Report

WITH secure

Salesforce を狙うサプライチェーン攻撃の仕組み

Salesforce とサードパーティとの統合部分を狙った
サプライチェーン攻撃を如何に防止するか

目次

1. はじめに
デジタルサプライチェーンにおけるリスク.....3

2. サードパーティとの統合はどのようにして
Salesforce に新しい脅威をもたらすのか.....6

3. Salesforce サプライ
チェーン攻撃の仕組み.....8

4. デジタルサプライチェーンのリスクを
軽減するためのベストプラクティス.....11

5. 2022年のデジタルサプライチェーンの
リスクに先んじるために.....14

1. はじめに
デジタルサプライチェーンにおけるリスク

現代の大企業は、多数のデジタルサプライヤーによって構成される巨大で複雑なネットワークの中心に位置しています。低コストの高速インターネットと急成長しているグローバルなクラウド市場のおかげで、企業はビジネスを成長させるために必要な要素を簡単にアウトソースすることができるようになりました。専門性の高いソフトウェアソリューションをSaaSモデルで利用したり、コンポーネントやプラグインを入手して自社のインフラを大幅にカスタマイズすることも可能です。

デジタルサプライチェーンは比類のない柔軟性と自由を提供するため、企業は新しい機能を迅速に取り込んでビジネスチャンスを活かすことが可能です。しかしその一方で、ネットへの露出が増え、サイバーリスクに晒されるという犠牲を伴います。

数千個もの可動部品が絡み合っている状況では、ITアセットの効果的な可視性を維持し、潜在的な脆弱性を特定することは非常に困難です。

そして、脅威アクターは積極的にこの状況を悪用しようとしています。SaaSサプライヤーやソフトウェアプラグイン開発者などのサードパーティとの接続部分を狙って攻撃することで、サイバー犯罪者は企業のセキュリティ防御を回避し、ネットワークの中核を攻撃します。このような接続部分を侵害して高度に破壊的な標的型ランサムウェアなどのマルウェアを企業内に送り込んだり、価値の高いデータを盗み出したり、コマンド＆コントロールを可能にしたりできます。

Gartner® はデジタルサプライチェーンにおけるリスクを2022年における主要なセキュリティおよびリスク管理のテーマの1つとして挙げており、「2025年までに、世界中の組織の45%（2021年の3倍）がソフトウェアサプライチェーンへの攻撃を経験するだろう。」と予測しています。[1]

現実に、2021年だけでサプライチェーン攻撃が3倍になったという試算もあります。昨年起きた最大のデータ流出事件のいくつかは、デジタルサプライチェーンを中心としたものでした。

1. Gartner のプレスリリース “Top Trends in Cybersecurity 2022” 2022 年2月18日付
アナリスト：Peter Firstbrook, Sam Olyaei, Pete Shoard, Katell Thielemann, Mary Ruddy, Felix Gaehtgens, Richard Addiscott, William Candrick

Log4Shell

この有名なエクスプロイトは、エラーメッセージのログ出力に広く使用されているApache Log4j 2 Javaライブラリに関連したものです。この脆弱性（正式にはCVE-2021-44228）により、攻撃者はテキストメッセージを介して特定のバージョンのLog4j 2を実行しているデバイスにリモートアクセスすることができます。この欠陥は2021年12月に発見され、すぐに修正されました。しかし、この欠陥は2013年にはすでに存在していた可能性があり、すべての企業のほぼ半数が、過去にこの脆弱性を狙われた可能性があると考えられています。

Okta

2022年3月、MFAプロバイダーであるOktaは、同年1月に重大なセキュリティ侵害に見舞われ、数百人の顧客が影響を受けたと発表しました。この侵害は、Oktaのサブプロセッサ（業務委託先）が侵害されたことが原因で、サードパーティとの統合がどのように狙われて侵害されるのかが改めて注目されました。攻撃者（Lapsus$として知られるハッキンググループ）は、リモートデスクトップツールを使用して顧客のネットワークに侵入し、データにアクセスしました。

Office 365

攻撃者は、大規模化するOffice365環境を標的型フィッシング攻撃で狙うことが増えています。ユーザーは、365アカウントにログインして新しいアプリケーションを確認するように促すEメールを受け取ります。このEメールはよくある偽のフィッシングサイトでは無く、ユーザーの本物のOffice365ログインページにリンクされています。この場合、アプリケーションそのものが不正なものであり、攻撃者はユーザーのファイルやEメールにアクセスすることができます。この不正なアプリケーションはすでに環境内にあるため、多要素認証（MFA）を回避できてしまいます。

SolarWinds

2020年に発生したにもかかわらず、SolarWinds攻撃は今でも最も有名なハイエンドのデジタルサプライチェーン攻撃です。このインシデントは、ソフトウェアベンダーのSolarWindsが、同社のOrionソリューションを狙った高度で多面的な攻撃によって侵害されたものであり、ロシアの支援を受けた攻撃者の仕業であると広く信じられています。攻撃者は、悪意のあるコードをソフトウェアのアップデートに密かに挿入し、米国財務省や司法省などの政府機関を含む数千人のユーザーのネットワークにアクセスできるようにしました。

これらの攻撃は、すべての企業がデジタルサプライチェーンのリスクを真剣に考える必要があることを示しています。たった1つのアプリケーションが侵害されただけで、世界中の何千もの組織に影響を与える可能性があります。企業は危険の程度を正確に理解し、デジタル接続の増加のペースに合わせてセキュリティ機能を更新する必要があります。

