SOPHOS
Cybersecurity evolved.

サプライチェーン攻撃のリスクを最小限に抑える：ベストプラクティスのガイドライン

2020年 12月、企業の IT 監視を専門とする SolarWinds 社に対するサイバー攻撃のニュースによって、サプライチェーン経由のサイバーセキュリティ攻撃が注目の的になりましたが、これは決して新しい現象ではありません。実際、2020年に 26か国 5,000人の IT 管理者を対象にソフォスが実施した調査によると、困ったことに、ランサムウェア攻撃の被害者のうち、ほぼ 10人に 1人 (9%) が、信頼できるサードパーティサプライヤーを介して攻撃を受けたとしています [1]。

しかし、いったいサプライチェーン攻撃とは何であり、どのように機能するのでしょうか？さらに重要なことは、サプライチェーン攻撃の影響から組織を保護するために何ができるかということです。

このホワイトペーパーでは、これらの質問および他の質問に回答しています。

1 ランサムウェアの現状 2020年版 - ソフォス、2020年

サプライチェーン攻撃とは？

組織は、何らかの形でサードパーティサプライヤーに依存して、IT インフラなど、特定のビジネス機能のすべてまたは一部を管理していることがよくあります。サードパーティサプライヤーが社内ネットワークに接続できるようにすることはビジネス上メリットがありますが (例：社内リソースを解放できるなど)、これに伴い、本質的なセキュリティリスクをもたらします。つまり、サプライチェーン攻撃による脆弱性です。

サプライチェーン攻撃で、攻撃者は直接侵入するのではなく、信頼できるサードパーティサプライヤーに既にある、システムへのアクセス権を悪用して、社内環境に足掛かりを得ます。いったん侵入すれば、あらゆる種類の悪意のあるアクティビティを実行できます。

サプライヤー 1社のみが社内ネットワークに接続している場合であっても、サプライチェーン攻撃のリスクが発生します。一方、中小規模の組織は平均で、社内システムに接続可能なサプライヤーが少なくとも 3社あると報告しています [2]。接続しているサプライヤーを保護することは、IT チームにとって大きな課題となり、作業負荷も増加します。さらにこれに加えて、サプライチェーン攻撃は、サプライチェーンのどこからでも発生する可能性があるため、検出はおろか防御が非常に困難であることはよく知られています。

サードパーティサプライヤーの種類

プロフェッショナルサービスと IT サービスプロバイダは共に、組織のネットワークに接続できる、最も一般的なサードパーティサプライヤーです。

プロフェッショナルサービス

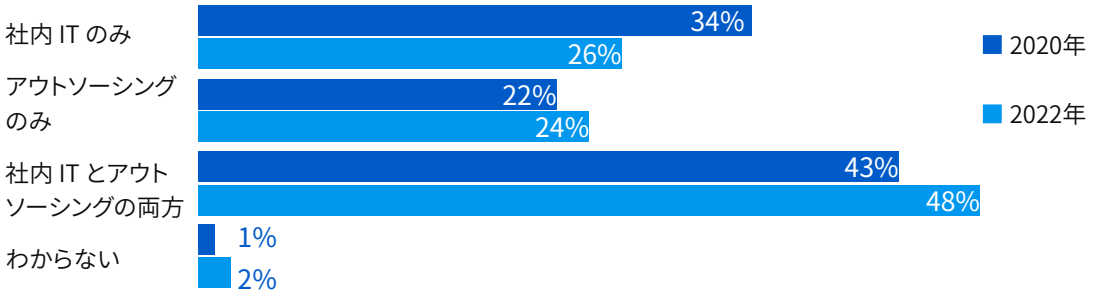
プロフェッショナルサービスは、必要とされる専門的なスキルや知識がない組織によって、個別にビジネス機能 (またはその一部) を管理するために使用されることがよくあります。たとえば、(ソフトウェアを使用して) 機密性の高い財務データにアクセスして、顧客に分析と洞察を提供する必要のある会計事務所などがあります。このような組織に対するサイバー攻撃が成功すると、顧客のポートフォリオに破壊的な打撃を与える可能性があることは想像できます。

