2021年10月

身代金を支払わないために

ランサムウェア対策のための3ステップ

Barracuda
Your journey, secured.

目次

ランサムウェアとその進化の過程

簡単に言うと、ランサムウェアとは、データを暗号化したり、自分のシステムにアクセスできないようにしたりする悪質なソフトウェアを指します。犯罪者は、復号化キーと引き換えに身代金を要求しますが、もちろん、そのキーが機能してデータを取り戻せるという保証はありません。

数年前のWannaCryのような「侵害して暗号化する」というストレートな攻撃に比べて、現在の攻撃者はより洗練されたマルチベクトルのアプローチを取っています。攻撃は依然として、多くの場合、スピアフィッシング場合メールから始まりますが、今日のランサムウェア攻撃は、ターゲットが悪意のあるリンクをクリックしてもすぐには起動しません。

サイバー犯罪者は、この段階で被害者の認証情報を盗みます。その認証情報を使って組織のネットワークにアクセスし、そこに潜んで資産、サーバ、データベース、メールプラットフォームなどを評価します。この潜入は、攻撃開始までに数週間から数ヶ月に及ぶこともあります。アイルランドの医療サービス機関である、HSEに対するランサムウェア攻撃では、まさにこういった事態が起こりました。攻撃者は、700GBの患者データを暗号化して盗む攻撃を開始する前に、何週間もかけてHSEのネットワークに侵入したと主張しています。

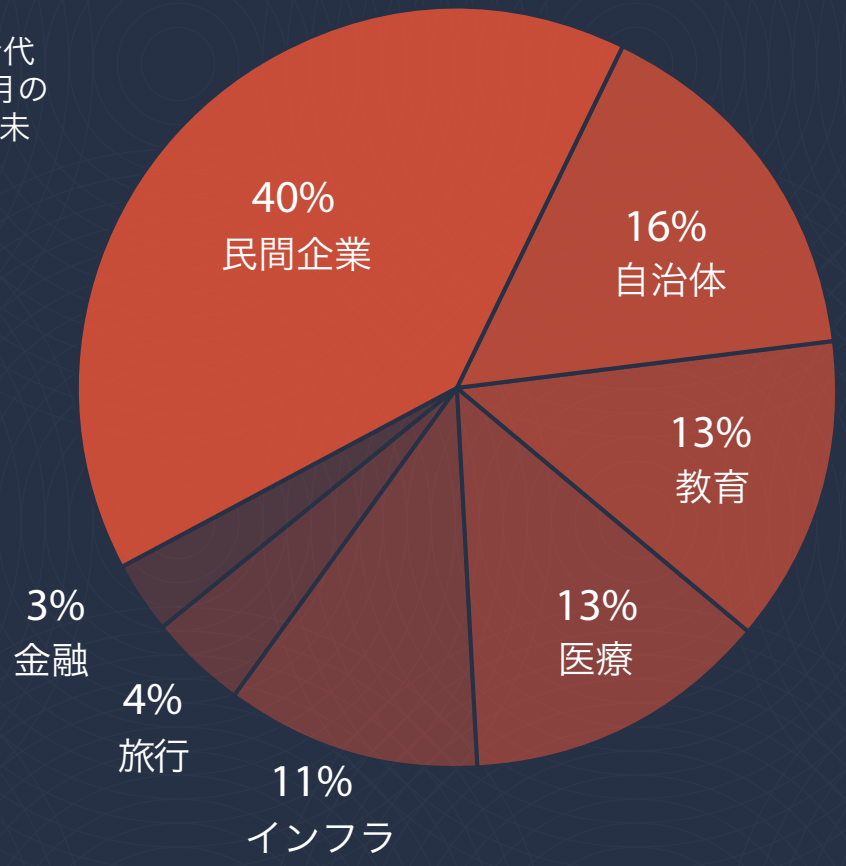
現在、ランサムウェアの話題を耳にする機会が増えている理由の一つは、参入障壁がなくなったことです。犯罪に必要なテクノロジは、より簡単に利用できるようになっています。今では、ランサムウェアのキットを購入して、ターゲットを選ぶことができます。ギャングは、身代金の一定割合と引き換えに技術サポートを提供します。それが難しい場合はサイバー犯罪者を雇って攻撃をしてもらう「Cybercrime-as-a-Service」という方法もあります。また、仮想通貨の価値が上がり、サイバー保険が普及したことで、サイバー犯罪者にとってランサムウェア攻撃はより収益性の高いものとなり、高度に組織化されたギャングを惹きつけ、国家がスポンサーとなったランサムウェア攻撃はサイバー戦争を新たなレベルに引き上げました。

サイバー犯罪者たちは危機感を募らせている

ランサムウェアによる攻撃は、各国政府がテロ行為として扱うほどにエスカレートしています。これは過剰反応ではありません。この攻撃は、地方自治体、法執行機関、教育機関、医療ネットワーク、重要インフラなどに大規模な業務上の混乱をもたらしています。どの業界、組織、政府機関も、これらの攻撃と無縁ではありません。

バラクーダによる最近の調査では、2020年8月から2021年7月の間に、インフラ、旅行、金融サービスなどの企業への攻撃がランサムウェア攻撃全体の57%を占めており、2020年の調査ではわずか18%だったことがわかりました。今では、インフラ関連の企業だけで、調査した全攻撃の11%を占めています。

身代金の額も劇的に増加しており、現在、インシデントごとの平均身代金要求額は1,000万ドルを超えています。2020年8月から2021年7月の間に弊社が分析したインシデントのうち、身代金要求額1,000万ドル未満がわずか18%で、3,000万ドル以上が30%でした。