デジタルトランスフォーメーションが進むにつれ、サードパーティのソフトウェアを統合したビジネスのあらゆる分野でサプライチェーンにおけるリスクが問題になります。そして、それが担うビジネス機能が重要であればあるほど、リスクは大きくなります。

Salesforceは世界中で150,000を超える企業が利用しているCRMシステムであり、攻撃に晒されるリスクが最も高いソフトウェア環境の1つです。今のところSalesforceインフラでは大きなサプライチェーン上のインシデントは発生していませんが、将来的にそれが起こる可能性を否定することはできません。

ENISA レポート

ENISAの「Threat Landscape for Supply Chain Attacks」レポートでは、2020年から2021年のサプライチェーン攻撃を分析し、以下のように推定しています：

- 攻撃の約50%に、有名なAPTグループが関与していた
- 攻撃の約62%が、企業からサプライヤーへの信頼を利用していた
- 62%のケースにマルウェアが関与していた
- 攻撃の66%で、顧客を標的にするためにサプライヤーのコードを侵害していた
- 攻撃の約58%は、顧客情報やIPなどのデータへのアクセスを目的としていた

2. サードパーティとの統合はどのようにしてSalesforce に新しい脅威をもたらすのか

Salesforce は多くの企業にとって必要不可欠なアセットであり、顧客管理および全体のデジタルエクスペリエンス戦略において決定的な役割を担っていることも少なくありません。そのため、さまざまな運用ニーズに合わせて環境をカスタマイズして設定する必要があり、そういった機能に対する市場からのニーズは非常に高いものとなっています。

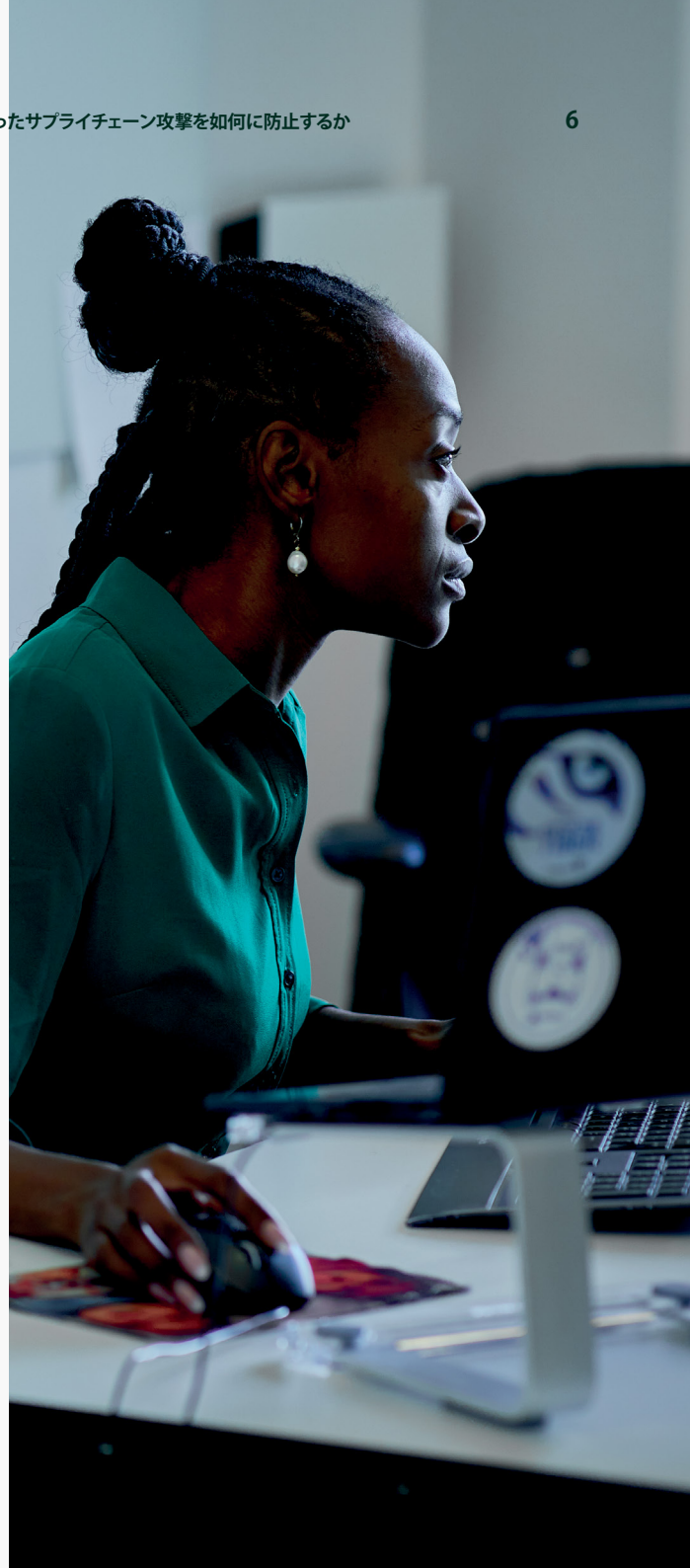
Salesforceプラットフォームは、サードパーティのアプリケーションやコンポーネント、そしてクラウドサービスを使用して、大幅にカスタマイズして拡張することができます。このプラットフォームの公式のアプリストアであるSalesforce AppExchangeでは、3,400個を超えるアプリケーションを提供しており、企業はSOAPまたはREST APIを介してSalesforce環境を外部のシステムやアプリケーションと接続することもできます。これらのシステムはさまざまなクラウド環境でホストされており、さまざまなプロプライエタリまたはオープンソースソフトウェアが使用されています。さらに、Salesforceプラットフォームは従来のEメールまたはWebフォームベースの統合もサポートします。

