サイバーニュース

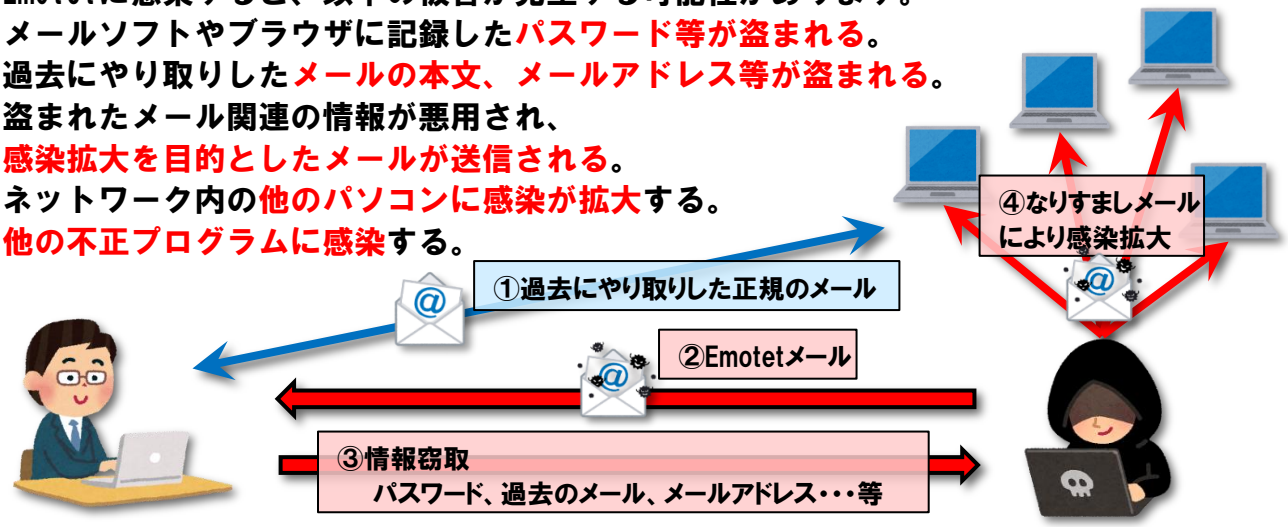
2022年5月
第４号

新たなEmotet(エモテット)について

Emotet（エモテット）は、主にメールの添付ファイルを感染経路とした不正プログラム（マルウェア）です。過去にやり取りしたメールへの返信を装ったメールを送信し、添付ファイルの開封を促します。

Emotetに感染すると、以下の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**パスワード等が盗まれる**。
- 過去にやり取りした**メールの本文、メールアドレス等が盗まれる**。
- 盗まれたメール関連の情報が悪用され、**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。
- **他の不正プログラムに感染**する。



これまでは、添付ファイルのマクロ機能を悪用されて感染していましたが、最近、ショートカットファイル（LNKファイル）を添付し、これをダブルクリックなどで開いた場合にEmotetに感染させる手口が新たに確認されています！

Emotetの対策について

ＯＳ、ウイルス対策ソフトなどを常に最新の状態に更新するといった**一般的なセキュリティ対策**に加え、

- **組織内への注意喚起**の実施
- **マクロの自動実行機能の無効化**
- **メールセキュリティ製品**の導入
- **不正通信ブロックサービス**の導入

などの対策を検討してください。

常に最新の状態へのアップデートをお願いします！

石川県警察本部生活安全部サイバー犯罪対策課
０７６－２２５－０１１０ cyber@police.pref.ishikawa.lg.jp