2021 年 12 月 28 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:テイクダウンされたマルウェア「Emotet」（エモテット）が活動再開

## 1. 概要

マルウェア「EMOTET」（エモテット）は 2017 年から存在が確認されているマルウェアです。外部にあるコマンド＆コントロール（C&C）サーバ（※1）から命令を受けて感染した端末にて不正活動を行いボットに分類されます。世界各国にて猛威を振るっていましたが、国際的な共同作戦が実施された結果、2021 年 1 月にはテイクダウン（無害化）が成功したとEUROPOL（欧州刑事警察機構）により発表されました。

しかし、2021 年 11 月 15 日以降、テイクダウンされていたはずの Emotet の活動再開が日本を含む世界各国にて確認されています。今回はこの活動再開した Emotet について活動再開の経緯や前回の感染拡大時との違いなどについてご紹介いたします。

※1:マルウェアに感染し攻撃者に乗っ取られた機器を「ボット」、ボットに対して攻撃の指示を出すサーバを「コマンド＆コントロール（C&C）サーバ」と呼びます。

## 2. 「Emotet」活動再開までの経緯

Emotet の初観測からこの度の活動再開までの時系列の概要については下記表 1 のとおりです。

| 年月 | 経緯 |
|---|---|
| 2014 年 | 銀行の認証情報を搾取するマルウェアとして Emotet を観測 |
| 2017 年～2019 年 | 他のマルウェアをダウンロードする機能を持つ「ローダー」として進化 |
| 2019 年 11 月 | メディアに取り上げられたことで世間での知名度が上がる |
| 2020 年 2 月 | JPCERT/CC の調査により 3,200 以上の国内組織の Emotet 感染が判明 |
| 2021 年 1 月 | EUROPOL（欧州刑事警察機構）により Emotet のボットネットのテイクダウン（無害化）が成功 |
| 2021 年 2 月 | 日本の総務省は国内の Emotet 感染の疑いがある端末の利用者に対して、感染の有無について調査し、もし感染していた場合は Emotet の除去を行うよう注意喚起を行う |
| 2021 年 11 月 | 「Trick bot」というボットネットを介してテイクダウンされていた Emotet が活動再開 |

【表 1 】Emotet 初観測から活動再開までの時系列

さらに、一度テイクダウンされた Emotet が活動再開し、被害を拡大させている背景には以下のような要因があります。

- 作成方法やノウハウの流用・継承

2021 年 1 月のテイクダウンにおいて Emotet を主導していた主要なハッカー集団は検挙されました。しかし、今回の活動再開では検挙された集団とは別のハッカー集団が Emotet の作成方法や運用ノウハウを何らかの手段で流用もしくは継承し、活動を行っているとみられています。