このように非常に多くのオプションが用意されているため、Salesforce環境に適用したいアダプションやエクステンションについて、企業は何らかのサードパーティからのサポートを必ず見つけることができます。しかし一方で、これらを新たに追加するたびに、デジタルサプライチェーンにおけるリスクも増加します。

考えられる脅威としては、以下のようなものがあります：

悪意のあるなりすまし

最悪のシナリオとしては、サードパーティのアセットそのものが攻撃ベクトルとして特別に作成されたものであるという可能性があります。組織的犯罪グループが正規のアプリケーションをダウンロードし、リバースエンジニアリングして悪意のあるコードを含むクローンを作成し、ダウンロード用に再公開するのです。SalesforceのAppExchangeではこのようなケースは報告されていませんが、AndroidやGoogle、およびその他のソースでは増加しています。Salesforceのセキュリティ審査要件は厳格なため、AppExchangeはソースとしては非常に安全ですが、それは他の多くのオンラインソフトウェアのリソースには当てはまりません。またインストール後にアプリケーションの動作を制御することは困難であることから、過去に検査済みのアプリが悪意のある目的で使用される可能性が残ります。



侵害されたソフトウェア

SolarWindsとKaseyaの侵害の例が示しているように、サイバー犯罪者は、まず最初にソフトウェアベンダーを狙ってデジタルサプライチェーンを侵害しようとします。これにより、過去に検査済みの正当なアプリケーションを悪用し、従来型のセキュリティソリューションの多くを回避できる効果的な攻撃ベクトルとして使用できるようになります。このような攻撃では攻撃側のリソースが大量に必要になるため、通常は価値の高い企業を標的とする組織的なグループや、ランサムウェアのような高度な攻撃で多数の被害者を攻撃しようとする犯罪グループによって行われることがほとんどです。このように、個々のSalesforceユーザーは収益性の高いターゲットではないかもしれませんが、Salesforce自体とその主要な統合パートナーを狙うことで、収益性は高まります。

脆弱なコード

脅威アクターが関与しなくとも、通常のデジタルアセットそのものがサイバーリスクをもたらす可能性があります。デジタル時代にビジネスを行う上で、ソフトウェアの脆弱性は避けられないリスクであり、2021年には過去最多となる19,733件が報告されました。完璧な評価を得ているベンダーの最も厳密にテストされたアプリケーションでさえ、少なくともいくつかの脆弱性が含まれていることは避けられません。

ソースが何であれ、サードパーティのアプリケーションまたはコンポーネントに安全でないものが1つでもあれば、重大なセキュリティ侵害を引き起こすには十分です。

追加のアプリケーションやプラグインが数百個もあるような複雑な環境であれば、管理は非常に困難になります。多数の蟻がさまざまなタスクを実行しているようなものですから、最高の管理者でさえ、蟻塚の向こう側で何が起こっているのかを確認するのには苦労するでしょう。

Salesforceだからというだけで、安全な環境が保たれると思い込んでしまうという傾向があるのは心配なことです。システム管理者や開発者・インフラ管理者は、AWSなどの他の環境ではセキュリティの確保が重要だと考えていますが、Salesforceはよりシンプルなものと思われているため、自己完結してセキュリティが確保されていると思われがちなのです。
AWSのような複雑なIaaS（Infrastructure-as-a-Service）プラットフォームの運用には、最初からIT、ネットワーク、セキュリティチームが関与しますが、Salesforceが同じ扱いを受けることはあまりありません。

