



Kagawa Cyber Security Information

香川県サイバーセキュリティ連絡ネットワーク通信Vol.52

マルウェア「Emotet」の感染攻撃に注意

2019年後半より被害が急増しているEmotet（エモテット）は、新型コロナウイルスに便乗するなどの内容が出回り、2020年2月以降目立った攻撃は収まっていました。

しかし、2020年7月中旬頃から、過去にEmotetに感染して窃取された情報が悪用されたと見られる攻撃メールが確認され、攻撃が活発化しています。

Emotetとは

当初はオンラインバンキングのID、パスワード等を盗むバンキングトロジャン(トロイの木馬)でしたが、現在は他のマルウェアをダウンロード・実行するものです。

特徴として

- 正規のメールを装う
 - ・ 実在する相手やメールアドレスを使っている
 - ・ 「返信」や「転送」の形式で送ってくる
 - ・ 新型コロナウイルス感染症等、社会の話題にしている
- Officeファイルが添付されている
- メール本文にURLが記載されている



等が挙げられます。

Emotetに感染すると

- パソコン内の情報を抜き取られる
 - ランサムウェアなど他のマルウェアをダウンロードする
 - Emotetをばら撒く踏み台とされる
- 等の被害が発生します。

未然に防ぐには

- 身に覚えのないメールは開かない
- メール本文中のURLはクリックしない
- 添付ファイルを開いた時、「マクロを有効にする」、「コンテンツの有効化」というボタンをクリックしない
- OSやセキュリティソフト等を常に最新の状態にする



感染してしまったら

- 感染したパソコンをネットワークから切り離す
- 使用していた全アカウントのパスワードを変更する