Ksisnetだより

発行:Ksisnet事務局
令和3年11月26日
Vol.100

Emotet（エモテット）による攻撃活動の再開!!

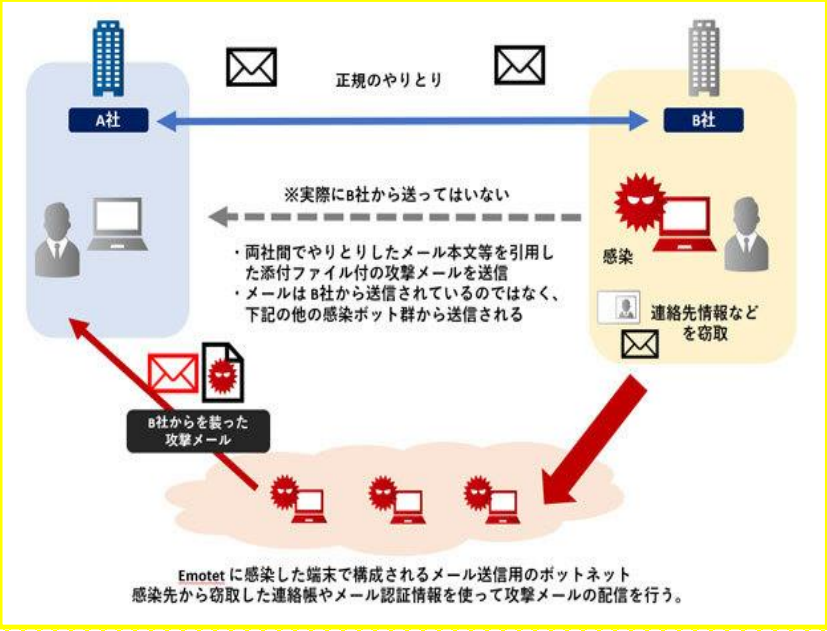
IPA（情報処理推進機構）等が、【Emotetの攻撃活動再開】について、注意喚起しています。
一度はテイクダウンしその攻撃活動は停止したかに思えましたが、再びその攻撃活動が再開されている兆候があります。
Emotetは過去に猛威をふるい、多くの企業や組織が被害に遭ったマルウェアであり警戒が必要です。

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

〇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。
〇ネットワーク内に感染が広がる。
〇メールアカウントとパスワードが窃取される。
〇 メール本文とアドレス帳の情報が窃取される。
〇 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。



出典　JPCERT/CC

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」を活用しましょう

JPCERT/CCは、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」を公開しています。
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」を活用して下さい。下記のウェブサイトから、

Emotetへの対応方法や使用方法

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://github.com/JPCERTCC/EmoCheck