サイバー攻撃の未然防止のために

POLICEファイアウォール

1号
2022年

マルウェア「Emotet」があなたのパソコンにも届いているかもしれません!!

ミスターB

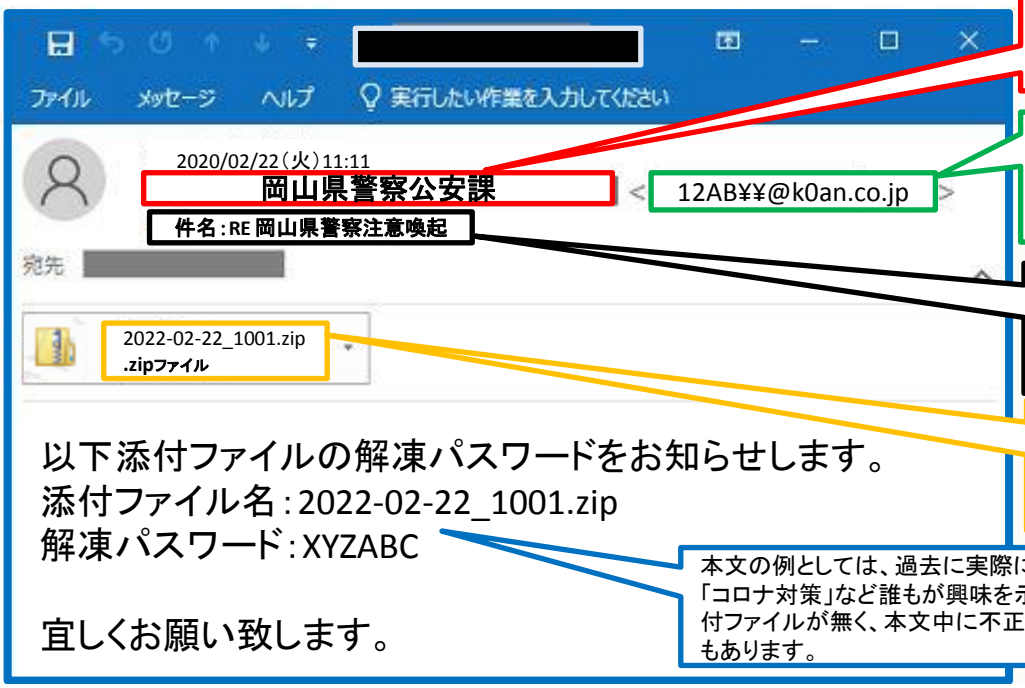
2020年に猛威をふるったマルウェア**「Emotet」**が昨年11月後半から活動を再開させているとして、JPCERT/CCやIPAなど各セキュリティ関係機関から注意喚起が発出されております。

「Emotet」は、メールを盗み見ることで実際の取引先を装う、マルウェアをZipファイル化してセキュリティをすり抜けるなど非常に巧妙な手口を使い、感染を拡大させております。

「完全に防ぎきる！」というのは、非常に困難ではありますが、皆様が意識すれば感染を最小限に止めることができます。

下に一例を示しますので、各セキュリティ関係機関から広報されている注意喚起と併せて対処法を確認し、被害に遭わないように努めて下さい。

Emotetのメールの一例



実際に取引のある関係者を騙ってメールが来ます。

送信元のメールアドレスは、第3者の知らないメールアドレスになります。

件名は、過去に使用したことがある件名が使われることがあります。

添付ファイルは、Zipファイルの他、WordやExcelのファイルなどもあります。

本文の例としては、過去に実際にやり取りしたメールの引用や、「コロナ対策」など誰もが興味を示す内容などもあります。また、添付ファイルが無く、本文中に不正なURLリンクが記載されていることもあります。

★★ミスターHからのお願い★★

IPAが【「Emotet」と呼ばれるウィルスへの感染を狙うメールについて】と題する記事（URL:https://www.ipa.go.jp/security/announce/20191202.html#L18）の中でウィルス対策として、以下の項目を推奨しています。

・身に覚えの無いメールの添付ファイルは開かない。メール本文中のURL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ィンドウが表示された際、その警告の意味が分からない場合は、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。

ぜひ、一読していただき、「Emotet」の対策に役立てていただければと思います。

質疑などがございましたら、岡山県警察本部警備部公安課サイバー攻撃対策係（086-234-0110 内線5576）までご連絡ください。