
SONICWALL®
サイバー攻撃の戦略のタイプと対抗策
電子書籍

はじめに

現代のサイバー犯罪者は、さまざまな動機、その多くは金銭的な利益を得ようとしてネットワークにこっそりと忍び込んだときに気づかれることを回避するため、ただでさえ複雑なテクニックをさらに進化させています。このようなサイバー攻撃者は、知的財産を盗み出すことや、スパイ行為、また、身代金を要求するために処理を妨害したりファイルを使用不能にしたりすることなど、さまざまな犯罪を企んでいます。サイバー犯罪者は検出されることを回避するために最新のテクニックを用いています。そしてアクセスを継続し、気づかれることなく悪意のある活動を行うことを目論んでいます。

攻撃者は標的の悪用が可能になると、感染したシステムにマルウェアをダウンロードしてインストールしようとします。多くの場合、使用されるマルウェアは新たに進化した亜種であり、旧来のウイルス対策ソリューションにとって未知のものです。

この電子書籍では、サイバー攻撃の戦略や、サイバー犯罪者がネットワークに侵入するために使用するツール、およびそのような戦略に対抗してサイバー犯罪者の活動を阻止する方法について解説します。

サイバー犯罪者は毎日24時間
あなたの弱点を悪用しようと
しています。

サイバー攻撃の戦略 #1
マルウェアを用いて
絶えずネットワークを攻撃する

マルウェアの総数は増加中であり、一部の国では数百万件という記録的な攻撃の試みが確認されています。攻撃はあらゆる経路から発生し、あなたのネットワークを標的にして侵害します。電子メール、モバイルデバイス、ウェブトラフィックなどがすべて標的となり、ハッカーは自動エクスプロイトを通じてあなたの情報を侵害することもできます。しかも、企業の規模は関係ありません。ハッカーにとってはあなたは1つのIPアドレス、電子メールアドレス、あるいは「水飲み場型攻撃」の潜在的な標的にすぎません。攻撃者は、昼夜を問わず自動化ツールを使用してエクスプロイトを実行したりフィッシングメールを発信したりしています。

多くの組織が直面している問題は、そのような行為に対する最適なツールが存在していないことです。トラフィックのスクラビング、エンドポイントの防御、悪質なメールのフィルタリングに役立つ自動化ツールが多くの企業にはありません。また、その他の企業でも、暗号化されたトラフィックに隠れた脅威を見つけることができないファイアウォールを運用していたり、マルウェアのシグネチャを保存するためのオンボードシステムメモリが限定的であったりします。

毎日24時間

対抗策 #1
毎日常にネットワークを防御する

何百種類もの未知のマルウェア亜種が次々と開発されており、組織はこれらの新しい脅威に対する最新のリアルタイム防御が必要です。効果的なセキュリティソリューションには、リアルタイムで危険性を検出し、毎日24時間常に組織を防御できる最新の技術が必要です。マルウェアの種類と亜種の増加により、ファイアウォールで使用可能なメモリは限界を超えています。Real-Time Deep Memory Inspection（RTDMI™）のような技術を採用しているセキュリティサービスソリューションは、マスマーケットを対象としたゼロデイ攻撃の脅威と未知のマルウェア亜種を先を見越して検知し、ブロックします。

ファイアウォールでは、マルウェアを可能な限り幅広く観察し、新しい亜種を発見して識別するためのクラウドベースのサンドボックスを使用する必要があります。また、IoT（モノのインターネット）デバイスは攻撃者に侵入点として利用される可能性があるため、セキュリティソリューションがファイアウォールゲートウェイだけでなく、モバイルエンドポイントやリモートエンドポイントでも防御機能の動的な更新をサポートしていることも不可欠です。

リアルタイムの自動侵害検出・防止機能で最新のマルウェアの脅威に対抗するためにクラウドの能力を活用するセキュリティプラットフォームが不可欠です。

サイバー犯罪者はさまざまな種類のマルウェアを使って不意を突いてきます。

サイバー攻撃の戦略 #2
さまざまな形のマルウェアを用いてネットワークを感染させる

サイバー犯罪者はネットワークを侵害するために複数の攻撃経路とマルウェア亜種を使います。代表的な5つのタイプは、ウイルス、ワーム、トロイの木馬、スパイウェア、ランサムウェアです。

