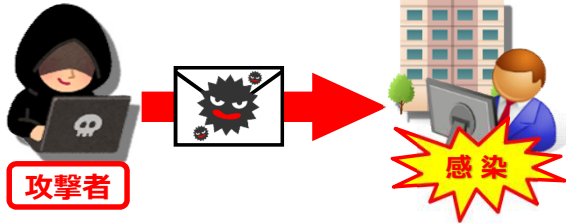




— マルウェア「Emotet（エモテット）」の感染が再び拡大中 —

今月、県内の企業でEmotetの感染事例が確認されました。
Emotetは、情報を盗み取り、その情報を悪用して他人へなりすましメールを送信したり、新たなウイルスに感染させたりするマルウェアです。



(例) メールに添付された**Word形式のファイル**を開いて、**コンテンツの有効化**をすると、不正なマクロが実行されて感染します。

Emotetが仕込まれたメールの特徴

- Wordファイルが添付されている
- メール本文にWordファイルをダウンロードするリンクが記載されている
- 添付されたPDFファイル内にWordファイルをダウンロードするリンクが記載されている



実際の攻撃メール（当県で確認されたもの）

受信した攻撃メール

件名 [spam] Inv S08192 from [redacted]

宛先 [redacted]

From: [redacted]
Sent: Tuesday, July 21, 2020 3:09 PM
To: [redacted]
Subject: [spam] Inv S08192 from [redacted]

Good Morning,
Please confirm.

[http://gabrielinsg-001-\[redacted\]/4vob4/nroq-4h-84/](http://gabrielinsg-001-[redacted]/4vob4/nroq-4h-84/)

Wordファイルをダウンロードするリンク

【不審なメールを受信した場合】

メールを受信しても、**不審なWordファイル**は絶対に開かないようにしてください。（受信しただけでは感染しません。）
速やかに情報セキュリティ担当者に報告してください。