内なる脅威

他のデジタル環境と同様に、Salesforceが正しく設定されていない場合、非常に脆弱になり得ます。

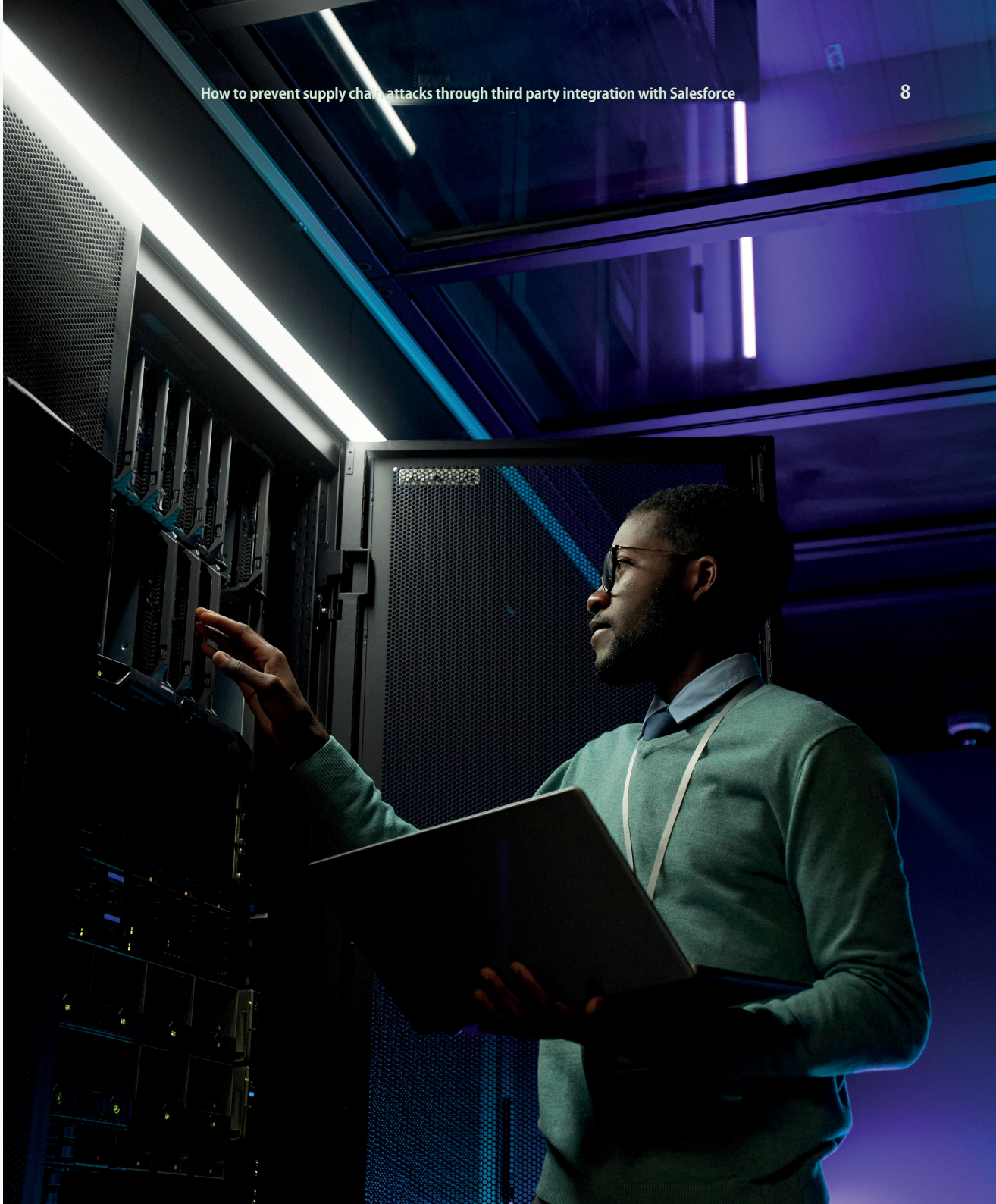
誤って設定されたアプリケーションと効果のないID管理は、その環境を即座に危険にさらします。脅威アクターは、セキュリティが不十分なユーザーアカウントやデフォルト設定のまま放置されたアプリケーションを見つけ出すことに長けていますし、アクセス制御が厳格で無いと、攻撃者が環境に侵入しやすくなります。

これは、サードパーティのアプリケーションやコンポーネントによって何百もの新しい要素が導入される前ですら、深刻な問題です。特に大企業では支店間や部門間の連携が不十分なことが多く、同じ作業を行うアプリやプラグインが重複して環境を肥大化させやすいという問題があります。中小企業では、より合理的な運用が行われる可能性がありますが、効果的な保護対策なしに新しいコンポーネントを追加してしまう可能性が高くなります。

なおSalesforceは、適切に設定されていない共有ルールを可視化してリスクを低減するための対策を講じ、デフォルト設定をより安全なものに変更したリリースアップデートを公開しています。たとえばLightning Experienceアプリケーションであるsalesforce Optimizerを使用すれば、定期的なチェックによってゲストユーザーに関する潜在的な問題を見つけ出すことができます。