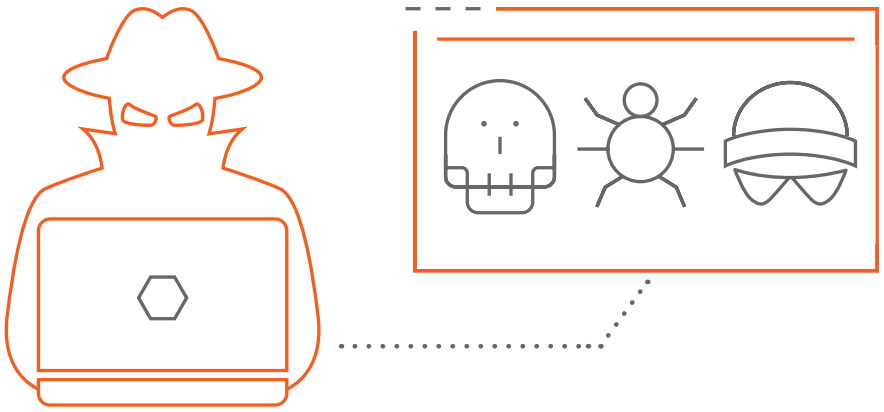
コンピューターウイルスは、当初は感染したメディアを共有することによって拡散するものでした。テクノロジーの進化により、拡散の方法も進化しました。今日では、ウイルスは正規のプログラム、ファイルの共有、ウェブからのダウンロード、電子メールの添付ファイルから拡散することが一般的です。ウイルスは、開いたり実行したりするとデータの破損からシステムのクラッシュまでさまざまな悪意のある動作を行う可能性があります。

コンピューターワームは1980年代後半から存在していますが、組織内のネットワーキングインフラストラクチャが一般的になるまでは流行していませんでした。コンピューターウイルスとは異なり、ワームは自己複製型であり、人間が介在しなくてもネットワークに侵入できます。ワームは急速な感染を引き起こし、ネットワークをトラフィックで過負荷状態にする可能性があります。

トロイの木馬は、正規のソフトウェアやファイルを装った悪意のあるプログラムで、ネットワークから機密データを盗み出すことに特化して設計されたものです。多くのタイプのトロイの木馬は、感染したシステムを乗っ取り、後でアクセスして攻撃するためのバックドアを開きます。また、トロイの木馬はボットネットの作成にも頻繁に使用されます。

スパイウェアは通常、本質的には悪意はありませんが、ウェブブラウザに感染し、ブラウザをほぼ操作不能にしてしまうことが多いため、非常に厄介な存在です。スパイウェアは正規のアプリケーションを装っている場合があり、ユーザーに何らかのメリットを提供する一方で、キーの入力や閲覧の履歴を密かに記録したり、個人データを盗み出したり、ユーザーの行動や使用のパターンを追跡したりします。盗み出されたデータは攻撃者に送信され、ユーザーのプライバシーやセキュリティが侵害されます。

ランサムウェアは、多くの場合、エンドポイントやサーバー全体のファイルを暗号化してアクセス不能にする攻撃です。サイバー犯罪者は、暗号化キーを受け取るための身代金を組織に要求します。通常はビットコインが使われます。ランサムウェアがビジネスに不可欠なシステムまで広がってしまうと、ランサムウェアのコストは数十万ドル以上に増える可能性があります。



脅威への対策として、マルウェアに対する複数の防御層を検討する必要があります。

対抗策 #2
ネットワークがあらゆる種類のマルウェアに対して防御されていることを確認する

すべてのファイアウォールがあらゆる種類のサイバー脅威から組織を防御する必要があります。最適に実現するには、以下の防御策を、ゲートウェイだけでなく、これまでの境界を超えてエンドポイントでも攻撃経路をブロックするシングルパスで低遅延のアプローチに統合することが必要です。必要な機能を見ていきましょう。