IT サービスプロバイダ

IT サービスプロバイダは、企業の IT インフラや IT セキュリティの運用を委託されている外部組織です。しばしば、マネージド サービス プロバイダ (MSP) またはマネージド セキュリティ サービス プロバイダ (MSSP) と呼ばれ、頻繁にサプライチェーン攻撃の対象になっています。

これは、多種多様な組織へのアクセスを可能にすることから、攻撃の対象として特に魅力的です。IT セキュリティをアウトソーシングする組織の割合は、2022年には72% に上昇すると予想されるなか [3]、委託先サービスプロバイダのセキュリティ状態は、各組織にとって非常に重要です。

IT セキュリティの提供方法：現在および 2022年



2、3 サイバーセキュリティ：企業を守る人材とスキルの現状 – ソフォス、2020年

サプライチェーン攻撃の種類

サプライチェーン攻撃の攻撃方法はそれぞれ異なりますが、多くの場合、攻撃の原則と最終目的は同じです。信頼されているサードパーティサプライヤーに侵入し、信頼されたアクセスを悪用してマルウェアを挿入したり、知的財産を盗んだり、内部コミュニケーションをひそかに監視したりします。

フィッシング攻撃

サプライチェーン攻撃者が利用する最も一般的な攻撃ベクトルの 1つがフィッシングメールです。攻撃者は、信頼されているサードパーティをフィッシングメール攻撃の標的にし、ネットワークを侵害してアクセスします。その後、ネットワークを介してサードパーティの顧客のシステムに侵入します。

侵害されたソフトウェアアップデート

より高度なサプライチェーン攻撃では、ハッカーはソフトウェア会社またはディストリビュータのインフラに侵入し、悪意のあるコードをソフトウェアのアップデートパッケージに挿入します。その後、サードパーティは、これらのアップデートを顧客に配布することで、知らないうちに感染を広げます。特に組織の顧客ポートフォリオが大規模な場合など、壊滅的な結果を招くことは想像できます。2020年 12月に発生した SolarWinds 攻撃は、まさにこの種の攻撃の例です。

サプライチェーン攻撃の事例：SolarWinds

2020年後半、企業の IT 管理を専門とする SolarWinds 社のサプライチェーンが侵害されたことが発見されました。この発見は世界中でニュースに取り上げられ、サプライチェーンのセキュリティの脆弱性が注目の的になりました。同社の 18,000社を超える顧客に影響を与えたと考えられています。

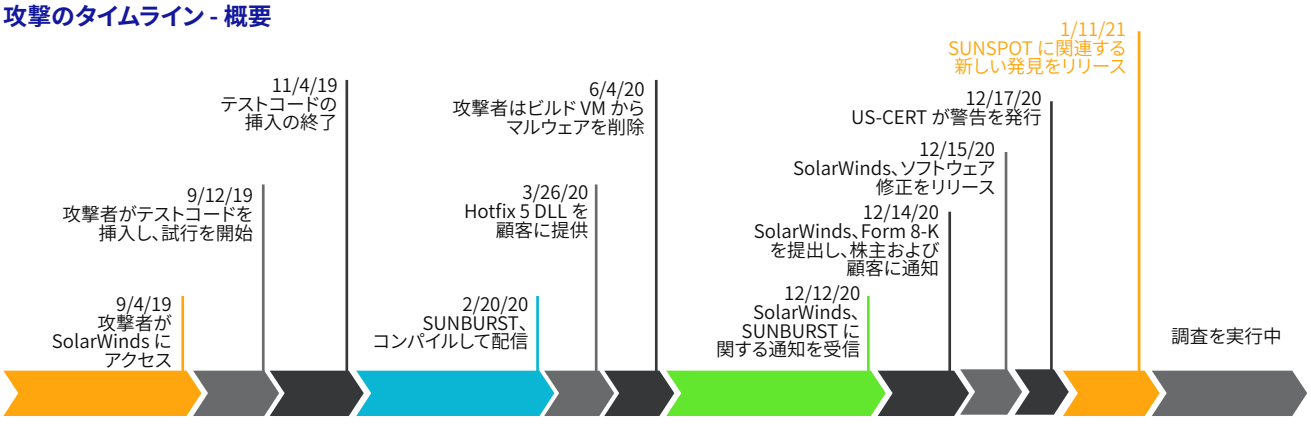
2021年 4月の現時点で、SolarWinds 攻撃に対する調査は実行中であり、変更される可能性があることに注意してください。

