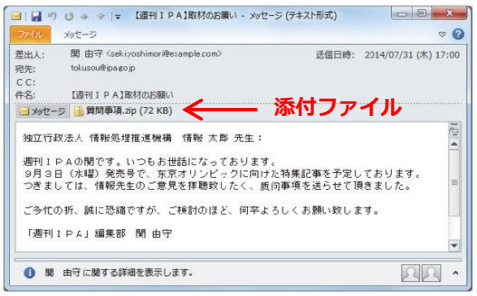
Ksisnet
京都中小企業情報セキュリティ支援ネットワーク
Ksisnetだより
平成28年3月18日 Vol. 9
発行：京都中小企業情報セキュリティ支援ネットワーク（Ksisnet）事務局

ランサムウェア「Locky（ロッキー）」*1による感染被害が多発!!

先日、京都府内の中小企業において、ランサムウェア（Locky:身代金要求型の不正プログラム）による被害が確認されました。同社では、定期的にデータのバックアップをとっていたことから、事なきを得ることができました。

どうしたら感染するの？（代表される2つの主な原因）

【受信メールの添付ファイル等からの感染】



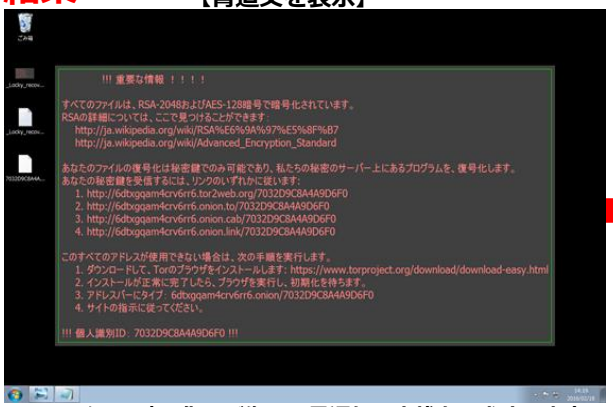
不用意に受信したメールに添付のファイルを開いたり、メール本文中のURLをクリックすることにより、不正プログラムが組み込まれたファイルが起動したり、ウェブサイトへ誘導され感染する被害が急増しています。

【ウェブサイトの閲覧等による感染】

最近では、改ざんされたウェブサイトを閲覧したり、不正プログラムが組み込まれたファイルをダウンロードすることによる感染被害が確認されています。

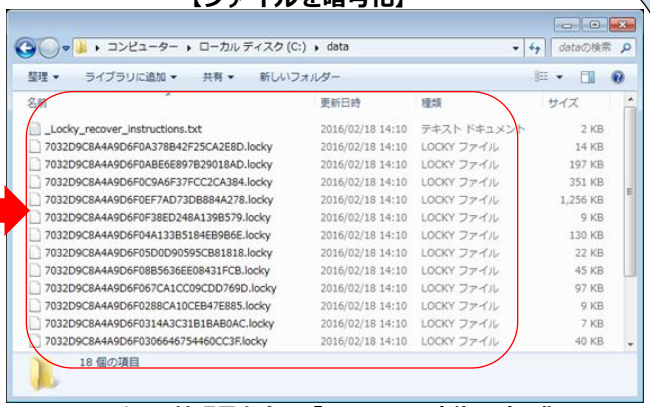
その結果

【脅迫文を表示】



ファイルの暗号化及び復元の見返りに金銭を要求する内容を強制的に表示

【ファイルを暗号化】



ファイルの拡張子を全て「.locky」に変換し暗号化

＊上記２画像は、トレンドマイクロ株式会社から引用

感染リスクの低減策（100%の対策は存在しないことに留意!!）

◎不審なメールは開かず、送信者・添付されたファイル（拡張子が.zip・.exeなど）・添付されたURL・文面を確認してください!!
◎ウェブサイトの改ざんは、URL等に変化がないため容易に発見できません!!
不用意にファイルやソフトをダウンロードせず、ウイルスチェックを徹底してください。
◎ウイルス対策ソフトやソフトウェアを最新の状態に更新してください!!（更新されていなければ、効果はありません）
◎大切なデータのバックアップを定期的に取りましょう。万が一、ランサムウェア等に感染しても、バックアップデータがあれば復元が可能です。ただし、バックアップに使用する媒体等は、バックアップ時のみパソコンと接続することが重要です。

お困りのときは!!

京都中小企業情報セキュリティ支援ネットワーク（Ksisnet）
ＩＴ相談窓口（公益財団法人京都産業２１ お客様相談室）
相談内容：情報セキュリティ対策、情報漏えい・流出事案等
※毎週月曜日～金曜日の９：００～１７：００（祝日を除く）
TEL 075-315-8660 メールアドレス okyaku@ki21.jp
公益財団法人京都産業２１ お客様相談室（〒600-8813 京都市下京区中堂寺南町134 京都府産業支援センター内）

別紙

※1 ランサムウェア「Locky」

ランサムウェアとは、身代金要求型の不正プログラムであり、感染するとパソコン内に保存している特定のファイル（オフィスドキュメント、圧縮ファイル、音楽、画像等）が勝手に暗号化処理され、さらに復元の引き換えとしてビットコイン等の金銭を要求する文面が表示されます。なかでも、「Locky」と呼ばれるランサムウェアは、世界各国の言語に対応した新種として日本国内でも感染被害が相次いでいます。