- ネットワークベースのマルウェア防御で、侵害されたシステムに攻撃者がマルウェアをダウンロード・送信することをブロック
- 継続的かつタイムリーな更新により、数百万もの新たなマルウェア亜種が発見されると直ちにネットワークを24時間体制で防御
- 侵入防止サービス（IPS）により、攻撃者による脆弱性の悪用を防止
- サンドボックスにより、疑わしいコードをクラウドベースの隔離された環境に転送し、未知のマルウェアを検出するためにデトネーションと分析を実施
- アクセスセキュリティにより、ネットワーク境界の内側と外側の両方で、モバイルおよびリモートのエンドポイントにユーザーアクセス制御の対策を適用
- 電子メールセキュリティで、電子メールを介して送信されるフィッシング、スパム、トロイの木馬、ソーシャルエンジニアリング攻撃をブロック

ネットワークにアクセスできるすべてのデバイスに最新のウイルス対策ソフトウェアが導入されていることにより、ネットワークのマルウェア防御のための追加レイヤーが提供されます。包括的なウイルス対策を行っているPCとネットワークファイアウォールを組み合わせることで、組織はサイバー犯罪者がネットワークを侵害するために使用するツールの多くを阻止できます。

サイバー攻撃の戦略 #3
最も脆弱なネットワークを見つけて侵害する

多くのファイアウォールベンダーは、優れた脅威防御機能の提供を主張していますが、そのソリューションの有効性を実証できるベンダーはほとんどありません。旧来型のファイアウォールを使用している組織は自社のネットワークが防御されていると信じているかもしれませんが、スキルの高いサイバー犯罪者は、複雑なアルゴリズムによって検出されることを回避してネットワークを侵害することで、適切なセキュリティ対策が欠けているファイアウォールをこっそりとすり抜けることができます。

一部のファイアウォールはパフォーマンスを犠牲にしてセキュリティを提供しており、ファイアウォールを使用する組織は高いネットワークパフォーマンスの要求に対応するためにセキュリティ対策を無効にしたり制限したくなる可能性があります。これは非常に危険な行為であり、避けるべきです。

ネットワークセキュリティにおけるもう一つの脆弱性は、人的要因によるものです。犯罪者は、人間の行動や振る舞いがネットワークの完全性、機密性、可用性を不用意に低下させる可能性を手掛かりにします。リスクをもたらし、セキュリティ対策を弱体化させるおそれがある行為として、フィッシング詐欺、ソーシャルエンジニアリング、不適切なシステム設定、ソフトウェアのパッチが未適用、セキュリティポリシーの無視などがあります。犯罪者はこれらの手口を悪用してログインやその他の認証情報を取得し、内部から攻撃させることでファイアウォールによる防御を犯罪者が簡単に回避できるようにします。さらに、従業員が適切なセキュリティ対策を講じていない状態で個人所有のデバイスを企業のネットワークに接続しているケースがあります。このような場合、個人所有のデバイスを紛失したり放置したりすると不正アクセスにつながり、ネットワークセキュリティ境界の外側で組織が侵害にさらされる可能性があります。

多くの場合、サイバー犯罪者は発見したネットワークの弱点に基づいて被害者を標的にします。

すべてのファイアウォールに、パフォーマンスを損なうことなく、内部と外部の両方の攻撃からネットワークを防御するエンジンが必要です。

対抗策 #3
優れた脅威防御対策、高パフォーマンス、集中管理を提供する包括的なセキュリティプラットフォームを選ぶ

ネットワークベースのマルウェア防御対策について第三者によるテストが行われて認定されたセキュリティソリューションが必要です。

あらゆるサイズと種類のファイルをスキャンして、変化するトラフィックフローに対応できるマルチコアプラットフォーム設計を検討する必要があります。すべてのファイアウォールに、パフォーマンスを損なうことなく、内部と外部の両方の攻撃からネットワークを防御するエンジンが必要です。

環境を標的にしている可能性がある未知のマルウェアを発見できるようにするには、クラウドベースのサンドボックスを提供するファイアウォールを探す必要があります。これらの選択は、通常の営業日になるか、サイバー犯罪者があなたのデジタル資産を人質に取る日になるかを左右する可能性があります。

セキュリティ戦略には、安全なモバイルアクセスのために、境界の内側と外側の両方でモバイルエンドポイントとリモートエンドポイントの防御が必要です。

さらに、フィッシング、スパム、ウイルス、ソーシャルエンジニアリング、電子メールを介して送信されるその他の脅威から防御するために電子メールセキュリティが必要です。無料のSonicWallフィッシングクイズなどのツールを使用して、組織の教育を行いましょう。

