2019 年 12 月 23 日

サービス＆セキュリティ株式会社 e-Gate センター

マルウェア「Emotet」(エモテット)最新攻撃メールについて

1. 概要

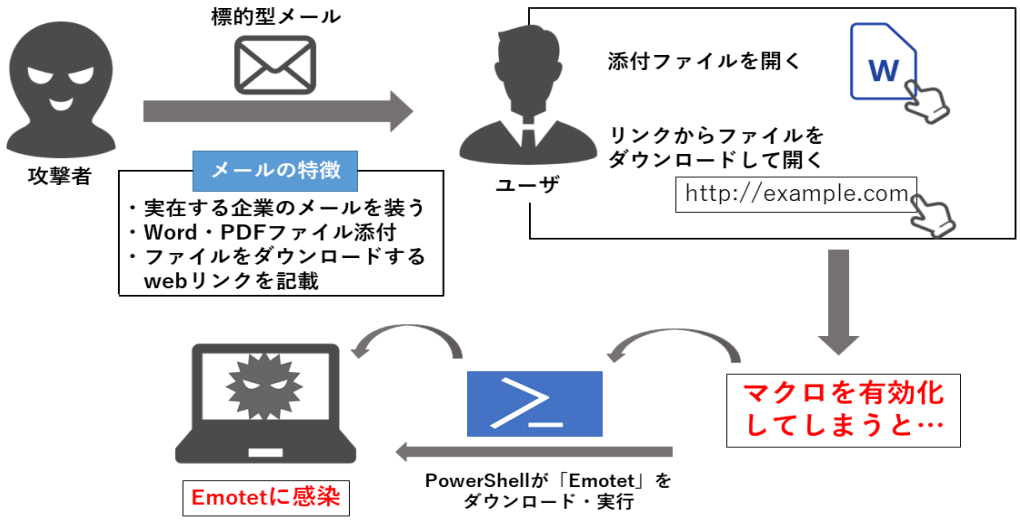
マルウェア「Emotet」(エモテット)による被害拡大が複数のサイバーセキュリティ情報サイトより公開されています。「Emotet」は変化・進化を続けているマルウェアとして知られていますが、現在日本国内にて感染が拡大している要因はマルウェア自体の変化・進化ではなく「メールによる配布」の巧妙化です。最近の不正なメール(以下、攻撃メール)は巧妙化がますます進んでいます。メールには関係者や当事者しかわからない文面があることから、事前に情報の窃取が行われ、その情報が巧みに悪用されていると推測されます。本稿では最新攻撃メールの実例とセキュリティ対策や関連情報をご紹介いたします。

2. 「Emotet」(エモテット)とは

「Emotet」は 2014 年観測当時、銀行の認証情報搾取を目的としたバンキングマルウェアとして認知されていました。しかし、この 5 年の間に新たな地域や業界を狙い、他の種類のマルウェアをダウンロードし拡散するローダーとして進化しました。感染すると重要なファイルが窃取され、同ネットワーク内の端末にまで感染する恐れがあります。

「Emotet」の感染拡大を狙う攻撃者は、特定の相手に絞った「標的型攻撃」を攻撃対象に行います。標的型攻撃で使われる攻撃メールは「標的型メール」と言われます。標的型メールは日々巧妙化しており、「Emotet」に限らず標的型メールに対しては注意が必要です。