攻撃者はどのようにして成功したのか？

簡単に言うと、ハッカーは、SolarWinds のインフラ監視・管理プラットフォーム Orion に悪意のあるコードを挿入することに成功しました。この悪意のあるコードは、その後、標準的なソフトウェアアップデートを介して、知らないうちにユーザーに送信されました。およそ 18,000社の顧客 (多くの Fortune 500企業と米国政府機関を含む) がこのアップデートをインストールし、結果として脆弱になったと報告されています。

以下のタイムラインからわかるように、困ったことに SolarWinds は、2019年 9月までさかのぼって不正行為の存在を疑っていました。これは、攻撃が計画的であり、かつ侵入時にできるだけ気付かれないように、攻撃者が細心の注意を払ったことの両方を示唆しています。Sunburst マルウェアの亜種が防御を回避する方法に関する、ソフォスの詳細な解析は、こちらを参照してください。

攻撃のタイムライン - 概要



すべてのイベント、日付、時刻はおおよそであり、調査の完了に伴い変更される可能性があります。

SolarWinds - https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst/

攻撃はどんな影響を与えたか？

「Sunburst」と呼ばれるこの攻撃の成功により、攻撃者は、企業や政府の情報システムへの広範なアクセスを獲得しました。これによって、被害規模が未知のデータ窃盗が発生し、まだ未発見ではあるが、攻撃者が足がかりを利用して企業ネットワークに他のバックドアを挿入したという懸念が持たれています。

さらに重要なことは、攻撃がグローバルに展開されたなか、サプライチェーン攻撃に対して、多くの組織の防御がいかに不十分であるかということが明らかになったということです。

毒パッケージ

あまり一般的ではありませんが、サプライチェーン攻撃の 1つで今後より頻繁に発生すると予想されるのは、ソフォスで「毒パッケージ」と呼んでいるものです。クラウド、Docker、アジャイル開発手法の使用が増えるに従い、開発ライフサイクルを短縮するために、既製のコンポーネントを使用することも増えています。攻撃者は、最終製品に組み込まれることを狙って、よく使用されるコンテナ、ライブラリ、およびその他のリソースにマルウェアを仕掛けるようになりました。

サプライチェーン攻撃に対する防御のガイドライン

サプライチェーン攻撃の複雑さと特徴を考えると、テクノロジーだけでそれを防止することはできません。代わりに、ここで説明するベストプラクティスのガイドラインは、サプライチェーン攻撃に関連するリスクを最小限に抑えることを目的としています。

1. 事後対応型から事前対応型サイバーセキュリティへの移行

SolarWinds は、世界中の多くの組織にとって警鐘を鳴らす事件となりました。攻撃が明らかになった時点では、既に手遅れであることがよくあります。犯罪者がペイロードをドロップした時点では、既に重要なデータが盗まれている可能性があり、多くの場合、既に何日もネットワークアクセスを実行しています。したがって、考え方を改める必要があります。常に侵害されていることを想定し、手遅れになる前に脅威を探すようにしてください。このアプローチをサポートできるテクノロジーとサービスがあります。それについては、後で詳しく説明します。

2. 攻撃の兆候の監視

Sophos Managed Threat Response (MTR) チームが実施した調査で、攻撃の兆候として際立っているのは次の2点です。1つは、リモートアクセスおよび管理目的で、営業時間外に行われる認証情報の使用です。もう 1つは、監視を行い、ネットワークからデータを盗むためのシステム管理ツールの悪用です。

正規のアカウントやユーザー自身のツールを使用して、アクセスを獲得し、システムに常駐することは、環境寄生型 (LOL) と呼ばれることがよくあります。これらの動作を検出するには、警戒とスキルが必要ですが、トレーニングを受けたセキュリティ運用アナリストにとっては明らかで、被害の大半が発生する前に攻撃を警告することができます。このような兆候を社内で監視するために必要なテクノロジーとトレーニングに投資するか、または MDR (Managed Threat Detection and Response) サービスプロバイダに監視を依頼する必要があります。

