平成２８年９月２７日

８月中の不正プログラム関連情報

※　ニュースの内容は、各種報道、インターネット等で公表されている情報に基づくもので、県警が事実を確認したものではありません。

鳥取県警察本部サイバー犯罪対策室

○　日本人を狙うマルウェア「Aveo」

ITmedia ニュースは８月 17 日、セキュリティ企業のパロアルトネットワークスが、日本人を狙うマルウェア「Aveo」による標的型サイバー攻撃への注意を呼び掛けたと報じた。

Aveo は Excel ファイルのアイコンに偽装した①WinRAR 自己解凍型の実行ファイルで、ユーザーがこれを実行すると偽の文書やトロイの木馬がダウンロードされる。偽の文書は大学の研究室の Web サイトで公開され、研究会参加者の一覧が記載されている。文書は日本語になっており、同時にダウンロードされるファイル（トロイの木馬）の名称も日本語になっていることから、パロアルトネットワークスはこの攻撃が日本人を狙ったものだと指摘している。

ダウンロードされたトロイの木馬は遠隔操作型で、感染先のコンピュータから攻撃者が設置したとみられる米国の複数ドメインに接続し、盗んだ情報を送信したり、攻撃者の命令を受信したりしているとみられる。感染した当初は、感染したコンピュータの Windows のバージョン、IP アドレス、ユーザー名などの情報を送信することが分かっている。

Aveo はその後も感染したコンピュータのレジストリを改ざんするなどして潜伏を続ける。攻撃者からは②インタラクティブシェルでのコマンド実行、ファイルの入手、書き込み、読み込み、ドライブのリスト等の命令を受け取り、実行する。

パロアルトネットワークスによると、Aveo は 2015 年に「訃報」メール等を通じて国内のハイテク製造業を狙う標的型攻撃に使われたマルウェア「FormerFirstRAT」と多くの類似性がみられるとのことであり、同社は脅威検出の手掛かりとなる情報も公開している。

○　ランサムウェア「Locky」の感染メール、日本の病院を標的として大量流通

米セキュリティ企業のファイア・アイは８月 17 日、PC のファイルを人質に取って身代金を要求するランサムウェア「Locky」に感染させようとする詐欺メールが、日米を中心に大量に出回っているとして同社ブログで注意を呼び掛けた。

ファイア・アイによると、Locky 感染メールの影響を受けている国は米国に次いで日本が２番目に多く、次いで韓国の順となっている。狙われている業界は多岐にわたるが、特に病院等のヘルスケア業界が突出している。

Locky を操る集団は、感染数を増やす狙いで継続的に手口を変更していて、今回はマクロ機能を有効にした Microsoft Word ファイル「docm」形式の文書を添付した電子メールが８月上旬から集中的に出回り始めたという。

---

① RAR 形式で圧縮されたファイル
② スクリプト言語を対話的（インタラクティブ）に使用するために使われる文字ベースのシェル