2018 年 10 月 22 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：ビジネスメール詐欺による脅威と対策

1. 概要

働き方改革が注目を浴びる中、ビジネスコミュニケーションツールとして企業向けチャットツール（メッセージアプリケーション）が年々普及しています。一方で依然として電子メールは企業間の重要なコミュニケーションツールとして位置づけられています。

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 2018』では第 3 位に「ビジネスメール詐欺による被害」がランクインしております。2018 年 8 月 27 日には IPA より、日本語によるビジネスメール詐欺（Business E-mail Compromise：BEC）の注意喚起が行われました。また、警察庁もビジネスメール詐欺に関する注意喚起サイトを開設しています。

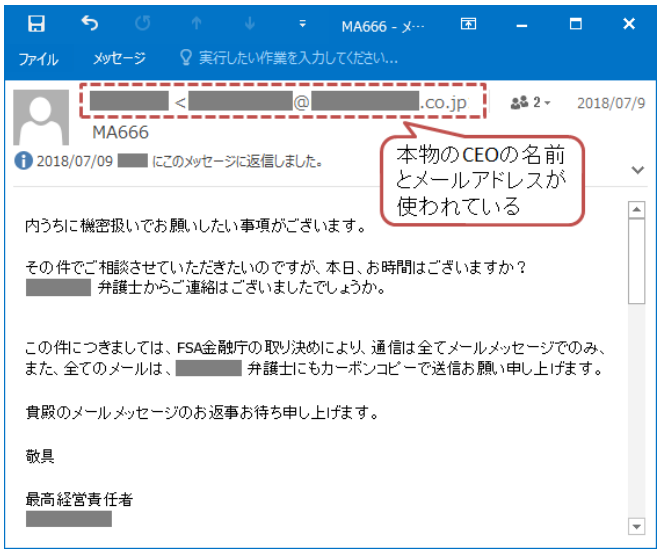
英文や不自然な日本語を使用した内容のメールは受信者も警戒していましたが、自然な日本語によるメールが増えるなど、攻撃は高度化、巧妙化し続けており、企業はさらなる対策を求められています。

2. ビジネスメール詐欺とは

ビジネスメール詐欺は企業で使用するメールを利用した詐欺行為です。

メールを盗聴することで取引状況を把握し、請求・支払などの絶妙なタイミングでなりすましメールを送信して、攻撃対象者を騙します。送信者のメールアカウントを乗っ取る、もしくは類似のドメインのメールアドレスからのメールを偽装するため、ビジネスメール詐欺であることに気付きにくいことが特徴です。

ビジネスメール詐欺の攻撃フローは一般的に、メールのやりとりを盗聴して取引状況を把握するための情報収集活動と、なりすましメールを送信するなどの詐欺活動から構成されます。



【図 1 日本語のビジネスメール詐欺の一例（引用元 IPA）】

一例として以下のような一連の攻撃活動があります。

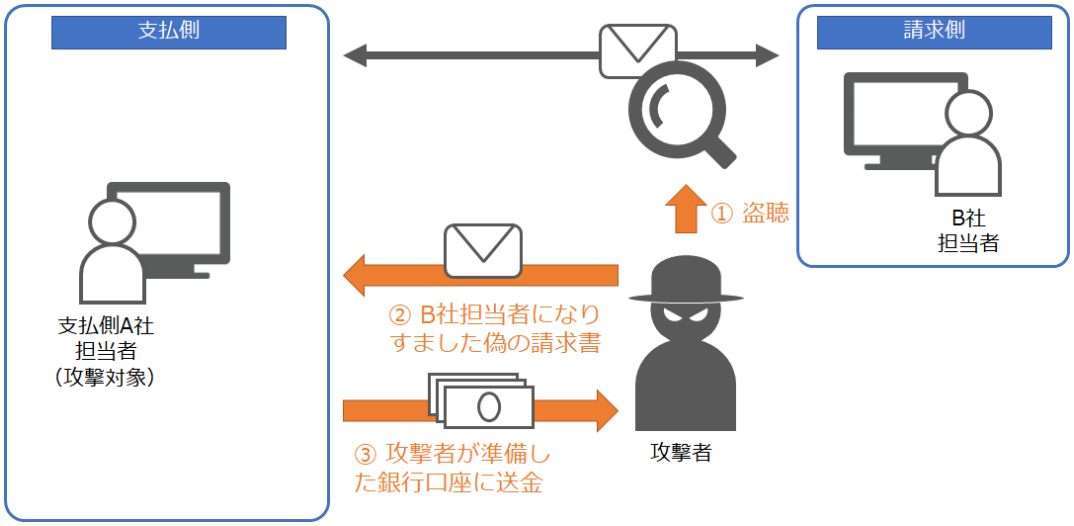
情報収集活動

① 攻撃者がキーロガー、通信の盗聴などによってメールのやり取りを把握。

詐欺活動

② 請求側の担当者になりすまして、支払側担当者に偽の請求書をメール送付。

③ 攻撃者が請求側担当者になりすました偽の請求書に支払側担当者は気付かず、攻撃者が準備した偽の銀行口座に送金。



【図 2】請求側担当者になりすましたビジネスメール詐欺

この他にもビジネスメール詐欺には以下のような種類があります。

- 会社幹部になりすまして、偽口座への振込指示を行う。
- 弁護士等、社外の権威ある第三者になりすまして、偽口座への振込指示を行う。

3. ビジネスメール詐欺への対策

ビジネスメール詐欺ではキーロガーや通信の盗聴以外にソーシャルエンジニアリング[1]によって重要情報を窃取するケースがあります。そのため、セキュリティ製品による技術的な対策だけではなく、管理的（人的・組織的）対策が求められます。

[1] social engineering. 個人が持つ秘密情報を、情報通信技術を使用せずに盗み出す方法

技術的対策

- 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 の導入。
- フィッシングサイトへの誘導など、情報収集活動から防御するためのメールセキュリティ製品の導入。
- 不正プログラム感染から防御するためのエンドポイント対策製品の導入。
- 標的型攻撃対策製品の導入。

管理的対策

- 取引に関する異例な要求のメールに対する運用体制の整備。
- ビジネスメール詐欺についての社内理解度を高めるためのセキュリティ教育や訓練。
- 従業員の肩書などをソーシャルメディアや企業サイトに公開することによる不正利用のリスク評価。
- 送金に関する社内規定や体制の整備（内部統制の整備と運用）。

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。SSK の総合セキュリティサービス「e-Gate」では、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」のセキュリティ監視サービスをご活用頂くことにより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。

■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）
  【注意喚起】偽口座への送金を促す“ビジネスメール詐欺”の手口（続報）
  https://www.ipa.go.jp/security/announce/201808-bec.html

- 警察庁 サイバー犯罪対策プロジェクト
  ビジネスメール詐欺の手口
  https://www.npa.go.jp/cyber/bec/main1.html

※本資料には弊社が管理しない第三者サイトへのリンクが含まれています。各サイトの掲げる使用条件に従ってご利用ください。リンク先のコンテンツは予告なく、変更、削除される場合があります。

«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