TCSP Toyama Prefectural Police Cyber Security Personnel
サイバーセキュリティの置き薬
2023年 第5号

「Emotet」ウイルスが活動再開！

Emotet（エモテット）は、令和4年 11 月頃から活動を停止していましたが、情報セキュリティ関係機関（JPCERT／CC）によると、令和5年3月7日から活動を再開したとのことです。

今回のウイルス配布手法は、メールにZIPファイルが添付されており、このファイルを展開すると500MBを超える文書ファイル（docファイル）が展開されるとのことです。

Emotetの感染メールには、取引先や知人からのメールと思わせるように差出人や件名が偽装されているものがあります。（例：件名「Re：〇〇について」）

メールに添付されているファイルやURLリンクは、すぐに開かず一呼吸おき、本物かどうか少しでも疑わしい場合は、送信元へ直接電話で問い合わせるなどして確認してください。

Emotetに感染してしまうと、『情報が盗まれる』、『ランサムウェア等の他のマルウェアにも感染する』などの被害に遭うおそれがあります。

以下の感染対策をお願いします。

ここに注意！

○　不審なメールは開かない
○　送信元が確認できないときは、
・添付ファイルを開かない
・パスワード付きZIPファイルを解凍しない
・メール本文のURLリンクをクリックしない
・Word／Excelのコンテンツの有効化ボタンをクリックしない

Youtube（富山県警察公式チャンネル）注意喚起動画配信中！

「Emotet」に関する注意喚起動画はこちら→

- Emotetの特徴や感染経路
- Emotetによる被害事例
- 被害防止対策や感染した際の措置

について、分かりやすく解説しています。

※通信費は、ご利用者の負担となります。

https://www.youtube.com/watch?v=baITB3THCu8

【参考】
JPCERT/CC：マルウェア Emotet の感染再拡大に関する注意喚起
https://www.jpcert.or.jp/at/2022/at220006.html
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