④ ボタンを見てもすぐに押さない

人の心理として、ボタンを見ると押したくなります。実際、添付ファイル付きのメールを受け取り、添付ファイルが怪しいとわかっていながら押してしまうこともあります。

しかし、「**押してしまえば被害に遭う**」と理解できていれば、押したいという気持ちを抑えることができるはずです。

~~編集を有効にする~~

~~コンテンツの有効化~~

しつこいくらいに従業員の方に対してサイバーセキュリティの重要性について教養を行い、安全な経営を継続しましょう。

★☆★ サイバー犯罪の侵入口はメールだけではありません ★☆★

Emotetを使ったサイバー犯罪においては、メールが悪用されたものが多数です。

しかし、2021年中にVPNやRDPといった単語とともに話題にあがった「脆弱性」に対しても、決して放っておいていいというものではありません。

サイバーセキュリティの対策といえば、基本中の基本である

① 修正プログラム（パッチ）をあてる

② OSやソフトウェアは最新の状態で使用するためアップデートする

③ ウイルス対策ソフト等セキュリティ製品を導入する

④ パスワードは英文字、数字、記号を含む複雑なものとし、使い回さないようにする

の４つは、人が目にすることができない部分を守ってくれるものだと認識し、確実に実施してください。

さらに、自社がサイバー犯罪の被害に遭わないための対策として、何をする必要があるのか確認の上、必要なセキュリティ製品の導入なども検討してください。

それでも被害に遭ってしまったら…

Emotetの感染発覚の経緯として、自社で検知できるセキュリティ製品を導入していない場合、突然、取引先から自社名義で不審なメールが送られてきたといった連絡を受けて発覚することがあります。

Emotetの感染は、感染した会社のメール情報（連絡先や本文内容）を使い、取引先等関係者に拡散していくことから、まずEmotetの感染実態を確認できるツール「**EmoCheck**」を使い事実確認をして、マルウェアの駆除作業に取りかかる、他の取引先に自社から不審なメールが送信される可能性があることを連絡し、感染を拡散させないため早期対応を心掛けましょう。

なお、サイバー犯罪の被害を受けた場合には、**近くの警察署への届け出**や、実害に至らずに済んだときでも、サイバーインシデントの対応や支援を行っている

・独立行政法人情報処理推進機構　情報セキュリティ安心相談窓口
https://www.ipa.go.jp/security/anshin/index.html

・JPCERTコーディネーションセンター　https://www.jpcert.or.jp/form

等の機関へ連絡・相談しておきましょう。

「EmoCheck」の使い方に関しては「マルウェア「Emotet(エモテット)」感染確認を！」
https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/CS_ad.files/EmoCheck.pdf
をご覧下さい。

警視庁では、サイバー犯罪やサイバーセキュリティに関する情報発信を行っています。

サイバーセキュリティインフォメーション　検索

https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/index.html

X（旧Twitter）
@MPD_cybersec

警視庁公式チャンネル
YouTube

街とともに、人とともに。
FOR MORE COMMUNICATION
けいしちょう

警視庁サイバーセキュリティ対策本部

20220301

いまの エモテット
Emotet
に対応できてますか？

注）Emotetに感染すると、勝手に取引先にマルウェアに感染したメールを送りつけるほか、PC内の機密データを知らぬ間に操作・窃取されたり、ランサムウェアがダウンロードされ、社内ネットワーク内のPCに感染を拡げて**金銭を要求**されたりするという被害につながる恐れがあります。

2014年　オンラインバンキングのアカウント情報（ユーザー名・パスワード）を窃取することを目的とした**トロイの木馬**（**バンキングマルウェア**）として認知

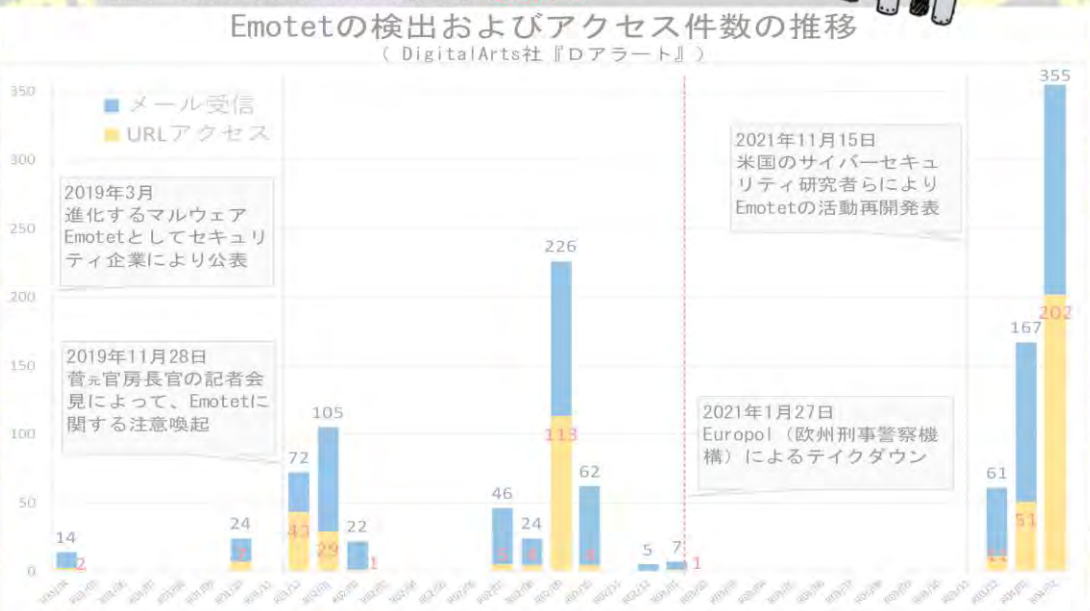
2017年　他のマルウェアや自己を拡散することを目的としたマルウェア（**ダウンローダー**）として進化

