INCIDENT PICKUP! STUDY

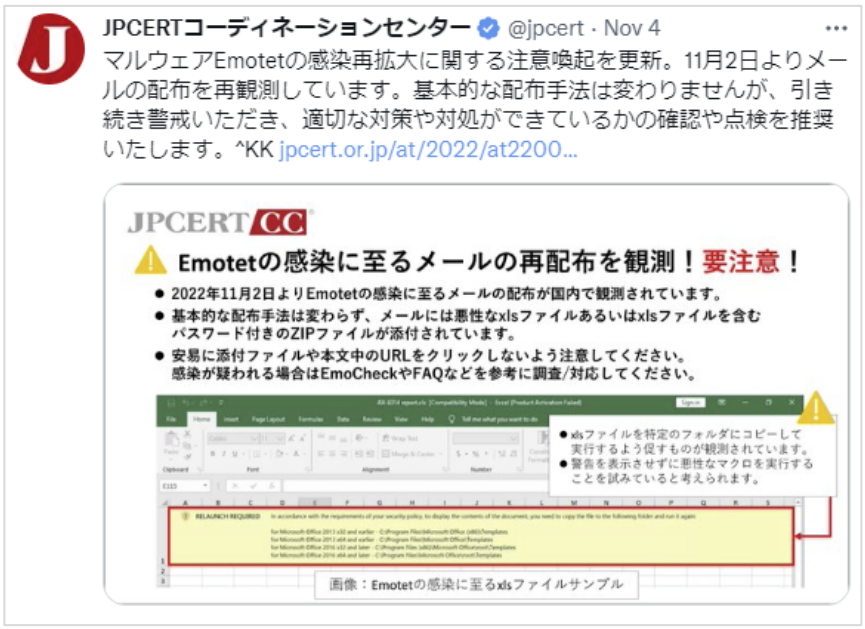
PICKUP!

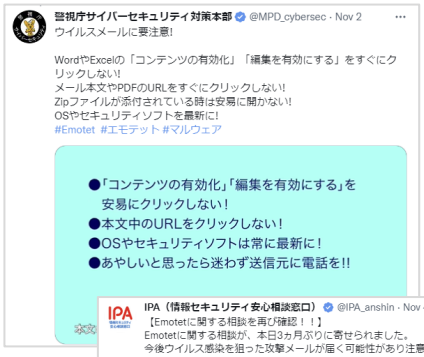
Fuva Brain

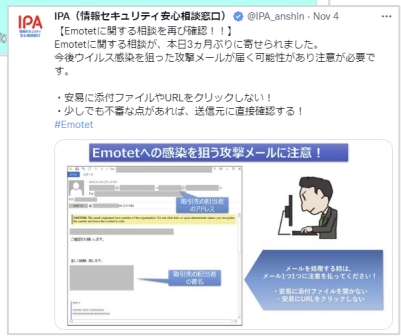
一定の停止期間を経て、Emotetの活動再開を観測、警戒を

出典：JPCERT/CC、IPA、警察庁の注意喚起ページ、Twitter

11月2日、マルウェアEmotetの活動再開を観測！
前回の危機的感染拡大を踏まえて、
各関係機関が早々に注意喚起を発信、ご注意ください。







参考情報

JPCERT/CC 提供

感染チェックツール「EmoCheck2.3.2」

JPCERTCC/EmoCheck - GitHub
https://github.com/JPCERTCC/EmoCheck/releases

EmoCheckの使用方法や更新履歴など
https://github.com/JPCERTCC/EmoCheck/blob/master/README_ja.md

マルウェアEmotetの感染再拡大に関する注意喚起

Emotetに関する最新動向
https://www.jpcert.or.jp/at/2022/at220006.html

マルウエアEmotetへの対応FAQ

Emotetに関する情報、対応を確認
https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html

