23年上半期の被害状況を公開

一般的な対策で攻撃は防げる

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。2023年上半期（1～6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

届け出企業の従業員から、ファイルサーバーにアクセスできないとの報告があった。確認したところ、当該サーバー内のファイルが暗号化され、脅迫文が残されていることを発見した。調査の結果、ランサムウエア「LockBit（ロックビット）3.0」による被害であることを確認した。また、この被害により、サーバー内に保管していた数万件の個人情報などが流出した可能性があることが判明した。

さらに、サーバー内のデータが暗号化された状態でバックアップ処理が行われたため、遠隔地に設置しているバックアップサーバーにも影響が及んだ。侵入の原因は不明だが、VPN（仮想専用線）装置の脆弱（ぜいじゃく）性を悪用されたものと推測している。

対応として、侵害の原因となったVPN装置のファームウエア（ハードウエアを制御する内臓ソフトウエア）のアップデートや設定の見直しを行った。また、感染したサーバーについては初期化したのち、暗号化の影響を受けなかったバックアップサーバーのデータから復旧させた。

再発防止策として、EDR（EndpointDetection and Response＝パソコンやサーバーにおける不審な挙動を検知し、迅速な対応を支援するセキュリティソリューション）の導入などを行った。

未然防止へ事例の活用を

【事例②】ソフトウエア配布サイトから取得したツールのプロキシ機能に起因する不正アクセス被害

届け出企業が使用するグローバルIPアドレスが、外部のインターネットバンキングにおいて発生した不正アクセス事案のアクセス元になっていると、外部機関より連絡があった。

調査の結果、組織内の従業員が使用していたパソコンに、第三者の通信を中継する機能を持ったツールがインストールされており、攻撃者がその機能を経由して、インターネットバンキングに不正アクセスしていたことが確認された。

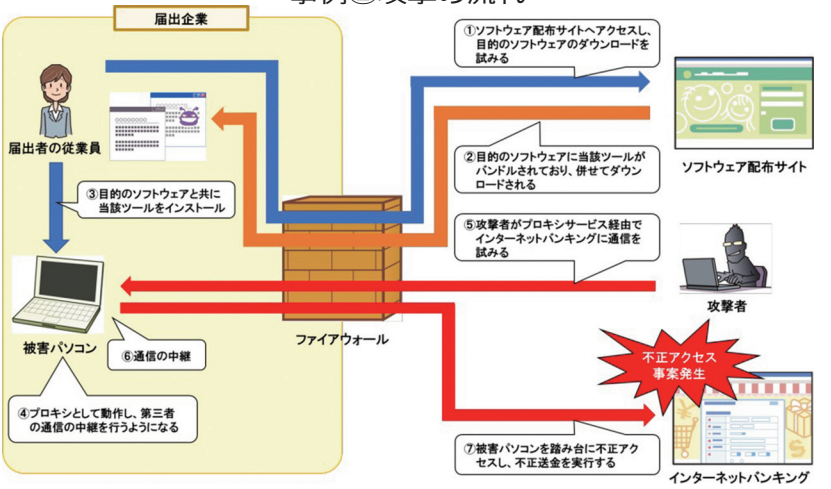
当該ツールが被害パソコン上に存在していた原因について、届け出者は、ソフトウエア配布サイトからダウンロードした本来の目的であるソフトウエアに当該ツールがバンドルされて（付属して）おり、従業員が誤ってインストールしてしまったと推測している。

被害対応として、外部機関へ報告・相談するとともに、発見した当該ツールの削除、同様の事象が発生している機器の有無の調査、当該ツールをバンドルして配布していた可能性があるウェブサイトへのアクセスの遮断、外部業者によるフォレンジック調査（専門技術による証拠収集・分析）などの技術的対応を行った。フォレンジック調査の結果、踏み台（被害パソコン）以外の不正操作や情報の改ざん、漏えいなどの被害は確認されなかった。

紹介した事例の詳細や、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。

事例②攻撃の流れ



（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