【注意喚起】マルウェアEmotetが10カ月ぶりに活動再開、日本も攻撃対象に | LAC WATCH

By サイバー救急センター

Published: 2021-11-19 · Archived: 2026-04-05 13:21:50 UTC

サイバー救急センターの脅威分析チームです。

日本時間の2021年11月15日、マルウェアEmotetの活動が再開され、11月17日頃から日本組織においても攻撃メールが届き始めていることを当社で確認しています。

これまでEmotetは、その攻撃手口から世界中で大きな被害をもたらし、当社では二度に渡り注意喚起を行ないました。現在は検知数が少ない状況ですが、このような背景から今後猛威をふるう可能性が十分考えられます。本注意喚起では、活動を再開したEmotetのポイントをまとめましたので対策にお役立てください。

関連記事

- 【注意喚起】猛威をふるっているマルウェアEmotetの検知状況について
- 【注意喚起】猛威をふるっているマルウェアEmotet検知数の急増と対策について

目次

Emotetの手口

Emotetへの感染は、Emotet自体が配信するメールによって引き起こされるケースと、自組織内の他の感染PCから横展開（ラテラルムーブメント）で感染するケース、Trickbotと呼ばれる別のマルウェアから二次感染するケースの3通りが確認されています。これらのうちメールに関しては、窃取されたメールの内容が悪用されて返信形式で届くことがあり、ユーザが開封しやすく注意が必要です。

Emotetの感染を目的としたメールは、過去の経緯を踏まえると、メール本文にURLリンクが記載されているもの（A）や、メールにファイルが添付されているもの（B,C,D）の4パターンが考えられます（図1）。11月17日時点ではA、C、Dの3パターンのメールが観測されている状況です。PDFファイルを使用したBのパターンについては確認していませんが、従来のEmotetが利用していた手口であり、今後悪用される可能性があるため、注意しておく必要があります。

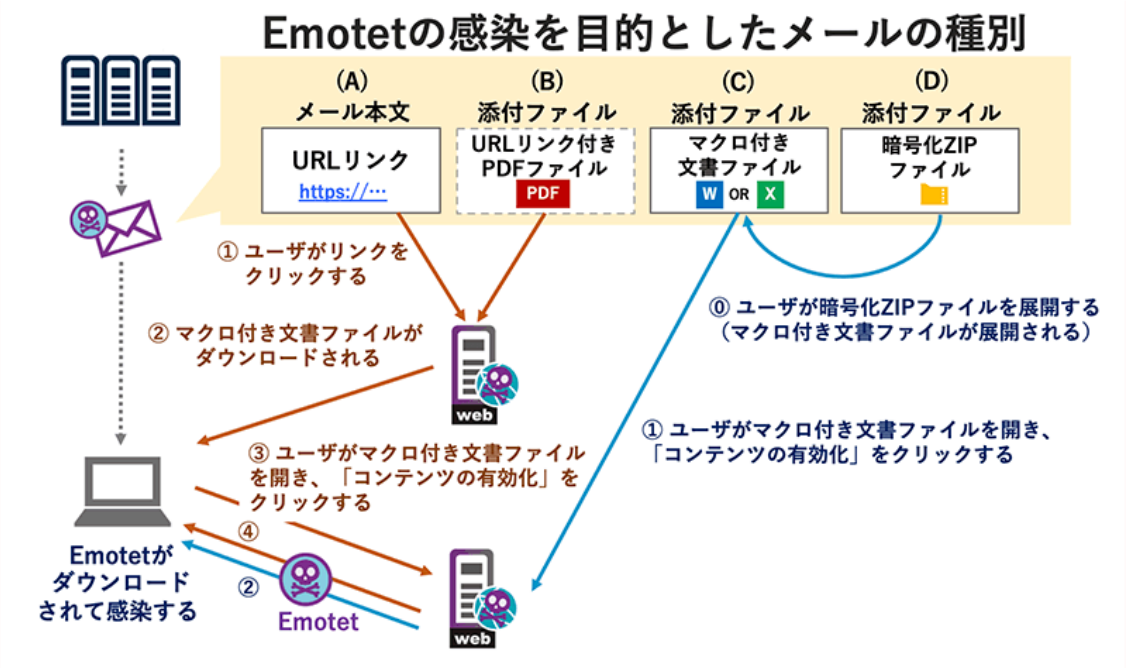


図1 Emotet感染までの流れ

いずれのケースでも最終的に不正なマクロ付き文書ファイルをユーザが開き、「コンテンツの有効化」をクリックすることでマクロが実行され、Emotetをダウンロードした後に感染に至ります。Emotetに感染してしまった場合は、ユーザの気づかないうちに、メールや添付ファイル、メールアドレス、Webブラウザやメーラーに保存されたパスワードなどの情報が窃取されることや、Emotetへの感染を引き起こすメールを他の組織や個人に送信することがあります。