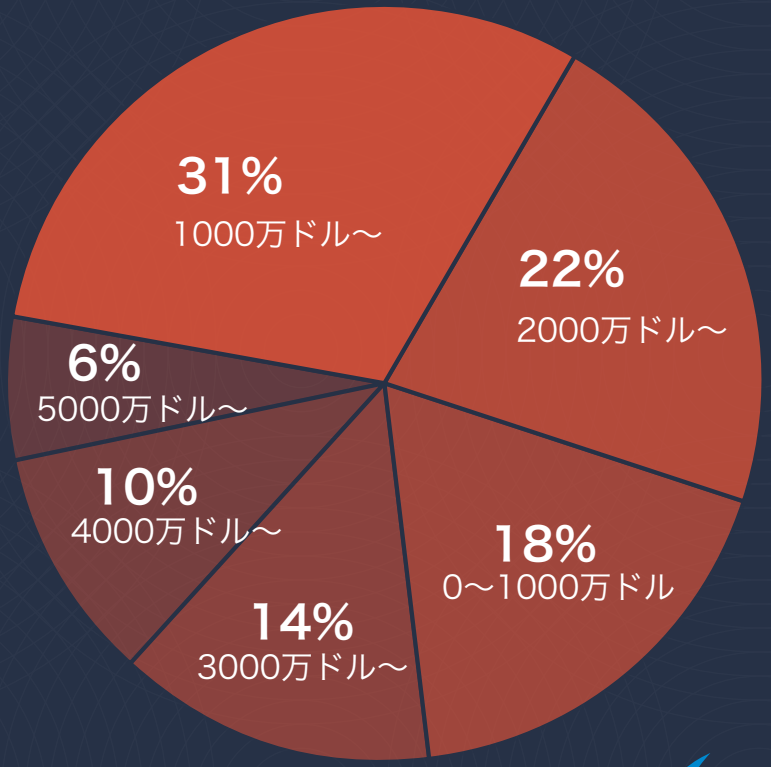


ランサムウェアは新しい脅威ではありませんが、より破壊的なものに進化しています。犯罪者たちは、スキルセットを拡大し、戦術を洗練させて、二重の恐喝スキームを生み出しました。犯罪者は、攻撃の前に行う調査に基づいて身代金を要求します。被害者から機密データを盗み、そのデータを他の犯罪者に公開したり販売したりしないという約束と引き換えに支払いを要求します。犯罪者は信用できないので、支払いを済ませた被害者は数ヶ月後に連絡を受け、盗んだデータを秘密にしておくために再度支払いを要求されることがよくあります。ランサムウェアの犯罪者の中には、支払いに応じるものの、それでもデータを売ってしまう者もいます。

身代金を支払えば、暗号化されたデータがすべて復元されるという保証は、これまでありませんでした。被害者は、ランサムウェア攻撃で盗まれたデータは永遠に危険な状態にあることを理解する必要があります。犯罪者に罪を償う理由はありません。

自社に対するランサムウェア攻撃があることを想定しておく必要があります。攻撃が成功した場合、身代金を支払わないための計画を立てるべきです。

ランサムウェア攻撃からあなたの会社を守るためには、データを保護することが重要です。これは「認証情報の保護」、「Webアプリケーションの保護」、「データのバックアップ」という3つの重点分野に分けて考えることができます。ここでは、それぞれのステップについて詳しく見ていきましょう。



ステップ1:認証情報の保護

はじめに、ランサムウェアは、メールからの侵入や認証情報の入手に依存しています。何万ものユーザ名とパスワードがオンラインで簡単に入手できるため、この最初のステップは恐ろしいほど簡単です。攻撃者は、盗んだ認証情報を使って、あなたのシステムにアクセスします。

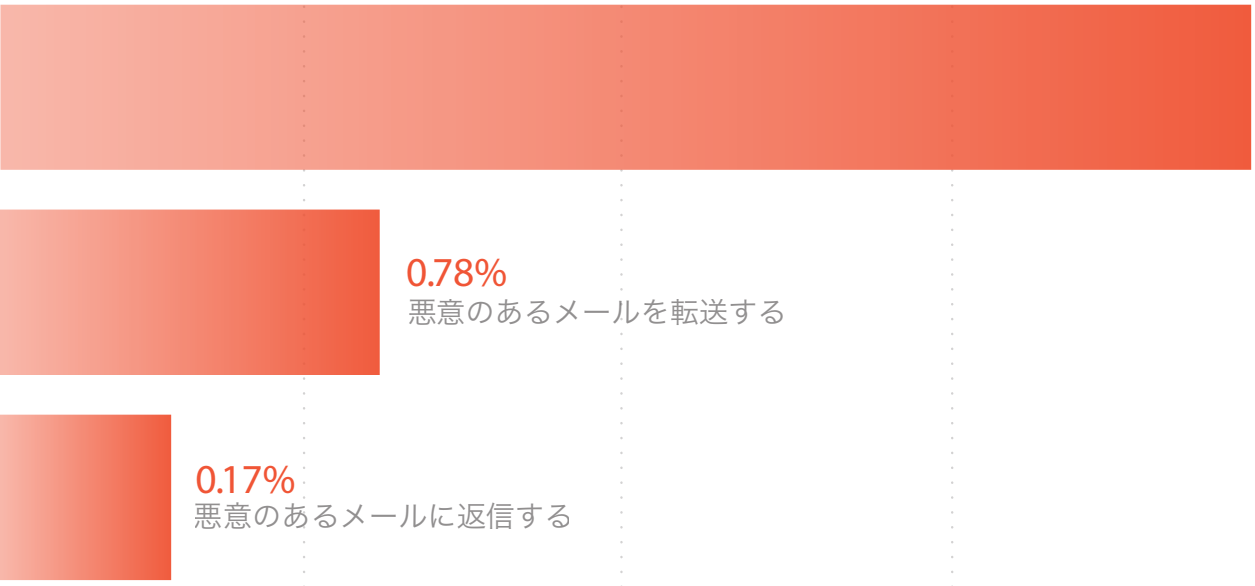
Barracuda

フィッシングはランサムウェアの主要な攻撃手段であるため、資格情報のセキュリティに対する意識を維持する必要があります。メールセキュリティについてユーザを教育するためのプロセスを開発し、異常な活動を識別してフラグを立てるアンチフィッシング技術を導入します。攻撃者が認証情報にアクセスできなければ、フィッシングからランサムウェアへと攻撃をエスカレートさせることがより困難になります。

