同じような方法をとることがあります。独自のハッキングソフトウェアを持ち込むのではなく、すでにコンピューターに組み込まれているツールやプログラムを使用するのです。攻撃者がこれらの「正規の」ツール(バイナリ)を悪用すると、これらのツールは通常、任意の日にコンピューター上で実行されることになっているツールであるため、セキュリティソフトウェアを騙すことができます。これらのツールをブロックしたり無効化したりすると、オペレーティングシステムの機能が損なわれる可能性が高くなります。

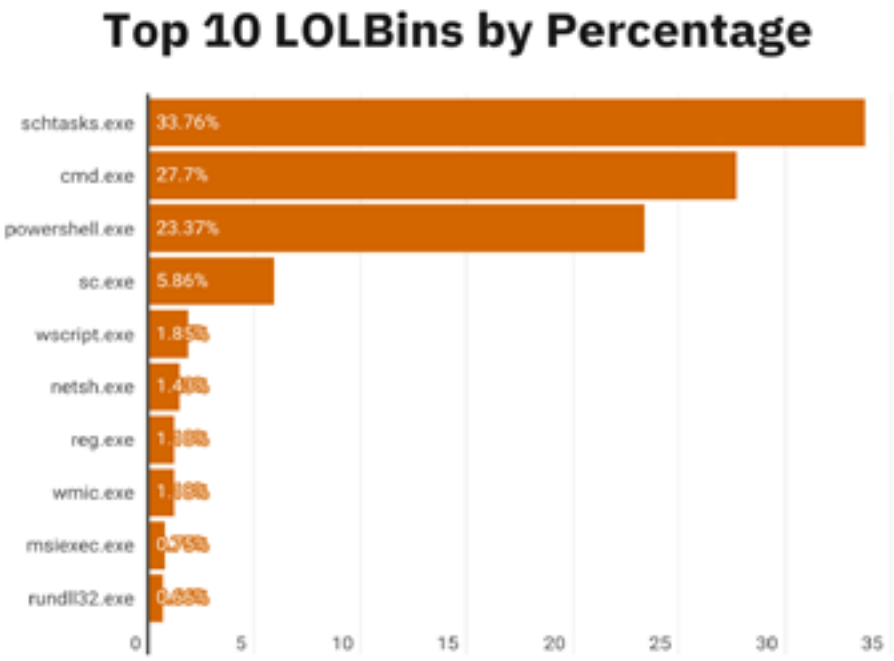
サイバー犯罪者は、侵害されたネットワーク内での水平移動と特権昇格のためにこれらのツールを利用します。一例を挙げると、CISA の報告では、LockBit とその関係者は偵察、認証情報の収集、特権昇格のために PowerShell やバッチスクリプトなどのツールを頻繁に使用しています。同様に、Sygnia の報告では、BlackCat(ALPHV)が PowerShell の技術や schtasks のようなツールを使用して水平移動を行い、Windows Defender を無効化していることが確認されています。

LOLBin の採用は、ファイルレスマルウェアの増加で見られているように、信頼されているインフラストラクチャを悪意のある目的のために悪用するという広範囲にわたるトレンドと一致しています。SonicWall の脅威研究者は schtasks.exe、cmd.exe、powershell.exe を最も悪用されている LOLBin として特定しており、発見された全ケースの80%以上をそれらが占めています。

LOLBinの悪用率

下記のグラフは、特定のバイナリの使用率が高いことを強調しています。schtasks.exe は、特定されたLOLBinの悪用のケースの34%で使用されており、攻撃者が持続性や悪意のあるスクリプトの実行のためにタスクをスケジュールすることを可能にしています。cmd.exe はケースの28%を占め、多くの場合、幅広いファイルレス攻撃の一環としてコマンドの実行に悪用されています。powershell.exe は23%を占め、非常に多用途であることが証明され、プロセスインジェクションやデータ流出のような高度な技術を可能にしています。特に、2024年版 SonicWall サイバー脅威レポート中間アップデートでは、普及しているマルウェアファミリーの90%が何らかの方法で PowerShell を利用していることを発見しています。sc.exe、wscript.exe、netsh.exe を含む他のバイナリの使用率は低いとはいえ依然として注意が必要であり、ニッチなまたは標的を絞った攻撃シナリオでの悪用を示しています。





サイバー攻撃の一般的なユースケース

LOLBinはファイルレスマルウェアの作戦に不可欠であり、攻撃者は従来のアーティファクトを残さないようにするためネイティブシステムツールを利用して、従来のシグネチャベースのソリューションによる検出を回避します。以下はその例です。

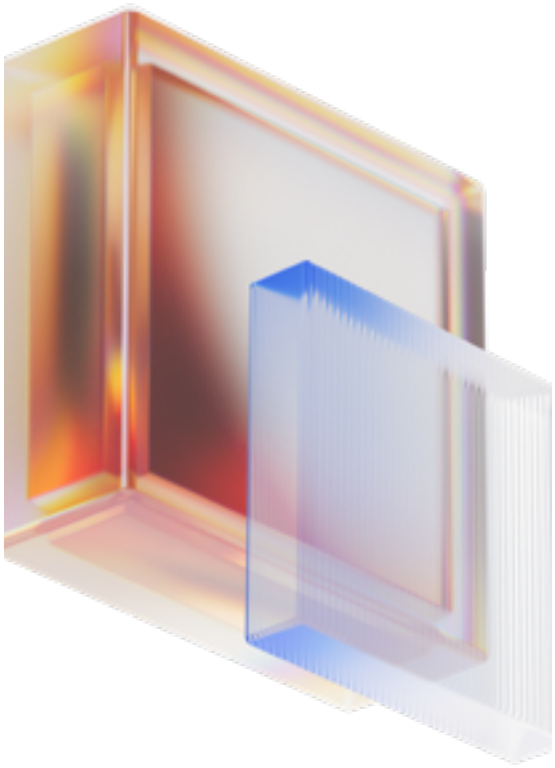
- wscript.exe：フィッシングで悪意のあるスクリプトを実行するために一般的に悪用され、攻撃者が VBScript のペイロードをひそかに実行することを可能にします。
- cmd.exe：サイバー犯罪者が侵害されたシステム上で直接コマンドを実行するために広く利用されており、多くの場合、より広範なコマンドアンドコントロールオペレーションのためのゲートウェイとして機能します。
- rundll32.exe：このツールはサイバー犯罪者によって最も広く利用されていた LOLBin の1つでした。ファイルレスマルウェアのより効果的な手法が増えたことで現在はわずか0.66%まで使用率が低下していますが、悪意のあるDLLを読み込んだり、サンドボックスの検出を回避したりするためには依然として有効です。

