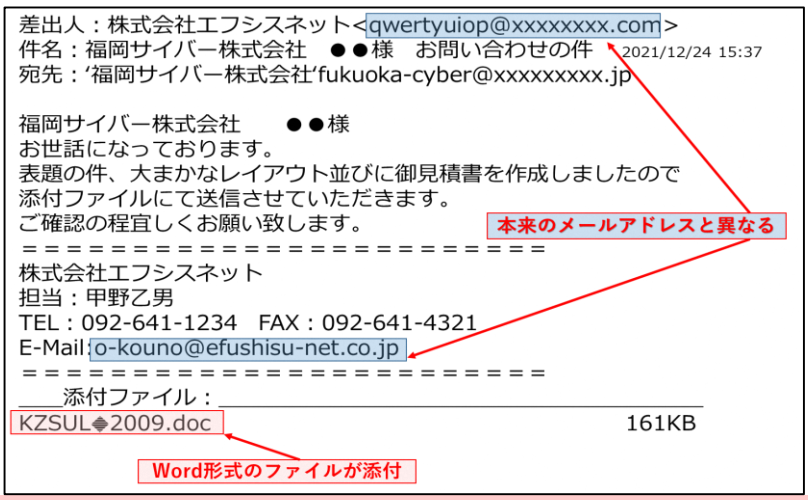
福岡県警サイバー犯罪対策課からのお知らせ

Emotet(エモテット)の感染が拡大しています

Emotet(エモテット)とは

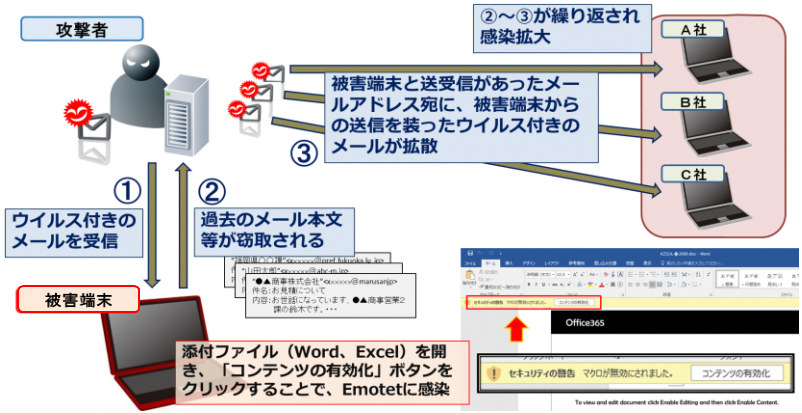
- Emotetとは、電子メールの添付ファイル(Word,Excel)を主な感染経路とするコンピュータウイルスです。
- 過去にやり取りしたメールへの返信を装ったメール等を送信し、添付ファイルの開封を促すのが特徴です。
- 2021年1月、EUROPOL(欧州刑事警察機構)を中心とした停止措置により活動を停止していましたが、同年11月頃から活動を再開していることが確認され、福岡県内の企業にもEmotetに感染誘導するメールが着信しています。

【Emotetに感染誘導するメールの一例】



感染拡大の流れ

- 添付ファイルを開くとファイルに埋め込まれたマクロの実行（「コンテンツの有効化」ボタンのクリック）を促す内容が表示され、実行すると感染。
- Emotetに感染した被害端末からメールアカウント、パスワード、メール本文等の情報を窃取し、これらの情報を悪用して感染拡大を目的としたメールを送信します。



Emotetに感染した企業の声

取引先からの指摘で当社のパソコンがEmotetに感染していることがわかりました…
感染メールを送ってしまった全ての取引先に弁護士を同行して謝罪して回りました…

Emotetに感染すると、自社の事業継続に支障があるだけではなく、取引先の業務の障害になるなど迷惑をかけることとなり、自社の信用に影響を及ぼします。また、Emotetへの感染を切っ掛けに別のコンピュータウイルス（ランサムウェア等）に感染した例もあります。

Emotetの感染防止対策については、一般的なセキュリティ対策に加え、

- ○　過去にメールのやり取りをした相手を装ってメールが送られることを知っておく
- ○　身に覚えがない、時期が合わないなど、不審なメールの添付ファイルは開かない
- ○　添付ファイルを開いてしまった際に、セキュリティ警告を無視する操作をしない
- ○　添付ファイルのマクロが自動実行されない設定にする

等について、職員一人一人に注意喚起を実施することが重要です。

対策!!

福岡県警察本部サイバー犯罪対策課では、最新のサイバー犯罪の手口や対策などを、TwitterやInstagram、ホームページに掲載していますので、ぜひご覧ください。

【Twitter】　【Instagram】　【ホームページ】