2019 年 2 月 26 日

サービス＆セキュリティ株式会社 e-Gate センター

サプライチェーン攻撃の脅威と対策について

1. 概要

サプライチェーン攻撃のリスクはかねてから指摘されていました。
経済産業省が 2015 年に公表した「サイバーセキュリティ経営ガイドライン」で、経営者が認識すべき 3 原則の 2 番目に「自社のみならず、系列企業やサプライチェーンのビジネスパートナー等を含めたセキュリティ対策が必要」と記し対策を促してきましたが、その手口は多様化し未だに被害が発生しています。2018 年 7 月セキュリティ企業 CrowdStrike が発表した調査によれば、調査対象の世界 8 カ国(日本を含む)で約 7 割の企業がこれまでにサプライチェーン攻撃の被害を経験しており、直近 12 ヵ月に絞り込んでもおよそ 3 分の 1 の企業がサプライチェーン攻撃の被害に遭っています。また、この調査で日本ではサプライチェーン攻撃に対する包括的な対応策を行っている企業が 37%に留まり、調査対象国のなかで最も低いと報告されています。
2019 年 1 月 IPA（情報処理推進機構）が発表した『情報セキュリティ 10 大脅威 2019』では第 4 位に「サプライチェーンの弱点を悪用した攻撃の高まり」が初めてランクインしており、ここ数年第 1 位に選ばれている「標的型攻撃」の手口として「サプライチェーン攻撃」が多用される恐れも懸念されています。

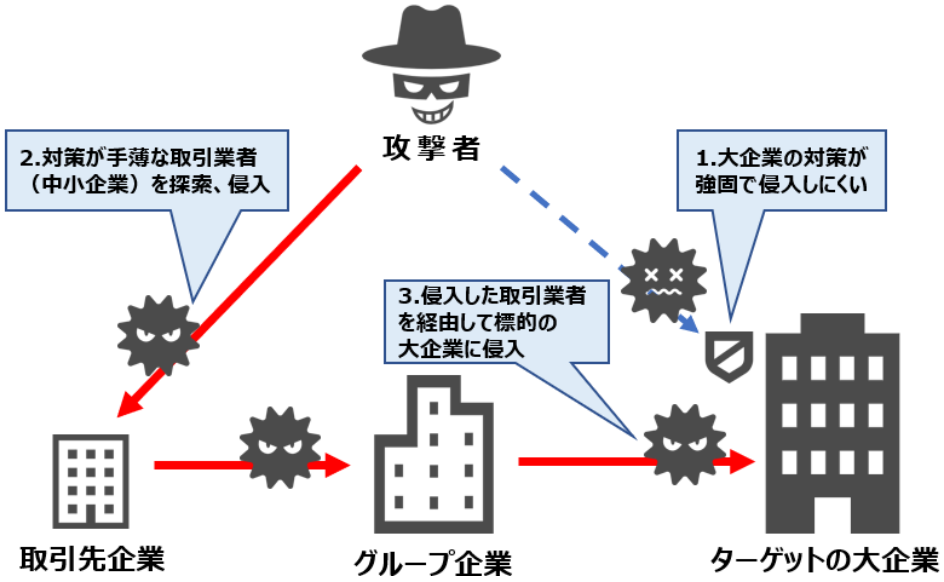
攻撃手法としては決して新しいものではありませんが、未だ有効な攻撃手法であり、複雑で巧妙な「サプライチェーン攻撃」の理解を深め、対策を講じることが重要です。

2. サプライチェーン攻撃手法と被害例

(1) サプライチェーン攻撃とは
サプライチェーンとは製品やサービス提供をするために行われる一連のビジネス活動の流れのことで、製造業で例えると設計開発、資材調達、生産、物流、販売という全プロセスをつなぐ連鎖構造を指しています。セキュリティ対策を強化している大企業を狙わず、取引先や関連企業といった中小規模でセキュリティ対策が手薄な企業を狙い、そこを踏み台にして大企業を攻撃する手法をサプライチェーン攻撃といいます。

サプライチェーン攻撃と呼ばれる手法は 2 種類存在します。

① 「関連組織を狙ったサプライチェーン攻撃」
ターゲット企業のグループ企業、取引先企業、関連組織などを攻撃し、それを足がかりにターゲット企業に侵入する手法です。



【図 1】取引先など関連組織を狙った攻撃の一例

大企業などを標的型攻撃のターゲットとするうえで、まずはセキュリティ対策の手薄なグループ企業、関連組織、取引先企業などを侵入口として攻撃し、そこからターゲットの企業／組織へ潜入します。

具体的には、以下のような手口が存在します。

① 攻撃者は取引先企業のメールを盗聴します。

② メールの盗聴が成功すると、攻撃者は取引先になりすました偽装メールをターゲット企業へ送ります。

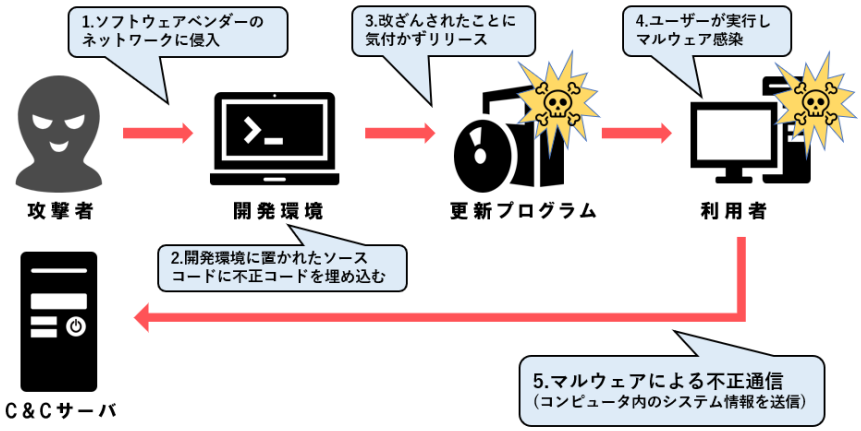
③ 偽装メールのやり取りが成功すると、攻撃者はターゲット企業へ侵入するための情報を入手します。

