サイバーセキュリティの置き薬

2022年 第12号

Emotet(エモテット)対策動画公開中！

現在、世界中で猛威を振るっている「Emotet(エモテット)」と呼ばれるウイルスに関する動画を作成しました。

- Emotetの特徴や感染経路
- Emotetによる被害事例
- 被害防止対策や感染した際の措置

について、分かりやすく説明しています。

動画投稿サイト「YouTube」
富山県警察公式チャンネル

動画はこちらから（YouTubeが開きます）

Emotetとは

主にメールの添付ファイルから感染する不正プログラムであり、感染すると、端末からメールアドレスやメール内容等の情報が窃取され、これを悪用して更にメールが拡散し、感染拡大してしまいます。

Emotetに感染すると…

以下のような被害が発生する可能性があります。

- メールソフトやブラウザに記録したパスワード、クレジットカード情報等が窃取される。
- 過去にやり取りしたメールの本文、メールアドレス等が窃取される。
- 窃取されたメールアドレス宛てに、感染拡大を目的としたメールが送信される。
- ネットワーク内の他のパソコンに感染が拡大する。
- 他のウイルスに感染する。

Emotetの被害に遭わないために

- 不審なメールは開かない。
- 送信元が確認できないときは、
  - 安易に添付ファイルを開かない。
  - パスワード付ZIPファイルを解凍しない。
  - メール本文中のURLリンクをクリックしない。
  - 文書ファイルの「コンテンツの有効化」ボタンをクリックしない。

OS、ウイルス対策ソフト、その他ソフトウェアを最新の状態に更新する等の一般的なセキュリティ対策も忘れずに！

【参考】警察庁：Emotetの解析結果について
https://www.npa.go.jp/cyberpolice/important/2020/202012111.html