ワークショップ
脅威インテリジェンスを使った防御策の設計

株式会社ワールドスカイ

架空会社「ABC株式会社」が直面したフィッシング攻撃

Worldsky

■企業概要

企業名：**ABC株式会社**

事業内容：**中小企業向けのサービス提供**

従業員数：**50名**

＜背景＞

架空企業ABC株式会社は、経理・会計業務を担当するチームがあり、請求書や支払い関連のメールを日常的に受信しています。最近、複数の従業員が偽の請求書メールを開いてしまい、機密情報が漏洩し、運営が一時停止する事態になってしまいました。今後の対応として、同様のフィッシングメールに対応できるようにするため、脅威インテリジェンスを活用した対策を進めていくことにしました。進め方としては四半期に1回、脅威についての調査結果を分析し、脅威インテリジェンスレポートとしてまとめることにしました。

作成された脅威インテリジェンスレポート

1. よくあるフィッシング手法

請求書や振込依頼のメール: 「支払いが未処理です」といった急を要する内容や「振込依頼」など、受信者が緊急に対応しなければならないと感じるメッセージが多い。偽のリンクや添付ファイルを含み、クリックやダウンロードによって攻撃者に情報を渡してしまう可能性がある。

配送通知を装ったメール: 「配達物が届きましたが、不在のため受け取りできませんでした」という内容でリンクをクリックさせようとするもの。配送業者のロゴや、普段見慣れたフォーマットを使用して信頼性を高めている。

アカウント確認依頼: 「アカウントがロックされました。確認のためこちらにアクセスしてください」などの内容。本物のサービスに見せかけたログインページへ誘導し、認証情報を取得しようとする。

2. 攻撃者の目的

資金詐取: 偽の請求書を送りつけて支払わせたり、不正送金を促す。

機密情報の盗難: 特定の企業の顧客情報や営業機密を狙い、売買や転売によって利益を得る。

システム破壊・業務妨害: 不正アクセスでシステムをダウンさせたり、業務を停止させることで企業に損害を与えることを狙う。

3. 最近の傾向（トレンド）

本物そっくりの攻撃: 送信元のドメイン名やメール内容が非常に信頼性が高く、本物そっくりに作り込まれている。例えば、ドメイン名の一文字を変えて正規のドメイン名に似せるなど。

中小企業向けにカスタマイズされた攻撃: 中小企業を狙い、業務に合わせた内容でフィッシングメールを送ることが増えている。

個人ワーク（15分）

1. 脅威インテリジェンスレポート内容から、どのようなことに注意すればフィッシングメールに引っかからないようにできるか、について考えてみてください。

2. 別紙、自社のシステム管理部門から届いたメールから、怪しいと思うところを指摘し、そう感じた理由を簡単に記してください。

   付加情報：自社ドメインは、abc-company.com

グループワーク（25分）

1. 組織としてフィッシング攻撃を防ぐために、どのような対策が必要かを話し合ってください。

2. 個人ワーク２で指摘したい内容をグループメンバーに共有し、「怪しい箇所のリスト」を作ってください

サンプルメール

差出人：システム管理部 <system-admin@abc-security.com>
宛先：あなたのメールアドレス
件名：【重要】アカウントセキュリティ更新のお願い

平素より弊社システムをご利用いただき、誠にありがとうございます。
最近、セキュリティ強化の一環として、全社員のアカウント情報の確認と更新を行っております。つきましては、以下のリンクよりログインし、パスワードの再設定と情報の確認をお願いいたします。

[アカウント情報の確認・更新はこちら](http://abc-security-update.com/login)
※本メール受信後、**24時間以内**にご対応いただけない場合、アカウントが一時的にロックされる可能性がございます。

ご不明な点がございましたら、システム管理部までお問い合わせください。
何卒よろしくお願いいたします。

株式会社ABC
システム管理部
電話：03-1234-5678
メール：support@abc-company.com


Worldsky