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．８
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

マルウェアについて再認識を!!

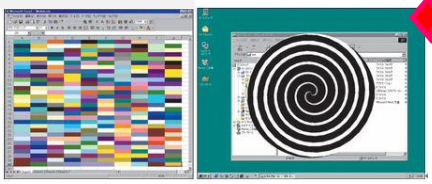
マルウェアとは、不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアの総称で、その種類には、ウイルス・キーロガー・ランサムウェア等があり、ユーザーが所有するファイル等の破壊、業務妨害、情報の窃取、金銭の要求等を目的としたものが挙げられます。
今回は、マルウェアの感染事例について、ご紹介します。

感染経路

感染経路は、受信したメールの添付ファイルやURLを不用意にクリックしたこと、ホームページを閲覧したりソフト等をダウンロードしたこと、感染している外部記録媒体をパソコンに接続したこと、ファイル共有ソフトからファイルをダウンロードしたこと等が考えられます。

感染例

【業務妨害】

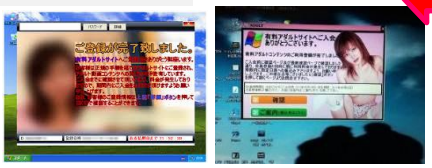


10年以上前から存在が確認されている業務妨害型ウイルスの感染事例です。
作業中のエクセルファイルを複数の色で塗りつぶしたり、パソコンの画面に渦巻き状の模様を表示して作業を妨害します。

【情報の窃取】

キーロガーと呼ばれる情報窃取型のプログラムに感染し情報を抜き取られる事例です。
ユーザーがキーボードに打ち込んだ1文字1文字をテキストファイル等で記録して読み取ります。
インターネットバンキング等のIDやパスワードを盗み取る手段として利用されています。

【金銭の要求①】



金銭要求型のプログラムに感染した事例です。
アダルトサイトを閲覧したユーザーのパソコンの記録を改ざんし、卑わいな文言や女性の裸体画像を表示させ、料金を支払うまで削除できないようにします。

【金銭の要求②】

ランサムウェアと呼ばれる身代金要求型のプログラムに感染した事例です。
標的型メール攻撃等に添付した実行ファイルを開かせる等により感染させ、ユーザーのデータを暗号化し、復号化する見返りとして身代金を要求します。30桁を超える暗号を用いるなど、データの復元を極めて困難にします。

感染リスクの低減策

感染リスクの低減策としては、不審なメールは開かない、ホームページから不用意にソフト等をダウンロードしない、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する、外部記録媒体はウイルスチェックした後にパソコンに接続するなどがあり、企業においては社員に周知徹底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）