Emotet(エモテット)感染を疑ったら

更新日：2022年3月7日

エモテットの感染が急激に拡大しています

「取引先等から変なメールが送られてきたとの連絡を受けた」、「メールに添付されたファイルの「コンテンツの有効化」ボタンを押してしまった」、「コンテンツの有効化ボタンを押したが、その後何も表示されなかった」などといった場合には、「EmoCheck」による確認と、最新の定義ファイルに更新したウイルス対策ソフトによるフルスキャンを実施しましょう。

エモテット感染の有無をチェックする

エモテットに感染したかもしれないと思ったら、直ぐに感染の有無をチェックしましょう。
エモテット専用の感染確認ツール「EmoCheck（エモチェック）」は、JPCERT/CC（ジェーピーサートコーディネーションセンター）から公開されていますので、どの端末のどこにエモテットが感染･潜伏しているのかを確認し、自社で可能であれば駆除も実行しましょう。
エモテットの駆除方法については、下記の外部ページにある「感染時の対応」など該当部分を参照の上、実施してください。
なお、エモテットに感染していない場合でも、他のマルウェアに感染していることがありますので、下段に記載の「他のマルウェア感染の有無を調査する」を実施しましょう。

EmoCheckの使い方の手引き

NOTICE「Emotetへの対応」（外部サイト）

JPCERT/CC「マルウェアEmotetへの対応FAQ」（外部サイト）

感染した端末のネットワークをインターネットから遮断する

エモテットの感染が発覚した場合、感染が疑われる端末をネットワークから、また、感染が疑われる端末が繋がっているネットワークを外部のインターネットから遮断しましょう。
発覚した時期が感染から間もない場合には、他の端末に感染を広げてしまうリスクを下げることができるため、確実に実施しましょう。

他のマルウェア感染の有無を調査する

EmoCheckによる確認で、感染が確認できなかったとしても、続けて他のマルウェア感染の有無について調査しましょう。
調査する範囲は、感染が疑われた端末からネットワーク内に広がっている可能性を考慮して、同じネットワーク内にあるすべての端末を対象にウイルス対策ソフトを最新の状態に更新した上で完全スキャン（フルスキャン）を実行しましょう。
自社でセキュリティベンダーと契約がある場合には、直ぐにベンダーへ連絡し、指示を仰ぎましょう。

注目情報

- Emotet(エモテット)感染を疑ったら
- 「ライブ配信を騙るフィッシング詐欺」に注意！
- CYBER POLICE（警視庁サイバーセキュリティ対策本部提携LINE公式アカウント）
- テレワーク勤務のサイバーセキュリティ対策！
- サイバーセキュリティ学習用ボードゲーム
- サイバー空間をめぐる脅威の情勢について
- ランサムウェアに要注意！
- 東京中小企業サイバーセキュリティ支援ネットワーク(Tcyss)
- Tcyss参加団体
- 疑わしい情報に惑わされないために
- コンピュータ・ウイルスに対する自己防衛

このページを見ている人はこんなページも見ています

- コンピュータ・ウイルスに対する自己防衛

感染したアカウントのメールアドレスとパスワードを変更する

エモテットはメール経由で外部に感染を拡大させていくため、エモテットに感染したアカウントのメールアドレスやパスワードの変更を行う必要があります。
感染した疑いがある端末も同様に変更しておかなければ、変更後の二次被害のリスクが残ってしまいます。
アカウント自体を削除・変更しても業務に支障が出ないようであれば、新しく作り直すことも事後対策の1つとして有効です。

感染した端末を初期化する

マルウェアに感染した端末をウイルススキャン等によって発見できたマルウェアの駆除後、再び使うこととなった場合、ウイルススキャンでは発見できなかったバックドアが残っており、再び犯罪者の侵入を許してしまうことがありますので、端末を初期化することをお勧めします。
ただし、初期化することで端末内に保存されているデータがすべて消えてしまうことになりますので、日頃のデータのバックアップ対策についても検討しておきましょう。

感染拡大を防止する

感染が判明してから時間が経過しているような場合には、マルウェア感染メールを発信した取引先に向けて感染拡大を防止することが必要です。
エモテットに感染し被害を受けている状況をできるだけ早く通知し、自社名で発出されたメールを受信した際には、単純に信用することなく開封せずに削除する等注意を促して、自社から発信したメールによる感染拡大を抑えるように努めましょう。
取引先等へ向けた注意喚起を迅速に行うため、自社にホームページがある企業であれば、ホームページに「お知らせ」などの方法で、より早く広く注意喚起できます。

情報発信元　警視庁　サイバーセキュリティ対策本部　対策担当
電話：03-3581-4321（警視庁代表）

ページトップへ戻る

ランサムウェアに要注意！
サイバーセキュリティad資料
運転免許に関する情報
FAQ よくある質問
情報が見つからないときは