Emotet(エモテット)感染

2022.03.15

なぜEmotetの話を・・・

- 認証情報やネットワーク内にある機密情報も含めて外部へ流出し、悪用される恐れ
- Emotet自体には不正なコードが含まれていないためウイルス対策ソフトに検知されづらい
- 3月に入って、日本語で書かれた新たなEmotetの攻撃メールが確認

Emotetとは何ですか？

- メール経由で外部に感染が拡大
- メールに添付される
- 認証情報やネットワーク内にある機密情報も含めて外部へ流出し、悪用される恐れ
- Emotet自体には不正なコードが含まれていないためウイルス対策ソフトに検知されづらい
- 3月に入って、日本語で書かれた新たなEmotetの攻撃メールが確認

Emotetの対策

- 参考サイト
  - 警視庁
    - エモテット(Emotet)の感染を疑ったら
    - https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/joho/emotet.html
  - IPA
    - https://www.ipa.go.jp/
  - JPCERT/CC（ジェーピーサートコーディネーションセンター）
    - https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html
    - エモチェック

Emotetの対策

- 身に覚えのないメールの添付ファイルは開かない。メール本文中のURLリンクはクリックしない。
- 自分が送信したメールへの返信に見えるメールであっても、不自然な点があれば添付ファイルは開かない。
- OSやアプリケーション、セキュリティソフトを常に最新の状態にする。
- 信頼できないメールに添付されたWord文書やExcelファイルを開いた時に、マクロやセキュリティに関する警告が表示された場合、「マクロを有効にする」「コンテンツの有効化」というボタンはクリックしない。
- メールや文書ファイルの閲覧中、身に覚えのない警告ウインドウが表示された際、その警告の意味が分からない場合は、操作を中断する。
- 身に覚えのないメールや添付ファイルを開いてしまった場合は、すぐにシステム管理部門等へ連絡する。
    - JPCERT/CC（ジェーピーサートコーディネーションセンター）
        - https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html