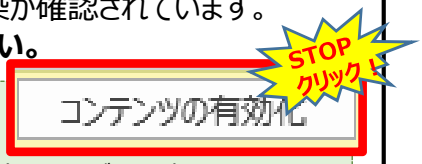
滋賀県警察サイバーセキュリティ情報
サイバーコネクトSHIG@
R４年度 No.18
今、注目のサイバーセキュリティに関する情報をお届けします。

「Emotet」拡大 メールの添付ファイルにご注意願います。

今月（2022年11月）に入り「Emotet」を使ったサイバー攻撃への警戒が高まっています。
Emotetは、感染すると端末からメール情報を盗み出したうえ、盗んだメールを使ってさらに感染を広げるウイルスです。Emotetの活動は、休止と再開を繰り返していますが、最近、添付ファイルにExcelを使い、端末内の信頼できる場所に保存させてマクロを実行させるという新たな手法による感染が確認されています。
業務でメールを使用される方は、特に添付ファイルの取扱には注意してください。



「Emotet（エモテット）」とは
Emotetは、情報の窃取に加え、更に、他のウイルス感染のために悪用されるウイルスです。
主にメールに添付された「Wordファイル」等を開いたうえ、「コンテンツの有効化」又は「編集を有効にする」ボタンを押すことで、マクロプログラムが実行され、外部サーバから不正プログラム（Emotet）がダウンロードされます。
Emotetに感染すると、PCに保存されている送受信メールの情報が盗まれるため、実在する人物の氏名やメールアドレスを使用することが可能となり、正規のメールへの返信を装って、別の人（取引先等）へ、標的型メールが送られます。
「コンテンツの有効化ボタン」は、安易に押さないようにしてください。

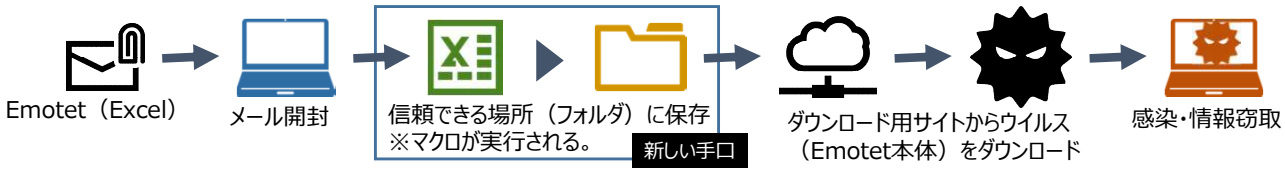
Emotetの新しい手法

最近確認されたEmotetは、添付ファイルにExcelを使用しており、Excelを開くと、**「"信頼できるフォルダ"に一度保存してから開くように」というメッセージが表示（英語）されます。**
"信頼できるフォルダ"にExcelを保存すると、ファイルを開いたときに、マクロプログラムが自動実行され、外部からウイルス（Emotet）をダウンロードして、端末の情報を盗み取ります。

新しい手法への対策

- **MicrosoftOfficeの信頼できる場所を無効化する。**
  Excelのオプション⇒セキュリティセンター⇒セキュリティセンターの設定⇒信頼できる場所⇒「全ての信頼できる場所を無効にする」に✓を入れて**「有効」**にする。
  （バージョンによって名称は異なります。また管理者権限が必要な場合があります。）

※MicrosoftOfficeには、信頼できる場所という保存場所（フォルダ）があり、その中のファイルは開いたときにマクロが自動的に有効化されます。



参照：トレンドマイクロ｜攻撃手法から考える防御策 2022年11月に活動再開したEMOTET（エモテット）を既存環境で防ぐ考え方
https://www.trendmicro.com/ja_jp/jp-security/22/k/securitytrend-20221114-01.html

脆弱性情報（緊急性、重要性の高い脆弱性情報等をピックアップしてご紹介します。）

～VMware製品の認証バイパスの脆弱性（2022年11月8日公表）ランサムウェアの感染に利用されるおそれあり～
VMware社が、リモート環境で管理者が利用者の端末操作をサポートするためのソフトである「Workspace ONE Assist」について、認証バイパス等の脆弱性に対応する修正パッチをリリースし、修正パッチの適用を呼びかけています。
詳細は、必ず、公式サイト及びIPA、JVN、JPCERT/CC等の脆弱性情報提供サイトを確認してください。

サービス名、機器名等（影響を受けるソフトウェア）	脆弱性の概要（悪用された場合の影響等）	CVE（共通脆弱性識別子）	対策（修正プログラムの公開情報等）
Workspace ONE Assist	アプリへの認証を必要とせず管理者権限を取得できる可能性があるなど。	CVE-2022-31685（CVSSスコア9.8）等	当該製品のバージョン確認と修正パッチの適用

参照：VMware|Advisories VMSA-2022-0028 https://www.vmware.com/security/advisories/VMSA-2022-0028.html

«CS情報SHIG@» キャッシュレス決済の不正利用が発生しています。パスワード変更をお願いします。

滋賀県警察本部 サイバー犯罪対策課 077-522-1231（代表）
県警webページ →
https://www.pref.shiga.lg.jp/police/seikatu/304409/index.html