3. サプライチェーンの監査

当たり前のように聞こえるかもしれませんが、接続しているすべての組織のリストを、多少時間をかけて作成することは重要です。その数は、恐らく予想を超えると思われます。このリストを作成することで、脆弱なリンク (例: サイバー犯罪の影響を受けやすい組織など) をすばやく特定し、関連するリスクを軽減するための措置をさらに講じることができます。次のようなサードパーティサプライヤーに接続されていることが予想されます。

- **IT サービスプロバイダ**
  - MSP / MSSP
  - クラウドプロバイダ
- **プロフェッショナルサービス**
  - 金融
  - 法律
  - セキュリティ
  - 清掃
- **サプライヤー**
  - 材料
  - サービス
  - 労働
  - 物流

接続先のサプライヤーを把握したら、ネットワークアクセスの種類と、該当する認証情報を使用してアクセスできる情報を評価できます。最小限以上のアクセス権がある場合は、そのアクセスをロックダウンし、アクセスを必要な情報のみに制限する必要があります。最も不要なアクセス権を持っているプロバイダからはじめて、順に他のプロバイダに対処します。

4. サプライヤーおよびビジネスパートナーのセキュリティ状態の評価

評価には多くのアプローチがありますが、大規模なサービスプロバイダ、クラウド事業者、支払い処理業者を対象にした、よく使用されるアプローチの 1つは、どのような種類の認定と監査の対象になっているかを判断することです。

たとえば、支払い処理業者は PCI DSS の対象になります。PCI DSS レベル 1 または 2 の対象である場合は、QSA / ISA によって発行された遵守報告書 (RoC) を要求するようにしてください。RoC は四半期ごとに確認し、期待に沿っていることを確認する必要があります。

監査の確認によく使用されるもう 1つの認定は、クラウド サービス プロバイダ対象の SOC 2/2+/3 です。SOC 監査は、5つの Trust サービス原則 (プライバシー、セキュリティ、可用性、処理の整合性、機密性) を基盤とした、セキュリティ制御と対策を評価します。

自社のセキュリティと同様に、多数の監査を行うことによって何かが保証されるわけではありませんが、それは、サプライヤーがセキュリティと遵守を真剣に受け止めていることを示します。その他、検討または要求できるのは、侵入テストレポート、GDPR への準拠、以前の欠陥やデータ侵害の頻度などです。

5. 自社の IT セキュリティ運用の予防策を常に確認

サプライヤーのセキュリティ状態はサプライチェーン攻撃から保護するうえで重要ですが、自社のサイバーセキュリティ予防策を怠らないようにしてください。多くの組織は、どのように取り組めばよいのかわからない、または、信頼できるパートナー経由で攻撃の対象になるほど自社が重要ではないと考えているため、このことを無視します。サイバーセキュリティ対策の実施は、多少の不便さと、壊滅的なデータ侵害の分かれ目を意味することがあります。

多要素認証 (MFA) を有効にする

組織がサプライチェーン攻撃の被害を受ける最も一般的な方法は、窃取した承認済みアクセスの使用です。サービスプロバイダに、社員と同じ権限のある認証情報が与えられていることがあまりに多くあります。

つまり、MFA を使用する必要がないため、攻撃者は、フィッシング攻撃によって窃取した認証情報と、従業員による認証情報の不正な再利用の両方を悪用することができます。ほとんどの組織は SSO (シングルサインオン) を導入しているため、このような認証情報を悪用して、現在のタスクに不要なあらゆる種類のシステムにアクセスすることが可能となり、悪意のある内部関係者や外部関係者からのリスクを増加させます。

サプライヤーのアクセスとアプリケーションの権限を確認する

もう 1つの一般的な間違いは、ソリューションを管理できるように、VPN、RDP やその他のリモートアクセステクノロジーを、サードパーティに無制限に提供することです。無制限とは、必要なリモートアクセスツールをセグメント化して慎重にセキュリティを強化するのではなく、ネットワーク全体へのアクセスを提供することを意味します。

外部に接続するツールはすべて、多要素認証の使用を要求し、単一のホストまたはシステムに限定する必要があります。追加のアクセスが必要な場合は、リスクを削減し、監視とログの機会を増やすために、「ジャンプホスト」を使用することを推奨します。

