proofpoint

サプライチェーン攻撃

ポイント

説明

サプライチェーン攻撃には、メール詐欺とサードパーティ ソフトウェアの２つのカテゴリがあります。これらの攻撃で、サイバー犯罪者はベンダーまたはサービスプロバイダーのシステムに侵入し、その顧客やパートナーへの攻撃を試みます。最初の段階のサプライヤーへの不正アクセスでは、多くの場合フィッシングやマルウェアが使用されます。サプライヤーへの侵入に成功すると、攻撃者は正規のメールアカウントを乗っ取り、サプライヤーの顧客に対してフィッシング、請求書詐欺などの攻撃を実行します。さらに、顧客のシステムへの侵入に成功すると、機密情報を盗み出したり、ランサムウェアをインストールしたりします。また、アクセス権を悪用し、さらなるフィッシングやメール詐欺攻撃を仕掛けてきます。

使用される手口

サプライチェーンに対する攻撃では、認証情報を取得する手法としてフィッシング（アカウント乗っ取り）、マルウェア（Stuxnet、NotPetya、Sunburst、Kwampirs）、ビジネスメール詐欺（BEC）などのなりすましが使用されます。

種類

- **ビジネスメール詐欺（BEC、メール詐欺）：**攻撃者は、メールの受信者が信頼する人物（ビジネスパートナーやサプライヤー、ベンダーなど）になりすまし、送金、偽の請求書や改ざんした請求書に対する支払い、給与の支払い、銀行口座の変更などを依頼します。メール詐欺では、サプライヤーの実際のメールアカウントを乗っ取り、サプライヤーを装って実際のメールスレッドに便乗する攻撃者もいます。
- **ソフトウェア サプライチェーン攻撃：**ソフトウェアまたはマネージド サービス プロバイダーのシステムに対するアクセス権を取得した攻撃者が、顧客やパートナーに配布されるビルドを改ざんする可能性もあります。前述の攻撃と比べると、この手段で攻撃が実行されることはあまりありません。しかし、攻撃に成功した場合、１回の侵害で非常に多くの被害者が発生する可能性があります。

リスク要因

- 専門サービスやコンサルティング サービスを提供するベンダーを利用している
- 適切なサイバーセキュリティ対策が実施されていない
- 注意深くないスタッフや、セキュリティ意識の低いスタッフにアクセスを許可している
- サプライチェーンの複雑化 — クラウドプラットフォームやSaaSサービスを利用する企業が増えている

ニュースで報じられたサプライチェーン攻撃

2013年、Targetでデータ侵害が発生、4,100万人分の顧客情報が流出し、和解金1,850万ドルを支払う

大手小売のTargetのベンダーからアカウント資格情報が盗まれ、Targetのシステムから4,100万人以上の顧客の決済情報が流出しました。

COVID-19ワクチン サプライチェーンが攻撃される

世界のCOVID-19ワクチン サプライチェーンに侵入するため、世界の44の企業の経営幹部にフィッシング攻撃が実行されました。

コミュニティ住宅の非営利団体がビジネスメール詐欺（BEC）で120万ドルの被害を受ける

ベンダーのドメインになりすました攻撃者が、英国のロンドン付近にある共同住宅協会から100万ポンドを盗み出しました。

サプライチェーン攻撃の手口

1. 侵入

攻撃者は、様々な方法を駆使して侵入を試みます。

- 自動化ツールを使用して総当たり攻撃を実行し、ユーザー名とパスワードを盗み出します。

- 受信者が信頼している相手を装い、フィッシングなどの詐欺メールや、マルウェア（キーロガー、スティーラなど）を含む添付ファイルやリンクを送信します。

- 信頼されたサプライヤーのアカウントを乗っ取ります。

2. 偵察

- 有効なログイン認証情報の盗み出しに成功すると、攻撃者はサプライチェーン ネットワークとそのレピュテーションの調査を開始します。攻撃者は、サプライヤーと顧客間のやり取りを傍受し、標的の絞り込みを行います。

3. 攻撃

- 偵察が完了すると、侵入に成功したサプライヤーのシステムを利用して、認証情報を求めるフィッシングメールを送信したり、偽の請求書やマルウェアを顧客に送信します。

研究から得られた知見

プルーフポイントは2021年2月、米国、英国、オーストラリアの様々な業界の組織のデータを分析しました（調査対象は3,000社、期間は1週間）。この期間、ほとんどの企業がサプライチェーン攻撃を受けていました。

98% サプライヤーになりすました攻撃者または侵害されたサプライヤーから攻撃を受けた組織の割合

このサンプルでは、国や業界による偏りありませんでした。

これらの攻撃の約4分の3でフィッシングまたはなりすましが行われていました。

30%未満 サプライヤーのドメインからマルウェアに感染したメールを受信した組織の割合

CRIME-AS-A-SERVICEがサプライチェーン攻撃を増長

ダークウェブは、エクスプロイトキットやカスタムマルウェアを扱う悪名高いマーケットプレイスです。ボットネットのレンタルやランサムウェア ソフトウェアなどのサービスも販売されています。SaaSプロバイダーがサービスを提供しているのと同じように、サイバー犯罪者がサプライチェーン攻撃、ランサムウェア攻撃などのサイバー犯罪で使用するツールやプラットフォームを提供しています。高度なスキルがなくても、このようなサービスを利用することで攻撃を簡単に実行することができます。