「Emotet」の感染パターンですが、下図 1 のように攻撃者による標的型メールに添付された Word 形式ファイルから感染します。



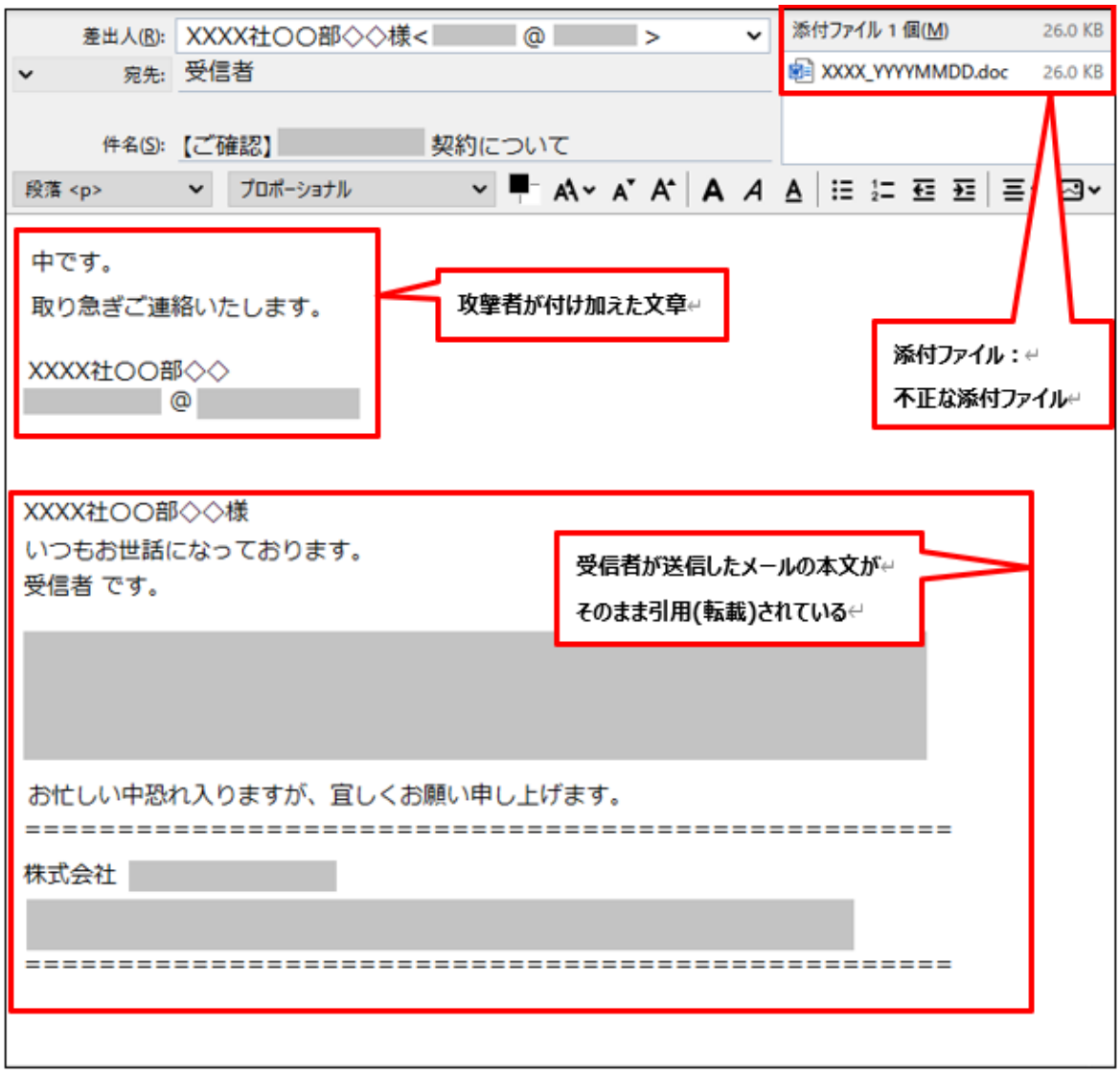
【図 1】「Emotet」感染イメージ

※ 「Emotet」の詳細は以下 URL をご参照ください。
『注意喚起:進化するマルウェア「Emotet」について』
https://www.ssk-kan.co.jp/topics/topics_cat05/?p=9657

次項で攻撃メールがどのようなものか、ご説明いたします。

3. 最新攻撃メール（攻撃者による標的型メール）の特徴

セキュリティ対策による攻撃メールの受信遮断や受信者自身の気付きによって添付ファイルをむやみに開くことは少ないと思われますが、攻撃メールの巧妙化により受信者が気付きにくくなっており、添付ファイルが開かれるケースが増えています。下図 2 は巧妙化する攻撃メールの例です。特徴部分に赤枠で注釈を記載しております。



【図 2】「Emotet」の感染を狙う攻撃メールの例

図２の攻撃メールの例に対して注意すべき点は以下のようなものが挙げられます。

■ 送信元

攻撃者は受信者の取引先になりすます為、送信元アドレスは存在するものになっています。

■ 件名

受信者が実際に送信していた過去のメールの返信であるかのような件名になっています。

■ 本文

メール本文も受信者の過去メールから引用された文章と攻撃者が付け加えた日本語文になっており、実在する受信者の取引先署名と読み取れる署名も追記されています。
表１は攻撃者が付け加えていた文章の実例の一部です。

