SQAT® Security Report

2022-2023年
秋冬号

サプライチェーン攻撃を知る

知る・守る
続ける

BBSecは内閣サイバーセキュリティセンターの
「サイバーセキュリティ普及啓発」に賛同しています

便利で安全なネットワーク社会を創造する
株式会社ブロードバンドセキュリティ

ごあいさつ

株式会社ブロードバンドセキュリティ
セキュリティサービス本部 本部長　齊藤 義人

2022年上半期は、サイバーセキュリティのトピックが濁流のように押し寄せてきました。ウクライナを襲った大規模なサイバー攻撃、それに関連した攻防からの余波も様々な分野に影響を及ぼしました。DDoS攻撃も規模が拡大していきました。毎秒2600万リクエストにもおよぶ過去最大規模のDDoS攻撃が発生したと思えば、2ケ月後には秒間4600万リクエストの攻撃が発生しました。更には自動車のハッキングや、多要素認証が標的とされたトピックなど、注目すべき情報がない日の方が少なかったように思います。セキュリティ関係者が危惧してきたようなサイバー危機の数々が、現実として起こっているのです。

本レポートは、株式会社ブロードバンドセキュリティ（以下、BBSec）の脆弱性診断サービス「SQAT®」における2022年上半期（1月～6月）の診断結果からデータを抽出し、集約したものを当社のエンジニアらの感性も交えてアウトプットしたものです。今号は、サプライチェーン攻撃やクレジットカード情報漏洩インシデントの現状に焦点をあてた企画や、奈良先端科学技術大学院大学の門林雄基教授に寄稿していただいた企画が掲載されております。

本レポートが、読者の皆様のセキュリティ対策における有益な情報としてご活用いただけることを願ってやみません。それこそが「便利で安全なネットワーク社会を創造する」をモットーに掲げる BBSec の使命であると考えております。

CONTENTS

SQAT®（Software Quality Analysis Team）とは
～スペシャリスト集団が組織の脆弱性対策をトータルに支援～

「SQAT®」は、BBSecがご提供する脆弱性診断サービスです。エンジニア、コンサルタント、ホワイトハッカー等から編成された精鋭チームが、あらゆる側面から網羅的な診断を実施。スペシャリストのノウハウを結集して組織の情報システム強化をお手伝いします。お客様は金融機関・インターネット事業者などの民間企業から、官公庁をはじめとする公共機関まで幅広く、これまでに延べ7,590組織、45,540を超えるシステムで利用されています。

※本レポートは、当社セキュリティサービス本部のホームページ「SQAT®.jp（URL：https://www.sqat.jp/）」https://www.sqat.jp/sqat-securityreport/からダウンロード可能です。

SQAT.jp

＜事業拠点＞

東京本社
〒160-0023
東京都新宿区西新宿8-5-1
野村不動産西新宿共同ビル4F
TEL：03-5338-7430

大阪支店
〒530-0001
大阪府大阪市北区梅田1-1-3
大阪駅前第3ビル30F
TEL：06-6345-3880

名古屋支店
〒460-0003
愛知県名古屋市中区錦1-6-18
J・伊藤ビル6F
TEL：052-265-7591

天王洲オフィス
〒140-0002
東京都品川区東品川2-5-8
天王洲パークサイドビル3F
TEL：03-6433-3116

東北セキュリティ診断センター
〒010-0001
秋田県秋田市中通1-4-32
秋田センタービル　8F
TEL:018-838-6330

韓国支店
15F, Samsung Life Seocho Tower
4 Seocho-daero 74-gil, Seocho-gu
Seoul 06620, Korea
TEL : +82-2-6011-4640

サプライチェーン攻撃を知る

国内外のサイバー攻撃や、セキュリティ対策に関する報道を追っている当社アナリストが堅牢なセキュリティを探る企画の第2弾。今号は「サプライチェーン攻撃」に焦点を当てる。攻撃の種類や対策方法はもちろん、今号は主に事故事例からサプライチェーン攻撃を紐解いていく。

SQAT® Security Report 編集部

セキュリティ対策の意義

情報資産の価値が上がる中、企業としてセキュリティ対策を行うのはいまや当たり前となっている。

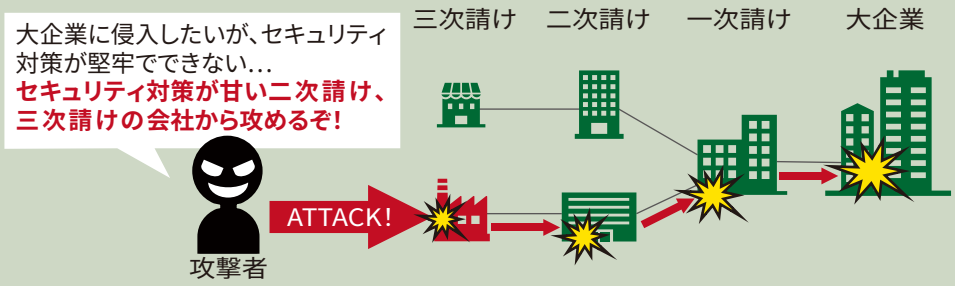
実際、セキュリティインシデントが発生すると、事業継続の危機にさらされる可能性があるため、セキュリティ対策は必須である。しかし、行うべき対応は多様かつ広範であり、すべてにおいて穴がないよう網羅的に行うのは至難の業だ。