2018年　Microsoft Outlookの**メール収集機能**を確認
7月、米コンピュータ緊急事態対応チームが、被害の修復に約100万ドルを費やしたとする注意喚起を公開
同年**11月、日本国内でも検出**

2019年　11月、被害拡大（数か月間の停止と稼働を繰り返し攻撃を続行）

2021年　1月、**欧州刑事警察機構（EUROPOL）により**ボットネットを**テイクダウン（制圧）**
（Emotetを使用した攻撃を封じ込め）
11月、サイバー攻撃組織によるEmotetの**インフラが再構築**
・　通信にHTTPS（通信の暗号化）を使用
・　Officeファイルに加えアプリインストーラーの偽装
等、新たな手法とともに**復活**

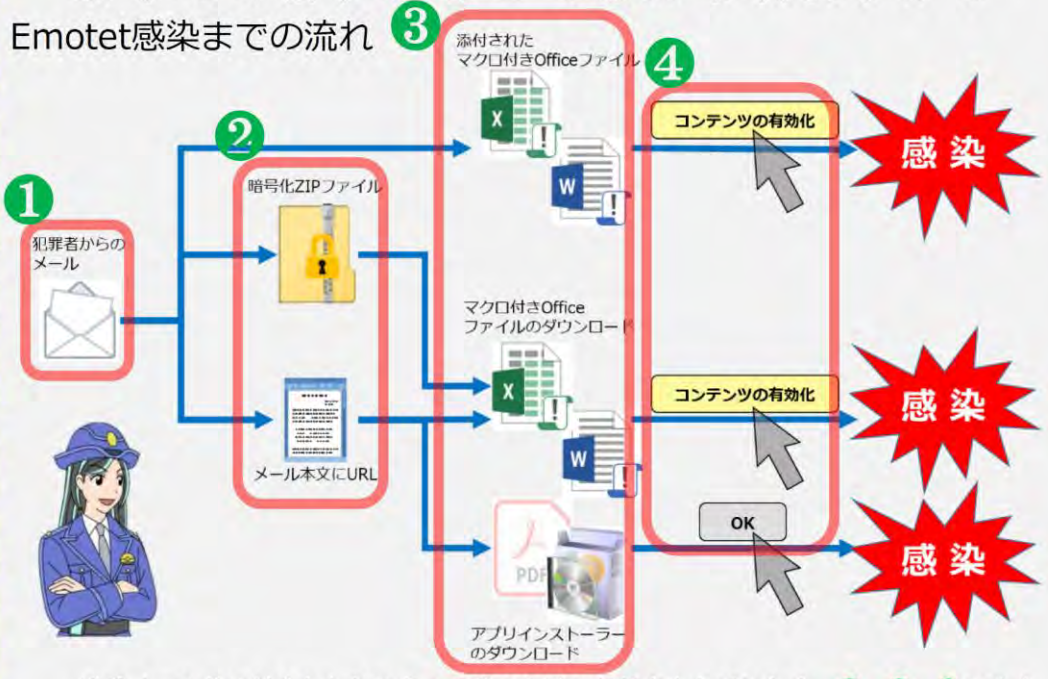
2022年　1月下旬からEmotetによる脅威**激増中!!**



引用　DigitalArts「Dアラート「サイバーリスク情報提供サービス」」の2019年1月から2022年3月1日までに公表数値を元にグラフ化したもの

あなたの会社、どこでとめられますか？

Emotet感染までの流れ



迷惑メール等に対応したシステムの導入や適切な設定をしていたら、❶・❷・❸の時点で感染を防ぐ確率は格段に上げられます。

しかし、システム等の隙を潜り抜け、マルウェアが仕込まれたファイルを従業員の方が開いてしまった後、❹のボタンが表示されたとき、従業員の方が認識して、感染させない自信は、どのくらいありますか？

