

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



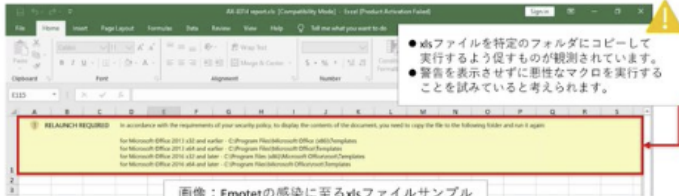
**11月2日、マルウェアEmotetの活動再開を観測！
前回の危機的感染拡大を踏まえて、
各関係機関が早々に注意喚起を発信、ご注意ください。**

J JPCERTコーディネーションセンター @jpcert · Nov 4
マルウェアEmotetの感染再拡大に関する注意喚起を更新。11月2日よりメールの配布を再観測しています。基本的な配布手法は変わりませんが、引き続き警戒いただき、適切な対策や対処ができていないかの確認や点検を推奨いたします。*KK jpcert.or.jp/at/2022/at2200...

JPCERT/CC

Emotetの感染に至るメールの再配布を観測！要注意！

- 2022年11月2日よりEmotetの感染に至るメールの配布が国内で観測されています。
- 基本的な配布手法は変わらず、メールには悪質なxls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ます。
- 安易に添付ファイルや本文中のURLをクリックしないよう注意してください。感染が疑われる場合はEmoCheckやFAQなどを参考に調査/対応してください。



画像：Emotetの感染に至るxlsファイルサンプル

監視庁サイバーセキュリティ対策本部 @MPD_cybersec · Nov 2
ウイルスメールに要注意!

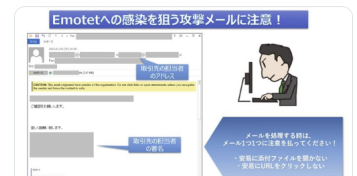
WordやExcelの「コンテンツの有効化」「編集を有効にする」をすぐにクリックしない!
メール本文やPDFのURLをすぐにクリックしない!
Zipファイルが添付されている時は安易に開かない!
OSやセキュリティソフトを最新に!
#Emotet #エモテット #マルウェア

- 「コンテンツの有効化」「編集を有効にする」を安易にクリックしない!
- 本文中のURLをクリックしない!
- OSやセキュリティソフトは常に最新に!
- あやしいと思ったら迷わず送信元に電話を!!

IPA (情報セキュリティ安心相談窓口) @IPA_anshin · Nov 4

【Emotetに関する相談を再び確認!!!】
Emotetに関する相談が、本日3ヵ月ぶりに寄せられました。今後ウイルス感染を狙った攻撃メールが層々増加する可能性があります。

- ・ 安易に添付ファイルやURLをクリックしない!
- ・ 少しでも不審な点があれば、送信元に直接確認する!



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

参考情報

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>

マルウェア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>



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

解説動画
社内周知
注意喚起に

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>



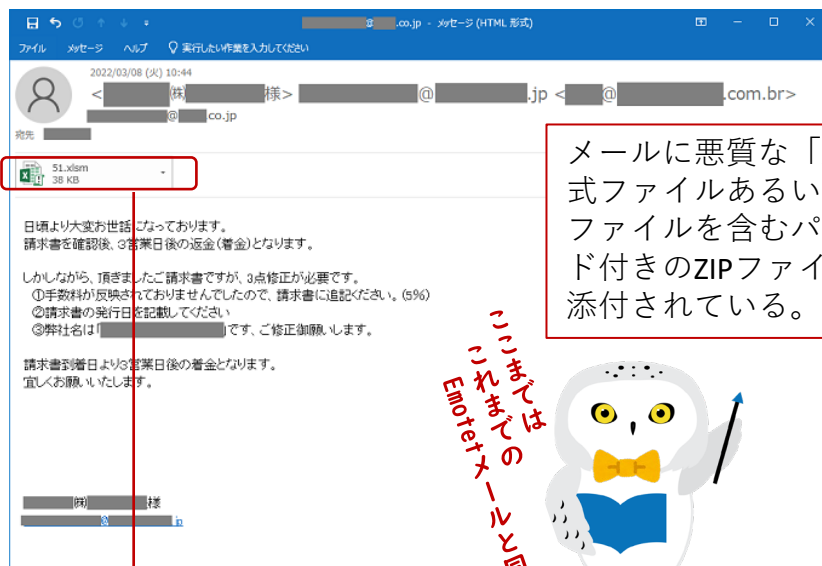


新たな手口として、メールに添付されたExcelファイル内に「コンテンツの有効化」を促す偽の指示

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。



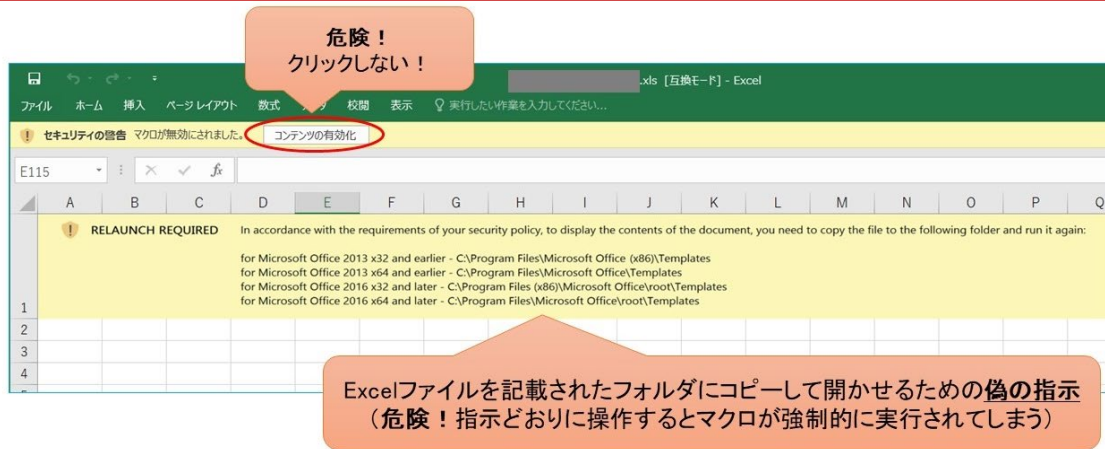
どこか「心当たりがある」と
思わせるメールに要注意です。



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。

ここまでは、
これまでは、
Emotetメールと同じ

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るも、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>