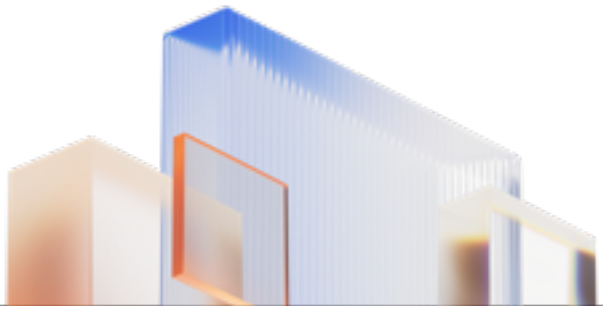
SOCの視点

保育施設で、当社のマネージドセキュリティサービス（MSS）チームは攻撃者が入退室管理機器を最初の入口として利用していることを発見しました。その機器はインターネットに直接接続されている、パッチが未適用の Windows マシンであり、攻撃者が既存のバイナリを使用して水平移動を行なうことを可能にしていました。続いて、攻撃者は隠れたオブジェクトをグループポリシーエディター内に埋め込むことによって持続性を確立しました。

AIの視点

LOLBin の悪用は、攻撃者がPowerShell、cmd.exe、schtasks.exe などの信頼されているシステムツールを利用することによって検出を回避するため、引き続き発生する可能性が高いと言えるでしょう。ファイルレスマルウェアとゼロトラストの採用が進むにつれて、攻撃者はこれらの戦術に磨きをかけてセキュリティ対策を回避するでしょう。高度な脅威ハンティングと行動監視は、このトレンドに対抗するために不可欠です。— Open AI、25/2/5、v4.0





AIによる自動化ツールが攻撃の複雑性を高める一方で参入障壁を低下

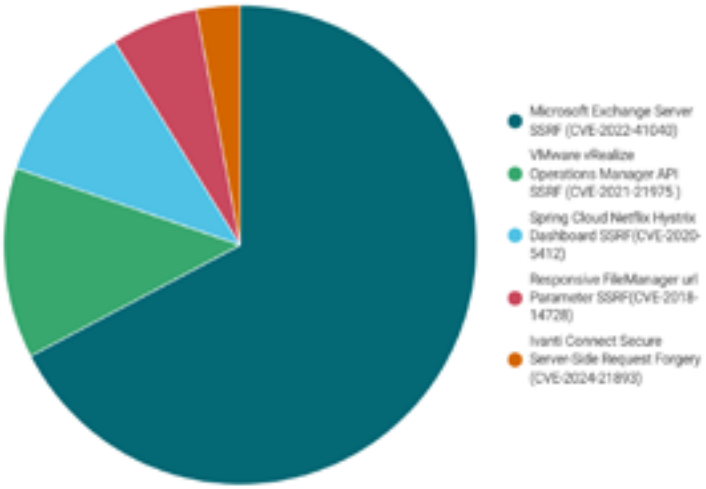
サーバーサイドリクエストフォージェリ（SSRF）攻撃は、サイバー犯罪者の武器庫の中で長い間好まれているツールです。このタイプの攻撃では、サイバー犯罪者は基本的にサーバーを騙して、組織内の機密性が高い可能性がある内部サービスにリクエストを送信させます。一部の攻撃では、サーバーが任意の外部サービスにアクセスするように強制できる可能性もあり、その結果、認証情報などの機密データが漏洩する可能性があります。従来のSSRF攻撃では、脆弱性の発見、ペイロードの作成、さまざまなサーバー構成の複雑さの調査にはかなりの専門知識が必要でした。AIを利用したツール、特に自然言語処理（NLP）や生成モデルを活用するツールの導入によって、技術的な参入障壁は低くなっています。AIツールは以下のような方法でこれらの攻撃の参入障壁を下げています。

- パッチ未適用のシステムの特定：AIを利用したスキャナーが、大規模で複雑なインフラストラクチャ内であっても、パッチ未適用のSSRFの脆弱性を持つレガシーシステムを特定します。
- エクスプロイトチェイニングの自動化：AIがSSRFと他の脆弱性との連鎖化のプロセスを効率化し、特権昇格や水平移動のための自動化されたワークフローを作成します。
- 検出の回避：AIが難読化の技術を強化し、SSRFのペイロードがセキュリティソリューションで検出されにくくします。

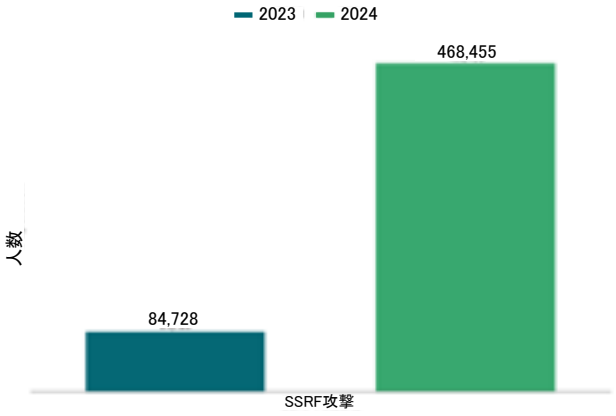
SSRFは2024年に重要なサイバーセキュリティの懸念事項となり、2023年と比較して452%という大幅な増加を記録しました。特権昇格やコマンドインジェクションなどのその他の脆弱性と合わせたSSRF攻撃の使用の増加は、SSRF攻撃の影響を拡大させ、サイバー犯罪者がより広範なアクセス権を手に入れて、より深く標的に侵入することを可能にしました。

AIによって活性化された旧来の脅威

2024年のSSRFの脆弱性トップ5



SSRF攻撃の前年比



最も広範囲に使用されているSSRFの脆弱性の一部は、実際には新しいものではありませんでした。攻撃者はAIツールを利用して、多くのシステムでパッチが未適用のままである旧来の脆弱性を新たに悪用しています。以下がその例です。

- VMware vRealize Operations Manager API の SSRF（CVE-2021-21975）：この脆弱性によって攻撃者はv Realize Operations Manager API を通じて内部サービスへのアクセスが可能になり、機密データの漏洩につながります。
- Microsoft Exchange Server のSSRF（CVE-2022-41040）：攻撃者が Microsoft Exchange サーバーを悪用できる重大な脆弱性です。認証をバイパスしてリモートコードの実行につながる可能性があります。

- Spring Cloud Netflix Hystrix Dashboard のSSRF（CVE-2020-5412）：Hystrix Dashboard の脆弱性が悪用され、内部サービスが標的となり、機密情報が漏洩されました。