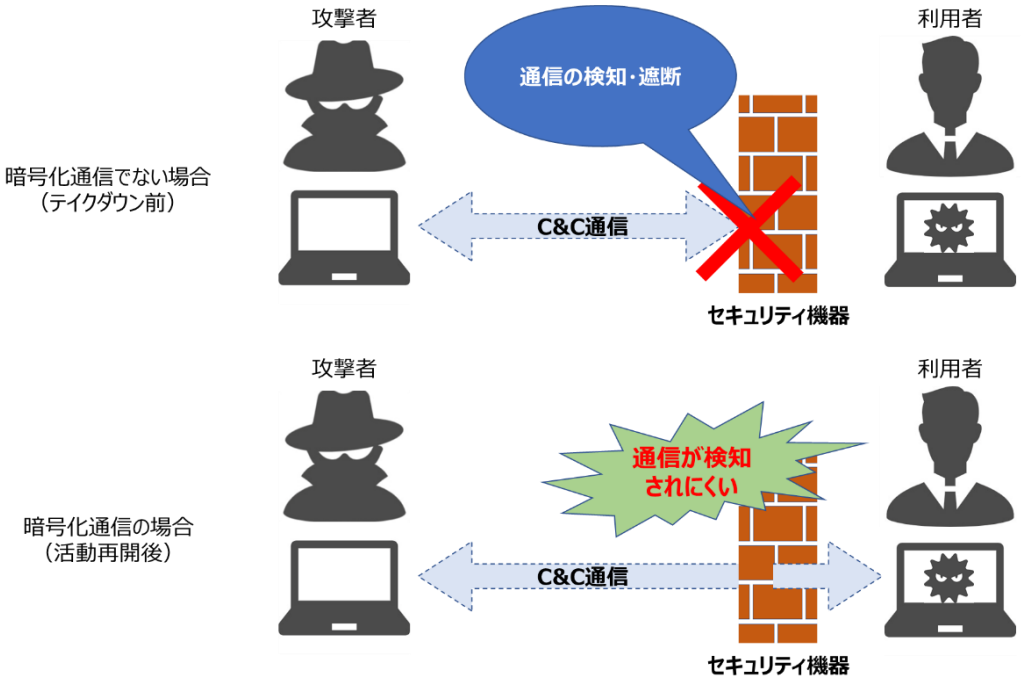

【図 1】作成方法やノウハウの継承

- 新たなボットネットの構築

2021 年 1 月のテイクダウン以降、それまで構築されていたボットネットは徐々に無害化されていきました。しかし、今回の活動再開により新たなボットネットが構築され始めたことで、テイクダウン以前の Emotet と同様な脅威となりつつあります。

- Emotet 自体の巧妙化

2021 年 1 月のテイクダウン以前に比べ C&C 通信が見つけにくく Emotet 自体が巧妙化されているため、感染に気付くことが遅れ被害がより拡大する恐れがあります。巧妙化の詳細につきましては後述の「3.活動再開前後の「Emotet」における共通点と相違点」にて説明しています。




【図 3】Emotet 自体の巧妙化

また、以下の過去に取り上げた Emotet に関するセキュリティニュースをご参照ください。
『マルウェア「Emotet」(エモテット)最新攻撃メールについて』（2019 年 12 月）
https://www.ssk-kan.co.jp/topics/topics_cat05/?p=10400

『Emotet テイクダウン成功後の現状と今後の対策』（2021 年 3 月）
https://www.ssk-kan.co.jp/topics/topics_cat05/?p=11545

## 3. 活動再開前後の「Emotet」における共通点と相違点

2021 年 1 月のテイクダウン以前と 2021 年 11 月の活動再開後の Emotet において主に下記のような共通点と相違点が確認されています。

＜共通点＞

- メールを利用して Emotet に感染させる手口を用いる点

  Emotet の感染を目的とした攻撃では、「実在するメール」への返信を装ったメールが利用されることがよくあり、Word ファイルや PDF ファイルが添付されるほか、メール本文中に URL リンクが記載されていることがあります。これらのファイルを有効化してしまう、または URL リンクにアクセスすることで、対象の端末機器が Emotet に感染してしまいます。

- Emotet 以外の様々なマルウェアに感染させられる点

  Emotet は単なるマルウェアではなく他のマルウェアをダウンロードする「ローダー」としての役割も持っています。そのため一般的なマルウェア感染の際に起こる情報漏洩被害のみならず、不正取得した個人情報などの重要な情報と引き換えに金銭を要求する「ランサムウェア」や、機器内のデータを破壊してしまうようなマルウェアによる被害も受けてしまう場合があります。

Emotet 活動再開後は上記の「共通点」にて言及した手口のほかに、新たな手口として「Excel ファイルを悪用する手口」と「PDF 閲覧ソフトを偽装する手口」の 2 つが確認されています。

＜相違点＞

- Excel ファイルを悪用する手口が用いる点

  メールの添付ファイルとして Excel ファイルが用いられる点以外はこれまでの Word ファイルの場合と同様の手口です。

- PDF 閲覧ソフトを偽装する手口が用いる点

  メール本文中に記載された URL リンクをクリックすると偽のウェブサイトに誘導されるという手口です。利用者は偽のウェブサイト上にて PDF 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られることで Emotet に感染します。

- 通信が難読化している点

  テイクダウン以前は C&C サーバやボットネットの通信は暗号化されていなかったため、不審な通信内容を検知することができました。しかし、Emotet 活動再開後は HTTPS などの暗号化通信を利用し、通信の巧妙化が確認されています。そのため、通信の特徴をもとに Emotet 関連の通信を検知することは以前より難しいです。

