Emotetの感染拡大および 新たな攻撃手法について

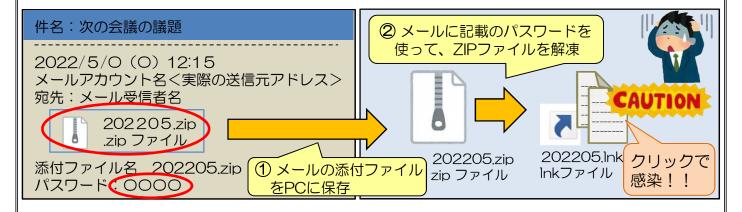


Emotetの感染に繋がる攻撃メールが急増しています。手口も巧妙化していますので、職場内での注意喚起が大切です。

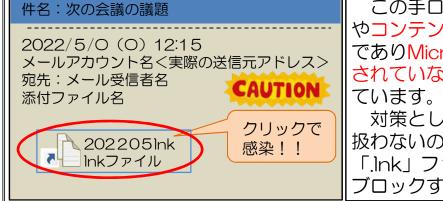
【新たな攻撃手法】

令和4年4月ころから、新たに確認された手口として、「ショートカットファイル(Inkファイル)をクリックするだけでEmotet等のコンピュータウイルスに感染する」ことが確認されています。

パターン1「.lnkファイル」が保存されたZIPファイルが添付されている場合



パターン2「.lnkファイル」が直接添付されている場合



この手口では、WordやExcelのマクロやコンテンツ有効化を必要としない方法でありMicrosoft Officeがインストールされていない環境でも感染するといわれています。

対策として、業務で「.lnk」ファイルを 扱わないのであればメールサーバー側で 「.lnk」ファイルが添付されたメールを ブロックする設定を行うことが有効です。

感染したかな?と思ったら

JPCERT/CCはコンピュータがEmotetに感染しているかどうかを確認できる EmoCheckV2.3.2を公開しています。感染が疑われる場合は活用してください。 無料ダウンロードURL https://github.com/JPCERTCC/EmoCheck/releases