効率的に対策を行うために、まずは企業がさらされている脅威について知っておかなければならない。今号はその中でもサプライチェーン攻撃について紹介する。

サプライチェーン攻撃

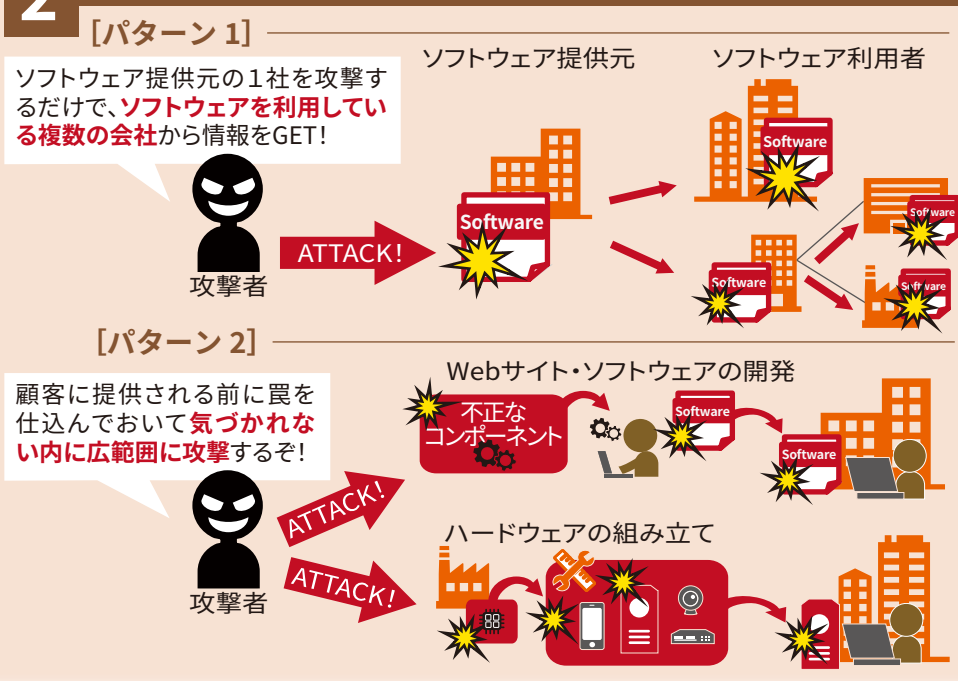
サプライチェーンとは調達、製造、配送、販売、消費といった、商品が消費者に届くまでの一連の流れを指す。これを利用して何らかのサイバー攻撃を仕掛けて情報奪取などを狙うのがサプライチェーン攻撃であり、IPAの「情報セキュリティ10大脅威　2022」で組織における脅威の第3位にランクインするなど、近年注目が集まっている。攻撃のパターンには、次のようなものがある。

1 組織間の弱い部分を狙う攻撃



- セキュリティ対策が比較的甘い中小企業が狙われる
- 中小企業から盗んだ情報をもとになりすましメールなどサプライチェーン上の他の企業に対してより効果的な攻撃を仕掛ける

2 広く利用されているコンポーネントを狙う攻撃



- 開発・組み立て時に使われる部品などに不正なプログラムを仕込み、提供元も気づかぬうちに顧客が情報を盗まれたり、マルウェア感染したりしてしまう
- アイロンや電気ケトルなど、一見ネットワークに関係なさそうな機器に仕込まれた事例も

対策のポイント

基本的な情報セキュリティ対策の実施を、サプライチェーン全体で取り組む

基本的な情報セキュリティ対策の例

- 情報資産の可視化
- OSやソフトウェアの最新状態へのアップデート
- 権限管理による重要情報取り扱い者の絞り込み
- パスワードの強化
- 脆弱性診断等によるセキュリティ上の問題の可視化
- マルウェア対策製品の導入
- アクセス制御ソリューションの導入
- 従業員全員に対するセキュリティ教育の定期実施
- インシデント発生時の対応手順等セキュリティに関するルールの策定・周知

サプライチェーン全体への取り組みの例

- アンケート等を用いたサプライチェーン上の各企業におけるセキュリティ状況の把握
- サプライチェーン上にセキュリティ水準の異なる企業があるか確認
- サプライチェーン上の企業間における重要情報の定義と取り扱い方法の取り決め実施

被害者が加害者にもなり得る

サプライチェーン攻撃は、セキュリティに比較的予算を割いて対策していると考えられる大手企業ばかりでなく、そこにつらなる中小企業も狙われやすい。また、多くの企業/組織が依存しているソフトウェア・機器がターゲットとされる場合もある。

気づかないうちにサプライチェーンにつらなる多数の企業/組織のシステムに深く侵入され、長期間にわたって侵害されていた、という被害事例もある。結果的に、被害を受けた自社/自組織が、意図せずサプライチェーン上にある多数の企業/組織に対する攻撃の加害者ともなり得るのだ。

そのような事態を招かないよう、基本的な情報セキュリティ対策は必ず実施し、サプライチェーン上の他の企業/組織と足並みを揃えて取り組む必要がある。もし自社/自組織に不足している対策やシステム上の弱点が明確でない場合は、外部のセキュリティ専門家の目を頼るのも有効な手段の1つである。