平成２８年８月３０日

7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

○　2016 年上半期のランサムウェアの動向

ITmedia ニュースは７月６日、2016 年上半期の国内セキュリティ動向について、ランサムウェアによる脅威の拡大が注目されたとして、セキュリティ各社のレポートを紹介した。

ランサムウェアは、コンピュータをロックしたり、ファイルを暗号化したりして使用不能にさせ、その状態を解除するための身代金をユーザーに要求するマルウェアの総称。

トレンドマイクロによると、今年１月から５月末までの間に全世界で 6,600 万件以上のランサムウェア関連の脅威が検出された。国別で被害が多いのはブラジル、米国、トルコなど。日本は 14 位で、これらの国に比べて少ないものの、被害に遭った法人からの報告件数は急増しているという。感染経路はメールが最も多く全体の約 64％で、残り 34％が Web サイト、２％が USB メモリ等であった。

攻撃者は、メールから直接ランサムウェアに感染させるというより、メールに記載されたリンク先の Web サイトを閲覧した際に不正プログラムが実行され、ランサムウェアがダウンロードされてしまうといった複数の段階を経る場合が多いという。

また、ファイア・アイは、２月から３月にかけて国内で感染被害が目立ったランサムウェア「Locky」が攻撃を再び活発化させていると報告した。Locky はファイルの①拡張子を「.locky」に変更して、ファイルを使用不能にする。同社によれば、６月 21 日から 23 日にかけて、Locky に感染させるための②スパムメールが日本や米国、韓国を中心に多数観測され、攻撃全体の約半数が日本を狙うものであったという。スパムメールは、主に未払い料金の請求を装う内容で、受信者のコンピュータに Locky を送り込むための不正なプログラム（ダウンローダー）が ZIP ファイルとして添付されている。また、メールの解析や仮想的なコンピュータ環境の分析で攻撃を検知されないための方法を取り入れていることも確認された。Locky の攻撃の再燃は今後しばらく続くとみられ、ファイア・アイは国内の個人や法人に注意を呼び掛けている。

○　ファイルを削除してしまうマルウェア「Ranscam」

露セキュリティ企業カスペルスキーは７月 21 日、新たに現れたマルウェア「Ranscam」について、自社ブログで注意喚起した。

ランサムウェアは被害者のデバイスやファイルのロック解除等を名目として身代金の支払いを求めるが、Ranscam はランサムウェアのように身代金を要求しながら、裏でファイルを削除してしまう悪質なマルウェア。Ranscam に感染すると、被害者のデバイスには身代金を要求するメッセージが表

示される。メッセージには、0.2[3]ビットコイン（約 14,000 円相当）を支払えば、隠されたパーティションに移動し暗号化したファイルを元に戻す旨が書かれているが、実は、脅迫文を表示する前にファイルを削除してしまっているという。

ランサムウェアの流行に乗じた詐欺マルウェアと見られ、カスペルスキー社は注意を呼び掛けている。

---

① ファイルの種類を識別するために、ファイル名の末尾につけられる文字列
② 無差別かつ大量に本人の許諾を得ず、一方的に送られる営利目的の広告メール
③ インターネット上で使用できる仮想通貨