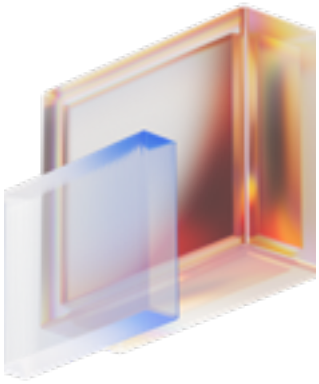
これらの旧来のSSRFの脆弱性が継続的に使用されていることは、パッチ管理の遅れという持続的なリスクを示しています。また、AI の支援による旧来の脆弱性の再利用は、組織がこれらの旧来の脆弱性について注意を続けつつ、同時に新しい脅威に備える必要があることを意味しています。

ビジネスメール詐欺

生成AIが登場する前には、サイバー犯罪者は企業の文体を模倣すること、状況に当てはまるようなフィッシングメールを作成すること、攻撃の実行中に従来のセキュリティシステムを作動させない方法を知っていることなど、専門的なスキルを持っている必要がありました。現在、AI ツールはサイバー犯罪者に代わってこれらのすべてを高いレベルで実行することができます。すなわち、AIプロンプトの作成方法を知っているサイバー犯罪者はこれらの攻撃のいずれかを実行できる可能性があります。

オープンソースソフトウェア（OSS）のセキュリティにおける生成AIの役割

生成AIはコーディングの高速化とアクセシビリティの向上というメリットを提供しますが、適切に検証しなければ、脆弱性をもたらす可能性もあります。また、攻撃者が組織のシステムの脆弱性を見つけて悪用するなどの悪意のある目的のために同じ AI ツールを利用してコーディングを高速化することもできます。そのため、より厳格なコードの検証とレビューのプロセスが必要となります。

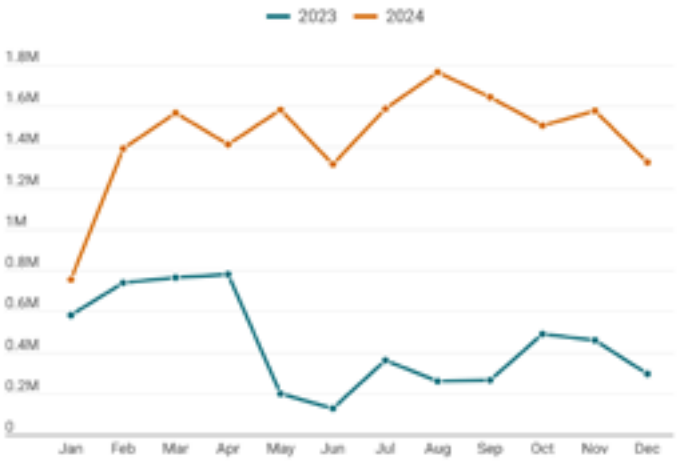


「私たちは、AIがサイバー脅威の情勢をどのように再構築しているかを常に目撃しています。攻撃者が既存の脆弱性を悪用し、高度な攻撃を自動化し、従来の防御を回避することが容易になっています。AIを活用したSSRF攻撃とビジネスメール詐欺の急増は、企業がもはやセキュリティに対して受動的なアプローチを取っている場合ではないことを示しています。組織には、リアルタイムで脅威を検出して軽減し、AIを活用した攻撃に対する防御を強化し、進化し続けるセキュリティ規制に準拠して新たに発生するリスクに備えることができるプロアクティブなセキュリティパートナーが必要です。」

—パートナーの視点
LUIS ALVAREZ 氏（ALVAREZ TECHNOLOGIES 社社長兼 CEO）

IoT（モノのインターネット）は引き続き拡大しており、IoTの脅威も同様に拡大

IPカメラを標的としたIoT攻撃は、サイバー犯罪者の主要な標的となりました。2024年だけで、SonicWall はIPカメラに対する1,700万件以上（毎月75万件から180万件）の攻撃を防ぎました。攻撃者は、政府や重要なインフラストラクチャで使用されるコネクテッドデバイスの防御能力が低い場合が多いことに注目し始めています。これらのデバイスは、監視操作や分散型サービス拒否（DDoS）攻撃などの妨害活動に対して脆弱なまま放置されています。IPカメラは多くの場合、政府の施設や投票所などの機密性の高い場所に設置されています。つまり、確認されている増加は、世界の2024年の選挙に少なくとも部分的に起因した可能性があります。最も警戒すべきIoTの脅威の1つは、Hikvision IP カメラコマンドインジェクション（CVE-2021-36260）の脆弱性であり、サイバー犯罪者はカメラのシステムにコマンドを直接入力でき、デバイスを完全に制御することが可能になります。



IoTボットネット

Reaper IoTボットネットはIoTデバイスの脆弱性を利用してデバイスを完全に制御し、サイバー犯罪者がボットネットを使用して大規模な攻撃を実行します。他のボットネットがパスワードの誤りなどの弱点を利用するのに対し、Reaper は脆弱性に注目して、IoTハードウェアに対する脅威レベルを高めています。

これらのトレンドは、機会をうかがった攻撃から、監視を弱体化させたり、重要なサービスを妨害したり、スパイ行為を可能にすることを目的とした、より標的を絞った作戦への移行を示しています。

オープンソースソフトウェア（OSS）

オープンソースソフトウェア（OSS）は、特にIoTデバイスにおいてソフトウェア開発に変革をもたらし、イノベーションとコスト効率の両立を可能にしました。その一方で、何千台ものIoTデバイスがすべて同じOSSを使用している場合、脆弱性が発生すると壊滅的な結果を招く可能性があります。SonicWall のデータは、他のプロジェクトよりも頻繁に利用されている3つのOSSプロジェクトがあり、これらはすべてIoTデバイスでも活用されていることを示しています。

- PHP：CVE-2017-9841、CVE-2018-20062、CVE-2024-4577のような脆弱性は、任意のコードの実行を可能にし、重大なリスクをもたらします。
- Apache：Log4j CVE-2021-44228のような既知の脆弱性は、リモートコードの実行やデータ漏洩を容易にします。
- OpenSSL：Heartbleed（CVE-2014-0160）のような問題は、機密データを漏洩させることができるため現在も悪用されています。