ベンダーのソフトウェア証明書によって署名されたアプリケーションすべてをデフォルトで許可することも、組織をサプライチェーン攻撃にさらします。証明書が盗まれ、マルウェアに署名するために悪用されることが繰り返し発生しています。セキュリティツールは可能な限りすべてを検証する必要があります。

サプライヤーのセキュリティ情報を積極的に監視する

脆弱性が発見された場合にパッチや対策を迅速に導入できるように、すべてのサプライヤーのセキュリティ情報を監視し、サプライヤーに関するニュースを注視するようにします。サプライヤーが緊急事態でインシデントに対応する際、通知対象の組織のリストで、自社の優先度があまり高くない可能性もあります。監視することで、アクセスをロックダウンし、サプライヤーの状況からの影響があるかどうかの調査を開始できます。

サイバーセキュリティ保険ポリシーを確認する (加入している場合)

最後に、サイバー保険に加入している場合は、サードパーティによる損失が補償されるかどうか、および必要な場合、どのようにして保険を請求するかなどを確認します。ベンダーと協力して、自社で加入している保険の補償範囲と、ベンダーが加入している保険の補償範囲を合わせることで、該当する状況がすべてカバーされることを確認します。

活用できるテクノロジーとサービス

前述したように、サプライチェーン攻撃に対する防御は本質的に複雑です。したがって、それらに関連するリスクに対処し、被害を最小限に留めることが狙いとなります。幸いにも、このリスクの軽減を支援する、理想的なテクノロジーやサービスがあります。

脅威ハンティング

サプライチェーン攻撃から保護するために、サイバーセキュリティに対してプロアクティブなアプローチに移行する必要があると前述しました。脅威ハンティングは、組織がこの考え方を取り入れるために導入する必要のある主な対策です。

EDR (Endpoint Detection and Response)

主要な脅威ハンティングは、EDR テクノロジーによって支えられています。EDR は、通常エンドポイント保護プラットフォームに統合されており、リアルタイムの継続的な監視とエンドポイントデータを、自動対応および解析機能と組み合わせています。これによって、セキュリティチームは脅威を迅速に特定して修復できます。

Sophos Intercept X Endpoint には、強力な EDR 機能が含まれていますSophos EDR は、セキュリティアナリストと IT 管理者の両方を対象に設計された最初のソリューションで、脅威を探し出し、IT セキュリティ運用の予防策を強化するために詳細な質問をする際のツールとして活用できます。すぐに使用可能でカスタマイズできる強力な SQL クエリにアクセスできるため、十分な情報に基づいて意思決定に必要な情報を得ることができます。

さらに、Sophos EDR の脅威の自動識別機能を使用すると、疑わしいアクティビティを自動的に検出し、脅威インジケータに優先順位を付け、エンドポイントとサーバー全体で潜在的な脅威をすばやく検索できます。

Sophos EDR の機能の詳細はこちら

MDR (Managed Threat Detection and Response) サービス

SolarWinds ハッキングなど、サイバー脅威の中で最も深刻なものは、一般に人間主導の攻撃を伴います。テクノロジー、特に EDR などの脅威ハンティングツールは重要な役割を担っていますが、それでも専門のオペレーターを必要とします。人間主導の攻撃を阻止するには、人間主導の脅威ハンティングが必要です。IT 管理者はこれを把握しており、48% が、このような対策を今後 1年間以内に取り込むことを計画しています[4]。

脅威ハンティングの人間主導のアプローチの 1つに、MDR サービスがあります。受賞歴のある Sophos MDR サービスである Sophos Managed Threat Response (MTR) は、単なる脅威通知にとどまらず、サイバーセキュリティ専門家のチームは依頼元の組織の IT チームを支援し、24時間体制で潜在的な脅威やインシデントをプロアクティブに追跡、検証、修復します。

