Counter-Terrorism Partnership Kagawa
テロ対策パートナーシップかがわ

会報
令和４年４月号

Emotetへの感染に注意!!

1 Emotetの特徴について

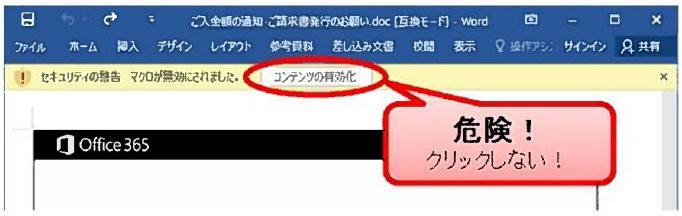
マルウェア「Emotet（エモテット）」には、
◆ 主にメールの添付ファイルを感染経路としたマルウェア
◆ 添付ファイルはOffice文書ファイルで、ZIP形式で圧縮されている場合もある
◆ Office文書ファイルを開きマクロを実行するとEmotetに感染
◆ 過去にやり取りしたメールの本文やアドレス帳、メールアカウント設定等の情報を窃取し、それを悪用して、他のパソコンへメールを送信することで感染を拡大
◆ 過去にやり取りしたメールに対する返信メールを偽装
などの特徴があります。

2 Emotetの活動再開について

マルウェア「Emotet」は、昨年1月27日のEUROPOL（欧州刑事警察機構）を中心とした撲滅作戦により活動を停止していましたが、昨年11月中旬頃から活動を再開していることが確認されています。

これまでに知られているEmotetでは、「Microsoft Outlook」を対象としてメール本文等の情報を窃取することが確認されていましたが、今回のEmotetではメールソフト「Thunderbird」も情報窃取の対象となっています。

県内でも多数の被害が発生していますので、改めて警戒を高めるとともに、適切な対処・対策が必要です。



3 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、
◆ 心当たりのないメールは開かない
◆ 添付ファイルを開いたとき、「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
◆ メールセキュリティ製品、不正通信ブロックサービスの導入
などの対策を周知検討して下さい。

万が一感染してしまった場合は、
◆ 感染パソコンをネットワークから切り離す
◆ 感染パソコンで使用していた全アカウントのパスワードを変更する
といった対応を取って下さい。

発　行：テロ対策パートナーシップかがわ事務局（香川県警察本部警備部）
電　話：０８７-８３３-０１１０
Eメール：kskouan@pref.kagawa.lg.jp