掲載日時: 2019-11-27 17:25

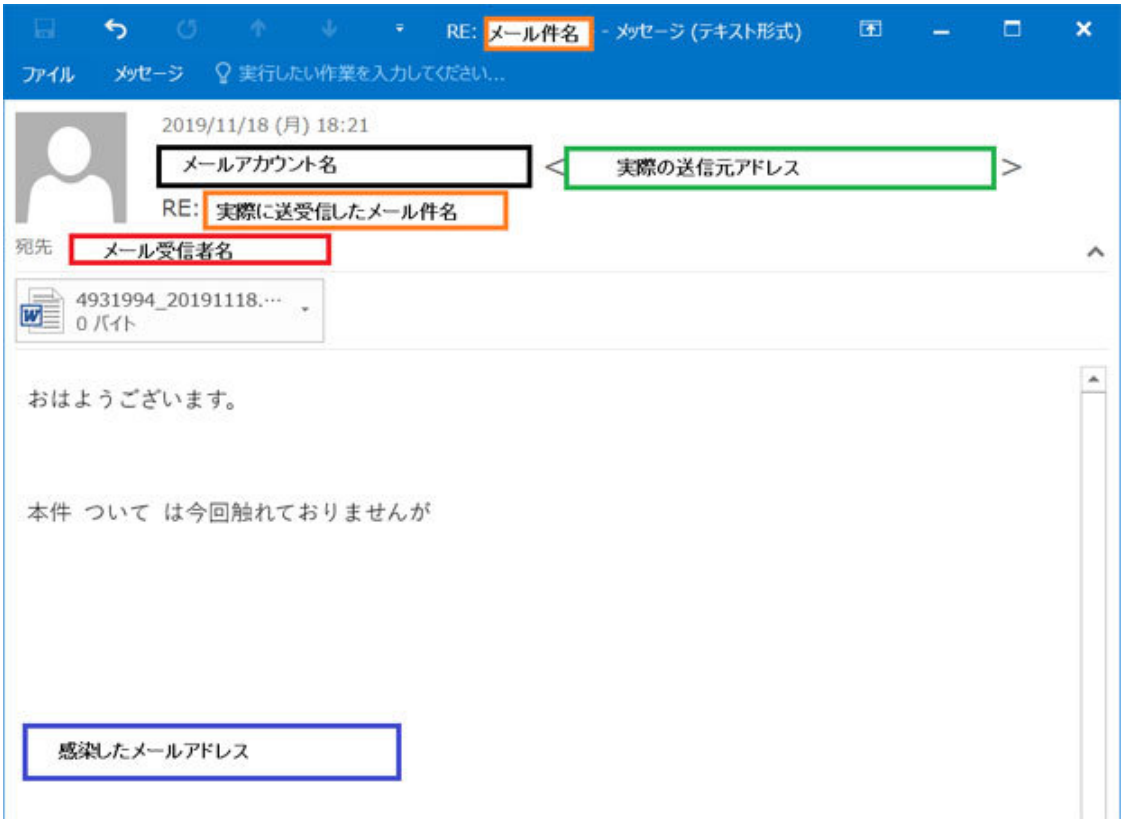
マルウェア「Emotet」の感染攻撃に注意喚起--基本的な防御策の徹底を

海外で被害が流行しているマルウェア「Emotet」の感染攻撃が日本でも拡大しているとして、セキュリティ機関が注意を呼び掛けている。

著者 : ZDNet Japan Staff

URL : https://japan.zdnet.com/article/35146030/

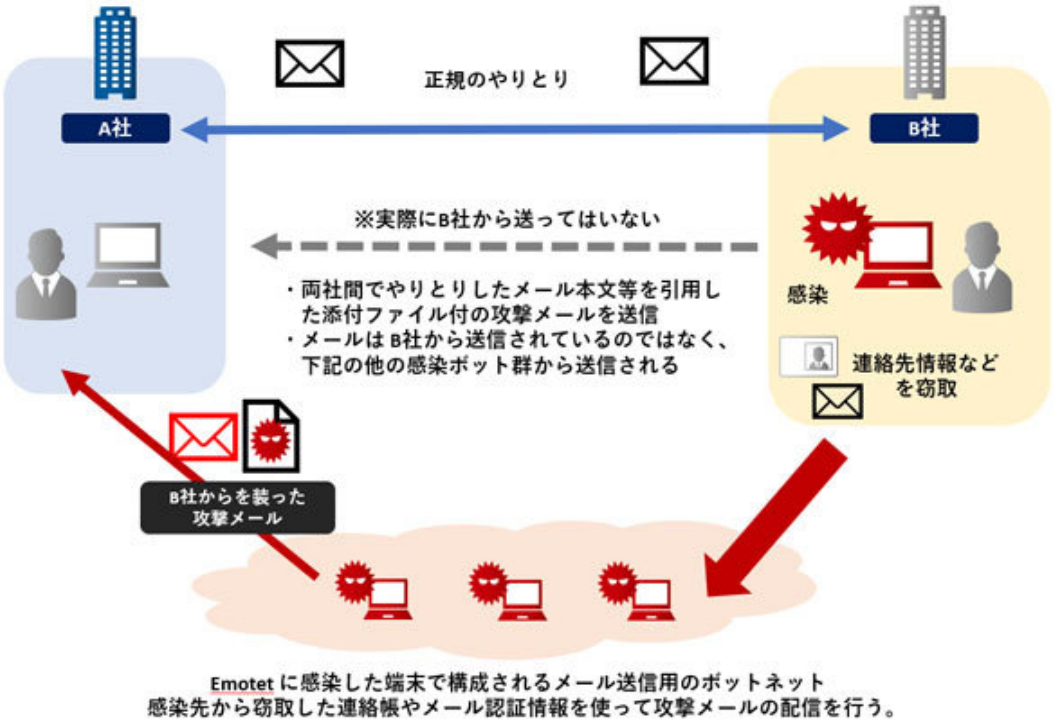
サイバー攻撃インフラと化しているマルウェア「Emotet」の脅威が日本でも拡大しているとしてJPCERT コーディネーションセンター（JPCERT/CC）が11月27日、国内企業などに注意を呼び掛けた。拡散では主にメールやOffice形式のファイルなどが悪用されていることから、これらにおける基本的な防御策の徹底が肝心になる。



攻撃メールのイメージ（一部、出典：JPCERT/CC）

JPCERT/CCによれば、国内では10月後半からEmotetの感染に関する相談が目立っている。実在の組織や人物になりすましたメールに添付される細工されたWordファイルによってEmotetに感染するケースが多いとされる。感染後は、重要な情報を盗み取られたり、別のサイバー攻撃に加担させられたりするほか、ランサムウェアにも感染してシステムやデータを破壊されたり、身代金を要求されたりする被害も報告されている。