組織を守るには

サプライチェーン詐欺やソフトウェア サプライチェーン攻撃を防ぐために、組織が実装しなければならないセキュリティ コントロールがいくつかあります。

サプライチェーン詐欺

サプライヤーになりすました請求詐欺に対しては、包括的で多層的な対策が必要です。多くの場合、攻撃者はサプライヤーになりすますだけでなく、乗っ取ったサプライヤーのアカウントも使用します。

ビジネスメール詐欺（BEC）は、信頼できる相手から届いたように見えるメールから始まります。攻撃者がその相手になりすましている場合もあれば、本人のアカウントを乗っ取り、悪用する場合もあります。BECには不正なペイロードがないため、レピュテーションやサンドボックスに頼る従来のゲートウェイでは、こうした攻撃に対応することはできません。

最も一般的で、被害の大きいサプライチェーン攻撃を防ぐには、次のことを行う必要があります。

サプライヤーを装うメール詐欺のリスクを可視化する
リスクを正確に把握し、回避するために、次のことを確認してください。

- どのようなBECリスクにさらされているか
- 最も脆弱なユーザーは誰か
- 自社にとってリスクのあるサプライヤーはどこか
- リスクを低減するために何をすべきか

現在なりすましの被害を最も多く受けているユーザーや、このような脅威の影響を最も受けやすいユーザーを特定する必要があります。

同時に、BEC脅威の詳細を可視化し、サプライヤーからの偽の請求、偽の給与振込先変更など、BECでよく使われるテーマを特定することで、BECのリスクをより正確に把握できます。

なりすましの脅威を早期に検知し、侵入を防ぐ
メールによるサプライヤー攻撃を阻止するには、表示名偽装、類似ドメイン、巧妙なサプライヤー詐欺など、メール詐欺のすべての手口を把握している必要があります。サプライヤー請求詐欺で使われる次のような手口を動的に分析できるソリューションを使用してください。

- Reply-toピボット（返信先の変更）
- 不正なIPの使用
- なりすましで利用されたサプライヤー ドメイン
- これらの詐欺攻撃でよく使われる語句

（大半のメールセキュリティ製品は、静的なルール照合のみを使用しています。あるいは、コンテキストデータが制限されているため、手動での調整が必要になります。）

サプライヤーになりすました請求詐欺に対しては、包括的で多層的な対策が必要です。多くの場合、攻撃者はサプライヤーになりすますだけでなく、乗っ取ったサプライヤーのアカウントも悪用します。

BECサプライチェーン攻撃に対するユーザーの耐性を強化
BECは人をターゲットにしています。人は、知らないうちに攻撃に加担してしまうことがあります。こうした攻撃ではソーシャル エンジニアリングやなりすましの手口が使われるため、ユーザーが防御の最後の砦となることも少なくありません。このため、BECのリスクを低減するには、技術だけでなく、ユーザーのトレーニングも必要になります。

ユーザーが不審な詐欺メールを識別し、報告できるようにトレーニングを行います。このトレーニングで、人の行動から始まる脅威を阻止するために必要な知識とスキルをユーザーが習得できるようにします。

メールの警告タグはメールのリスクを識別するのに役立ちます。たとえば、ユーザーが外部の送信者や新規登録のドメインからのメッセージを受信したときに、的確な情報に基づいて、怪しいメールかどうか判断することができます。

メール詐欺攻撃での自社ブランドの使用の防止
サプライヤーによるリスクは他人事ではありません。自社の顧客も同様の不安を感じているかもしれません。

攻撃者は会社名やブランドを悪用して、その企業の顧客やビジネスパートナーに詐欺を行います。金銭的な被害が直接発生しなくても、会社の評判が傷つき、顧客からの信頼を失う可能性があります。結果的に被害を受けることは間違いありません。

ユーザーが直接送信したか、指定したサードパーティ経由かどうかにかかわらず、詐欺メールの送信を阻止するにはDMARCメール認証を使用します。

ソフトウェア サプライチェーン攻撃

サードパーティのマネージドサービスを利用する組織が増えていますが、それに伴い、前述のサプライチェーン攻撃を超える新たなサプライチェーンのリスクが発生しています。

ソフトウェアやクラウドサービスを提供するプロバイダーに侵入した攻撃者がソースコードを改ざんし、ビルドやアップデートプロセスにマルウェアを潜ませる可能性があります。このような攻撃に成功すれば、プログラムやサービスとともに不正なペイロードを顧客やパートナーに配布することができます。

多くの場合、使用中のサードパーティ プログラムをユーザー側で検証することはできません。ソフトウェアベンダーやサプライヤーが堅牢な保護対策を実施していなければ、ユーザーはこのような被害を受けることになります。感染したソフトウェアが組織に配布されれば、データの窃盗からランサムウェア感染まで、あらゆる攻撃が可能になります。

この種の攻撃を阻止するのは容易ではありません。サイバー攻撃でよく狙われるのは、パッチが適用されていないソフトウェアの脆弱性です。ソフトウェアを常に最新のバージョンにしておくのはベストプラクティスですが、この新たなリスクでは、アップデートが感染経路になっています。

詳細

ニュースの見出しを独占したサプライチェーン攻撃を見ると、外部のサービス、ベンダー、委託業者が組織のセキュリティに対して重大なリスクになることは明らかです。このリスクを回避するには、新しい攻撃ツール、ターゲット、手口を検出するPeople-Centricなセキュリティ ソリューションが役立ちます。

サプライチェーン攻撃を効果的に阻止する方法については、**www.proofpoint.com/jp**をご覧ください。