フィッシング攻撃が有効なのは、人々が何かをクリックする行為を好むためです。ハッカーは、一般に公開されている被害者の個人情報を収集し、被害者の危機感を煽って反応を得ることで、被害者に合わせた攻撃を慎重に行います。攻撃者にとっては、組織内の1人がリンクをクリックしたり、添付ファイルを開いたりするだけでいいのです。

最近の弊社調査によると、フィッシングメールを受信した人のうち、平均3%がリンクをクリックするという結果が出ています。通常、この攻撃の目的は、アカウントの認証情報を取得することで、ハッカーが社内を横断的に移動し、組織全体の身代金を要求できるようにすることです。

認証情報とアクセスを保護するためには、2つのアプローチが必要です。まず、検知・対応ツールに投資し、次にユーザトレーニングに注力します。



出典：Threat Spotlight（バラクーダが注目する脅威）:メール攻撃と受信の防御

検知・対応ツール

メール保護技術は、リンクや添付ファイルを介して配信される悪意のあるペイロードの検出だけでなく、フィルタリング技術をバイパスしてユーザを騙して行動を起こさせるように設計されたソーシャルエンジニアリングの手法を用いた攻撃についても、認識する必要があります。また、悪意のあるペイロードが含まれていない場合でも、メール内に悪意があるかどうかを確認する必要があります。機械学習アルゴリズムを用いたメールセキュリティは、通常のコミュニケーションパターンからのわずかな逸脱を探すことで、より高い精度でソーシャルエンジニアリング攻撃を検知することができます。

ユーザの認証情報を保護するために、アカウントの乗っ取りに対する適切な保護が不可欠です。多要素認証（MFA）は、依然としてベストプラクティスであり、今日すべての組織で採用されるべきものです。しかし、それは特効薬のようなものではなく、必ずしも十分ではありません。攻撃者は、ユーザを騙して認証デバイスにマルウェアをインストールさせたり、偽のアプリケーションにアカウントへのアクセス権を与えたりすることで、MFAを回避する方法を見つけようとします。企業には、不審なログインや侵害されたアカウントからの攻撃など悪意のあるアクティビティを迅速に特定し、警告するアカウント乗っ取り防止策の導入が必要です。

認証情報とアクセスの保護には、2つのアプローチが必要です。

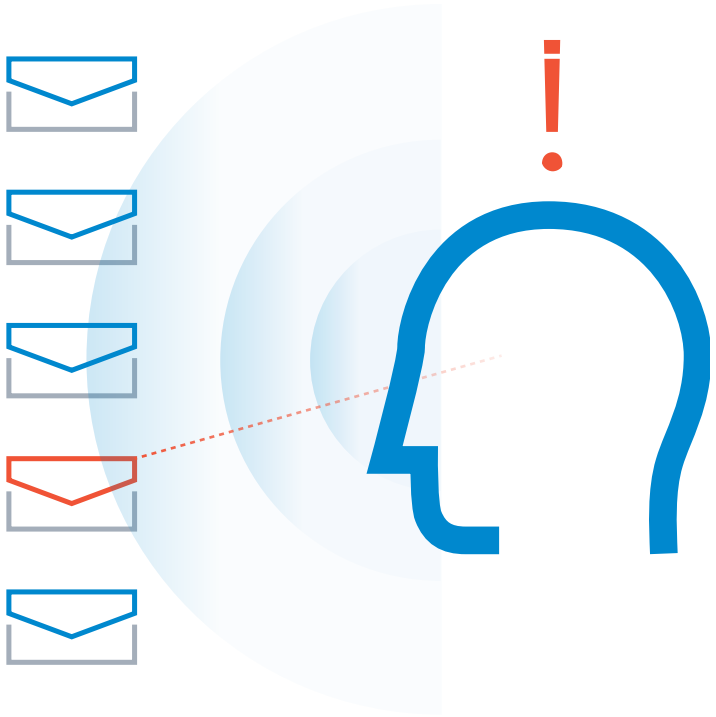
まず、検知・対応ツールに投資し次にユーザのトレーニングに注力します。

ユーザの育成

最後の砦として、従業員が攻撃を認識し、報告できるようにトレーニングすることは非常に重要です。メールセキュリティ戦略の一環として、セキュリティ意識向上トレーニングやフィッシングシミュレーションを実施しましょう。歴史的に見て、フィッシング攻撃はメールのみを対象としていましたが、現在、サイバー犯罪者はSMSや音声などの他のチャネルを利用します。メール、ボイスメール、SMSのフィッシングシミュレーションを利用して、サイバー攻撃を特定するためのトレーニングを行い、トレーニングの効果を検証し、攻撃を受けやすいユーザを評価します。

サイバーセキュリティのトレーニングは、新入社員へ入社日に実施するだけでは不十分です。進化する脅威に対応するためには、継続的なトレーニングが必要です。例えば、今日のギャングは、見破るのが難しい高度なソーシャルエンジニアリングを使用しています。スピアフィッシング攻撃は、ある個人、または財務などの1つの部門の一部を対象に、非常にカスタマイズされたメッセージを送信します。

重要なのは、トレーニングによって社員の信頼を獲得し、たとえそれが自分が誤って起こしたミスであっても、進んで警告を発してくれるようにすることです。是正トレーニングが必要な場合もありますが、警告を発した従業員を罰してはいけません。多くの攻撃は、社員がリンクをクリックしたり、添付ファイルを開いたりしたことで非難されることを恐れているため、報告されていません。早期の警告は非常に貴重であり、賞賛されるべきものです。



ステップ2：Webアプリケーションとアクセスの保護

リモートワークへの移行により、さらに多くのアプリケーションがデータセンターからインターネットに接続されるようになりました。ビジネスサービスの機能維持を急いだ結果、セキュリティが見落とされることがあり、サイバー犯罪者はこれらの脆弱性を利用する準備ができています。