4 サイバーセキュリティ：企業を守る人材とスキルの現状 – ソフォス、2020年

脅威ハンターと対応の専門家である Sophos MTR チームは、次のことを行います。

- 潜在的な脅威とインシデントをプロアクティブに追跡し、検証
- 利用可能なすべての情報を使用し、脅威の範囲や重大度を判定
- 有効な脅威に対して適切なビジネスコンテキストを適用
- 脅威をリモートから阻止、封じ込め、無力化するアクションを開始
- 再発するインシデントの根本原因に対処するための実用的なアドバイスを提供

Sophos MTR の詳細はこちら

サイバーセキュリティのゼロトラスト アプローチへの進化

先ほど、特に MFA を有効化し、アクセス権限とアプリケーション権限の両方を常に確認するなど、自社のセキュリティ対策を確認することについて検討しました。こうしたことはすべて、サイバーセキュリティへのゼロトラストアプローチに移行することで実現できます。

ゼロトラストは、「何も信頼せず、すべてを検証する」という原則に基づいており、物理的またはデジタルの場所に関係なくリソースを保護することに重点を置いています。ゼロトラストを単独で実現できるベンダー、製品、テクノロジーはありません。むしろ、組織内の文化的な変革と、リソースを保護するパラダイムを変化させるさまざまなソリューションが必要です。しかし、このモデルに向けた 1つのステップは、ZTNA (Zero Trust Network Access) ソリューションの導入です。

ZTNA は、その名前からわかるように、ゼロトラストの原則に基づいています。これにより、ユーザーはどこからでも安全にデータにアクセスできるようになり、一方、管理者は非常に詳細に制御することができるようになります。

ZTNA はユーザーの認証に関する考え方です。通常は多要素認証と ID プロバイダを使用してユーザーを検証し、次に (登録済みであるか、最新の状態になっているか、適切に保護されているか、暗号化は有効になっているか、など) デバイスのセキュリティ状態とコンプライアンスを確認します。その次に、その情報を使い、ポリシーに基づいて、重要なネットワークアプリケーションへのアクセスと権限を決定します。ZTNA は、リモートアクセス VPN の代替として最適です。誰が何にアクセスできるかを非常に詳細に制御できるので、サプライヤーがシステムにアクセスすることに依存する、サプライチェーン攻撃から保護するうえで重要です。

ソフォスの新しいクラウドで提供・管理されるネットワーク アクセス ソリューションである Sophos ZTNA は、現在 EAP (アーリー アクセス プログラム) を実施中です。一般提供の開始は 2021年半ばを予定しています。オンプレミスネットワーク、もしくはパブリッククラウドやその他のホスティングサイトでホストされるネットワークアプリケーションを保護します。ネットワークファイル共有への RDP アクセスから Jira、Wiki などのアプリケーション、ソースコードリポジトリ、サポートおよびチケットアプリまですべてが対象です。

Sophos ZTNA の詳細はこちら

まとめ

その複雑さを考えると、サプライチェーン経由の攻撃を防ぐことはほぼ不可能です。しかし、このホワイトペーパーのガイドラインに従うことで、攻撃の被害を受けるリスクを削減し、攻撃によるビジネスへの影響を最小限にとどめることができます。サマリー:

1. 事後対応型から事前対応型サイバーセキュリティへの移行
2. 攻撃の兆候の監視
3. サプライチェーンの監査
4. サプライヤーおよびビジネスパートナーのセキュリティ状態の評価
5. 自社の IT セキュリティ運用の予防策を常に確認

さらに、EDR、MTR、ZTNA などのテクノロジーやサービスを導入して、サプライチェーンのセキュリティの目標を支援することも検討してください。

脅威の状況は進化を続け、サプライチェーンへの侵入は、規模の大小を問わず、すべての組織の課題となっています。誰もがサプライチェーンを介した攻撃の対象になっており、サードパーティのサプライチェーンのリスクを最小限に抑えることは、これまでになく重要です。

業界をリードするソフォスのサイバーセキュリティ
ソリューションと専門知識の詳細はこちら：
sophos.com/ja-jp

ソフォスは、業界をリードするサイバーセキュリティソリューションをあらゆる規模の企業に提供し、マルウェア、ランサムウェア、フィッシングなどの高度な脅威をリアルタイムで保護します。実績のある次世代機能により、AI と機械学習を駆使した製品でビジネスデータを効率的に保護できます。

2021-04-14 (SB-NP)

SOPHOS