また、自組織内のネットワークの他のPCへ感染を広げる機能も存在するため、自組織の多数のPCがEmotetに感染する可能性もあります。これらの動作は、Emotetが追加機能（モジュール）をダウンロードした場合に起こるものであるため、被害は環境や状況に応じて異なります。

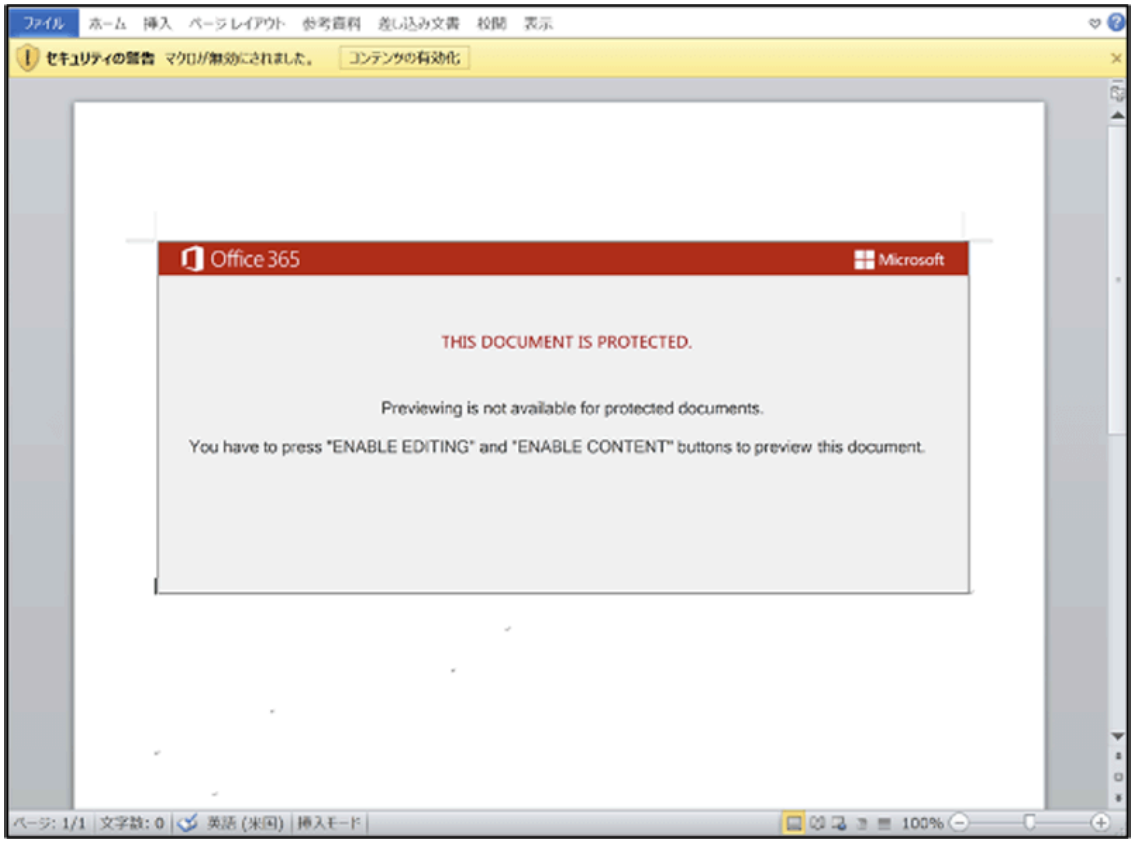
その他、Emotetの感染後にランサムウェアやバンキングマルウェアなどの他のマルウェアに追加で感染する過去事例も当社では確認しています。