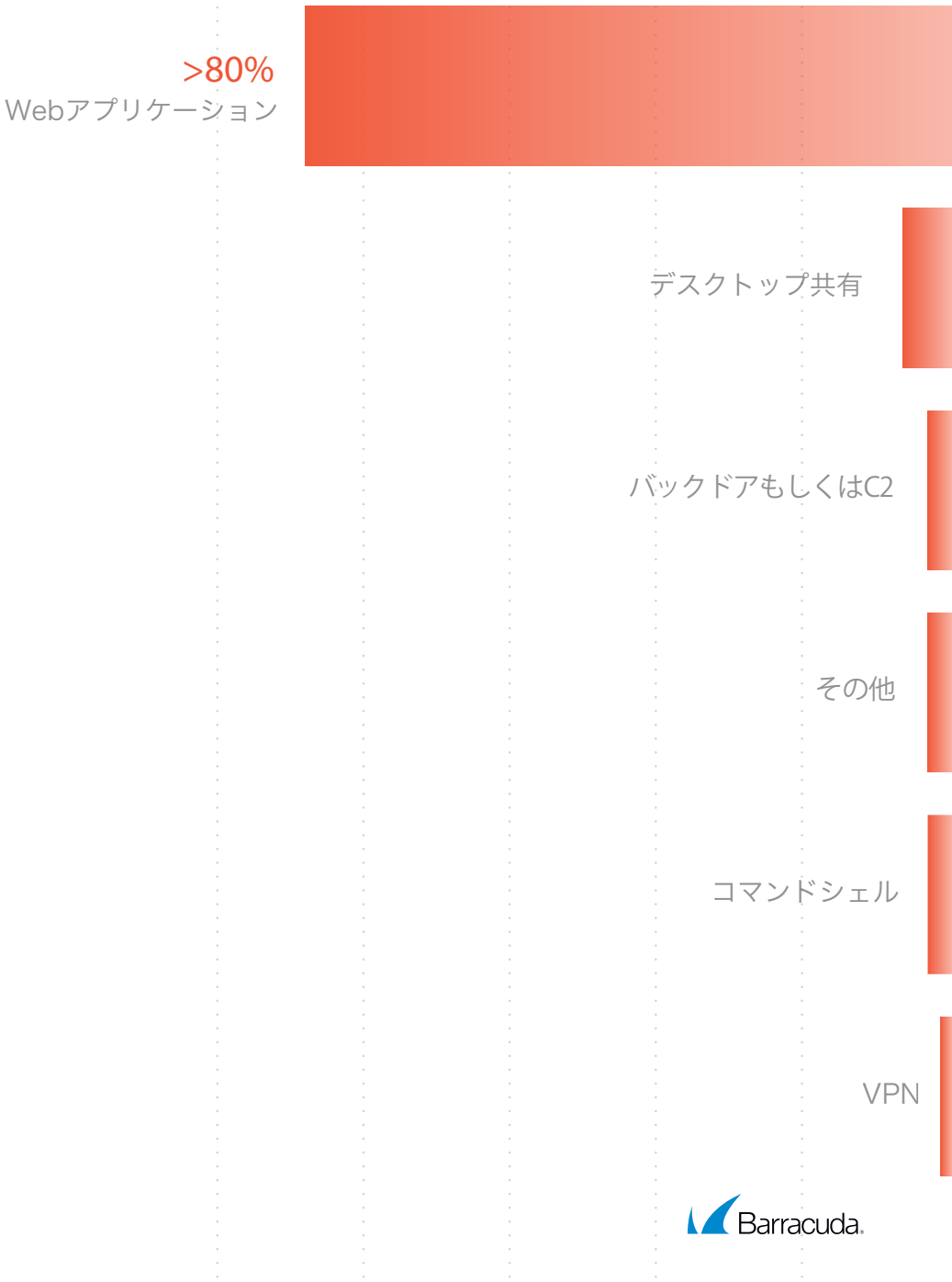
Barracuda

ベライゾンの2021年データ漏洩/侵害調査報告書（DBIR）によると、ハッキングにおいて、Webアプリケーションが最大の攻撃手段として使用されており、データ漏洩の80%以上を占めています。

ファイル共有サービス、Webフォーム、Eコマース（電子商取引）サイトなどのオンラインアプリケーションは、攻撃者によって侵害される可能性があります。Webアプリケーションは、ユーザインタフェースやAPIインタフェースを通じて攻撃されます。多くの場合これらの攻撃には、クレデンシャルスタッフィング、ブルートフォース攻撃、またはOWASPの脆弱性が含まれます。アプリケーションが侵害されると、攻撃者はランサムウェアやその他のマルウェアをシステムに侵入させます。このようなマルウェアは、さらに横断的に移動して、アプリケーションのユーザだけでなく、ネットワークにも感染する可能性があります。

ランサムウェアなどのマルウェアから身を守るためには、アプリケーションやアクセスを保護することが、メールセキュリティと同様に重要であると理解することが大切です。Open Web Application Security Project（OWASP）は、ランサムウェア攻撃に悪用される可能性のある、最も一般的なアプリケーションの脆弱性について、一般の人々の認識を高める活動を行っています。

出典：ベライゾン2021年データ漏洩/侵害調査報告書



最近の例では、2021年7月に明るみに出た「REvil」ランサムウェアによるサプライチェーンハッキングがあります。公開されているインターネット上のMSPアプリケーションの脆弱性が悪用され、顧客にランサムウェアが拡散されました。このようなハッキングは、インターネットに接続されたアプリケーションで発生する可能性があり、攻撃者はアプリケーションに侵入した後、横断的に移動して大惨事を引き起こします。同様のシナリオは、たとえデフォルトのポートを変更したとしても、RDPシステムをインターネットに公開したままにしておくと発生する可能性があります。攻撃者は、このようなRDPシステムに対して取得した認証情報を使用して、保護されていないこの攻撃経路を通じてネットワーク全体をランサムウェアに感染させようとします。