AIの視点

IoT攻撃は、セキュリティが脆弱なコネクテッドデバイスが重要な部門に展開されるケースの増加に伴って、引き続き増えるでしょう。サイバー犯罪者は、Reaper のようなボットネットやIPカメラおよびOSSコンポーネントの脆弱性を利用する標的を絞った攻撃に移行しています。より強力なセキュリティフレームワーク、パッチ管理、脅威の監視がない場合、IoTデバイスはサイバー犯罪者にとって最高な標的のままでしょう。— OpenAI、24/2/5、v4

攻撃タイプのさらなる多様化：サイバー犯罪者は創造性を高めている

サイバー攻撃は多様化しています。サイバー犯罪者は新しい戦略を作り出し、実績のある戦略に磨きをかけて脆弱性を悪用しています。サイバー攻撃のコストは上昇しています。そのコストは金銭的なものだけではありません。サイバー攻撃は、長期的な風評をもたらし、長期にわたって影響を及ぼす可能性があります。

Strela Stealer 戦略がマルウェアと共に拡大

Strela Stealer は2022年11月に初めて検出され、それ以降、欧州では最も持続的で危険な脅威の1つとなっています。SonicWall Capture Labs では、2024年を通じて常に活動が確認されました。特に、以下の時期に活発な活動が見られました。

- 7月と12月：休日や休暇のような、従業員が不足している可能性が高く、リソースに余裕がない期間に関連していると思われます。
- 10月：この月は多くの企業にとって財務報告の開始時期であり、より機密性の高い情報の受け渡しが行われされることを意味します。サイバー犯罪者にとっては攻撃に最適な時期です。

元来、サイバー犯罪者は、Microsoft Outlook や Mozilla Thunderbird のようなプラットフォームからメールの認証情報を手に入れるために、メールの添付ファイル内の JavaScript ファイル

を通じて Strela Stealer を配布していました。2024年には、マルウェアは向上された隠蔽技術を使用して特定の地域を標的にすることによって、さらに高度になりました。おそらくは地政学的理由から、ロシアを攻撃することを避け、ドイツ、スペイン、ポーランド、イタリアのような国に焦点を合わせています。Strela Stealer が検出を回避する方法の1つとして、システムの言語設定とキーボードのレイアウトをチェックし、標的としている国であるかどうかを判断します。このマルウェアは、サイバー犯罪者がツールを改良しているだけでなく、攻撃においてもより戦略的になっていることを浮き彫りにしています。

「サイバー犯罪者はより戦略的になり、新しい攻撃方法と実績のある戦術を組み合わせて脆弱性を悪用しています。サイバー攻撃のコストは金銭的なものだけではありません。企業の評判が永続的に損なわれたり、業務を混乱させる可能性もあります。企業は、進化し続ける脅威に備え、自社の最も重要な資産を守るためのプロアクティブな保護、リアルタイムの監視、戦略的な防御を提供するセキュリティパートナーを必要としています。」

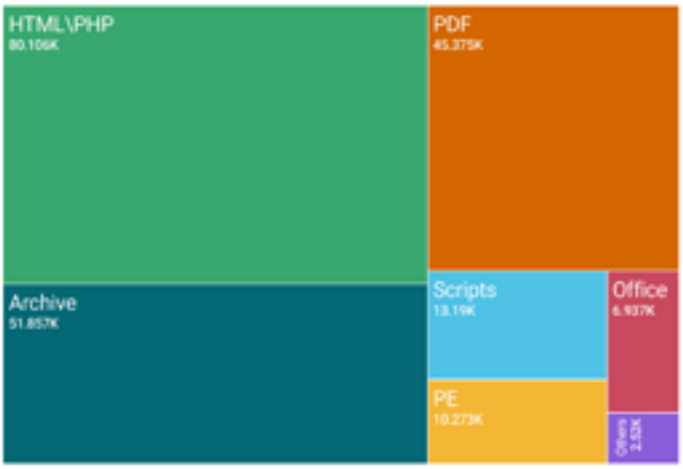
—パートナーの視点
JOSH SKEENS 氏
（LOGICALLY 社 CEO）

AIの視点

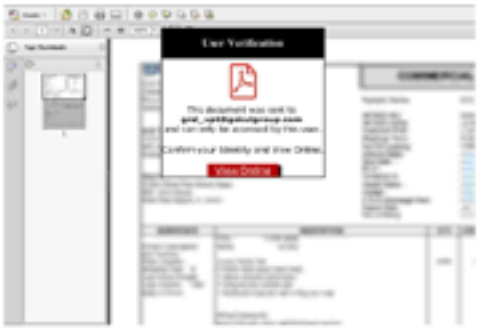
2024年には、世界のデータ侵害の平均コストは488万ドルに達し、前年から10%の増加を記録しました。これはパンデミック以後最大の年間増加率です。— OpenAI、25/1/29、v4.0

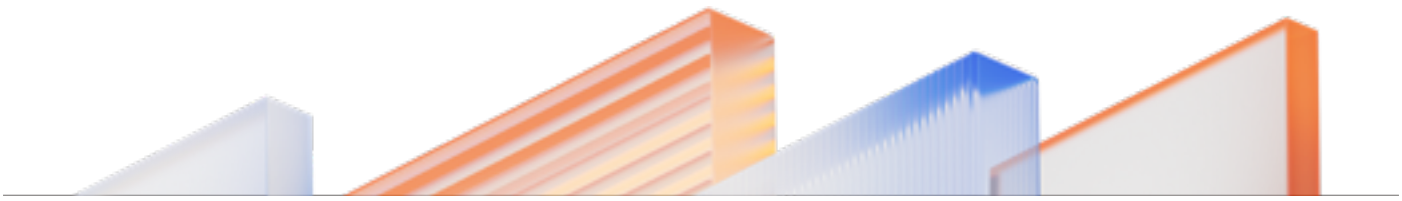
日常生活における隠れたリスク：PDF、HTMLフィッシング、偽モバイルアプリ

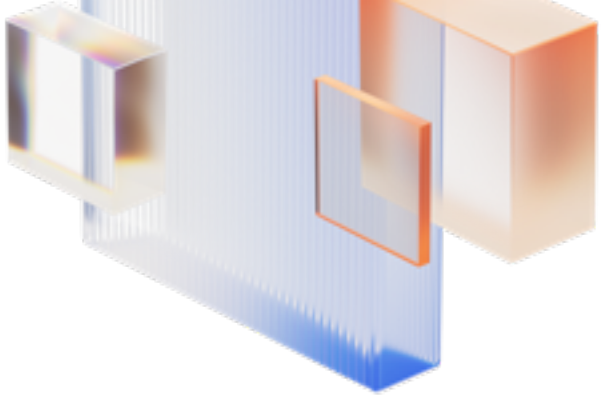
ファイルベースの攻撃、特に悪意のあるPDFや HTML フィッシングファイルが大幅に増加しました。SonicWall のデータでは、検出された悪意のあるファイルの38%は HTML ベースであり、PDF が22%でその後に続いています。