3. Salesforce サプライチェーン攻撃の仕組み

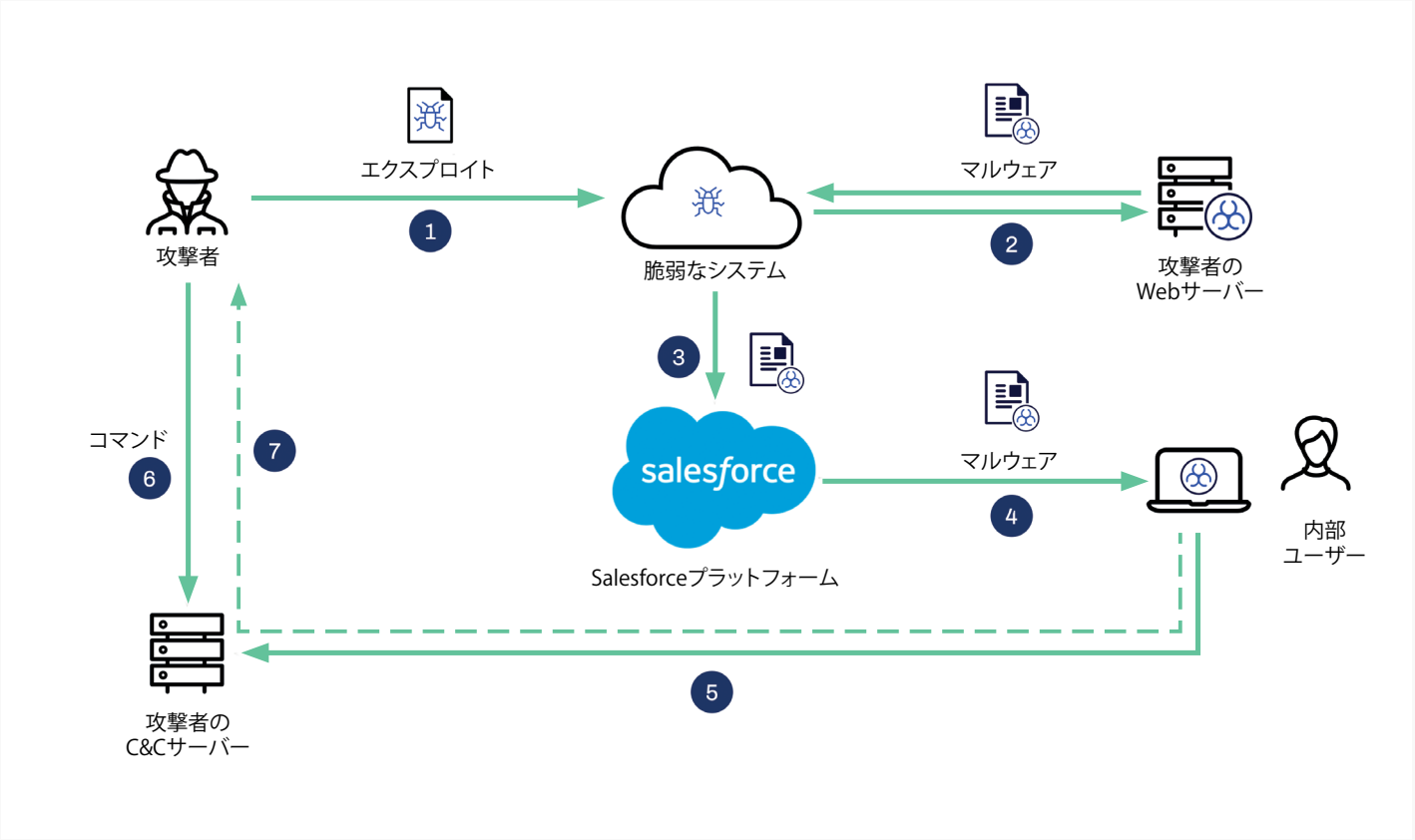
Salesforce環境は広範かつ複雑であるため、デジタルサプライチェーン攻撃の一環として狙われ、侵害される可能性があります。ここでは攻撃シナリオの例を2つ、ご紹介します。



シナリオ 1：脆弱なサードパーティーシステム

シナリオ1では、攻撃者はSalesforceと統合されたソフトウェアアプリケーション（例：分析用のデータを取得するツール）の脆弱性を見つけ出し、それを悪用してシステムにリモートアクセスします。この脆弱なアプリケーションはAPIを介してSalesforceと連携していますが、これらは通常人間（ユーザー）よりも信頼レベルが高いため、攻撃者は比較的簡単にシステムにアクセスできてしまいます。

攻撃者はそこでSalesforce内のデータを盗んだり破壊したりすることもありますが、プラットフォームの機能を攻撃チェーンの一部として利用することもできます。たとえば悪意のあるドキュメントやURLを環境全体にばらまいて、従業員や顧客、その他の関係者など、疑いを持たないユーザーがクリックしたりダウンロードしたりできるようにすることも可能です。そしてこれらのユーザーが侵害され、彼らのシステムアクセスが悪用されると、企業の他のITインフラへも攻撃を継続できる可能性があります。



