Akamai

ホワイトペーパー

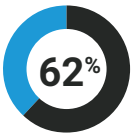
中小企業が直面している大きな脅威

概要

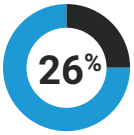
大企業に対するサイバー攻撃が注目されていますが、中小企業（SMB）も大企業と同じサイバーセキュリティリスクに直面するケースが増えています。今日の脆弱性攻撃の多くは、金銭的利益のみを目的としているため、標的を規模で区別しません。攻撃者にとって、お金が稼げるのであれば、企業の規模は関係ないのです。犯罪者はさまざまな方法を駆使して、企業の従業員や彼らが依存するデバイス、そして広く使用されているインテリジェントな接続デバイスさえも標的にします。インターネット・サービス・プロバイダーは、SMB による自己防衛の支援に適した立場にあります。

この文書では、SMB が直面する最も一般的な脅威とその影響について説明します。

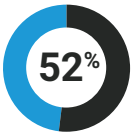
National Small Business Association が発表した Technology and Small Business Survey で、興味深い統計情報がいくつか明らかにされました。



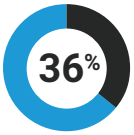
中小企業経営者の 62% がサイバーセキュリティは非常に重要な関心事であると回答しました。さらに、33% がやや重要と回答し、重要ではないとの回答はわずか 5% でした。



サイバーセキュリティ問題への対処法を理解していると回答した企業経営者はわずか 26% でした。



自社がサイバー攻撃の影響を受ける可能性があることを非常に懸念しているという回答は 52% に上り、やや懸念しているという回答も 44% ありました。35% の回答者はサイバー攻撃の被害者になったことがあると報告しています。



ドメインまたはメールアドレスから情報が不正に送信されたという回答が 36%、機密情報が盗まれたという回答が 5%、銀行口座にアクセスされたという回答が 4% ありました。また 52% の回答者が攻撃によってサービスが中断されたと報告しています。

今日の Web ベースの脅威は、大きく分けてマルウェアとフィッシングという 2 つの主要領域に分類できます。ボットネットはマルウェアの重要な一部であり、特に注意を要します。

マルウェアは、デバイスに密かにインストールされる悪性のソフトウェアです。侵害された Web サイトでは、デバイス上のソフトウェアの欠陥が利用され、マルウェアが読み込まれる可能性があります。また、ユーザーが悪性の Web サイトに誘導され、そこでクリックすることで悪性ファイルが読み込まれることもあります。一部のマルウェアは、デバイス上でアクティベートされ、それ自体のネットワークを通じて伝播します。企業を標的とするマルウェアには、以下のようにさまざまな種類があります。

暗号資産マイナーは、被害者の同意なしにデバイスの処理能力を使用するプログラムです。SMB のリソースが侵害されても、ランサムウェアとは違ってデバイスの所有者が金銭の支払いを要求されることはありません。そのため、この種の攻撃は検知が困難になる可能性があります。

POS デバイスに読み込まれる**特殊マルウェア**は、カードデータをキャプチャして攻撃者にアップロードし、企業経営者にリスクをもたらします。

巧妙な持続型脅威（APT：Advanced persistent threat）は、ネットワークにアクセスして貴重なデータを収集、抽出します。APT は非常に検知されにくいため、長期にわたってアクティブな状態を保つことができます。SMP は貴重なデータを失うだけでなく、さらに重要なこととして顧客の信頼も失う可能性があります。また、個人情報が漏洩した場合は、規制措置の対象となる場合もあります。

ランサムウェアは、デバイスまたはサーバー上のすべてを暗号化することでファイルへのアクセスをブロックします。攻撃者は高額で復号化キーを提供しますが、身代金を手に入れてもキーを送信しないケースもあります。SMB は運が良かった場合でも身代金を失い、最悪の場合は資金と重要な事業データの**両方**を失うことになります。

マルウェアは、次に示すようないくつかの方法で貴重なデータを収集します。**スパイウェア**は、ログイン資格情報や財務データなどのデータを探し、犯罪者にレポートをオフロードします。**データ流出**マルウェアは、コンピューターで貴重なデータを探し、特定して抽出することを目的に設計されています。**キーロガー**はキーストロークを記録します。トレーニングによって、金融口座やソーシャルメディアへのログイン情報といった貴重な情報への犯罪者のアクセスが可能になります。**銀行を標的とするトロイの木馬**は、ユーザーの行動を監視してログイン認証情報を学習したり、銀行の Web サイトになりすまして金銭を盗み取ったりします。