攻撃者がこれらのタイプのファイルを使用する理由は、セキュリティシステムを回避しやすく、簡単に人的要因を悪用して認証情報などの機密情報を盗み取ることができるからです。サイバー犯罪者は、悪意のある PDF 内に埋め込まれたQRコードを通じて被害者をフィッシングサイトに誘導しています。被害者は、QRコードをスキャンすると、正規のログインページのように見えるページに誘導されます。実際には、被害者が入力する情報はサイバー犯罪者に送信され、悪用されます。このタイプの攻撃は、多くの場合、第一段階にすぎません。攻撃者は、認証情報を盗み取ると、通常は BEC、企業スパイ活動、データ窃盗のような戦術を利用して攻撃を続けます。



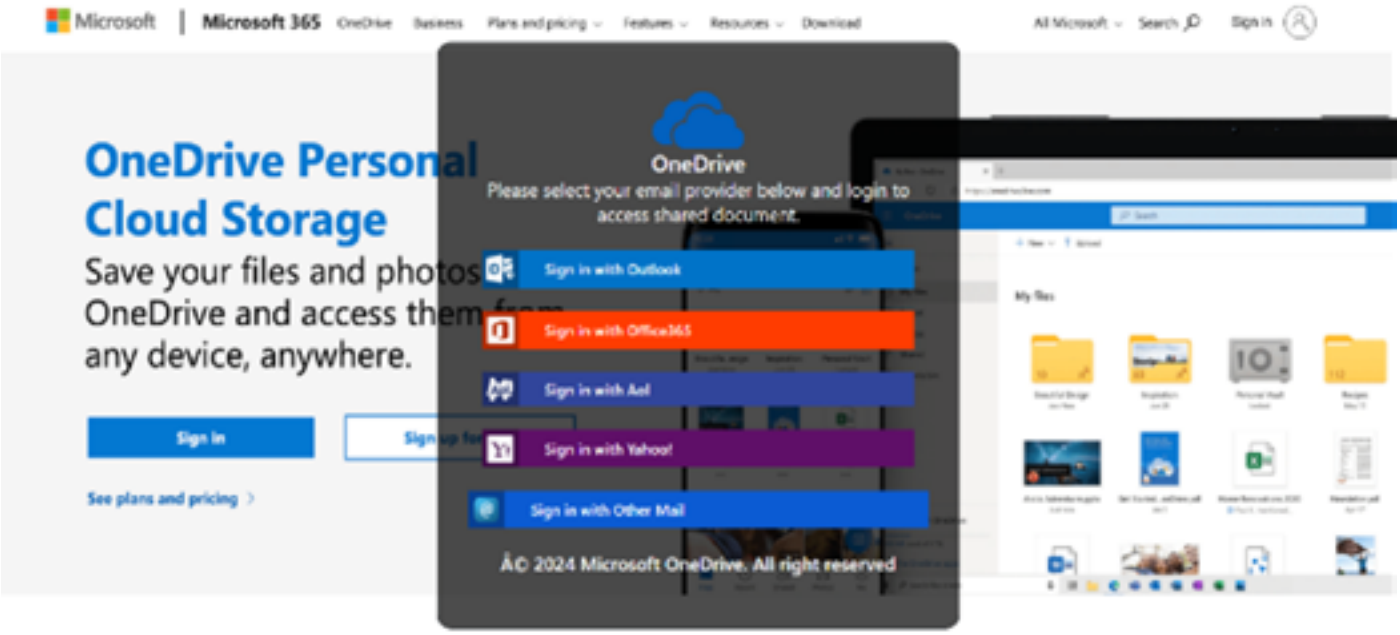




HTML フィッシング攻撃は10%増加し、ユーザーの認証情報を侵害する主要な手段となっています。HTML フィッシングでサイバー犯罪者が使用する手法には以下のようなものがあります。

- フォームベースのフィッシング：HTML フィッシングページは、多くの場合、被害者のメールアドレスを事前に入力して信憑性を高め、ユーザーにパスワードの入力を促します。
- アーカイブによる配布：HTML ファイルは、セキュリティ対策を回避し、ユーザーの好奇心を引き起こすため、一般的にZIPまたは RAR アーカイブ内で配布されます。

