モノづくりプリザーブ
Preservation for Industries in kyoto

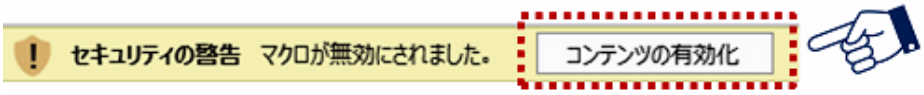
モノプリ・ニュース / 第43号

Emotet（エモテット）の攻撃活動再開について

今年11月14日頃から、Emotetの攻撃活動再開の兆候が確認されたという情報があります。また、Emotetへの感染を狙う攻撃メールが着信しているという情報も複数観測されている状況です。

これらは悪意のあるマクロ（プログラム）が仕込まれたもので、今年１月までの攻撃と同様の手口です。引き続き、特にメールを経由して入手したOffice文書ファイルについて、信頼できるものと判断できる場合でなければ、「編集を有効にする」「コンテンツの有効化」というボタンはクリックしないよう、注意してください。2019年から2020年にかけ、多くの企業・組織が被害に遭いました。念のため、警戒をお願いします。

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。

Emotetへの対策

- 身に覚えのないメールの添付ファイルは開かない。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。
- メールや文書ファイルの閲覧中、身に覚えのない警告ウインドウが表示された際、その警告の意味がわからない場合は、操作を中断する。
- 身に覚えのないメールや添付ファイルを開いてしまった場合は、すぐにシステム管理部門等へ連絡する。

【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（2021年11月16日追記）
URL：https://www.ipa.go.jp/security/announce/20191202.html#L16

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）