【表 1】 文面の例

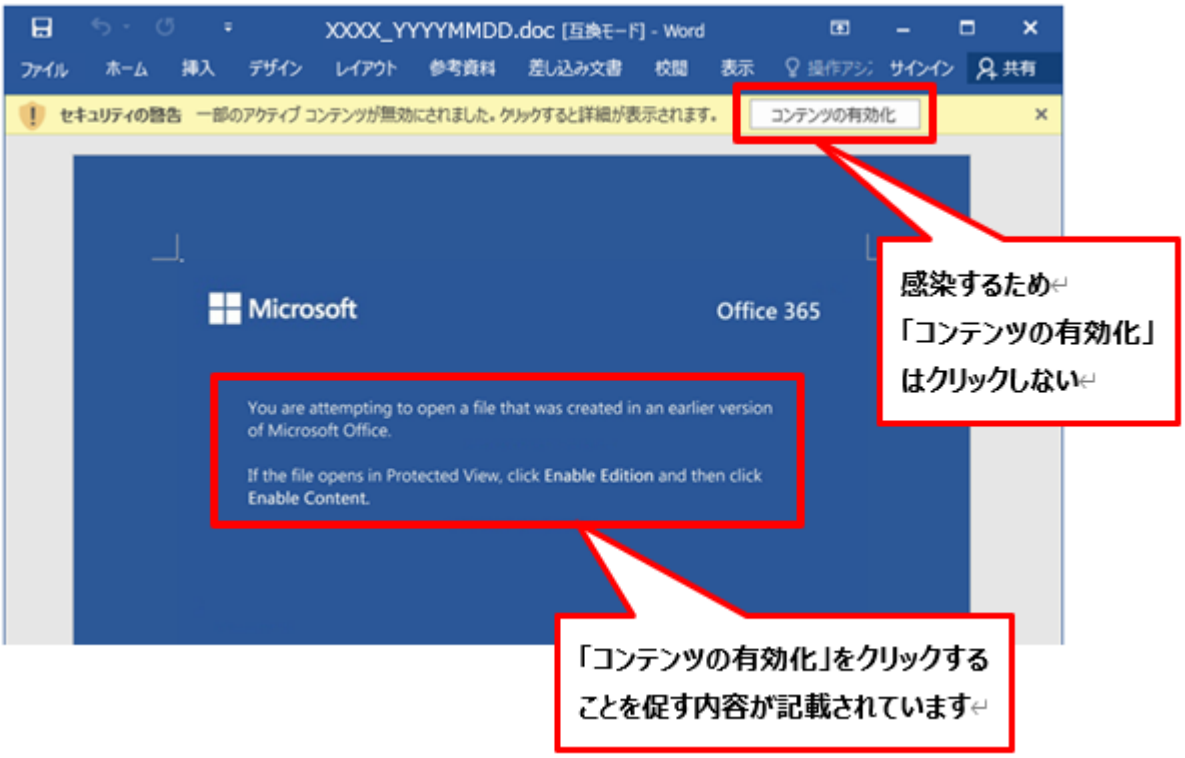
おはようございます。 謄本及び公図を送りします。 どうぞよろしくお願い申し上げます。
おはようございます。 本件 ついて は今回触れておりませんが 以上、よろしくお願い致します。
おはようございます。 約款について送らせていただきます。 取り急ぎご連絡いたします。
支援機能は、添付のリストから選定願います 以上、よろしくお願い致します。
おはようございます。 訂をお願いします。
予定です。 取り急ぎご連絡いたします。

これらの文章のほかに件名や文面が受信者と全く関係のないケースや引用部分の存在しないケース等も存在します。多くは１行から３行程度で、不自然な点があるものの受信者が攻撃メールとはっきりと判断できるものではありません。また、今後攻撃者側の技術向上によってはさらに文章精度も向上し、文面のみの確認では攻撃メールと判断することが更に困難になると思われます。

■ 添付ファイル

Word 形式のファイルが添付されていますが、添付ファイルを開かない限り感染することはありません。

下図 3 は添付ファイルを開いてしてしまった場合の画面例です。



【図 3】 添付ファイルを開いた時の画面の例

コンテンツの有効化を促す内容が記載されており、有効化してしまうと「Emotet」がダウンロードされてしまいます。

Microsoft Office 内の「マクロの設定」という項目を変更している場合、有効化の警告が表示されずに「Emotet」がダウンロードされてしまう場合があります。

