Ksisnetだより
発行:Ksisnet事務局
令和５年 Vol. 2

Emotetの活動再開及び新たな手口に注意

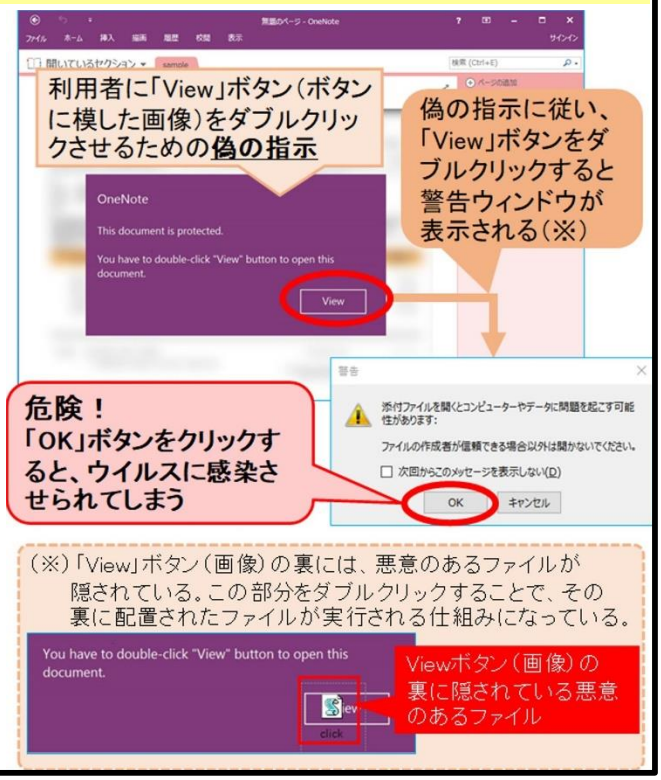
マルウェアEmotet（エモテット）は、令和４年11月上旬より攻撃メールの配信が確認されていない状態でしたが、先月７日から活動再開が確認されています。

また、新たにMicrosoft OneNote形式のファイルを悪用する手口と500MBを超えるWord文書ファイルを送信する手口が確認されています。

攻撃メールの件名や本文に日本語が使われているものもあることから、既に国内企業にも配信されている可能性が高いと考えられます。

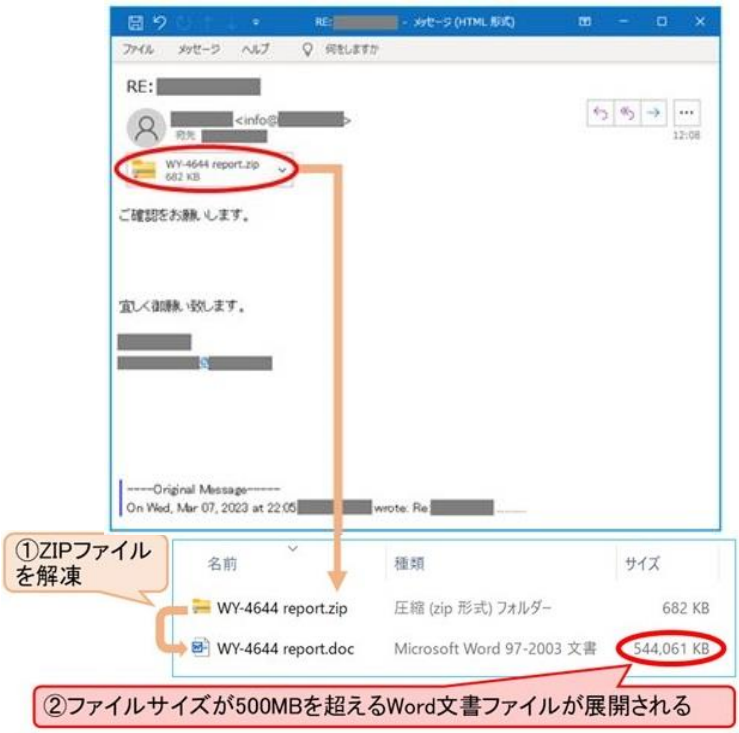
Microsoft OneNoteを悪用した手口

Microsoft OneNote形式のファイルを開き、偽の指示に従い「View」ボタンをダブルクリックすると、悪意のあるファイルが実行され、Emotetに感染する。



大容量のWord文書ファイルを送信する手口

ZIPファイルを解凍し、さらにWord文書ファイルの「マクロを有効にする」「コンテンツの有効化」を実行すると、悪意のあるマクロが実行され、Emotetに感染する。



【被害防止対策】

- Excel、Wordマクロの自動実行の無効化
- メールセキュリティ製品の導入によるマルウェア付きメールの検知
- メールの監査ログの有効化
- OSに定期的にパッチを適用、ウイルス対策ソフトの更新
- 定期的なオフラインバックアップの取得
- 組織内への注意喚起の実施
  （メールに添付されたデータは、送信元に内容確認後に開く等のルールを徹底）

参考　ＩＰＡ（情報処理推進機構）、JPCERT/CC