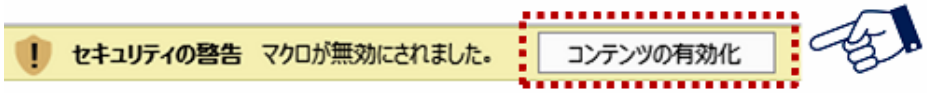
モノづくりプリザーブ
Preservation for Industries in kyoto
モノプリ・ニュース！ 第36号

マルウェア「Emotet」（エモテット）の感染に繋がるメールの配布活動が再開

昨年10月から国内で感染事例が相次いでいた「Emotet」の攻撃メールは、今年２月上旬以降観測されない状態が続いていましたが、７月中旬から活動が再開しています。攻撃の手口はこれまでと大きくは変わらないため、受信したメールに添付されたWord文書ファイル等が信頼できるものと判断できない限り「コンテンツの有効化」ボタンをクリックしないよう、引き続き注意してください。

「Emotet」の概要



Emotetは、情報の窃取に加え、更に他のウイルスへの感染のために悪用されるウイルスであり、悪意のある者によって、不正なメール（攻撃メール）に添付される等して、感染の拡大が試みられています。

Emotetへの感染を狙う攻撃メールの中には、正規のメールへの返信を装う手口が使われている場合があります。これは、攻撃対象者（攻撃メールの受信者）が過去にやり取りしたことのある、実在の相手の氏名、メールアドレス、メールの内容等の一部が流用された、あたかもその相手からの返信メールであるかのように見える攻撃メールです。このようなメールは、Emotetに感染してしまった組織から窃取された、正規のメール文面やメールアドレス等の情報が使われていると考えられます。

感染防止に向けた対策

Emotetへの感染を防ぐというためだけにとどまらず、一般的なウイルス対策として、以下のような対応をすることをお勧めします。

- 身に覚えのないメールの添付ファイルは開かない。メール本文中のURLリンクはクリックしない。
- 自分が送信したメールへの返信に見えるメールであっても、不自然な点があれば添付ファイルは開かない。
- OSやアプリケーション、セキュリティソフトを常に最新の状態にする。
- 信頼できないメールに添付されたWord文書やExcelファイルを開いた時に、マクロやセキュリティに関する警告が表示された場合、「マクロを有効にする」「コンテンツの有効化」というボタンはクリックしない。

【本号出典】IPA 「Emotet」と呼ばれるウイルスへの感染を狙うメールについて（2020年７月28日更新）
URL：https://www.ipa.go.jp/security/announce/20191202.html
【関連情報】JPCERT/CC マルウェアEmotetの感染に繋がるメールの配布活動の再開について
URL：https://www.jpcert.or.jp/newsflash/2020072001.html

京都府警察本部モノづくりプリザーブ事務局 075-451-9111(内線 5821)