これまでのEmotetとの相違点

新しいEmotetは以前のものから変更が加えられており、通信の方法やデータの暗号化手法などが異なります。ここでは相違点を紹介します。

文書ファイル（ダウンローダ）

ダウンローダとしては、docm形式とxlsm形式の文書ファイルが確認されています。文書ファイルを開いた場合、図2の内容が表示されます。このとき「コンテンツの有効化」ボタンをクリックすると、マクロが実行されてEmotetをダウンロードする通信が発生します。なお、文書ファイルの内容は頻繁に変更されるため、下図以外のケースにご注意ください。



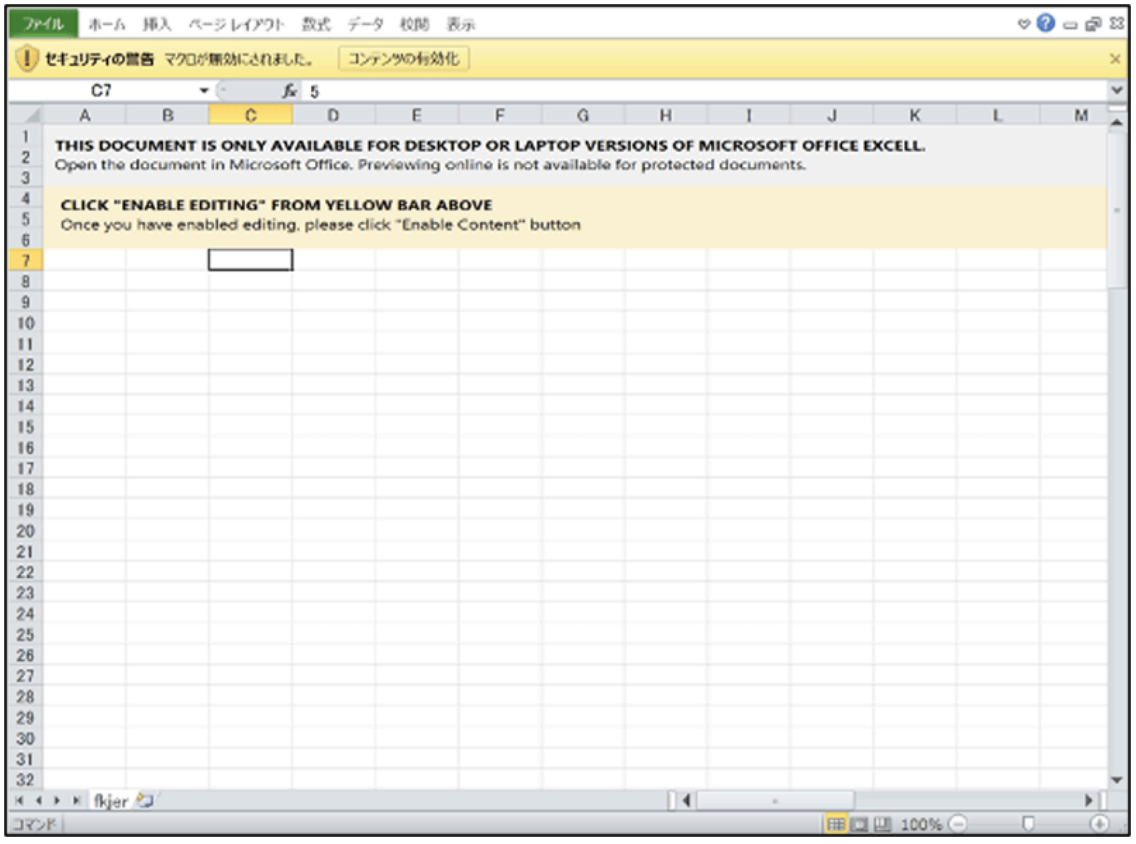


図2 Emotetへの感染を引き起こす文書ファイル（2021年11月17日時点）

ダウンローダの通信例を図3に示します。ダウンローダの通信は以前の傾向と大きな変化はありませんが、User-Agentに「WindowsPowerShell」が含まれることがあります。
この通信によってサーバからDLL形式のEmotetがダウンロードされ、その後Emotetが実行されます。なお、このとき接続するサーバは、多くの場合正規のサイトが改ざんされたものです。

```
GET /wp-includes/OxiAACCoic/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT; Windows NT 6.1; ja-JP) WindowsPowerShell/
5.1.14409.1005
Host: [redacted]

HTTP/1.1 200 OK
Date: Wed, 17 Nov 2021 06:36:22 GMT
Server: Apache
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Expires: Wed, 17 Nov 2021 06:36:22 GMT
Content-Disposition: attachment; filename="qK8Z1LM.dll"
Content-Transfer-Encoding: binary
Set-Cookie: 6194a2e63e155=1637130982; expires=Wed, 17-Nov-2021 06:37:22 GMT; Max-Age=60;
path=/
Upgrade: h2,h2c
Connection: Upgrade
Last-Modified: Wed, 17 Nov 2021 06:36:22 GMT
