2021 年 07 月 30 日

サービス＆セキュリティ株式会社 e-Gate センター

注意喚起：オリンピックにおけるサイバー攻撃事例とセキュリティ対策

1. 概要

オリンピックは世界中が注目する一大イベントであり、様々なサイバー攻撃が予想されます。攻撃者の動機、標的、手段、手法などは多岐にわたります。従来の攻撃手法に加え、第 5 世代移動通信システム（5G）など最新のシステムや技術が狙われる危険性もあります。過去のオリンピックでは標的型攻撃によりマルウェアが仕掛けられ、チケットの発券が一時不可能になる事態が起こりました。この攻撃はサプライチェーン攻撃と呼ばれ、大会本部だけでなく、参画している企業、さらにはオリンピックと関わりのない企業も警戒すべき攻撃です。今回はサプライチェーン攻撃を含め、オリンピックで懸念されるサイバー攻撃とその対策をご紹介いたします。

2. 過去のオリンピックで確認されたサイバー攻撃

近年、オリンピックの運営は IT に大きく依存しており、注目度が高い分、サイバー攻撃の対象として狙われやすい傾向にあります。過去の攻撃事例を紹介します。

(1) 大会本部や競技会場を狙った攻撃

・2012 年のロンドンオリンピックでは大会の公式サイトに対し、開催期間 2 週間で 2 億 2,100 万回に及ぶサイバー攻撃がありました。また、競技会場の照明システムに対し、40 分間、1,000 万回に及ぶ DoS 攻撃が行われました。

・2016 年のリオデジャネイロオリンピックでは、ボット感染により組織委員会にて個人情報の漏えいが発生しました。また、IoT ボットネットを利用した大規模な DDoS 攻撃も行われました。

・2018 年の平昌オリンピックでは、標的型マルウェア「Olympic Destroyer」を用いた攻撃が行われ、会場の無線 LAN が使えなくなり、チケットの印刷が出来なくなる障害が発生しました。感染の発端は組織委員会の内部ではなく、大会に関連する海外の IT サービス会社でした。

