不正アクセスの被害状況公開

一般的な対策も有効

独立行政法人情報処理推進機構（ＩＰＡ）では、経済産業省の告示に基づき、コンピュータウイルスなどによる被害の状況把握や対策検討を目的として、コンピュータウイルス・不正アクセスに関する届け出を受け付けている。２０２２年下半期（7～12月）に届け出のあった被害について全体を通して見ると、これまでと同様に、一般的によく知られたセキュリティ対策を実施していれば、被害を防ぐことができたと思われるものが多かった。今回は届け出の中から特徴的な被害事例を二つ紹介する。

【事例①】ＶＰＮ装置の脆弱性を悪用したサイバー攻撃

届け出企業の複数台のサーバーとパソコン上のファイルが暗号化され、脅迫文とみられるテキストファイルが残されていたことに従業員が気付いた。脅迫文や暗号化されたファイルの拡張子などから、Ｃｒｉｎｇ（クリング）と呼ばれるランサムウエアの攻撃を受けたものと推定している。原因については、不審なＶＰＮ（仮想専用線）接続ログが見つかったことから、ＶＰＮ装置の脆弱（ぜいじゃく）性を悪用して社内に侵入されたものと推測している。発覚後、ファイルが暗号化された機器はネットワークから切断した上で、全ての機器に対してセキュリティソフトでのフルスキャンを実施した。被害を受けたサーバーは、約2週間前のバックアップデータを基に復旧作業を行った。再発防止策として、従来のセキュリティソフトに加え、不審なプログラムの動作を検知し、抑止する機能を持つ別のセキュリティソフトを導入した。さらに、資産管理ソフトの導入により、管理者によるアプリケーションの利用制限を行う仕組みとした。

【事例②】初動対応後に再度の攻撃と複数の影響が発生した被害

届け出企業が運用するレンタルサーバーのウェブサイト上に不審なページが公開されていることをレンタルサーバーの提供会社から連絡があった。調査の結果、サーバー内に複数のフィッシングサイトが設置されており、さらに、フィッシングサイトに入力された認証情報を外部にメール送信しようとした痕跡も確認された。しかし、メールは導入していた誤送信防止システムにより、外部への送信には至らなかった。その後、届け出企業が復旧作業を進める中で、サーバーが動作不能な状態となったため、再調査を行ったところ、サーバー上のシステム領域も含めたファイルの消去が行われたことが判明した。原因は、脆弱なバージョンのＣＭＳ（Ｍｏｖａｂｌｅ Ｔｙｐｅ＝コンテンツ管理システム）を使用していたため、その脆弱性を悪用した攻撃を受けたものと推測している。対応として、当初、脆弱性の存在に気付かず、不正に作成されたサイトを削除するなどの措置であったため、再び不正アクセスが確認されたことから、ウェブサイトを停止し、社外からウェブサーバーへのアクセスを遮断した。再発防止策として、ウェブサイトを閉鎖し、不正アクセスの原因に対する対策を実施した上で、セキュリティが強化されたサービスへと移行した。

ＩＰＡの報告書活用を

本事例の詳細や、その他の被害事例については、ＩＰＡのホームページに報告書が掲載されているので確認してほしい。

同様被害の早期発見や未然防止といったセキュリティ上の取り組みの促進につながることを期待する。

（独立行政法人情報処理推進機構・江島将和）

コンピュータウイルス・不正アクセスに関する届け出について

事例②初回の攻撃の流れのイメージ