2019 年 3 月 26 日

サービス＆セキュリティ株式会社 e-Gate センター

# 注意喚起:進化するマルウェア「Emotet」について

## 1. 概要

AI 技術を用いるなどセキュリティが進化していく中で、マルウェアも日々進化しています。
「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。
米コンピュータ緊急事態対策チーム（US-CERT）は、2018 年 7 月に Emotet による被害の修復に約 100 万ドルを費やしたとする注意喚起を公開しています。日本国内も例外ではなく、2018 年 11 月には日本国内でも検出されており今後の被害拡大が懸念されています。

今回は、「Emotet」の進化の歴史と、現在確認されている最新のマルウェア動向と対策についてご紹介いたします。

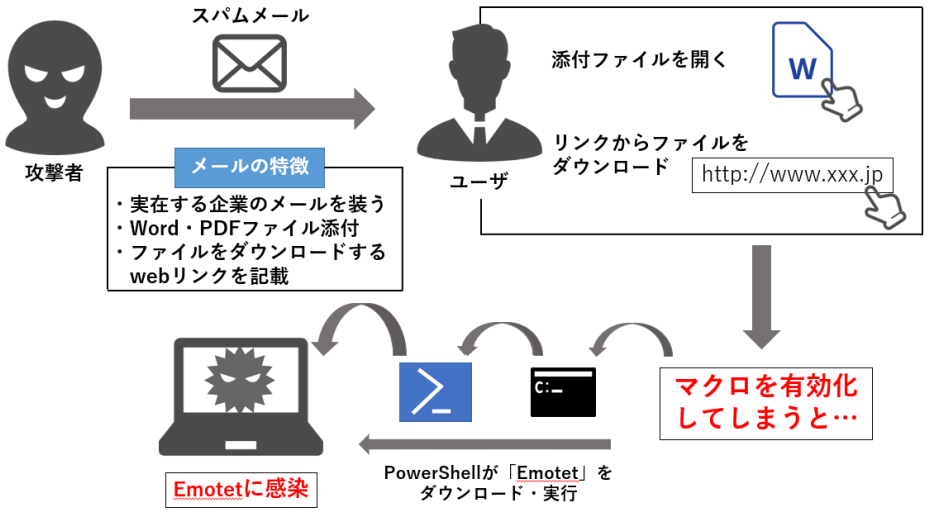
## 2. 進化の歴史

前述の通り 2014 年に観測されて以来、下記のような進化を遂げています。
2014 年:オンラインバンキングを標的としたトロイの木馬として利用
2015 年:標的地域を拡大しモジュール性の強いマルウェアへと進化
2017 年:他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へと進化
2018 年:Microsoft Outlook のメール収集機能が確認される

特に 2017 年の進化はターニングポイントでありシマンテック社は、銀行側の対策が進んだことで、他の収益源としてマルウェア拡散にビジネスモデルを変化させた可能性があると推測しています。
被害者側の対策が強化されることで今後も攻撃手法が異なるマルウェアへの進化が予想されます。

## 3. 「Emotet」概要

(1) 感染経路
「Emotet」の感染経路はメールです。攻撃者は企業やその組織関係者を装ったメールを送付します。
メールには Word ファイルや PDF ファイルが添付されていたり、web サイトから Word ファイルをダウンロードするためのリンクが含まれています。ユーザがファイルを開きマクロを有効にしてしまうと Microsoft CMD(コマンドプロンプト)、PowerShell が実行され外部の制御用サーバ(C&C サーバ)への接続が発生し、最終的に Emotet 本体である exe ファイルがダウンロード・実行されます。




【図 1】「Emotet」感染のイメージ

(2) 感染後の動き

① 自身のアップデートと拡張機能の追加

・C&C サーバへ接続しアップデートすることで常に最新の Emotet を感染 PC に設置します。

・主な目的となる機能を持った部品(モジュール)をダウンロードし、拡張機能を追加します。

② 情報窃取

・メール内容や設定情報、あらゆる認証情報を窃取し、C&C サーバへ送信します。

③ 自己拡散

・窃取したメール情報を利用して自身の送付を行います。

・Windows のネットワーク環境でファイル共有などに利用される「Server Message Block（SMB）」プロトコルの脆弱性を悪用してネットワーク内で横方向に広がる仕組みを備えているモジュールを利用し拡散します。

