ＩＳＩＳＳ通信

Ishikawa Small and Medium Businesses Information Security Support News

Ｈ29．7
Ｖol.11

クローズドネットワークを狙ったサイバー攻撃の手口!!

企業が保有する機密情報については、独立したクローズドネットワークで保存・運用する方法が普及していますが、この様なインターネットと隔離されたネットワークに保存された情報を狙う手口が発見されました。

○ 情報窃取の手口

① 攻撃者は、インターネットに接続された事務用ネットワーク端末をウイルスに感染させる

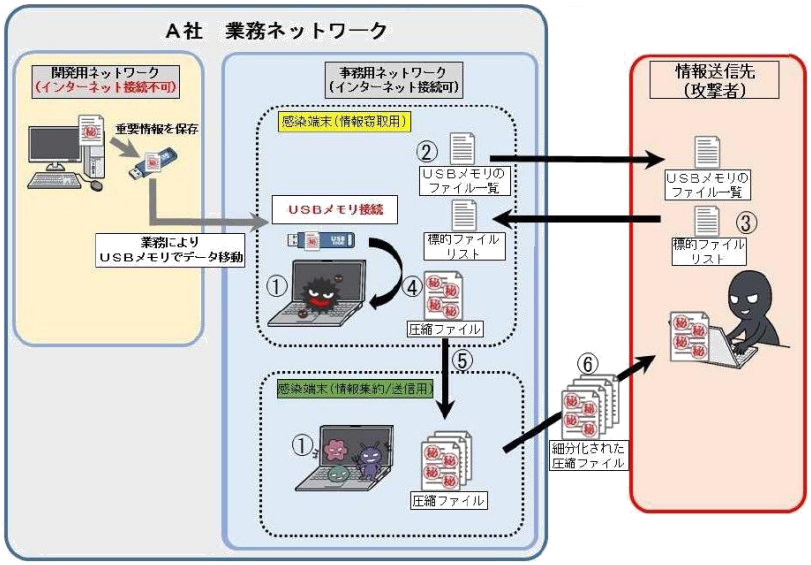
② ＵＳＢメモリが感染端末（情報窃取用）に接続されるとウイルスが起動し、ＵＳＢメモリに保存された情報の「ファイル一覧」を作成して、端末に保存する

③ 攻撃者は、インターネットを通じて「ファイル一覧」を取得し、一覧から窃取したい「標的ファイルリスト」を作成の上、感染端末（情報窃取用）に送信する

④ 感染端末（情報窃取用）のウイルスは、ＵＳＢメモリに保存された情報のうち、リストで指定されたファイルを圧縮して端末に保存する

⑤ 圧縮されたファイルは、事務用ネットワークの感染端末（情報集約/送信用）に送信される

⑥ 感染端末（情報集約/送信用）のウイルスが、圧縮ファイルを加工・細分化し、攻撃者へ送信する



○ 対策の一例

① 感染の調査方法

パソコンの「C:¥intel¥logs」や「C:¥Windows¥system32」の下に、

- 正規の実行ファイルに似た名前のファイル（「intelu.exe」など）
- 「interad.log」などといった不正なファイル

などがないか確認する

② 情報漏えい対策

機密性の高い情報を扱うネットワークからデータを持ち出す際は、暗号化を行う

③ その他の一般的な措置

プロキシログの監視、ファイアウォールの設定やＩＰＳの導入、ウイルス対策ソフト、ＯＳやアプリケーションの最新版への更新などを行う

※ 詳しい情報は「＠ｐｏｌｉｃｅ（http://www.npa.go.jp/cyberpolice）」をご覧ください

サイバー犯罪（インターネットに関する犯罪）の通報やご相談は･･･

石川県警察本部生活環境課サイバー犯罪対策室

076−225−0110　cyber@police.pref.ishikawa.lg.jp