(2) 個人を狙った攻撃

例年以下のような事象が発生しています。個人情報の窃取や金銭が目的と考えられます。

・オリンピックに関わる内容のフィッシングメールを不特定多数に送りつける

・公式サイトを改ざんし、閲覧者にマルウェアをダウンロードさせる

・競技会場にて偽の無線 LAN アクセスポイントを設置し、来場者にアクセスさせる

次章では、平昌オリンピックで被害のあった「サプライチェーン攻撃」について説明します。

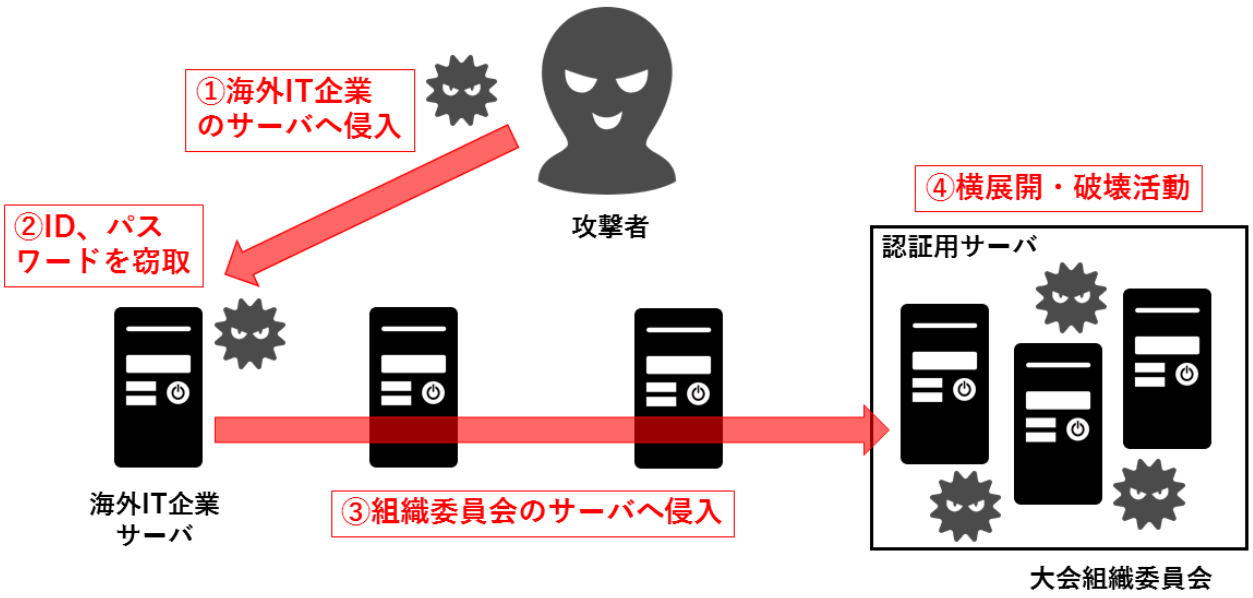
3. サプライチェーン攻撃の手法と対策

サプライチェーン攻撃とは、標的企業を直接狙うのではなく、業務関係があり比較的セキュリティ対策がなされていない企業のシステムを乗っ取り、本命の標的企業を狙う攻撃です。または、ベンダーが発行するソフトウェアを改ざんし、ソフトウェア利用者にマルウェアをダウンロードさせる「ソフトウェアサプライチェーン攻撃」を指します。

攻撃方法に関して詳細は過去に取り上げている以下の記事をご参照ください。
『サプライチェーン攻撃の脅威と対策について』
https://www.ssk-kan.co.jp/topics/topics_cat05/?p=9606

(1) 2018 年平昌オリンピックでのサイバー攻撃事例

以下の図は、2018 年平昌オリンピックにて実際に行われた攻撃を示しています。標的型マルウェア「Olympic Destroyer」により、大会本部のサーバに障害が発生しましたが、発端は大会に関係する海外の IT サービス企業でした。



【図 1】2018 年平昌オリンピックで確認された「Olympic Destroyer」による攻撃の流れ

① 攻撃者が、大会に関係する企業の端末をマルウェアに感染させる。
② ①の端末から、ID やパスワードを窃取する。
③ ②で窃取した情報をもとに、マルウェアを大会組織委員会のサーバへ侵入させる。
④ 大会組織委員会のサーバにてマルウェアが横展開し、ファイルの破壊活動を行う。

このように本命の標的企業のセキュリティが強固であっても、関係企業を踏み台にすることで、直接侵入するよりも比較的簡単に侵入することができます。攻撃者は関係企業や標的企業にマルウェアを展開し、機密情報を窃取することも可能です。実際に委託業務を行う委託先企業が不正アクセスを受け、個人情報などの機密情報が外部に漏えいする事案が報じられています。

サプライチェーン攻撃は IPA の「情報セキュリティ 10 大脅威 2021 [組織編]」でも 4 位にランクインしています。関係企業・委託先企業のセキュリティ対策が不足していることの危険性を認識する必要があります。

(2) サプライチェーン攻撃の対策について

サプライチェーン攻撃に対しては、企業・団体の規模や業種にかかわらず、セキュリティ対策を強固にしておくことが必須です。人的対策としては、例えば以下のような対策が挙げられます。

・脆弱なネットワークを使用しない
・不審なファイルをダウンロードしない
・不審なメールを開かない
・不審なファイルを実行しない

サプライチェーン攻撃は情報セキュリティを担当する部署だけでなく、社内全体、社員一人一人への徹底した周知が必要です。また、サイバー攻撃を想定した訓練を実行して、初動対応の流れを掴んでおくとなお良いでしょう。

