22年度上半期の被害状況を公開

特徴的な事例を紹介

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（QRコード参照）。2022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、被害を防げ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】PDFファイルを悪用したサイバー攻撃

届け出企業で、社内から外部の不正なウェブサイトへの通信が発生したことを検知し遮断した。外部からダウンロードしたPDFファイルに不正サイトへのリンクが含まれており、社内のパソコンで当該PDFファイルを開いたことで不正サイトへの通信が発生したとみられる。通信の検知後に、当該のパソコンに対し、セキュリティソフトによるスキャンを実施したところ16件の疑わしいファイルが検知された。なお、パソコンは検知後に初期化したため、不正なPDFファイルとの関係は不明である。また、セキュリティソフトで社内の機器に対してウイルススキャンを行ったところ、ファイルサーバから6個の疑わしいファイルが発見されたため削除した。これらのファイルは数年前から存在していた。

再発防止策として、全てのパソコン・サーバに新たなセキュリティソフトの導入と、不正な通信を検知し遮断するファイアウォールの精度を向上させるための設定を行った。

【事例②】複数の脆弱性とBitLockerを悪用した侵入型ランサムウエア攻撃

届け出企業のシステム管理者に、従業員から使用するパソコンでBitLocker（データを暗号化して閲覧できなくする機能）が設定していないのに稼働しているとの連絡があった。さらに社内システムへの接続不可に関する問い合わせの連絡があり、調査したところ、基幹システムのサーバにおいてもBitLockerによる暗号化がされていることが判明した。その後の調査により約130台のパソコンやサーバでBitLocker機能による暗号化が行われており、多数のシステムが停止を余儀なくされていたことが確認された。原因は不正アクセスによるものであり、VPN（インターネット上の、特定の人だけが利用できる仮想専用線）装置の脆弱（ぜいじゃく）性を悪用して認証情報を窃取した攻撃者が侵入し、さらにドメインコントローラ（コンピュータのアクセス権限等の管理／認証を行うコンピュータ）の脆弱性を悪用して、その管理下の複数の端末へ被害を広めていたことが判明した。

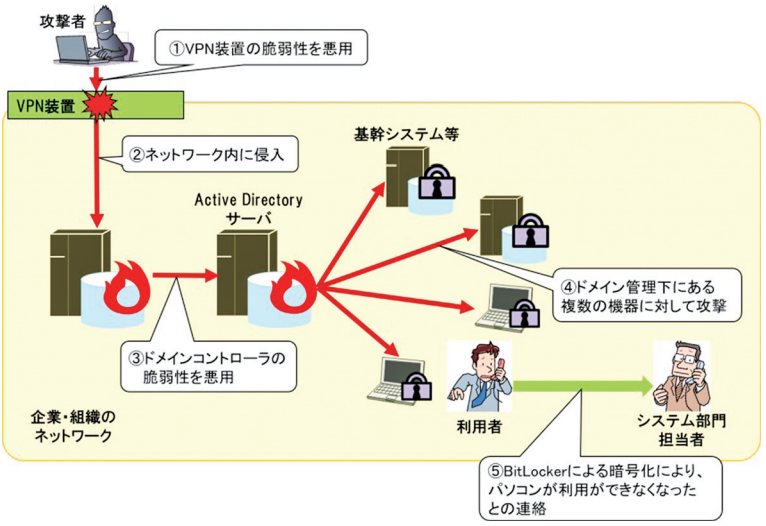
対応として、被害を受けたパソコンとサーバは初期化し、バックアップデータを用いて復旧を行い、各端末のウイルススキャンや修正プログラムの適用を行った。再発防止策として、ドメインコントローラやネットワーク機器への脆弱性対策運用の確立、SSL-VPN（SSL暗号通信でつなぐVPN）サービスの全てのアカウントのパスワード変更などを行った。

◇　◇　◇

各事例の詳細や、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）

侵入型ランサムウエア攻撃の流れのイメージ



コンピュータウイルス・不正アクセスに関する届け出はこちら