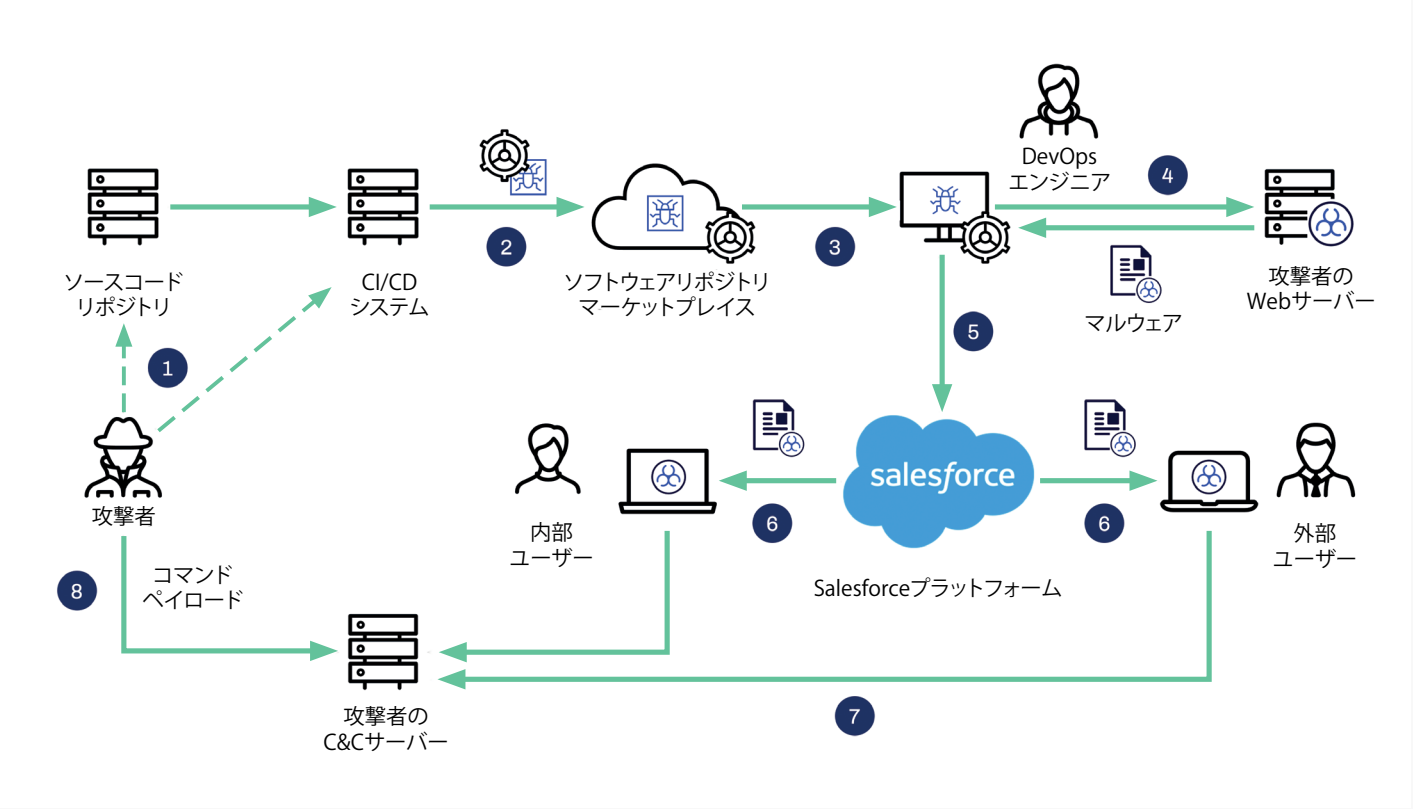
1. 攻撃者は、Salesforceに接続されたサードパーティのクラウド（またはオンプレミス）システムの脆弱性を侵害します。
2. 攻撃者がエクスプロイトコードを実行して脆弱なシステムにアクセスし、特別なWebサーバーからマルウェアをダウンロードします。
3. 攻撃者がマルウェアをSalesforceプラットフォームに「注入」します。マルウェアはケースに添付されたり、Chatterで投稿されたり、共通のファイルライブラリにアップロードされたりします。
4. 内部ユーザーはマルウェアを含むファイルをダウンロードし、自分のデバイスで開きます。このとき、ユーザーは何も異常に気づきません。
5. マルウェアが、攻撃者がホストするコマンド＆コントロール（C＆C）サーバーに接続します。
6. 攻撃者は、マルウェアが内部に侵入し、C＆Cサーバーに正常に接続したことを確認します。攻撃者は、追加のコマンドまたはペイロードを送信することにより、マルウェアと通信します。
7. 攻撃者が内部ユーザーのコンピュータやSalesforceから機密データを盗み出します。

シナリオ 2: 侵害された開発ツール

このシナリオでは、脅威アクターはまず最初にソフトウェアベンダーのソースコードリポジトリ、またはCI/CDシステムを標的とします。これは、その製品に悪意のあるコードを注入するためです。最初のシステムアクセスにはさまざまな手法が使われますが、SolarWindsでも見られたように、フィッシングを利用してユーザーの認証情報を取得するという手法が最も一般的です。

その後アプリケーションやコンポーネントがSalesforce環境に統合されると、攻撃者はその接続性を利用して他のユーザーやエンドポイントを侵害できるようになります。この時点で、攻撃者はどのような目標でも達成することができます。このプロセスを繰り返し、標的の企業をサプライチェーン攻撃の新たな足がかりとすることもあります。

攻撃者は最初の段階でSalesforceインスタンスに直接アクセスすることもありますが、バックドアを設置してソフトウェアベンダーが本番へのアクセスを行うまで待機することもあります。開発者は有名ベンダーのツールであれば、その安全性を盲目的に信頼してしまう傾向がありますが、SolarWindsの例が示すように、組織的な攻撃者によって侵害された場合には、定評のあるベンダーであってもリスクの源になることはあり得ます。



1. 攻撃者が公開されたソースコードリポジトリをスキャンして、CI/CDシステムの認証情報を見つけ出し、最終的にアクセス権を獲得します。
2. 攻撃者が、CI/CDシステムによってビルドされ公式ソフトウェアリポジトリまたはマーケットプレイスに公開されたソフトウェアパッケージに、特別に細工したペイロードを「注入」します。
3. DevOpsエンジニアが、これらのリポジトリやマーケットプレイスからペイロードを含むパッケージを入手し、自分のコンピュータで実行します。
4. ペイロードが攻撃者のWebサーバーからマルウェアをダウンロードします。
5. DevOpsエンジニアはSalesforceにアクセスできるため、マルウェアはSalesforceにアップロードされます。
6. 社内/社外のユーザーがマルウェアをダウンロードし、自分のコンピュータで開きます。
7. マルウェアが、攻撃者のコマンド＆コントロール（C&C）サーバーに接続します。
8. 攻撃者は、被害者のコンピュータにコマンドと追加の悪意のあるペイロードを送信します。

4. デジタルサプライチェーンのリスクを軽減するためのベストプラクティス

サイバーセキュリティは複雑な問題であり、すべてを解決できる魔法の弾丸はありません。これはSalesforceのような大規模かつ高密度なクラウド環境で特に顕著です。そのため、Salesforceに対するデジタルサプライチェーン攻撃のリスクを軽減するためには、適切なセキュリティソリューションと適切なプロセスおよびポリシーを組み合わせた多層的なアプローチが必要になります。Salesforceのセキュリティ戦略にとって最も重要な要素には、次のようなものがあります：