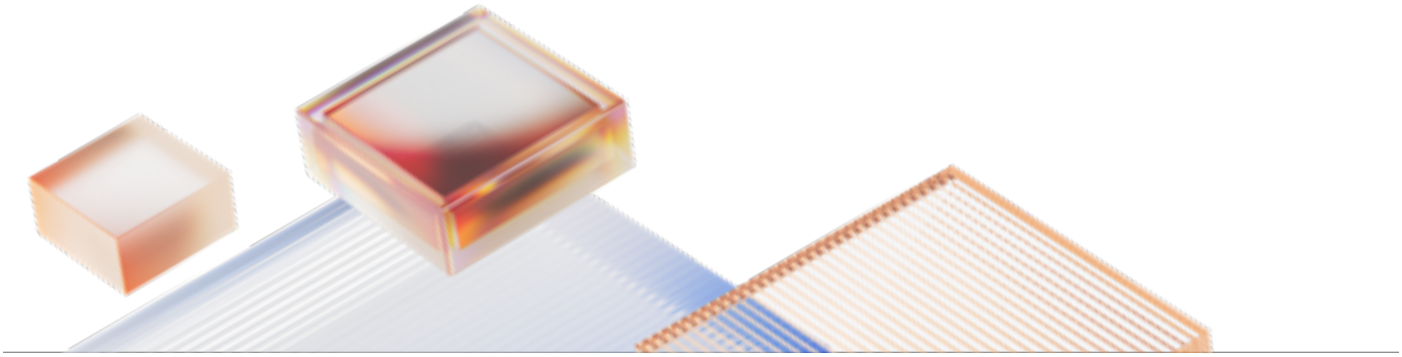
以下は実際の例です。



一般的なファイル、一般的ではない脅威

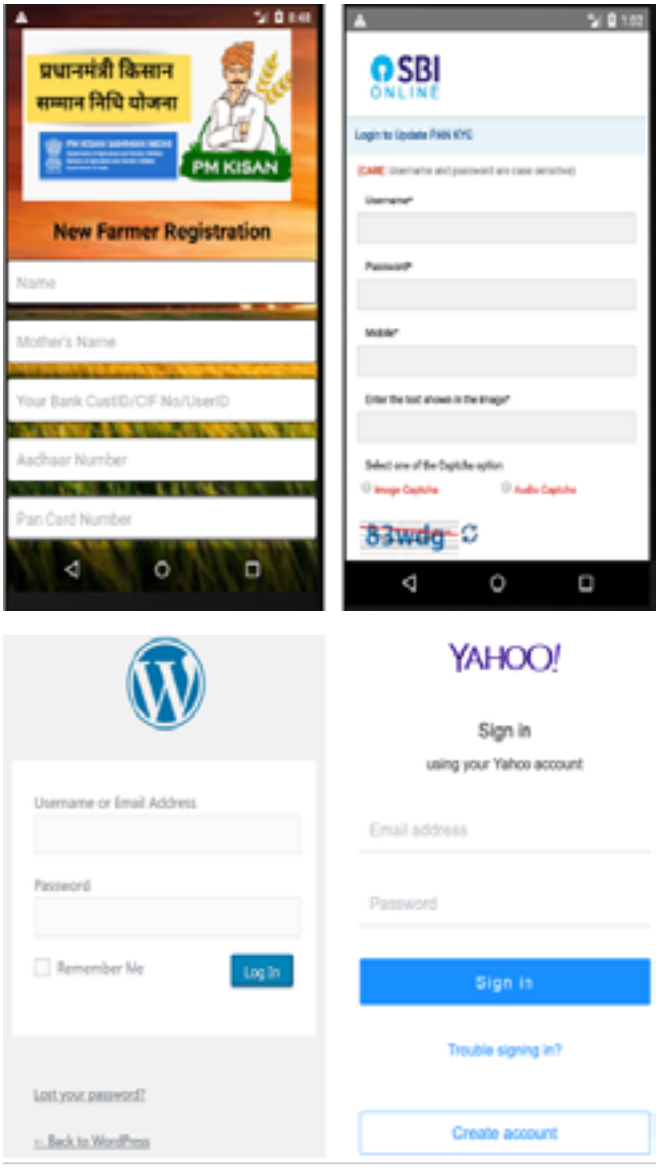
悪意のあるペイロードが含まれているZIPファイルや RAR ファイルは、メールのフィルタリングを回避する一般的な手段にもなっています。これらの脅威は、ランサムウェア、トロイの木馬、リモートアクセスツール（RAT）を無防備な標的に配布することによって機能します。これらの方法は、Bumblebee マルウェアローダーなどの近ごろ注目を集めている攻撃で使用されました。この方法では、検出を回避するために悪意のある LNK ファイルが含まれたZIPアーカイブを添付したフィッシングメールを送信します。

HTML、PDF、その他のファイルベースの攻撃の増加は、これらの新しい攻撃方法を作り出す際のサイバー犯罪者の多様性と創造性が高まっていることをよく表しています。これらの攻撃は、さまざまな業界やあらゆる規模のビジネスに及んでいます。通常あるいは一般的に見えるファイルに悪意のあるペイロードをパッケージ化することによって、被害が発生する前に従来のセキュリティの手法でこれらの攻撃を検出することは非常に難しくなります。



偽Androidアプリ:モバイル詐欺のための信頼と権限の悪用

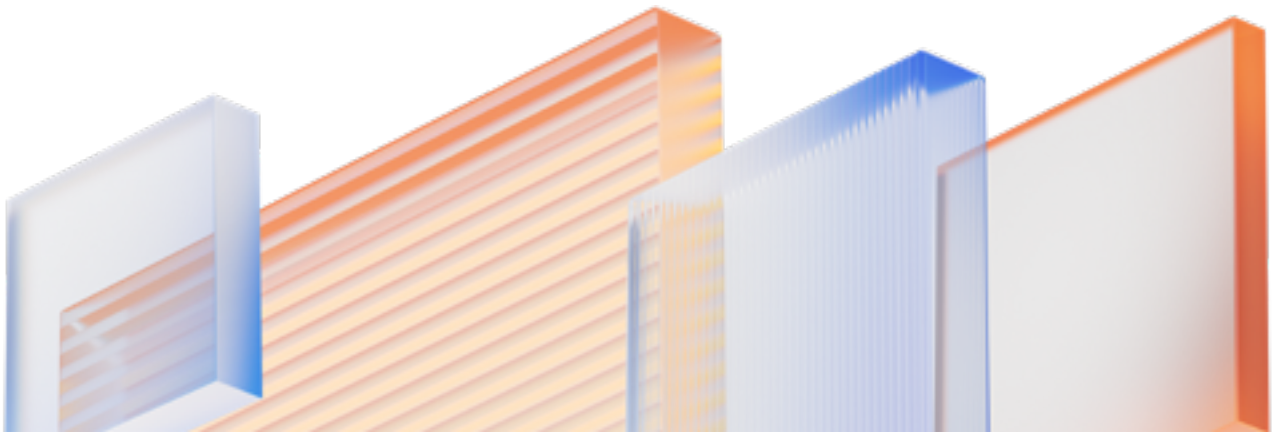
偽 Android アプリは特にアジア太平洋(APAC)地域で深刻なサイバー脅威となっており、モバイル詐欺全体が急増しています。この地域のサイバー犯罪者は、Android スマートフォンの高い普及率と関係当局に対する一般大衆の文化的信頼を利用しています。これらの偽アプリは、デバイスがテキストメッセージを受信して読み込む機能など、実際はアプリの動作のために必要ではないユーザーのデバイスからの権限を要求することによって動作します。攻撃者はこの権限を利用してワンタイムパスワード(OTP)を傍受し、ユーザーアカウントを乗っ取ります。これらのアプリは、多くの場合、正規の金融サービスや政府のサービスを装っています。犯罪者がデジタルリテラシーの低い被害者を標的にしているという事実と合わせると、機密情報を提供するように被害者を騙すことができる方法が簡単に理解できます。



効果的なセキュリティ戦略を持つための課題

良好なサイバーセキュリティの慣行を維持するという課題を理解することが、セキュリティパートナー、MSP、MSSP にとって不可欠です。進化し続ける脅威の情勢は、組織がサイバーセキュリティに対してプロアクティブな多層型のアプローチを採用することを求めています。これらの課題に対処するには、リアルタイムの監視、迅速なパッチの展開、ゼロトラストセキュリティモデル、継続的なユーザー教育が必要です。これらの課題を協力して克服することによって、私たちはすべての人々にとってより安全な環境を作り出すことができます。