最大で

1500

の企業がREvilのサプライチェーン攻撃の影響を受けた

Barracuda

Webアプリケーションに対する4つの攻撃ベクトル

現在、アプリケーションはランサムウェアの主要な標的となっているため、保護すべき攻撃ベクトルは、アプリケーションへのアクセス、Webアプリケーションの脆弱性、インフラへのアクセス、ラテラルムーブメント（侵入拡大）の4つです。

1. アプリケーションへのアクセス

アプリケーションアクセスが組織にとって危険な問題であるかどうかを特定するためには、いくつかの重要な質問に答える必要があります。

- **リモートワーカーや契約社員は管理されていないデバイスや個人保有の携帯用機器（BYOD: Bring Your Own Device）を使用していますか？**モバイルデバイスはその最も一般的な例です。管理されていないデバイスやBYODデバイスが侵害されると、認証情報の採取やアプリケーションへのさらなる攻撃に使用される可能性があります。
- **ネットワーク上のすべてのユーザとデバイスを可視化していますか？**例えば、誰がゲストネットワークに接続しているのか、それが適切にセグメント化されているのかを知る必要があります。
- **誰がいつ何にアクセスしたかを記録する監査証跡はありますか？**誰がアプリケーションにアクセスしているか、どのようにアクセスしているか、適切な権限を持っているかなどを振り返ることができなければなりません。

本来ネットワークに接続してはいけない機器がネットワークに接続されていて、誰かがその機器にハッキングツールを設定していたとしたら、それは深刻な問題です。また、これらすべてを可視化できなければ、誰が何にアクセスしているのか、どのような脆弱性があるのかを特定することが困難になり、表面化した脆弱性を閉じたり、攻撃者のアクセスを遮断したりすることができなくなります。

2. Webアプリケーションの脆弱性

Webアプリケーションの脆弱性は、自社アプリケーションが実際にどれだけ安全かを判断するために評価する必要がある次の攻撃ベクトルです。

以下の質問について考えてみてください。

- Webサイトの安全は保たれていますか？最後に更新されたのはいつですか？
- Webサイトにフォームはありますか？フォームを介した攻撃をどのように防ぎますか？
- Webサイトでファイルのアップロードを受け付けていますか？マルウェアへの対策はどうなっていますか？

HTTPSを有効にするだけでは、サイトの安全性は確保できません。これは単に、攻撃者がサイトにログインしている人の認証情報を盗むことができないことを意味します。サイバー犯罪者は、HTTPSフレーム内でブルートフォース攻撃を行い、サイトの正しいログイン情報を見つけ出そうとすることができます。

CAPTCHAやreCAPTCHAをサイトのログインフォームの前に設置することも、これらのサービスを自動化し回避することが容易であるため、不十分です。

ログインやIPのレート制限も、ハッカーがパスワードスプレー攻撃（low-and-slow attack）や、さまざまな自動化システムを使って簡単に回避できるセキュリティ対策のひとつです。

また、ファイルのアップロードを受け付けている場合は、別の問題に対処する必要があります。攻撃者がウイルスやランサムウェアをアップロードしてWebサイトに侵入しようとすることはよくあることです。

3. インフラへのアクセス

COVID-19の流行が始まって以来、多くの組織が社内でホスティングされたアプリケーションへのアクセスを提供するためにVPNを使用してきました。これは、自社でホストしているアプリケーションの一部に、代替となるSaaSが存在しない場合に起こります。自宅からのVPNアクセスを提供することは、ビジネスを継続するための唯一の方法です。しかし、適切なIDとアクセスの実装がなければ、このアプローチは"爆発を待つ時限爆弾"のようなものです。すでに盗まれた認証情報の多くは、インフラへのアクセスに使用されるユーザ名とパスワードを共有している可能性があるため、ネットワーク、アプリケーション、データを流出させてしまう真のリスクが生じます。

4. ラテラルムーブメント（侵入拡大）

盗まれた認証情報を使ってアプリケーションやインフラを侵害した後、攻撃者はネットワークの奥深くに入り込み、そこからさらに攻撃を行おうとします。これが対処すべき4つ目の攻撃ベクトルです。以下の質問をしてみてください。

- 企業ネットワークは適切に保護されたセグメントに分割されていますか？
- ネットワークへのアクセスに多要素認証を導入していますか？

ネットワークに適切なセグメントを設定するには多くの時間と労力が必要ですが、2つのセグメントを開放したり、あるセグメントから別のセグメントへのアクセスを許可したりする理由は簡単に見つかります。最終的に、それはあなたが望まなかった方法でアクセスが開かれることにつながるからです。

多要素認証は、攻撃者がネットワークにアクセスするのを阻止するために、もう一つの重要な保護層を追加します。

Barracuda

ランサムウェア攻撃がアプリケーションの脆弱性を悪用する方法

もう一つのシナリオを紹介します。貧弱なアプリケーションセキュリティを悪用してランサムウェア攻撃を成功させるために、攻撃者が実行するであろう、架空でありながら現実的な一連の手順です。この攻撃では、再燃しているブラウザのクーポンプラグインを利用して、一般的なクーポン詐欺を試みようとしています。

ステップ1

攻撃者は、正規のクーポンサイトを模倣したウェブサイトを作成します。攻撃者は、人気のあるクーポンサイトになりすましますが、これはドメインの偽装や自動Webスクレイピングを使えば比較的簡単にできます。この偽サイトをWebサイトXと呼びます。

ステップ2

攻撃者は、OWASPのトップ10脆弱性のうちの1つ以上を調査し、正規だが保護が不十分な企業のWebサイト（ここではウェブサイトYと呼びます）から認証情報を盗みます。認証の不備や機密データの漏洩などの脆弱性により、ハッカーはWebサイトYからユーザの認証情報やその他の機密情報を取得します。

