



Emotetの新機能実装に関する情報提供

Emotetについて

Emotetは、**主にメールを感染経路としたマルウェア(不正プログラム)**で、メールソフトに登録されている連絡先から知り合いのメールアドレスを盗んで使うなどして、本人作成のメールであると信じ込ませ、不審に思わず開封してしまいそうなメールの返信を装います。

現状

本年4月下旬以降、ショートカットファイル(LNKファイル)を添付し、これをダブルクリックなどで開いた場合にEmotetに感染させる手口が確認されるなど手口が巧妙化され、6月9日、**ウェブブラウザChrome上に保存されたクレジットカード情報を窃取し、C2サーバに送信するモジュールが追加されました。**

懸念

今後、国内においてEmotet感染端末から**クレジットカード情報を窃取される事案の発生が懸念されます。**

対処方法

- ・不用意にメールの添付ファイルを開かないようにする。
- ・ウイルス対策ソフトやOSを最新の状態にアップデートする。

神奈川県企業サイバーセキュリティ対策官民合同プロジェクト

このプロジェクトは、神奈川県警察が事務局を務め、神奈川県内の企業、団体、学術機関、行政機関が緊密に連携し、県内企業のサイバー空間の脅威への対処能力向上を図ることを目的に活動しています。

こんなメール↓

差出人: taro.kanagawa(kanagawa@++++.com)
 送信日時: 2021年10月1日金曜日 6:22
 宛先: ichiro.yokohama(yokohama@****.co.jp)
 件名: ■■■費用について
 添付ファイル: 2320013290_30390021.doc

取引先になりすまし

不審な添付ファイル

返信のように装った本文

神奈川です。
 取り急ぎご連絡いたします。

 株式会社●●● 総務課
 神奈川 太郎
 kanagawa@++++.com

>株式会社▲▲▲ 総務課 神奈川様
 >
 >いつもお世話になっております。
 >株式会社●●●の横浜です

詳しい情報についてはこちらから



【警察庁 @police】

警察庁より、ネットワークセキュリティに関する様々な情報を提供しています。



情報発信元：
 神奈川県警察
 サイバー

セキュリティ対策本部