1. 脆弱性の迅速な悪用：サイバー犯罪者がセキュリティギャップを利用するスピードは、これまで以上に速くなっています。75%の確率で、ハッカーは脆弱性を悪用する方法が公開されてから4日以内にそのセキュリティの脆弱性を利用し始めています。このため、セキュリティ担当チームは脆弱性を迅速に特定して対処することに大きなプレッシャーを受けます。
2. ランサムウェアの脅威と復旧コストの増加：ランサムウェア攻撃は最もダメージの大きいサイバー脅威の1つであり続けています。一例を挙げると、米国の医療業界だけで1億9,800万人以上が侵害の影響を受けており、復旧コストはインシデント1件あたり491万ドルを超え、バックアップソリューションや復旧計画がない場合の危険性が浮き彫りになっています。
3. ヒューマンエラー：個人によるミスは、サイバーセキュリティ体制に大きな影響を与えます。これらのミスは、意図せずにデータ侵害や不正アクセスのリスクを高めるおそれがあります。
4. ビジネスメール詐欺（BEC）攻撃の急増：BEC 攻撃が急増しており、現在では、報告されているサイバー保険の全請求の3分の1を占めています。攻撃者は高度なAIドリブンの技術を使用しており、これらの詐欺を検出することを難しくしています。
5. IoTデバイスからの攻撃対象領域の拡大：インターネットに接続されているデバイスの数が増えており、それに伴って新たなセキュリティの課題が発生しています。攻撃者は、設定の脆弱性を理由にこれらのデバイスを標的にしています。
6. AIドリブンのサイバー攻撃の複雑性の高まり：サイバー攻撃におけるAIの使用は増え続けています。サーバーサイドリクエストフォージェリ（SSRF）攻撃をはじめとするAIドリブンの攻撃が大幅に増加しました。
7. ファイルベースの攻撃方法と悪意のある自動化：悪意のあるフィッシング攻撃、特にPDFやHTMLファイルを通じた攻撃が増加しています。多くの場合、これらの攻撃には偽のリンクや QR コードが含まれており、検出を難しくしています。



サイバーセキュリティ防御を強化するための戦略的な行動

脅威の情勢はこれまで以上のペースで進化し続けており、どのような組織であっても無縁ではいられません。しかし、常に変わらないことが1つだけあります。このレポートで力説されている多くの攻撃は、強力なサイバーセキュリティハイジーンによって防ぐことができます。以下のようにプロアクティブな対策を取ることによって、セキュリティ体制を大幅に強化できます。

リアルタイムパッチ管理の導入 – パッチ管理のハイジーンが良好ではない組織は、サイバー攻撃に対して非常に脆弱です。継続的にスキャンを行いパッチを適用することによって、企業はサイバー犯罪者が既知の脆弱性を利用する前にランサムウェアの感染、データ侵害、システム侵害を阻止できます。

ゼロトラストセキュリティモデルの採用 – サイバー犯罪者はAIと自動化を利用してネットワークに侵入します。セキュリティ担当チームは厳格なアクセス制御を適用し、暗黙的な信頼を前提とするのではなく、すべてのアクセス要求を検証する必要があります。

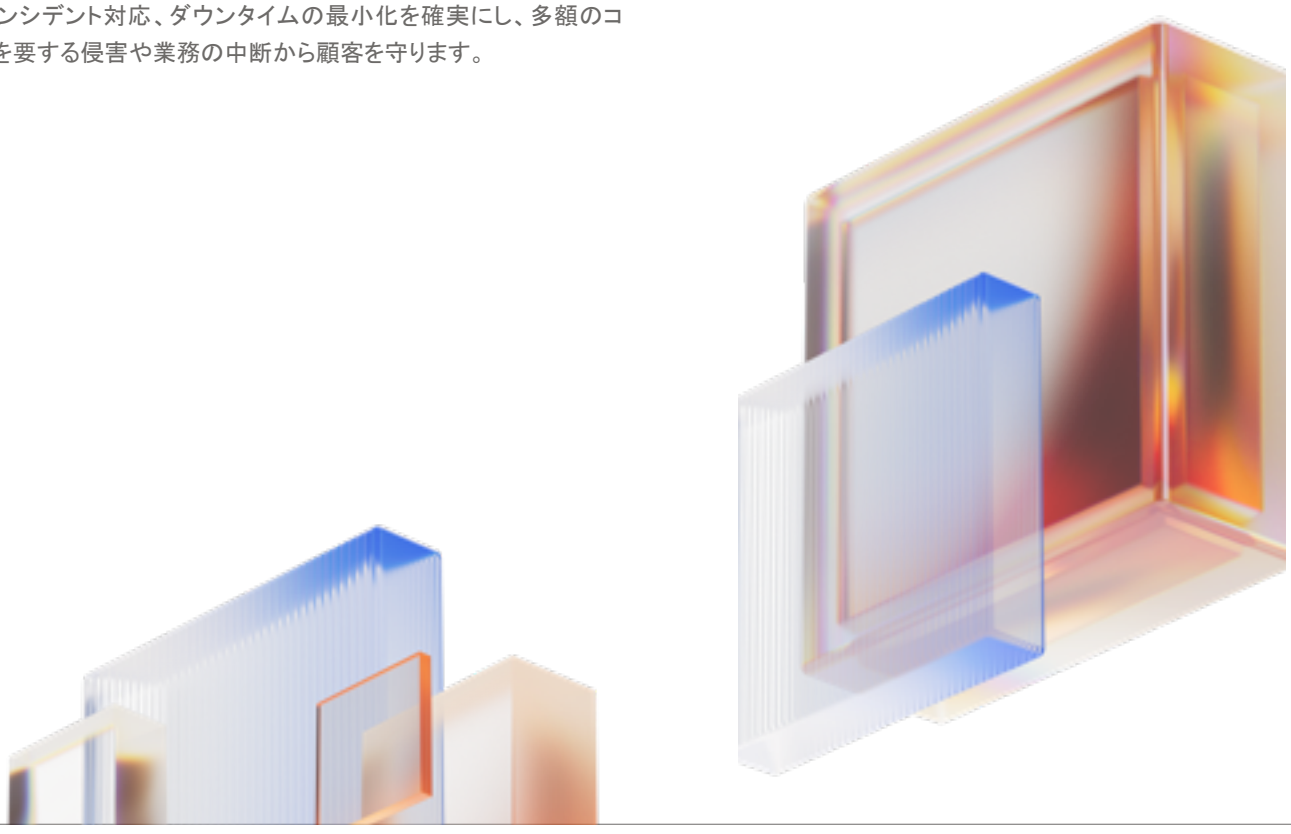
リアルタイムで脅威から防御するための毎日24時間体制のSOCサービス – MSP/MSSP は、サイバー脅威が急速に進化しており、攻撃者は発見から数時間以内に脆弱性を悪用するため、SOC サービスと毎日24時間体制の監視を提供するセキュリティベンダーと提携するべきです。継続的な監視はリアルタイムの脅威検出、迅速なインシデント対応、ダウンタイムの最小化を確実にし、多額のコストを要する侵害や業務の中断から顧客を守ります。