ステップ3

攻撃者は、盗んだ認証情報を使用して、WebサイトZと呼ばれる正規のEコマースサイトに対してクレデンシャルスタッフィング攻撃を開始します。これは、数週間にわたってゆっくりと実行できる自動化された攻撃です。この攻撃では、盗んだ認証情報をこれらのサイトの実際のアカウントと照合しようとします。

ステップ4

この攻撃で一致するものが見つかり、ハッカーが被害者のアカウントにログインできた場合、次のステップでは、そのアカウントを使ってWebサイトZに人気商品のレビューを投稿します。このステップでの一般的な例は、「この商品は最高です！ここをクリックして、このクーポンで価格から50%オフにしてください」というものです。クーポンへのリンクは、訪問者をステップ1の偽のWebサイトであるWebサイトXへと導きます。

ステップ5

WebサイトZにログインした潜在的な被害者は、ドメイン名、URL、サイト証明書などの詳細を注意深く見ない限り、詐欺サイトに誘導されたことに気づかず、WebサイトXへのリンクをたどって製品レビューをクリックしていきます。このサイトを信用した被害者は、クーポンと引き換えに連絡先を提供します。攻撃者は現在、そのサイトからのメールを期待している人のアドレスを知っています。攻撃者は被害者の信頼を得ており、被害者は警戒心を失っているのです。

ステップ6

被害者は製品とクーポンに関するパーソナライズされたメールを受け取り、クーポンを有効にするためインストールするように指示された添付ファイルを受け取ります。この添付ファイルは、実行ファイルである場合もあれば、攻撃を実行するためにJavaScriptを使用するブラウザ拡張である場合もあります。このメールは完全にカスタマイズされていて、受信者が期待しているものであるため、従来のメール防御では許可される可能性があります。被害者のOSは、信頼できない実行ファイルをインストールしないように促しますが、この時点で被害者は攻撃者を全面的に信頼しており、クリックしてしまいます。

ステップ7

被害者が添付ファイルをインストールすると、ランサムウェア攻撃が開始されます。実行ファイルがインストールされると、マスタブートレコードへの感染、ファイルシステムテーブルの暗号化、さらにはOSの起動を阻止するなど、いくつかのタイプの攻撃が開始されます。攻撃者は通常、この攻撃を拡大し、より多くの認証情報やネットワーク上に存在するその他のデータを採取しようとします。これが完了すると、ランサムウェアはネットワークデータを暗号化します。

この例では、ランサムウェアが成功したのは、複数のWebサイトに存在するアプリケーションセキュリティの脆弱性により、ステップ1での正規サイトのWebスクレイピング、ステップ2での認証情報の窃取、ステップ3でのクレデンシャルスタッフィング、ステップ4と5でのコメントスパムと悪意のあるURL、ステップ7での実行ファイルのインストールという説得力のあるシナリオを構築することができたためです。これらのステップのいずれかにおいて、適切なアプリケーションセキュリティがあれば、この攻撃を阻止できたはずです。

アプリケーションとアクセスを保護する方法

ネットワークの保護

ランサムウェアのネットワーク内での拡散を防ぐには、ネットワークのセグメンテーションと侵入防止機能が不可欠ですが、そのためには次のような次世代ファイアウォールソリューションが必要です。

- ゼロデイ攻撃を含む高度な脅威をブロックする多層構造のセキュリティを提供
- 侵入防止機能とマルウェアのサンドボックス化機能を搭載
- 強力なネットワークセグメンテーション機能により、ネットワーク内の横断的移動を防止

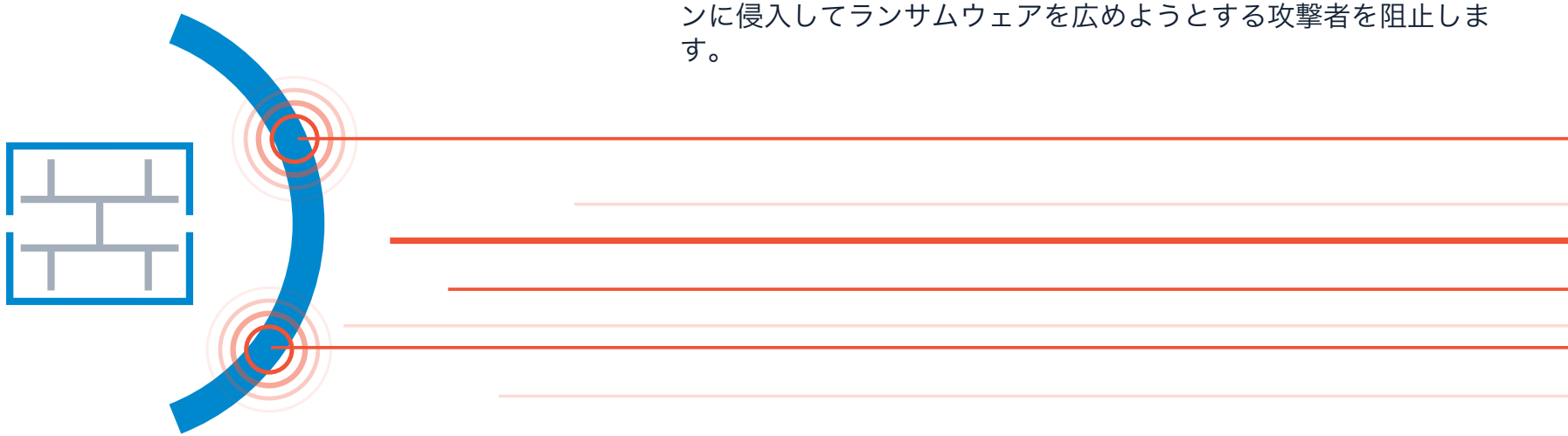
アプリケーションアクセスの保護

あらゆるデバイス、あらゆる場所からアプリケーションやワークロードへの安全なアクセスを提供するZTNA（Zero Trust Network Access）ソリューションを用いて、アプリケーションアクセスを保護する必要があります。