Application Portfolio Management（APM）の導入

Salesforce 環境に導入する前に、すべてのアプリケーションとコンポーネントを徹底的に検査する必要があります。アセットとそれを供給するベンダーについて既知の脆弱性や過去のインシデントを調査し、これらの問題が解決されていることを確認してください。
アプリケーションポートフォリオ管理（APM）プロセスを導入することで、新規のアプリケーションを検査し、既存のアセットをインベントリ化することができます。デューデリジェンスはベンダー自体についても行う必要があり、企業はすべてのサードパーティがサプライチェーン攻撃のリスクを軽減するために適切なレベルのセキュリティを備えていることを確認しなければなりません。これには、脆弱性が誤ってアップデートに紛れ込むリスクも含まれます。

リスクが特に高い企業では、セキュリティ要件をサービスレベルアグリーメント（SLA）に含めても良いでしょう。また、今日の地政学的な状況下において国家が支援する攻撃者によるリスクを最小化するために、ベンダーの出自には特に注意を払う必要があります。

潜在的な侵害の影響に関するリスクのマッピング

企業はアセットの検査に加え、Salesforce環境におけるそのアセットの位置付けを詳細に検査し、そのアセットが侵害に関与した場合の影響を確認する必要があります。これは、その製品がどのような機能を持ち、SalesforceやITインフラの他の領域とどのように連携しているかを検討するということです。

リスクの受け入れはビジネスを行う上で避けられないコストですが、企業は新しいコンポーネントを導入するメリットに対してリスクレベルが許容範囲にあるかどうかを確認し、それをセキュリティ戦略に統合する必要があります。

サードパーティのアセットを一元的に管理

数百におよぶサードパーティのコンポーネントを含む大規模なSalesforce環境では、すべてを把握することはほとんど不可能です。しかし、見逃しは重大なインシデントにつながる可能性があるため、管理者は可視性をできる限り高めるよう取り組む必要があります。

理想的には、最も重要でリスクの高いサードパーティーのアセットを優先的に可視化して制御し、そこから徐々に対象を広げて行くのが良いでしょう。また、新しいアセットを導入する際のポリシーを構造化しておくことで、環境が拡大しても可視性を維持し、類似したアプリケーションが追加されるリスクを低減することができます。

設定ミスやアクセス上の問題を排除

企業は、デジタルサプライチェーンの外側だけでなく、内部のプロセスにも目を向ける必要があります。アプリケーションに設定ミスがあったり、アクセス管理が不適切だったりすると、サードパーティー導入の有無にかかわらず、攻撃者を呼び込んでしまう可能性があります。

管理者はSalesforce環境を監査して、アプリケーションのアクセス権が適切なレベルに設定されていることを確認する必要があります。理想的には、すべてのアセットについて必要最小限のアクセス権しか設定せず、特に必要な場合を除いて共有機能は無効にしておくべきです。

これはユーザーにも当てはまります。ユーザー（人間）のプロファイルと自動化されたシステムの両方について、職務上のロールに必要なアクセス権のみを認める最小特権のアプローチをとる必要があります。これは、システム管理者に関して特に重要です。多くの企業では、システムに接続するすべてのユーザーにデフォルトで管理者権限を与えてしまう傾向があるからです。

システムアクセスに関するベストプラクティスに従うことで、脅威アクターが環境を侵害する可能性を低下させ、ユーザーやアプリケーションが侵害された場合の影響を軽減することができます。

そして、これは1回行えば良いというものではないことに注意してください。Salesforceのすべての新機能について、提供されるリリースノートによって定期的に確認する必要があります。

企業が持つ環境が特に大規模な場合、定期的にシステム構成の詳細なレビューを行うことが理想的です。ウィズセキュアのクラウドコンサルティングサービスでは、見逃しの無いように専門家の専門知識を提供します。

Salesforce 上の悪意のあるコンテンツをブロック

脅威アクターはさまざまな方法でサプライチェーン攻撃を行いますが、最も一般的なアプローチは盗んだ資格情報の使用です。フィッシングやユーザーの資格情報の盗難、あるいはマルウェアを使ったサプライチェーン攻撃を防ぐためには、エンドポイント、ネットワーク、クラウドベースの保護を含む、セキュリティに対する総合的なアプローチが必要です。

ウィズセキュアは、お客様が最新の攻撃を防止し、検知して対応するためのさまざまなソリューションを提供しています。

しかし、Salesforce自身が攻撃経路として悪用される可能性があることも忘れてはいけません。例えば、保険会社の顧客が保険金請求書類や身分証明書をアップロードしたり、人材紹介会社が求人情報を送受信したりするためには、コンテンツのアップロードとダウンロードの機能が不可欠です。

しかしこの機能を悪用すれば、悪意のあるファイルやURLをSalesforceにアップロードし、メールベースのフィッシングに代わる効果的な手段として利用することが可能になります。また、Salesforce環境が侵害されて、悪意のあるコンテンツがユーザーや顧客と共有される可能性もあります。

セールスフォース・ドットコム社には環境内のデータを保護する責任がありますが、アップロードまたはダウンロードされるコンテンツを監視することはできません。それについての責任は、企業側にあります。

