

マルウェアEmotet感染確認ツール 「EmoCheck」の活用を!

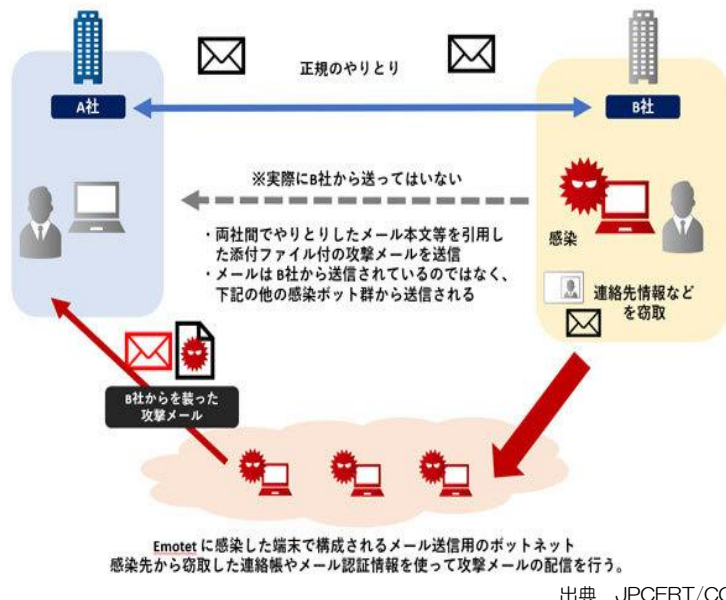
Emotetとは…

過去に送受信した実際のメール情報から「なりすましメール」を作成し、不正なファイルを添付して、過去にやりとりのある相手へ送信します。

不正な添付ファイルを開くと、Emotetに感染してしまいます。

Emotetに感染すると…

- 端末やブラウザに保存されたパスワード等の認証情報が窃取される
- ネットワーク内に感染が広がる
- メールアカウントとパスワードが窃取される
- メール本文とアドレス帳の情報が窃取される
- 窃取されたメールアカウントや本文などが悪用され、Emotetの感染を広げるメールが送信される



Emotetはアップデートを繰り返しており、最新のウイルス対策ソフトでも即座に見つけることは難しい

Emotet感染確認ツール

「EmoCheck」を使ってみよう



昨年10月以降日本国内においてEmotetの感染事例が急増していることを受け、JPCERT/CCは、本年2月、コンピュータがEmotetに感染しているかどうかを確認できるツール「EmoCheck」を公開しました。

Emotetは感染していることが判別しにくいので、感染が疑われる端末に、「EmoCheck」を利用してみてはどうでしょうか？

下記のウェブサイトから、

Emotetへの対応方法

「EmoCheck」の使用方法

が確認でき、「EmoCheck」の無料ダウンロードをすることができます。

<https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html>

Emotet感染予防対策も、上記ウェブサイトであわせて確認しておきましょう。