4. オリンピック開催中のセキュリティ対策注意点

オリンピックでは企業、個人問わず様々なサイバー攻撃を受けることが予想されます。例えば以下のような攻撃が考えられます。

・関係団体

大会組織委員会に対する DDoS 攻撃や、選手村や競技場など大会に関わる自治体に対する標的型メール攻撃を受ける可能性が考えられます。

・社会インフラ

電気ガス水道、通信といった社会インフラ業界を中心に、一般企業も攻撃を受ける可能性があります。平昌オリンピックで猛威を奮ったサプライチェーン攻撃に引き続き注意を払う必要があるでしょう。個人情報を含む機密情報の漏えいなどが懸念されます。

・個人

SNS やメール、無線 LAN などに気をつける必要があります。大会のチケットや中継の視聴に関するスパムメールやフィッシングメール、公共の Wi-Fi を悪用した個人情報の窃取が挙げられます。

そして、企業、個人ともに IoT 機器への攻撃も忘れてはいけません。オリンピックでは、入場者の管理、ネットワークカメラによる中継を始めとして様々な場面で IoT 機器が普及しつつあります。IoT 機器は便利な反面、機器が増加すればするほど、それだけ攻撃対象が増えることになります。家庭でも Wi-Fi ルーターや TV、ブルーレイレコーダーなど、ネットワークに接続している機器は狙われる危険があり、個人も攻撃の対象となりえます。

IoT 機器は一般に CPU 性能やメモリ容量が少なく、セキュリティソフトを導入できないため、マルウェアに感染しやすい傾向にあります。2016 年には「Mirai」と呼ばれる IoT 機器を狙ったマルウェアが大流行しました。攻撃者は多数の IoT 機器を感染させ、それらの機器を用いて企業などへ DDoS 攻撃を仕掛けます。DDoS 攻撃によるサービスの停止が懸念されるため、今回の東京オリンピックでは大会本部、関係機関・団体や通信インフラにおいて万全のセキュリティ対策が行われているでしょう。

一般的な IoT 機器への攻撃対策としては、IoT 機器を直接インターネットに接続することは避け、セキュリティ対策を行っているネットワークに接続すること、ソフトウェアのアップデートを行い、最新の状態を保つことが挙げられます。

攻撃方法に関して詳細は過去に取り上げている以下の記事をご参照ください。

『IoT 機器に対するサイバー攻撃の脅威と対策』

https://www.ssk-kan.co.jp/topics/topics_cat05/?p=9126

いずれの場合においても自分は関係ないと思わず、一人一人が攻撃と対策を理解し、万が一のケースが発生した場合でも対処できるよう心がけておくことが肝要です。e-Gate センターでも東京オリンピック・パラリンピック開催期間中における攻撃動向を詳細に分析し、注意喚起を行ってまいります。

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 2021

https://www.ipa.go.jp/files/000088835.pdf

・独立行政法人情報処理推進機構（IPA）

東京 2020 オリンピック・パラリンピック競技大会に向けて～SC3 会員企業・組織の経営者へのサイバーセキュリティ対策に関するメッセージ～

https://www.ipa.go.jp/files/000092539.pdf

6. e-Gate の監視サービスについて

e-Gate のセキュリティ機器運用監視サービスでは、24 時間 365 日、リアルタイムでセキュリティログの有人監視を行っております。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い、通信が攻撃かどうかの分析、判断をして、セキュリティインシデント発生時に適切に対処できるようにすることが重要です。e-Gate のセキュリティ監視サービスをご活用いただきますと、迅速なセキュリティインシデント対応が可能となります。

また、e-Gate の脆弱性診断サービスでは、お客様のシステムにて潜在する脆弱性を診断し、検出されたリスクへの対策をご提案させていただいております。

監視サービスや脆弱性診断サービスをご活用いただきますと、セキュリティインシデントの発生を予防、また発生時にも迅速な対処が可能なため、対策コストや被害を抑えることができます。

■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」と最新のメソッドで構築した「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”サービスです。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/

«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