ランサムウェアに対する備えの強化 – 組織は、壊滅的なランサムウェアによる侵害への備えという現実に直面しています。定期的なバックアップ、ネットワークのセグメンテーション、エンドポイント検出/応答(EDR)ソリューションの導入が必要です。

IoTセキュリティの強化 – IoT 攻撃は2024年に124%増加しました。デフォルトの認証情報を変更し、ファームウェアの更新を適用し、ネットワークアクセスを制限することによってIoTデバイスを保護する必要があります。

クラウド環境とSaaSアプリケーションの監視 – セキュリティアラートの78%はクラウドベースの脅威に関連するものでした。多要素認証(MFA)、CASB ソリューション、最小権限のアクセスポリシーを適用する必要があります。

定期的なサイバーセキュリティ意識向上トレーニングの実施 – ヒューマンエラーは依然として主要な攻撃手段です。フィッシング、ソーシャルエンジニアリング、認証情報の管理に関する定期的なトレーニングによって、リスクを大幅に減少させることができます。



重要なポイント

SOCの視点

- ランサムウェア攻撃は2024年末の時点で25%の急増となっています。これは、Fog Ransomware、Akira、SafePay のようなグループの攻撃的な活動によるものです。
- 大手コンサルティング会社がBEC攻撃に直面しました。信頼性の高いアカウントが侵害され、上級役員を騙して認証情報を漏洩させ、攻撃者が連絡先リストを通じて詐欺を拡散することを許ししました。
- 攻撃者が、保育施設のインターネットに接続されたパッチ未適用の入退室管理機器を悪用して水平移動を行い、グループポリシーエディターを介して持続性を確立しました。

AIの視点

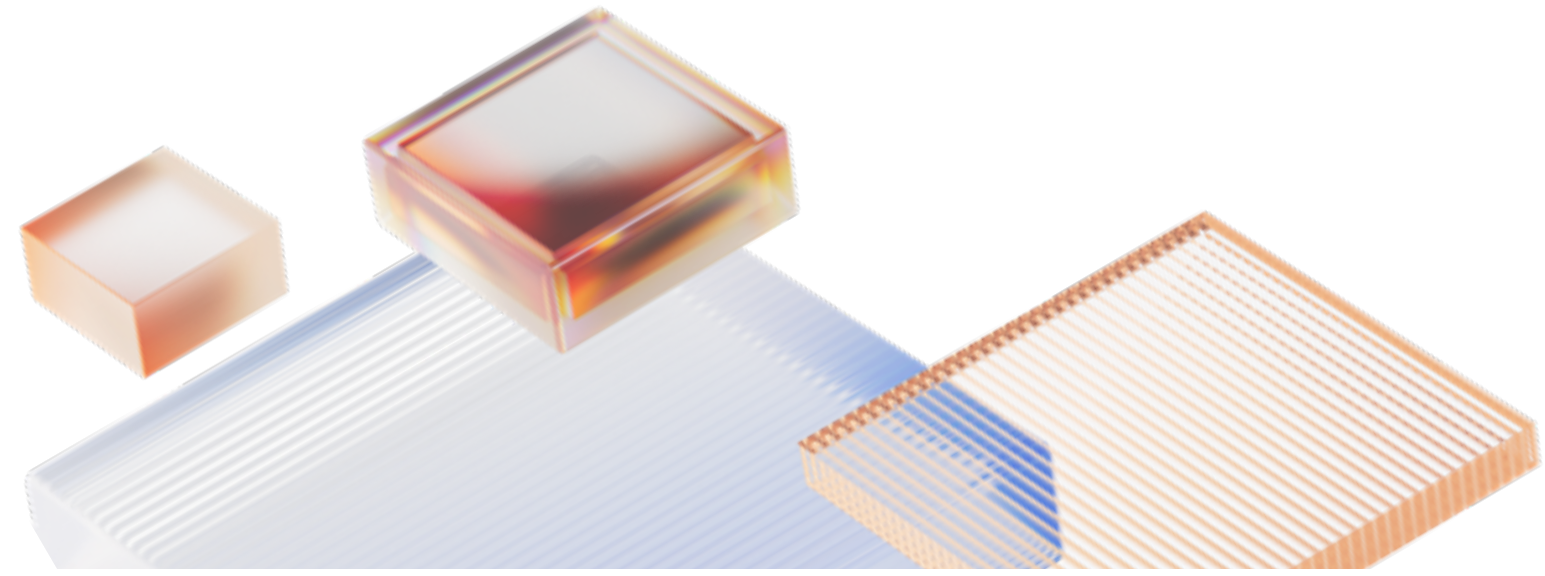
- 検出を回避するために攻撃者がPowerShell や cmd.exe のような信頼されているシステムツールを悪用するケースが増えており、高度な脅威ハンティングと行動監視が、LOLBin の悪用に対抗するために不可欠です。
- セキュリティが脆弱なIoTデバイスが重要な分野に氾濫し、Reaper のようなボットネットを使用した標的を絞った攻撃が急増することによって、より強力なセキュリティフレームワークとプロアクティブな監視が今すぐに必要であることが浮き彫りになっています。
- 世界のデータ侵害の平均コストは2024年に488万ドルに急増し、パンデミック以後最大の年間あたりの増加を記録しました。

サイバー保険の視点

- ランサムウェア攻撃の総コストは平均491万ドルであり、復旧費用の急増によって、平均85万0,700ドルという身代金支払額の5倍以上になっています。
- グローバルな BEC 攻撃による損失は29億5,000万ドルを超え、CISA の年間総予算である28億ドルを1億5,000万ドル上回っています。

パートナーの視点

- サイバー犯罪者が脆弱性を数日以内に悪用する中、企業は、多額のコストを要するような侵害に拡大する前に脅威をプロアクティブに監視、検出、対応できるMSPを必要としています。
- SSRF や BEC のような AI を活用した攻撃が加速しており、進化し続けるリスクに企業が備えるためには、プロアクティブでリアルタイムの脅威検出と防御が不可欠です。
- 企業は、進化し続けるサイバー脅威に対してプロアクティブな保護、リアルタイムの監視、戦略的な防御を提供するセキュリティパートナーを必要としています。



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。