サイバー攻撃の戦略 #4
頻繁に形を変えて世界中で攻撃する

新しい脅威が世界中で
数秒単位で出現しています。

多くのサイバー犯罪者は、継続的に新しいマルウェアを発明して世界中の同業者と共有することによって成功を収めています。これは、世界中で数秒単位で新しい脅威が出現していることを意味します。サイバー犯罪者の多くは、「スマッシュ&グラブ」という攻撃の手口を採用しています。侵入し、できる限り収奪し、誰かが警告を発する前に脱出するのです。犯罪者は、被害者が攻撃されたことに気づく前に侵入して脱出できます。また、じっくりと長期間にわたってより多くのデータにアクセスしようとする犯罪者もいます。ウェブを介して行われる攻撃や、電子メールを介して、または過去にネットワークセキュリティ境界の外側でローミング中に感染したデバイスのネットワークに直接侵入するような攻撃もあります。

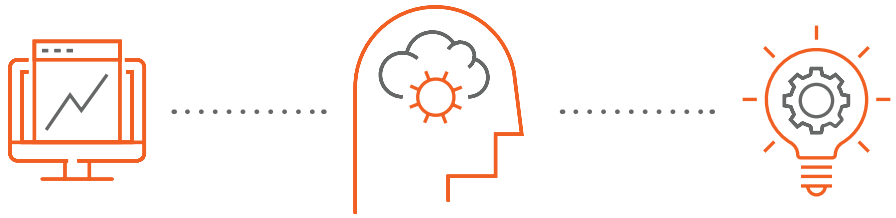
最新のグローバルな脅威をブロックするには、グローバルな脅威インテリジェンスを備えたセキュリティソリューションに投資する必要があります。

対抗策 #4
グローバルな脅威から防御できるファイアウォールを選ぶ

脅威に迅速に対応することは、防御を最大化するために重要です。新たな脅威に対する対策を速やかに展開するためには、独自の脅威インテリジェンス、調査、対策チームを持っているセキュリティソリューションプロバイダーを探す必要があります。さらに、SonicWallサイバー脅威レポートと同様に、より幅広いセキュリティコミュニティと協力して、そのチームの活動範囲を拡大する必要があります。

幅広いソリューションが、グローバルレベルで包括的なクラウドベースのマルウェアカタログを利用してローカルファイアウォール分析を強化します。

最後に、シンプルなファイアウォールでは地理的な識別とブロックは可能ですが、より高度な次世代のファイアウォールでは、ボットネットフィルタリング機能を追加して、危険なドメインからのトラフィックをブロックしたり、悪意のある場所との接続をブロックしたりすることにより、既知のグローバルな脅威にさらされる可能性を低くします。



まとめ

ネットワークベースのサイバー攻撃に対する効果的な防御戦略を策定する場合、強力なセキュリティ対策と、パフォーマンスを損なうことなくネットワークの異常な動作を検出して対応できる効果的なセキュリティツールの使用を取り入れた包括的なアプローチを実装する必要があります。進化を続けている脅威に積極的に適応することによって、未知の脅威から自分自身と組織を守りましょう。

組織の固有のニーズに合わせた対策ソリューションの評価をご希望のお客様は、SonicWallの担当者にお問い合わせいただくか、オンラインでSonicWallの次世代ファイアウォール（NGFW）の詳細情報をご覧ください。

詳細について


SonicWallのセキュリティ専門家にお問い合わせください。


SonicWallの製品群のライブデモをご覧ください。


当社のウェブページ、次世代ファイアウォールをご覧ください。


最新の攻撃の発生状況については、当社のCapture Labs Security Centerでご覧ください。

About SonicWall

SonicWallは、Boundless Cybersecurityを提供することにより、誰もがリモート/モバイルで危険にさらされながら仕事をするという超分散化時代のビジネスの現実に対処します。未知の領域を探求し、リアルタイムの可視性を提供しながら経済の大躍進を実現しているSonicWallは、サイバーセキュリティ業務上の課題を解決して世界中の企業や政府、中小企業をサポートします。詳しくはwww.sonicwall.comをご覧ください。

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
その他の情報については当社のウェブサイトをご覧ください。
www.sonicwall.com

Ebook-TypesofCyberattacks-JK-8854