中小企業のセキュリティ対策

ビジネスメール詐欺に注意

（独立行政法人情報処理推進機構・江島将和）

攻撃の手口と対策　レポートを公開

電子メール（以下、「メール」）は取引先とのビジネスや日常の業務を行うために欠かせない。それ故に、攻撃者にとっても企業組織を攻撃するための格好の手段となる。メールを悪用した攻撃では、「人の心理的な弱点に付け込む」もしくは「相手に対する信頼感を逆手に取り」ターゲットをだますソーシャルエンジニアリングの手法が昔から多用され、その手口には大きな変化はない。

独立行政法人情報処理推進機構（IPA）が開設している「企業組織向けサイバーセキュリティ相談窓口」には、メールを悪用した攻撃の被害に関する相談が多数寄せられている。IPAはこれを受け、企業組織を狙うメールを悪用した攻撃の手口、発生する被害、対策を解説したレポートを公開した。本稿ではその中から「ビジネスメール詐欺」について紹介する。

ビジネスメール詐欺とは、巧妙なだましの手口を駆使した偽のメールを企業組織に送り付け、従業員をだまして攻撃者の用意した口座へ送金させる詐欺の手口である。代表的な手口として以下に示す二つのタイプがある。

企業を狙う　なりすまし事例

■タイプ１：取引先との請求書の偽装

タイプ１（**下図**）は、海外の取引先との間で発生することが多く、攻撃者が、被害組織と取引先とのメールのやりとりを盗み見ることから攻撃が始まる。攻撃者は、途中から取引先になりすまして、被害組織の担当者に偽のメールを送る。ビジネスメール詐欺で使われる典型的な偽のメールには、支払いに使う送金先口座の変更依頼が書かれている。指定された口座は、取引先になりすました攻撃者のもので、送金した資金を奪われてしまう。

攻撃者が、取引先のメールアカウントに不正ログインして、取引先の正規アカウントからメールを送信する場合があること、これまでのやりとりの途中で攻撃者が自然に割り込んでくることから、不正に気が付くのが難しく、被害につながる場合がある。

■タイプ２：経営者などへのなりすまし

タイプ２は、攻撃者が企業組織の経営者や幹部などになりすまし、企業組織の従業員に攻撃者の用意した口座へ振り込みをさせるというもの。このとき、事前に攻撃者はなんらかの方法によって、企業の役員などのメールアドレスを調べ、より本物らしくなりすましを行う場合もある。

タイプ１とタイプ２は共に、なりすます人物のメールアカウントを乗っ取り、正規アカウントから偽メールを送る。もしくは、なりすます人物の組織ドメインとよく似たドメイン名を取得した上で偽メールを送ることで、一見すると本人が正規のアカウントから送ったように見せかける巧妙な偽装が行われることもある。

企業組織向けサイバーセキュリティ相談窓口で受け付けた相談では、海外の取引先になりすました「タイプ１」の事例が多くを占めている。ビジネスメール詐欺の手口の詳細や、タイプ１とタイプ２の具体例については、IPAが公開している記事を参照していただきたい。

◇

本レポートの読者は、中小企業のシステム担当者や情報セキュリティ担当者を想定しているが、メールを悪用した攻撃は、組織の誰もがターゲットとなり得る。そのため、組織全体に対策を浸透させる必要がある。本レポートで解説している「さまざまな攻撃の手口」を知り、被害を防ぐための「事前の対策」や被害が発生した後の「事後の対応」に役立てていただきたい。

（会議所ニュース９月21日号（日本商工会議所発行）より転載）

「企業組織を狙うメールを悪用した攻撃の手口とその対策」についてはこちらを参照

図　詐欺の手口 タイプ１：取引先との請求書の偽装