Emotetは2014年頃に、オンラインバンキングサービスの認証情報などを窃取するトロイの木馬として出現したとされる。その後にサイバー攻撃グループが繰り返し機能を拡張し、現在ではオンライン詐欺や情報窃取、不正プログラムの拡散など多機能なサイバー攻撃基盤のボットネットと化した。



マルウェア「Emotet」の感染攻撃イメージ（出典：JPCERT/CC）

拡散攻撃では、既にEmotetに感染している組織から窃取した情報をもとに攻撃者がなりすましメールを別の組織に送り付ける。このメールには、Emotetに感染させるための不正なマクロを埋め込んだWordなどのOffice形式のファイルが添付されている。受信者が端末にインストールされたOfficeアプリケーションのマクロを有効にした状態でファイルを開いてしまうと、幾つかの段階を経てEmotetに感染する。そして、ボットに組み込まれてしまい、上述のようなさまざまな被害に遭う恐れがある。Emotetは感染端末からネットワークの認証情報も窃取するため、メールではなく組織内のネットワークを経由して感染が広がる場合もある。

JPCERT/CCが推奨している基本的な対策は下記の通り。

組織内への注意喚起の実施

マクロの自動実行の無効化（事前にセキュリティセンターのマクロの設定で「警告を表示してすべてのマクロを無効にする」を選択しておく）

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（SMBの脆弱性を突く感染拡大に対する対策）

定期的なオフラインバックアップの取得（標的型ランサムウエア攻撃に対する対策）

セキュリティ センターのマクロ無効化の設定。Office 365/2019の場合はスタートページの「オプション」から「セキュリティ センター」を開き、「セキュリティ センターの設定」ボタンを押す（出典：JPCERT/CC）