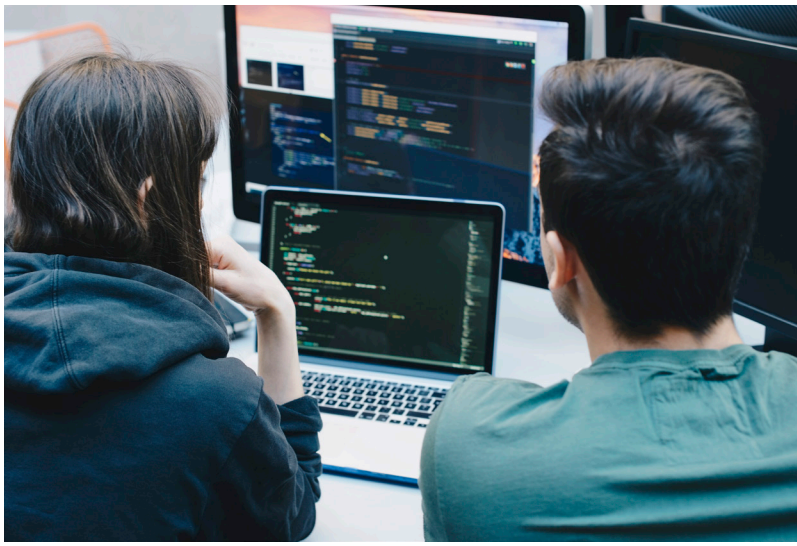
ボットネットとは、同じマルウェアに感染したデバイスのネットワークです。このマルウェアは、共通の犯罪者またはグループがコマンド & コントロール（C2）と呼ばれる中央チャネルを通じて制御します。ボットネットはレンタルサービスとして利用される場合が多く、ほとんどのボットネットは前述のような多様な機能を実行して金銭を得ます。

フィッシングは、特にソーシャルエンジニアリングを利用する手口で被害者をだまし、攻撃者が収益化できるような情報を開示させます。これまでのフィッシング攻撃では、ユーザーに迷惑メールのリンクをクリックさせて、機密情報を開示するように促していました。フィッシング攻撃の開発者はこの手法を多様化し、今では、ソーシャルメディアの投稿やコメント、テキストメッセージ、SMS、Skype、Messenger などのサービスにもフィッシング URL を組み込んでいます。

モバイルデバイスはフィッシングの主な標的となります。これは、画面が小さく、リンクが悪性であることを示すわずかな手がかりをマルチタスクユーザーが見逃すことが多いためです。さらに紛らわしくするために、フィッシング詐欺者は異なる文字セットの類似文字を使用して正規のドメイン名を模倣します。

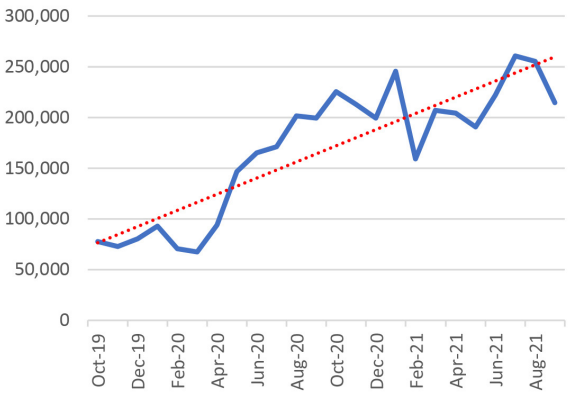
以下は使用された文字列の実例です。

7eleven.com
Adidas.com
adidas.com
philippineairlines.com
rolex.com
singaporeair.com
thaiairways.com



最近、フィッシングは増加傾向にあります。Anti-Phishing Working Group が発行した 2021 年第 3 四半期 の Phishing Activity Trends Report によると、「フィッシングは第 3 四半期に月間記録を達成し、2019 年後半以降、攻撃件数が倍増」しているとのことです。以下のチャートは同レポートから引用したもので、この傾向が示されています。このような傾向が見られるのは、ソフトウェアの欠陥を悪用するよりも、ユーザーを騙して意図せずにアクションを実行させる方が簡単だからです。

フィッシング攻撃、2019 年第 4 四半期～2021 年第 3 四半期



Akamai のキャリアおよびエンタープライズ・セキュリティ・リサーチチームが収集したデータによると、フィッシングに使用されるドメイン名の寿命はますます短くなり、2019 年 3 月の平均寿命は約 1.5 時間になっています。これは、保護にも直接的な影響を及ぼします。防御は攻撃と同様にアジャイルであることが必要だからです。

結論

これは、Web 脅威の包括的なリストではありません。攻撃者は、利益を最大化するために攻撃の実行可能性を常に評価し、攻撃の見え方も機能も変化させています。また、望まない広告やコンテンツの表示など、主として集中を妨げたり不愉快にさせるようなマルウェアも存在します。

SMB は、各社固有のニーズや制約に対応したソリューションを使用して、Web ベースの脅威から身を守る必要があります。Akamai は、SMB 向けに設計された Secure Internet Access サービスを提供しています。これらのサービスは、管理負担を課すことなく、この文書で説明したさまざまな攻撃から SMB を保護します。職場のすべてのデバイスとすべての人がゲストも含めて自動的に保護されます。企業の管理者は、シンプルなグラフィカルポータルを通じて、ネットワークで起きていることや、阻止された脅威をすぐに確認できます。

Akamai Secure Internet Access サービスは、以下の点で ISP に役立つように設計されています。

- SMB 向けのエンタープライズグレードのセキュリティ防御によって収益を創出できる
- スピードと信頼性だけでなく、セキュリティに基づいて SMB サービスを差別化できる
- クラウド版の Secure Internet Access サービスによって、導入障壁を最小限に抑え、コストを軽減し、サービス配信をシンプル化できる

このサービスは、各ブランドに合わせたルック & フィールに完全にカスタマイズできます。また、機能セットと脅威インテリジェンスも、地域の市場要件に応じて調整できます。

どんな人も、どんなデバイスも、いつでも、Akamai がお手伝いします。
詳細については、Akamai にお問い合わせください。