

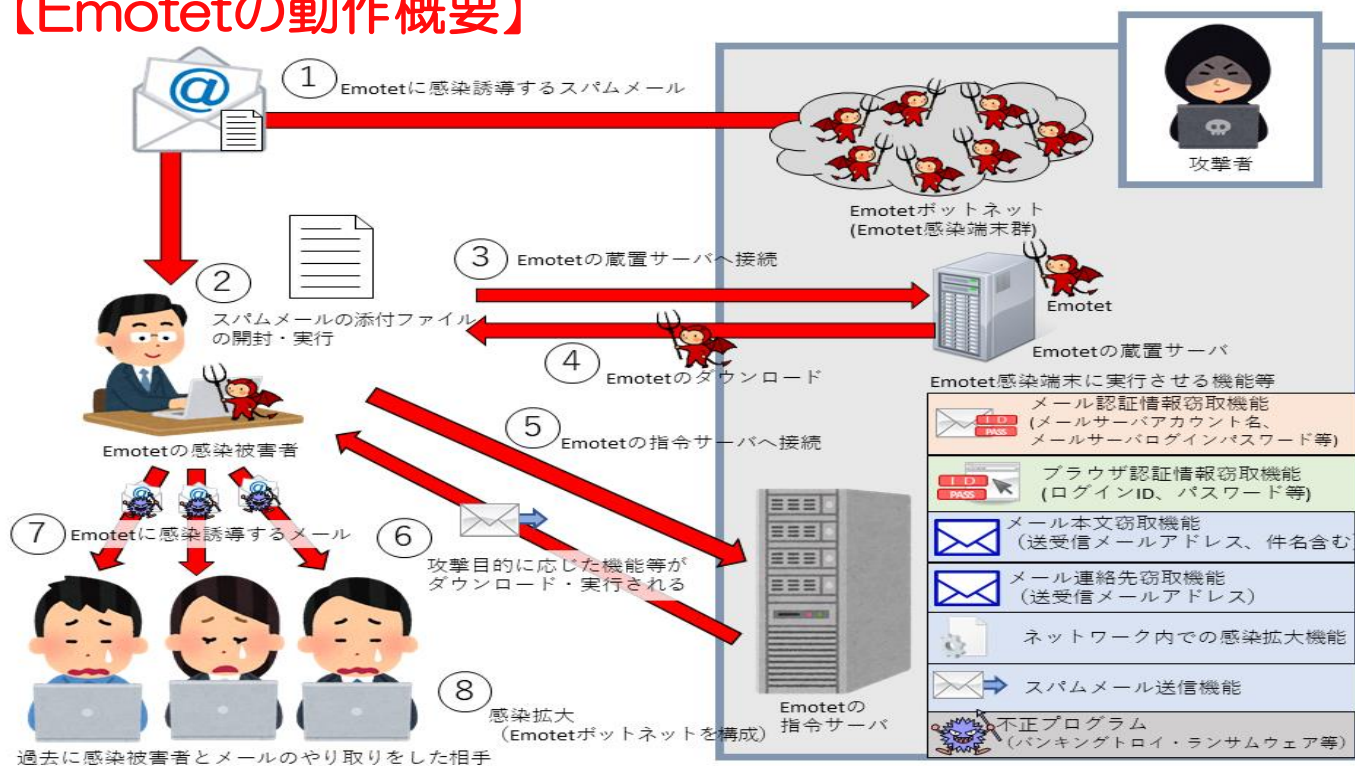
Emotetにクレジットカード情報を盗み取る新機能が確認されています！



Emotetの新機能として、ウェブブラウザ「Google Chrome」に保存されたクレジットカード番号、名義人氏名や有効期限といった情報を盗み、外部に送信する機能が追加されました。

「Google Chrome」では個人情報を暗号化して安全に保存しているものの、Emotetに新たに追加された機能は、暗号データを復旧するための鍵も同時に窃取するため、感染するとクレジットカード情報が第三者に知られるおそれがあります。

【Emotetの動作概要】



出典：警察庁HP

被害防止対策

- 組織内への注意喚起の実施 (メールに添付されたデータは送信元に確認した上で開くなどのルールを徹底)
- Excel、Wordマクロの自動実行の無効化
- メールセキュリティ製品の導入によるマルウェア付きメールの検知
- メールの監査ログの有効化
- OSに定期的にパッチを適用、ウイルス対策ソフトの更新
- 定期的なオンラインバックアップの取得

Emotetに関して、Ksisnetだより第70号、第75号、第83号、第84号、第100号、第106号において情報提供しています。職場内での注意喚起を行ってください。