解説動画 社内周知 注意喚起に

JPCERT/CC 提供

日本中で感染が広がるマルウェアEmotet

JPCERTCC/Emotetの解説動画
https://youtu.be/wvu9sWiB2_U

EMOTET感染の確認方法と対策

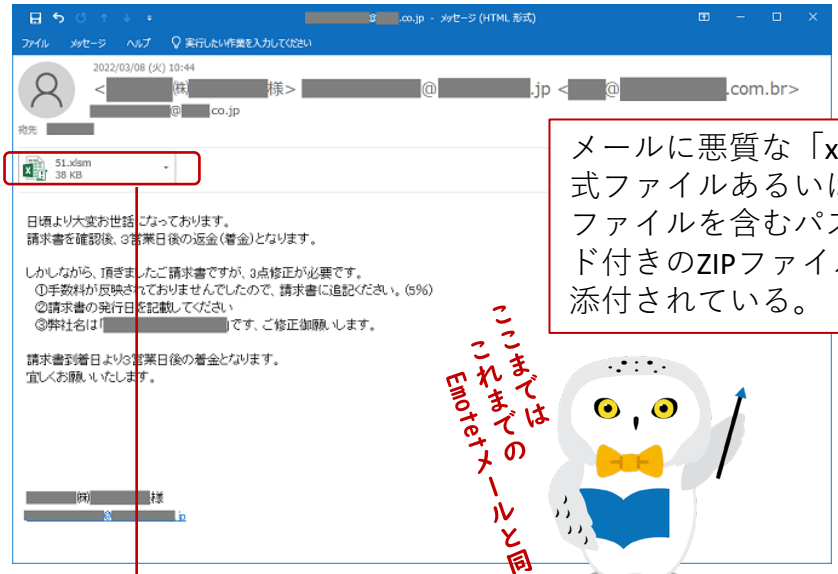
JPCERTCC/Emotetの感染確認方法と対策解説動画
https://youtu.be/nqxikr1x2ag

Emotetの新たな手口とは？巧妙に「コンテンツの有効化」を促す「偽の指示」

出典：IPA Emotet（エモテット）と呼ばれるウイルスへの感染を狙うメールについて
https://www.ipa.go.jp/security/announce/20191202.html#L22

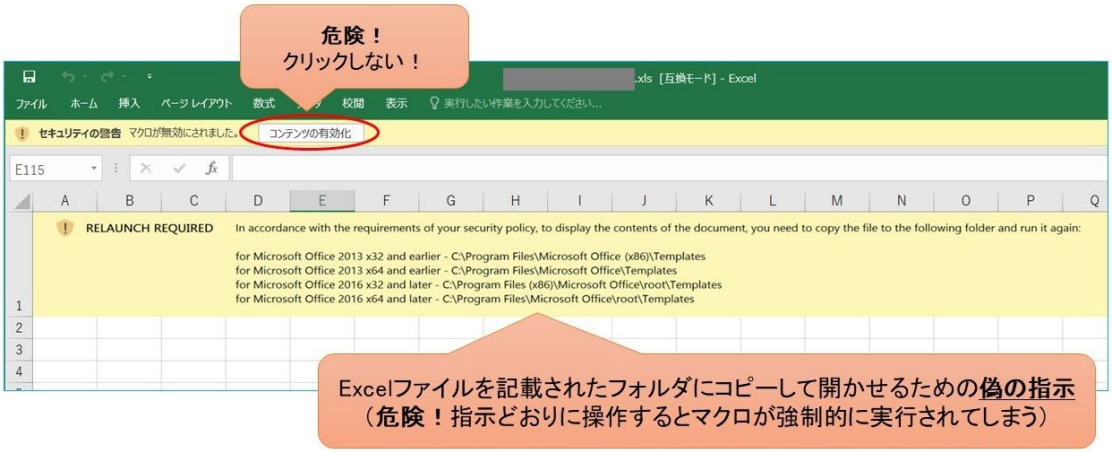
新たな手口として、メールに添付されたExcelファイル内に「コンテンツの有効化」を促す偽の指示

IPA（独立行政法人情報処理推進機構）およびJPCERT/CC（一般社団法人JPCERT コーディネーションセンター）は11月4日、Emotetの感染再拡大への注意喚起を公開した。



メールに悪質な「xls」形式ファイルあるいはxlsファイルを含むパスワード付きのZIPファイルが添付されている。

Excelファイル内に書かれている「偽の指示」に注意！



Emotetの攻撃手口は従来と大きな変化はないが、攻撃メールに添付されたExcelファイル内に書かれている偽の指示が、コンテンツの有効化を促す内容から特定のフォルダにExcelファイルをコピーして開かせるように促す内容に変化している。

この指示どおりに、Excelファイルを、記載されたTemplatesフォルダにコピーして開くと、マクロを無効化する設定にしていても、ファイルに含まれている悪意のあるマクロが強制的に実行されてしまいます。これは、コピー先のTemplatesフォルダが“信頼できる場所”としてデフォルトで設定されているため※1で、このフォルダに格納されたファイルは、安全性の高いファイルとみなされ、マクロが実行可能になります。危険ですので、偽の指示に従って操作しないよう注意してください。

※1 Microsoft Office ファイルの信頼できる場所 https://learn.microsoft.com/ja-jp/deployoffice/security/trusted-locations