月刊インフォメーション

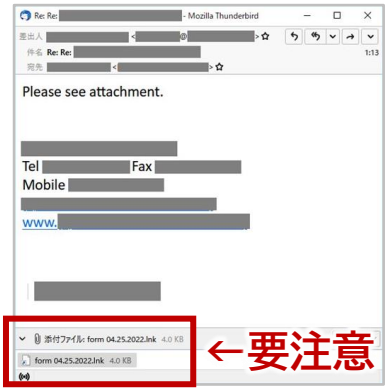
2022年
5月号

!? 2022年4月25日頃、Emotet拡散に新たな手口を確認

メールに添付されたファイル(ExcelやWord、ZIP等)にマルウェア「Emotet」を仕込み、なりすましメールを送る「Emotet」の拡散方法。
今までは、ExcelやWord、ZIP等のファイルが添付されており、「マクロ無効」の設定をすれば防げていました。
今回の新手法は「ショートカットファイル」が添付されており、ダブルクリックするとカンタンに感染する、安易な手口となっており、注意が必要です。

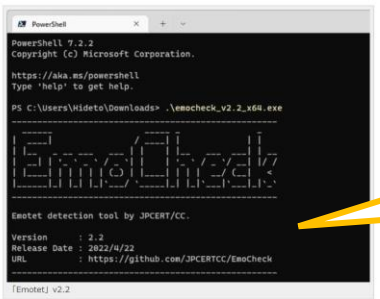
? ファイルを開くだけで感染!?

右図のように、**メールに「ショートカットファイル(LNKファイル)」や、そのZIPファイル(解凍するとショートカットファイル)が添付**されています。
今までの「マクロの設定」を必要としない、**ファイルをダブルクリックすると感染する**、といった、**カンタンに感染しやすい**、安易な手法へ変わっているので、**不用意に添付ファイルを開かないよう、注意が必要です。**



? Emotet感染の確認方法は？

Emotetに感染しているかは、**Emotet感染チェックツール「エモチェック」**(右図参照)を実行するだけで、確認できます。



←Emotet感染チェックツール「エモチェック」(JPCERT/CC提供)

最新は「version:2.2」

右記URL、もしくは、「エモチェック」で検索！

https://ccsi.jp/781/

エモチェック 検索

! 今すぐできる感染対策

- **受信したメールの送信元メールアドレスを確認。**
- **ExcelやWordの「マクロが自動的に実行されない」ように設定を確認。**
- **本文中に挿入されているURLをクリックしない。**
- 重要システムやデータの**バックアップを取っておく。**

! Emotetの最新情報

Emotetに関する情報は下記をご参照ください。

◆ Emotet感染再拡大に関する注意喚起
https://www.jpcert.or.jp/at/2022/at220006.html

◆ Emotetへの対応FAQ
https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html

これらの対策は今すぐに実行でき、従業員のみなさんに徹底すれば、効果が得られます。しかし、これは簡易的な予防処置であり、日々巧妙化するEmotetに対してはどれも安全とは言えません。セキュリティ対策に関して、本格的に検討することをオススメします。

フィッシング報告、1日あたり約3,067件。過去最多!

実在する組織を騙って、ユーザーネーム、パスワード、アカウントID、ATMの暗証番号、クレジットカード番号といった**個人情報を詐取する「フィッシング詐欺」**。主に、**メール、もしくは、ショートメール(SMS)、Twitter等のSNS、から偽ホームページへ誘導されるケースが増えています。**
2022年4月にフィッシング対策協議会へ寄せられたフィッシング報告は、前月4月の8万2,380件をさらに更新し、9万2,094件となり、**過去最多**となりました。

偽ブランドを騙る主なブランドは？

- AmazonやZOZOTOWNといった、大手通販事業
- えきねっと(JR東日本)などの公共交通機関
- ドコモ、au等のモバイルキャリア
- クレジット、信販系、都市銀行、ネット銀行等金融系
- ヤマト運輸、日本郵便の不在通知を装うSMSについては、不正なアプリ(マルウェア等)のインストールへ誘導。
- **PaypayやFamipay等電子マネー。**
- **出前館、日本年金機構**を騙るフィッシングも確認。

▲金融系の偽サイト

ここで問題です。どっちが本物？

右記はauIDのログイン画面です。どちらが本物か、見分けられますか？

A. 正解は、左の画像です。
今のフィッシングサイトは、**画面をコピーして、そっくり同じもの**を作っています。**今回の見分けるポイントは、サイトアドレス**です。

左画像：connect.auone.jp ←本物のサイトアドレス
右画像：myau-net.com

フィッシング詐欺に騙されないための方法は？

本物そっくりの偽サイトに誘導し、アカウントの情報を入力させて情報を騙し取るために、多くのメールがばらまかれるようになりました。「自分は騙されない、大丈夫」と思っていても、実際に偽サイトを見てみると、本物のサイトに非常によく似せて作られていて、すぐには判断できません。

◆ **気をつけたいポイント**
- **ログインを急かすタイトル・内容のメールは疑ってかかる。**
- メール内のURLではなく、**ブックマークや検索からログイン**する。
- 本物か詐欺か迷うときは、**公式サイトと比べたり、メール内のタイトルなどを検索して詐欺メール情報を確認**する。
- **アカウントの2段階認証を設定**する。

ネット詐欺に騙されないためには、常に平常心を保ち、「ログインするだけで5,000円プレゼント!」といった、**一見おいしい話を疑うこと**を身につけましょう。

お問い合わせ
株式会社オーニシ
〒812-0016
福岡市博多区博多駅南5丁目15番32号
TEL：(092)451-1216 / FAX：(092)451-4348
担当営業
このカタログの記載内容は、2022年5月現在のものです