## 4. 「Emotet」を含むマルウェアへの対策方法

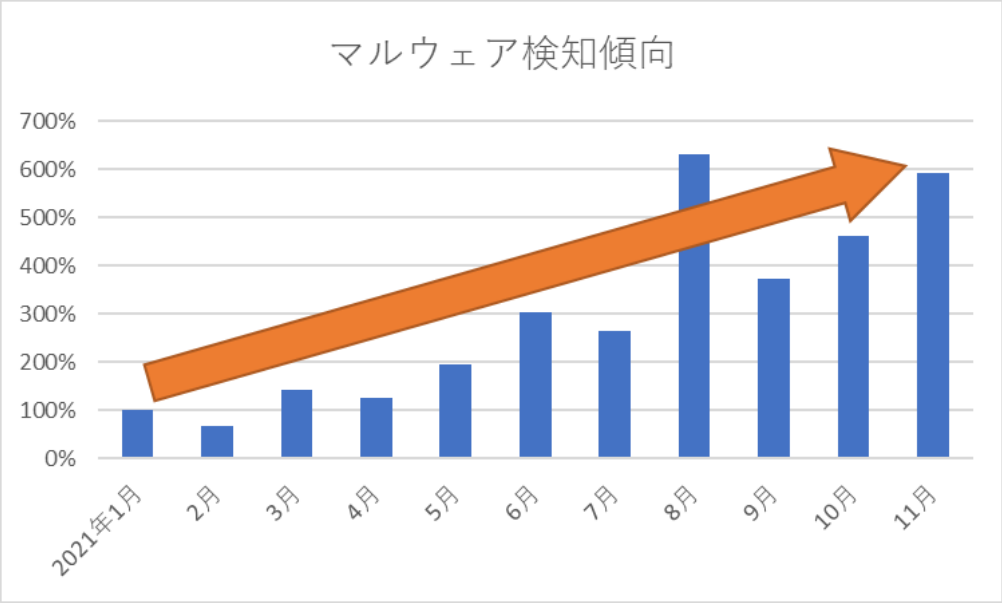
Emotet の攻撃と同様にメールを利用した標的型攻撃に対しては下記のような対策が有効です。

- 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 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
- メールセキュリティ製品の導入
- マルウェア不正通信ブロックサービスの導入
- ソフトウェアのマクロ自動実行機能の無効化

## 5. e-Gate センターにおける攻撃検知の推移

e-Gate センターのマルウェア関連の攻撃統計について 2021 年 1 月からの状況は下図４のように全体としては増加傾向です。マルウェアを利用したサイバー攻撃は 2021 年 1 月に Emotet がテイクダウンされたことで一旦減少しましたが、その他のマルウェアを利用した攻撃は日々増加していると考えられます。

また、8 月に件数が一時的に増加している点については東京オリンピック・パラリンピック関連のサイバー攻撃の増加が影響していると考えられます。




【図 4】e-Gate センターにおけるマルウェア検知傾向

（2021 年 1 月を 100%として算出）

## 6. 参考情報

・LAC

【注意喚起】マルウェア Emotet が 10 カ月ぶりに活動再開

https://www.lac.co.jp/lacwatch/alert/20211119_002801.html

・lanscope

最恐のマルウェア“Emotet（エモテット）”を徹底解剖。特徴と今必要な対策を解説します。

https://www.lanscope.jp/trend/16983/

・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

https://www.ipa.go.jp/security/announce/20191202.html

## 7. e-Gate の監視サービスについて

e-Gate のセキュリティ機器運用監視サービスでは、24 時間 365 日、リアルタイムでセキュリティログの有人監視を行っております。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いただきますと、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。

また、e-Gate の脆弱性診断サービスでは、お客様のシステムにて潜在する脆弱性を診断し、検出されたリスクへの対策をご提案させていただいております。

監視サービスや脆弱性診断サービスをご活用いただきますと、セキュリティインシデントの発生を予防、また発生時にも迅速な対処が可能なため、対策コストや被害を抑えることができます。

■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」と最新のメソッドで構築した「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”サービスです。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