また、「Emotet」に限らず、メールと添付ファイルを使用した攻撃に Office ファイル(Word や Excel 等)のマクロ機能を利用したものは少なくありません。信用できない添付ファイルは開かないこと、開いてしまってもコンテンツの有効化をしない、もしくは編集を有効にしないことを推奨します。

攻撃メールの巧妙な点は、①受信者を絞り込み、②受信者が過去に送信したメールを事前に窃取し、③攻撃者を正当な返信者と誤認させるところにあります。また、攻撃者が事前に窃取しているということは、今回の攻撃メールとは別の方法で受信者の情報が流出している可能性が極めて高く、受信者以外(組織内の他のユーザやなりすまされた取引相手等)のセキュリティ対策についても確認が必要です。

4. 攻撃メールへの対策について

「Emotet」の感染を防ぐ為、その対策をご紹介します。この対策は「Emotet」の感染のみを防ぐものではなく、ウイルス全般に有効なものとなりますので、今後導入されることを推奨します。

- 身に覚えのないメールを開かない
- 身に覚えのないメールの添付ファイルを開かない
- 身に覚えのないメールに記載のある URL をクリックしない
- 例え自身が送信したメールへの返信メールであっても不自然な点があれば添付ファイルを開かない
- 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
- 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
- メールや文書ファイルの閲覧中、身に覚えのない警告ウイ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
- 組織内への注意喚起を行う

「～ ない」もしくは「～ しない」とした前半 5 つの対策は、人為的ミスによってウイルス感染するリスクを孕んでいますが、後半 4 つの対策は、人為的ミスから発生した感染リスクを軽減し、事後対応とはなりますが感染拡大を防ぐことにもつながりますので特に実施することを推奨します。

上記、対策を実施したにもかかわらず以下のような状況を確認した場合は、自身が所属する組織内において「Emotet」に感染した端末が存在する可能性があります。

- 組織内のメールアドレスになりすまし、Word 形式のファイルを送るメールが届いたと別組織から連絡を受けた場合
- 組織内のメールサーバなどを確認し、Word 形式のファイルが添付されたメールや、なりすましメールが大量に送信されていることを確認した場合

組織内の端末やシステムにおいて「Emotet」の感染が確認された場合、被害拡大防止の観点より初期対応として以下の対処を行うことを推奨します。

- 感染した端末のネットワークからの隔離
- 感染した端末が利用していたメールアカウントのパスワード変更

その後、必要に応じてセキュリティ専門ベンダなどと相談の上、以下のような対処を行うことを推奨します。

- 組織内の全端末のウイルス対策ソフトによるフルスキャン
- 感染した端末を利用していたアカウントのパスワード変更
- ネットワークトラフィックログの監視
- 調査後の感染した端末の初期化

5. 参考情報

独立行政法人情報処理推進機構（IPA）

- 「Emotet」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

一般社団法人 JPCERT コーディネーションセンター

- マルウエア Emotet の感染に関する注意喚起
  https://www.jpcert.or.jp/at/2019/at190044.html

6. e-Gate の監視サービスについて

上記の攻撃メールへの対策を行ったうえで、よりセキュリティ対策を強固にするために、”e-Gate”の MSS の導入をご検討ください。e-Gate サービスでは 24 時間 365 日で監視を行います。サイバー攻撃への対策としてセキュリティ機器を導入する場合、それらの機器の運用監視を行い、通信が攻撃かどうかの分析、判断をして、セキュリティインシデント発生時に適切に対処できるようにすることが重要です。“e-Gate“のセキュリティ監視サービスをご活用頂きますと、迅速なセキュリティインシデント対応が可能となります。

■総合セキュリティサービス e-Gate

SSK（サービス＆セキュリティ株式会社）が 40 年以上に渡って築き上げてきた IT 運用のノウハウと、最新のメソッド、次世代 SOC“e-Gate センター“この 2 つを融合させることによりお客様の情報セキュリティ全体をトータルにサポートするのが SSK の“e-Gate”です。e-Gate センターを核として人材・運用監視・対策支援という 3 つのサービスを軸に全方位のセキュリティサービスを展開しています。

【参考 URL】
https://www.ssk-kan.co.jp/e-gate/

«お問合せ先»
サービス＆セキュリティ株式会社
〒150-0011
東京都渋谷区東 3 丁目 14 番 15 号 MO ビル 2F
TEL 03-3499-2077
FAX 03-5464-9977
sales@ssk-kan.co.jp