・感染端末上のシステムに保存されているパスワード情報を窃取し、同じネットワーク上のコンピュータに対する総当たりアクセスを試みます。

・他種類のマルウェアの感染を広めます。

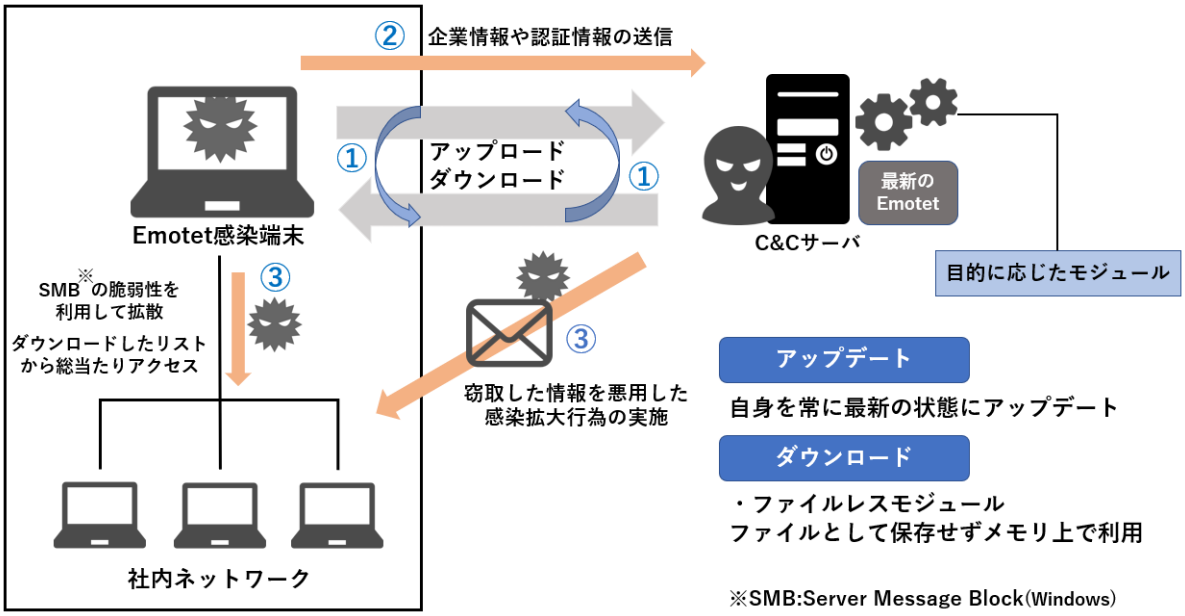
以下の耐解析機能も備えています。

・ファイルレスモジュール

ダウンロードしたモジュールをファイルとして保存せずにメモリ上で利用します。本体には目立った不正な処理のコードを置かないことでウイルススキャンソフトから検出されづらくなります。

・複数の C&C サーバへの接続

Emotet 本体には、複数の C&C サーバの接続先情報が存在します。複数のアドレスを使用することにより追跡を撹乱します。




【図 2】感染後の動きのイメージ

このように感染コンピュータを踏み台とし、窃取した情報を利用した精度の高い有効な攻撃で周囲のコンピュータに感染させ、組織内で拡散しています。

## 4. 「Emotet」への対策

感染後の攻撃手法は脅威ではありますが、標的型攻撃メールの対策を実施していれば感染のリスクは大幅に軽減されます。しかし、アップデートによって攻撃手法が大きく変更され対策を行っていたとしても感染してしまう恐れがあります。
いち早く感染に気付くためにも監視体制を徹底しておくことが肝要です。

### 運用管理対策

- 不審なメールのリンクや添付ファイルを開かない。
- マクロが無効化されていることを確認し、文書ファイルのマクロは有効化しない。
- 定期的なパスワード変更、多要素認証を導入。
- 定期的なバックアップの取得。
- OS、ソフトウェア、セキュリティ製品を常に最新の状態に更新しておく。

### 技術的対策

- メール無害化等の標的型メール攻撃対策製品の導入。
- 悪性 IP(C&C サーバ)との通信遮断機能を持った製品の導入。
- PowerShell の起動制限設定。

PowerShell のポリシーでの無効化では、バイパスされる恐れがあります。
PowerShell 自体の起動を制限しておくことを推奨いたします。

**検出対策**

- ウイルス対策ソフトなどの定義ファイルを常に最新の状態に更新しておく。
- ネットワークを常時監視し、C&C サーバ等への不審な外部通信や内部の拡散活動の検知。
- 未知のマルウェアから防御可能なエンドポイント対策製品の導入。

不審なメールを開いたり、マクロを実行しないよう定期的なユーザ教育を実施することが対策へと繋がります。
また、被害にあわないよう定期的に情報収集し、情報に合わせた有効な対策を実施することをお勧めいたします。

## 5. e-Gate の活用について

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うことが重要です。
24 時間 365 日有人監視体制のセキュリティ監視サービス “e-Gate“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、最新の分析システムを活用し精度の高い検知、また専任のアナリストによる分析を行っております。
“e-Gate”の MSS の導入をぜひご検討ください。

■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/

## 6. 参考情報

- 米コンピュータ緊急事態対策チーム US-CERT
  Emotet 注意喚起(英文)
  https://www.us-cert.gov/ncas/alerts/TA18-201A

- ESET
  バンキングマルウェア「Emotet」が国内で流行の兆し
  https://ascii.jp/elem/000/001/789/1789760/

- Trend Micro
  「EMOTET」運用の仕組み
  https://blog.trendmicro.co.jp/archives/20222

※本資料には弊社が管理しない第三者サイトへのリンクが含まれています。各サイトの掲げる使用条件に従ってご利用ください。リンク先のコンテンツは予告なく、変更、削除される場合があります。



**«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