マルウェアがセキュリティシステムを抜けてしまった後、最後の砦は従業員の方のサイバーセキュリティに関する意識です。

会社を守るため、従業員の方に対するサイバーセキュリティ教養を確実に行いましょう。

❶ 不審なメールだと思える意識、ありますか

最近、Emotet感染を目的としたサイバー犯罪を含み、犯罪者によって送られてくるメールの特徴に

- 日本語のメールに返信したかのような件名
- マクロが含まれるWordやExcel等のファイルが添付されている

といったものがあります。

たったこれだけの意識(認識)ですが、これを知っているか否かでサイバー犯罪の被害に遭う確率を下げることができます。

犯罪者は、これを「業」としているため、いかにしてお金を手に入れるかを考えており、人を騙すことを考えている状況ともいえるので、最新の犯行手口を日頃から意識して、被害に遭わないようにしましょう。

<Emotetメールの件名の一例>

賞与支払届
請求書の件です
会議への招待
Re: [redacted]
Fwd: [redacted]様[redacted]送ります　①
通知 2020 Jan 29
[redacted]メリークリスマス　②

①：取引先とのやり取りを偽装した件名
②：新型コロナウイルス等の時事ネタを本文とする時の件名

独立行政法人情報処理推進機構「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」より

❷ パスワード付きZipファイル（PPAP）やURLリンク、当然のようにクリックしていませんか？

犯罪者は、ターゲットにマルウェア感染させなければ犯行は成功しません。そこで悪用されているのが、今や当たり前のように誰もが使っている電子メールです。

そのため、マルウェアを仕込んだメールをターゲットの手元まで確実に届けるため、ウイルス対策ソフトなどのセキュリティ製品に検出されないように

- 悪用したマクロ機能を載せたOfficeファイルをパスワード付きzipファイルに入れて送る
- 確実に受信させた後、マルウェアをターゲット本人にダウンロードさせるため、メールの本文にURLリンクを貼って送る

という手法を使ってきています。

安易にクリックしてマルウェア感染してしまうと、犯罪者の思惑どおりになりますので、気をつけましょう。

❸ Officeファイルだけではなくなった!?

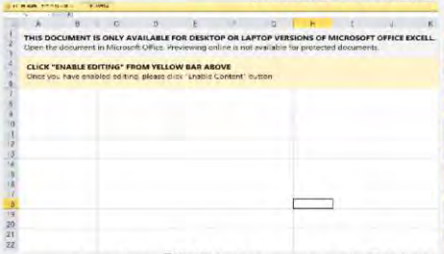
Emotetの感染事象で最も有名な犯行手口といえば、添付ファイルとして送られたOfficeファイルのマクロ機能の悪用です。

マルウェアに感染させるため、まずはターゲットにマクロを起動させるため、ファイルを開いた際に表示される[コンテンツの有効化]ボタンを押させようと企んでいます。

今のところ、Officeファイルを開いてしまったとしても、[コンテンツの有効化]ボタンさえ押さなければ、Emotetに感染することはないと言われていますが、だからといって開いても安全という保証はありません。

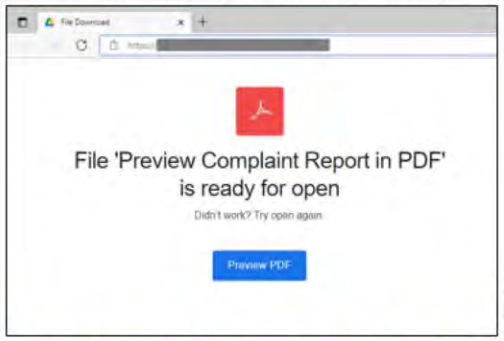
そんな中、新たな手口として登場したのが、アプリのインストーラーのダウンロードを装った手口です。スマートフォンを使っている方であれば、アプリをダウンロードすることに違和感が少ないところを突いた攻撃ともいえます。

↑Wordファイル画面　↓Excelファイル画面



DigitalArts「復活したEmotetの1か月」より

この手口は、メール本文中のURLをクリックすると、閲覧可能なPDFファイルが存在するかのようなページへ誘導され、そこでPDFファイルの閲覧ソフトを装ったウイルスファイルをダウンロードさせ、マルウェアに感染させるというものです。



2021年11月のEmotet再稼働でニュースとして報じられた際には、PDF文書用のダウンロードという手口が発見されましたが、今後、他のアプリのインストーラー等をダウンロードさせる手口が出てくることも想像できます。

どんな新手が出たとしても、知っていれば被害を防ぐことも可能です。

独立行政法人情報処理推進機構（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」より