次のようなソリューションを探してください。

- 適切なデバイスを持つ適切な人だけが会社のリソースにアクセスできるよう継続的に検証
- ロールベースおよび属性ベースのアクセスコントロールを実施し、最小限の権限でのアクセスを実現

ZTNAは、不正なアクセスをブロックすることでアプリケーションに侵入してランサムウェアを広めようとする攻撃者を阻止します。



Webアプリケーションの保護

アプリケーションセキュリティを導入するための最良の方法の一つは、Webアプリケーションファイアウォール（WAF）を使用して、ソフトウェア、ユーザ、およびそれらのデータをどこでも保護することです。これにより、ボット攻撃やサービス拒否攻撃を阻止し、何が起こっているのかをより詳しく知ることができます。ソリューションには次のような特徴があります。

導入が簡単で環境に合わせたカスタマイズが可能

WAFは、自社環境に合わせた設定ができなければ、完全な保護ができません。

スケーラブル

ビジネスの成長、デジタルトランスフォーメーション、その他の要因により、アプリケーションやWebサイトへの要求が高まります。WAFは、必要に応じてビジネスと共に成長できるものでなければなりません。

高度な脅威に対する包括的な保護

OWASPトップ10保護と、アプリケーション層のDDoS保護は、優れたWAFに期待される重要な要素です。完全な保護には、ゼロデイ攻撃、クレデンシャルスタッフィング、データ漏洩、悪意のあるボットなどを防御するソリューションが必要です。

容易なアップデート

WAFは、デバイスのセキュリティと機能を向上させるために、定期的にファームウェアをアップデートする必要があります。管理者が介入しなくても自動的にアップデートされるホスト型ソリューションが理想的です。

継続的な脅威インテリジェンス

新しい攻撃は日々開発され、数時間のうちに世界中に拡散されていきます。WAFは、これらの攻撃に関する最新情報をリアルタイムで受け取り、機械学習を採用して亜種に適応する必要があります。

優れたWebアプリケーションファイアウォールは、一般的なWebアプリケーションの脆弱性やゼロデイの脅威をブロックすることで、ランサムウェアのシステムへの侵入を防ぎます。

Barracuda

ステップ3：データのバックアップ

本格的なランサムウェア対策には、まずバックアップとディザスタリカバリについて考える必要があります。問題は、犯罪者もこれを知っているということです。

バックアップソリューションは、攻撃者がネットワークを探索している「潜伏期間」に注目されます。バックアップの管理コンソールは、バックアップのスケジュール、設定、保持ポリシー、そして削除を開始する機能にアクセスできるため、特に重要です。

Barracuda

攻撃者は、バックアップストレージ自体も標的とし、プライマリバックアップサーバや、ディザスタリカバリ用のセカンダリバックアップコピーを削除しようとします。Active Directoryのパスワードを取得し、誰も自分のアカウントにログインできないようにすると、そこが引き金となります。彼らはコントロールできるのです。

また、よくありがちな誤解として、データがクラウド上にあるからランサムウェアの被害を受けない、というものがあります。しかし、それは真実ではありません。

例えば、自宅で学校のタブレットやノートパソコンを使ってWebを閲覧している子どもは、簡単に騙されて悪意のあるリンクをクリックしてしまうことがあります。そのデバイスが学校のOffice 365アカウントの一部であるOneDriveに接続・同期されている場合、ランサムウェアのファイルが自動的にOneDriveにアップロードされ、Microsoftのクラウドに保管されている学校のファイルやデータが暗号化されてしまいます。

また、SharePointやExchangeなどのデータソースが攻撃される例も見られます。ネットワークドライブが「エクスプローラで開く」機能を使ってOffice 365のドキュメントライブラリにマッピングされている場合、ランサムウェアは接続されたドライブ上のファイルをスキャンして感染させることもできます。

ディザスタリカバリは、インフラ上重要かつ戦略の一部であると考えてください。定期的で現実的なテストを行います。これは単に稼働を確認するだけでなく実際のリストアの実行を、意味します。

クラウドやSaaSのデータもランサムウェアで暗号化される可能性があります。Microsoftは、サービスの可用性を保証していますが、サードパーティのバックアップソリューションを使用したデータのバックアップを推奨しています。お客様のデータはMicrosoft Office 365に保存されているかもしれませんが、Office 365は、ランサムウェアの攻撃後に必要になるかもしれないインスタンス全体の復旧を目的としていません。

Barracuda

そのため、バックアップデータを適切に保護し、分離する必要があります。システムをミラーリングする頻度と、そのイメージからシステムを再構築する速度を考えてみてください。

妥当な時間内に、最新の情報を用いてバックアップバージョンからのシステムの復元が可能であることを確認する必要があります。データが適切な頻度で正確に複製されているかどうかを確認するためには、ログをチェックするだけでは不十分です。

システムが機能することを証明するためには、実際に訓練を行う必要があります。すべてを停止させるのではなく、1つの部門、あるいは1つのアプリケーションだけを選択することもできるでしょう。しかし、自信を持ってタイムリーにシステムを復旧させることが重要です。

これは、あなたの最終防御策です。たとえ他のすべてが失敗したとしても、最新で安全なバックアップがあれば、犯罪者はあなたを止めることはできません。

ディザスタリカバリは、インフラ上重要かつ戦略の一部であると考えてください。定期的かつ現実的にテストしてください。それは、単に動作を確認するだけでなく、実際のリストアの実行を意味します。

バックアップソリューションに必要なもの

ランサムウェアに関連するリスクを軽減するためには、以下を提供する包括的なバックアップソリューションが必要です。

アクセス不能なストレージ

攻撃者がバックアップにアクセスしたとしても、そのデータを修正したり削除したりすることはできません。

エアギャップクラウド

分離されたネットワーク上にある安全なクラウドにバックアップのコピーを保持します。

多要素認証(MFA)