④ 入手した情報を使い、攻撃者はターゲット企業のネットワークへ侵入します。

強固なセキュリティを備えた正面突破が難しい組織であっても、攻撃者はセキュリティ対策の遅れている子会社や関連組織を踏み台にすることで比較的簡単に侵入できてしまいます。

② 「ソフトウェアサプライチェーン攻撃」

ソフトウェア製品のサプライチェーンの脆弱性につけこんで製品そのものや、アップデートプログラムやパッチにマルウェアやバックドアを埋め込んで感染させる手法です。



【図 2】ソフトウェアサプライチェーン攻撃の一例

攻撃者はソフトウェアベンダーのネットワークに侵入します。ターゲットであるソフトウェア製品の開発環境に保管されたソースコードに不正コードを埋め込みます。改ざんされたことに気付かずリリースされたソフトウェアをユーザーが実行してしまうと、マルウェア感染や、埋め込まれたバックドアを通じてマルウェアがダウンロードされてしまいます。

開発元や配布元から直接提供された普段利用している正規のソフトであれば、受け取ったユーザーは疑う余地もなく使用してしまいます。強固なセキュリティ対策を施した企業であってもソフトウェア製品のパッチやアップデートの経路を通じ巧妙に侵入を果たします。

(2) サプライチェーン攻撃の被害例

① 「MeDoc 税務会計ソフト アップデート改ざん」

2017 年 6 月、税務会計ソフトウェア「MeDoc」のアップデートデータが改ざんされ、多くの企業にマルウェアがばらまかれました。ユーザーはその多くがウクライナの国内企業や組織、また同国と取引のある他国籍企業で、被害は全欧州に広がりました。ベンダーが提供する正規のソフトウェアアップデートであり、ユーザーが疑う余地はありませんでした。

② 「CCleaner を踏み台にしたマルウェア混入」

2017 年 8 月から 9 月にかけて、PC 最適化無料ツール「CCleaner」にマルウェアが混入された状態で配布され、世界の大企業に標的型攻撃が実行されるという出来事が発生しました。このマルウェア入りの CCleaner 実行ファイルは、正規のダウンロードサーバで配布されていたことから、配布元に対するサプライチェーン攻撃であったとされています。
およそ 200 万台の PC に対して不正なアップデートが配信されたと推定されています。

3. サプライチェーン攻撃への対策

サプライチェーン攻撃に対して決定的な対策を取ることは困難ですが、共通する対策として以下は効果的といえます。

- 不正な通信からネットワークやサーバ、エンドポイントを防御するための IPS 導入。
- 不正な挙動を検知し、感染した後の対応を迅速に行える EDR 製品の導入。
- 被害の最小化を目的としたセキュリティシステムやネットワークの常時監視。
- サプライチェーン全体のセキュリティ対策状況の把握、及び教育の実施。

侵入への防御を固めると同時に、万が一侵入されてしまった場合に迅速な対応がとれるよう普段からの備えが大切です。そのためにも、最新鋭のセキュリティ製品を導入し、適切に運用するとともに、いち早く検知できるような監視体制を徹底しておくことが肝要です。

また、自社のセキュリティ対策の強化だけでなく、サプライチェーンも含めてセキュリティ対策の強化が求められています。
サプライヤーや取引先企業のセキュリティ状況を連携し合い、改善を促していき、よりセキュアな環境を共同で構築していくことが重要になります。

4. e-Gate の活用について

サイバー攻撃への対策としてセキュリティ機器を導入する場合、それらの機器の運用監視を行うことが重要です。
24 時間 365 日有人監視体制のセキュリティ監視サービス “e-Gate“をご活用頂きますと、迅速なセキュリティインシデント対応、最新の分析システムを活用し精度の高い検知、また専任のアナリストによる分析を行っております。
“e-Gate”の MSS の導入をぜひご検討ください。

■総合セキュリティサービス e-Gate

SSK（サービス＆セキュリティ株式会社）が 40 年以上に渡って築き上げてきた IT 運用のノウハウと、最新のメソッド、次世代 SOC“e-Gate センター“この 2 つを融合させることによりお客様の情報セキュリティ全体をトータルにサポートするのが SSK の“e-Gate”です。e-Gate センターを核として人材・運用監視・対策支援という 3 つのサービスを軸に全方位のセキュリティサービスを展開しています。
【参考 URL】
https://www.ssk-kan.co.jp/e-gate/

5. 参考情報

- 独立行政法人情報処理推進機構（IPA）
  情報セキュリティ 10 大脅威 2019
  https://www.ipa.go.jp/files/000071191.pdf

- 経済産業省
  サイバーセキュリティ経営ガイドライン Ver2.0
  http://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0.pdf

- CrowdStrike
  サプライチェーン攻撃に関する調査（英文）
  https://www.crowdstrike.com/resources/wp-content/brochures/pr/CrowdStrike-Security-Supply-Chain.pdf

«お問合せ先»
サービス＆セキュリティ株式会社
〒150-0011
東京都渋谷区東 3 丁目 14 番 15 号 MO ビル 2F
TEL 03-3499-2077
FAX 03-5464-9977
sales@ssk-kan.co.jp