WithSecure™ Cloud Protection for Salesforceは、これらの攻撃経路を塞ぐための最も効果的な方法の1つです。これは、企業のセキュリティ境界の外にいるユーザーや高度な犯罪グループがSalesforceにアップロードする悪意のあるファイルやURLを使った攻撃を防ぐために設計された、マーケットを主導するソリューションです。

このソリューションは、アップロードおよびダウンロードされるすべてのコンテンツをリアルタイムにスキャンして、ウィズセキュアの最新の脅威インテリジェンスによって悪意のあるコンテンツを特定し、ブロックします。Cloud Protection for Salesforceは、セールスフォース・ドットコム社との協力の基で開発され、従業員やユーザーの使用体験に影響を与えることなく、強力な保護機能を提供します。

効果的な対応計画の用意

最後になりますが、データ流出の脅威は、「もし起きたら」ではなく「いつ起きるか」という状況になっていることを認識することが重要です。完成したセキュリティ戦略を持ち、巨額の予算でサポートされている企業であっても、十分なスキルと決意を持った攻撃者が相手であれば、いずれは侵入される可能性があります。

そのため、すべての企業は、Salesforce環境に影響を与えるデジタルサプライチェーン攻撃の最悪のシナリオに備える必要があります。ここで優先すべきなのは、脅威を迅速に特定して封じ込め、通常のビジネスオペレーションを可能な限り迅速に復元するために、効果的なインシデント対応および復旧の計画をたてることです。

ウィズセキュアが提供しているSalesforce Shieldサービスでは、詳細なロギングやフィールド単位の暗号化などの機能を利用できます。これにより、インシデントの検知と分析に役立つアクティビティ監視などの重要な要望に応えることができます。

企業はまた、侵害の原因を突き止め、隠れたマルウェアやコマンド＆コントロールプログラムなどの環境内に残る脅威を取り除くために必要な専門スキルやツールに、迅速にアクセスできなければなりません。このような能力を獲得するためには、専門のパートナーと連携することが最も費用対効果の高い方法の1つです。

また、Salesforce環境が侵害されるとCRMのプロセス全体が停止する可能性があるため、その影響を緩和するための計画も必要です。定期的なシステムのバックアップと代替の通信手段を用意することで、問題が解決するまでの間もビジネスを継続させることができます。

5. 2022年のデジタルサプライチェーンのリスクに先んじるために

- 脅威アクターは企業の防御策を回避するための新たな攻撃経路を常に探しており、サプライチェーンのリスクは急速に高まっています
- 拡大したSalesforce環境は、企業が対策を講じない限り、攻撃経路として脆弱なままです
- 侵害される前に、企業は今すぐ準備を始める必要があります

サプライチェーンにおけるリスクは、デジタル時代にビジネスを行う上では避けることはできません。企業は、自社のサプライチェーンが拡大すると同時に脅威が増加することを認識する必要があります。そして脅威アクターは、企業のセキュリティ防御策を回避するための新しい方法を探し続けています。

デジタルがカバーするエリアが拡大し、より多くのサードパーティが連携するようになっているため、企業はサプライチェーンを監視して制御する能力を拡大と同じスピードで強化する必要があります。

Salesforceは重要なCRMシステムであると同時に、何百もの異なるサードパーティのコンポーネントが存在する環境であるため、これらのセキュリティ計画において非常に重要です。

セールスフォース・ドットコム社は自分自身のインフラを保護する責任を負っていますが、その環境に導入されるサードパーティのコンポーネントとコンテンツに対して責任を負うのはユーザーです。これは、責任共有モデルと呼ばれるアプローチです。

SolarWinds、Kaseya、Log4Jといった有名なインシデントは、長い間見出しを独占し、サプライチェーンのリスクに対する認識を高めました。しかし、Salesforceはまだそのリストに加わらずに済んでいます。
今すぐ私たちにご連絡いただき、脅威アクターがこれらの攻撃経路を見つけて侵害を試みる前に、ウィズセキュアがどのように役立つのかをご確認ください。

WithSecure™ について

WithSecure™ は、ITサービスプロバイダー、MSSP、ユーザー企業、大手金融機関、メーカー、通信テクノロジープロバイダー数千社から、業務を保護し成果を出すサイバーセキュリティパートナーとして大きな信頼を勝ち取っています。私たちはAIを活用した保護機能によりエンドポイントやクラウドコラボレーションを保護し、インテリジェントな検知と対応によりプロアクティブに脅威を探し出し、当社のセキュリティエキスパートが現実世界のサイバー攻撃に立ち向かっています。当社のコンサルタントは、テクノロジーに挑戦する企業とパートナーシップを結び、経験と実績に基づくセキュリティアドバイスを通じてレジリエンスを構築します。当社は30年以上に渡ってビジネス目標を達成するためのテクノロジーを構築してきた経験を活かし、柔軟な商業モデルを通じてパートナーとともに成長するポートフォリオを構築しています。

1988年に設立されたWithSecure™は本社をフィンランド・ヘルシンキに、日本法人であるウィズセキュア株式会社を東京都港区に置いています。また、NASDAQ ヘルシンキに上場しています。

ウィズセキュア株式会社
〒105-0004 東京都港区新橋2丁目2番9号 KDX新橋ビル2階
Tel: 03-4578-7710 / E-mail : japan@f-secure.co.jp
https://www.withsecure.com/
2022/05

WITH secure