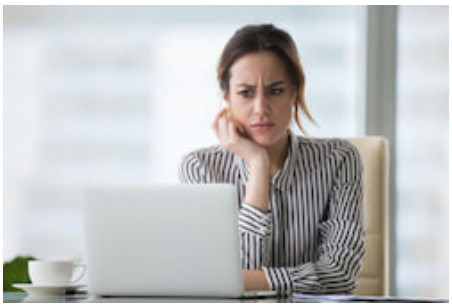
潜行するサイバー攻撃（第8回）

FBIから届いた「偽メール」の正体

2022.01.05



ビジネスはもちろん、プライベートでも広く利用されている便利な電子メール。しかし最近、その安全性を揺るがす事件が発生して話題になった。舞台となったのは米国FBI（連邦捜査局）。同局の正式なメールアカウントから大量の偽メールが送信された。なぜこのようなことが起きたのか、これまでに判明した情報から考えてみたい。

2021年11月13日（現地時間）、米国FBIから「公式メールアカウントが乗っ取られ、偽の電子メールが送信された」との発表があった。メールの内容は某セキュリティ関連企業の創業者を非難する類のものだった。送信元のアドレス末尾はFBIを示す「fbi.gov」。正規のメールサーバーを通じて送信され、世界各国10万件以上のメールアドレスに偽メールが送り付けられる事態になった。FBIは問題発覚後、直ちに当該サーバーを停止するとともに、被害状況の把握と原因究明に乗り出した。

その後、攻撃者とみられる人物からジャーナリストに連絡が入り、自らの行為を説明する異例の展開となった。「Pompompurin」と名乗る攻撃者は、FBIのシステムの脆弱性を指摘するのが攻撃の目的だとし、FBIが関係機関に提供するポータルサービス「Law Enforcement Enterprise Portal（LEEP）」の設定の問題を悪用してシステムに侵入、偽メールを送信したと語った。続いて11月15日にFBIからも同様の内容が発表され、図らずも攻撃者の解説を追認する形となった。

偽メールは確かにFBIのメールサーバーから送信されていたが、このサーバーはLEEP専用に使われるもので、データの窃取や機密情報漏えいにつながる恐れはないとFBIは発表している。この事件は個人のハッカーが引き起こした愉快犯的犯罪に分類されるが、これまで偽メールを見抜く手段として一般的だった「正規のドメインか確認する」という方法が、攻撃者がサーバーを乗っ取ることで簡単に破られてしまう問題を明らかにした。

巧妙化する「なりすまし」「フィッシング」… 続きを読む