バックアップへのアクセスに使用されるアカウントと認証情報を保護します。

冗長化

オンプレミスとクラウドのバックアップを別の場所に複製します。

ロールベースのアクセス制御

バックアップシステムにアクセスするすべてのユーザに対して、最小特権の原則に従います。

Barracuda

結論

あなたの会社には身代金を支払うためのサイバー保険などがあるかもしれませんが、身代金を支払えばデータが復元されると考えるのは非常に危険です。身代金を支払っても、ハッカーがデータの暗号化を解除する保証はなく、仮に解除されたとしても、最新の調査では、身代金を支払った組織の80%が再び攻撃を受けたという結果が出ています。

上記のような対策をすべて行っていたとしても、攻撃を受ける可能性はあります。最善の防御策を講じていても、最悪の事態に備えておくべきです。犯罪者は、システムに侵入するために何百万ドルもの投資をしています。いつか侵入されるかもしれないという可能性を想定して準備しましょう。

その日に何が起こるかを考えておく必要があります。身代金を払わない計画が必要です。

- ランサムウェア対応チームには誰がいますか？
- 週末や休日に何かが起こった場合、誰が連絡を取りますか？責任者は誰ですか？
- いつ顧客やサプライヤに報告しますか？
- 誰が法的なアドバイスをしますか？
- 規制当局や警察に報告する必要がありますか？
- 最初から広報担当者が必要ですか？

これはまるで消防訓練です。訓練する時間は、オフィスが燃えているときではありません。ただし、現在の攻撃や今後高い確率で起こり得る攻撃は、時間の経過とともに変化するため、戦略や防御戦術は定期的に更新する必要があります。

ランサムウェアのチェックリストをダウンロードして、計画のスタートにご利用ください。

Barracuda

攻撃を受けたときの準備

攻撃が確認された瞬間に何が起こるのか、そしてその攻撃が侵害となった場合に何が起こるのかを考える必要があります。ネットワークトラフィックを停止することで、攻撃を抑制したり、インフラの一部分に限定したりすることは可能でしょうか？システムを一時的にオフラインにする必要があるでしょうか？その場合、誰がその責任を負うのでしょうか？

ここではスピードが不可欠です。スピードを重視してください。CTOからの折り返し電話を待っている場合ではありません。誰もが今すぐに何をすべきかを知っている必要があります。

これが迅速に行われれば、暗号化を未然に防ぐことができるかもしれません。また、システム全体を迅速にチェックして、何が起こっているのかを明確に把握する計画も必要です。

最近の攻撃者は、複数の攻撃タイプを同時に使用する傾向があります。DoS攻撃への対応に追われている間に、ランサムウェア攻撃が別の場所に向けられているかもしれません。何がどこで起きたのかを理解した上で、マルウェアを駆除し、システムをオンラインに戻すために何をすべきか考えましょう。

攻撃を隔離するか、あるいはバックアップからシステムとデータを復元し、破損したデータや欠落したデータがないかどうかを確認したら、フォレンジックを開始します。

実際の攻撃に対して対応がどのように機能したかを評価します。何がうまくいったのか、何が幸運だったからこそうまくいったのか、何が足りなかったのかを分析し、次回の対応をどのように改善すべきかを検討しましょう。

適切なシステムが導入されていれば、フォレンジックデータが豊富に得られます。警察が調査を開始するのに十分なデータがあるでしょう。どのようなデータであっても、時間をかけて対応チームに報告し、学んだ教訓について考える必要があります。

繰り返しになりますが、これはテクノロジだけではなく、人やプロセスにも関わることです。スタッフのトレーニングを見直す必要があるでしょうか？対応チームはうまく機能していたでしょうか、それとも強化する必要があるでしょうか？

情報収集

今日の防衛戦略は、単なるリアクティブなものではなく、アクティブなものである必要があります。セキュリティシステムには、可能な限りの透明性が求められます。何が、いつ、どのくらいの頻度で起きているのかを監視する必要があります。ランサムウェアの攻撃者は、特定のバーティカル市場や地域をターゲットにしていることが多いため、同業者にも注意を払う必要があります。また、弊社ブログなどのリソースで、最新の脅威、トレンド、および業界のニュースを把握する必要があります。

セキュリティ戦略を成功させるためには、データが非常に重要です。組織のスタンスやプロファイルは、時間とともに変化する可能性があります。必要に応じて変更できるように、準備と情報を整えておきましょう。Security-as-a-Serviceは、特に今日のサイバーセキュリティの状況がかつてないほど急速に変化している中で、変化に対応するための煩雑な作業を軽減するのに役立ちます。

積極的な活動を行っている企業やリスクの高い企業では、攻撃の可能性を早期に察知するために、専任のスタッフが諜報活動を行うこともあります。

しかし、多くの企業にとっては、必要以上のことであり、そこまで出来ません。適切なパートナーを選び、基本をしっかりと身につけましょう。実際の攻撃者は、映画やテレビで見るのとは異なり、最も精巧なセキュリティシステムを破壊することを好むような邪悪な天才ではありません。ほとんどの場合、彼らは注意を怠ったり、適切なセキュリティに投資しなかったりした人から簡単にお金を得ようとしています。

認証情報の保護、Webアプリケーションとアクセスの保護、データのバックアップという3つのステップを踏んでも、ランサムウェアからの攻撃を受けないことが保証されるわけではありません。しかし、データを取り戻すために身代金を支払う必要がないことは保証されます。

バラクーダについて

バラクーダは世界をより安全な場所にするために尽力しています。

バラクーダは、すべてのお客様が購入、導入、使用しやすい、クラウド対応かつエンタープライズレベルのセキュリティソリューションを使用できることが当然であると考えています。また、お客様のビジネスとともに成長および変化する革新的なソリューションによってメール、ネットワーク、データ、アプリケーションなどを保護しています。

世界中の20万を超えるお客様がバラクーダを信頼しています。お客様がリスクにさらされていることを知らない場合でも、バラクーダはお客様を保護できます。このため、お客様はビジネスを次の段階に移行することに注力できます。

詳細については、barracuda.co.jpをご参照ください。

Barracuda
Your journey, secured.