Transfer-Encoding: chunked
Content-Type: application/x-msdownload

4000
MZ.....@.....                .!..L.!
This program cannot be run in DOS mode.

$.....I.....I.....I.....I.....?.
.....#.....#.....#.....#.....Rich.....PE..L...-s.a.....!.....
0.....O.....@.....
.....@.....L.....
```

図3 ダウンローダの通信例

Emotet（本体）

Emotet本体は、C2通信の動作に変更があり、HTTPSを使用するようになりました（図4）。これにより、トラフィックを復号していないプロキシサーバのログでは通信の特徴をもとにC2通信を見つけ出すことが難しくなったといえます。
その他の変更点としては、HTTPリクエストにおいてPOSTメソッドからGETメソッドに変わったことやUser-Agentがセットされていないこと、Cookieを使用することなどが挙げられます。

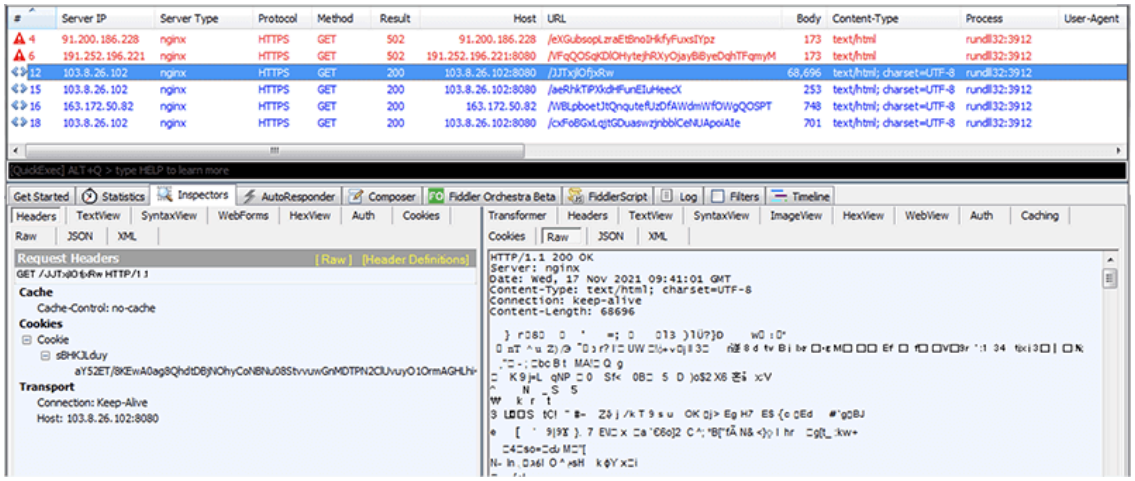


図4 Emotetの通信例

C2通信先に関しては従来通りEmotet本体にハードコーディングされていますが、こちらも変更が行われており、XORで暗号化されています。図5に示す通り、C2通信先はIPアドレスであり、80や443、7080、8080番ポートを使用する傾向があります。

図5 Emotetの通信先

Emotetのボットネットの状況

Emotetは、2021年1月にEUROPOL（欧州刑事警察機構）によってボットネットのテイクダウンが行われたことで一時的に終息に向かいました。しかしながら、今回Emotetの活動が再開されたことでボットネットが新たに構築され始めた状況にあります。新たなボットネットは、テイクダウン前まで利用されていたボットネットであるEpoch1～Epoch3を踏襲し、Epoch4およびEpoch5と呼ばれています。

EmotetのC2通信先を可視化したものを図6に示します。赤色の点がEmotet、紫色の点がC2通信先を表しています。左が11月15日にTrickbot経由で最初に配られたとされるEmotet、中央と右が11月17日に観測したEmotetです。徐々にC2通信先数が増えており、ボットネットが拡大していることが窺えます。

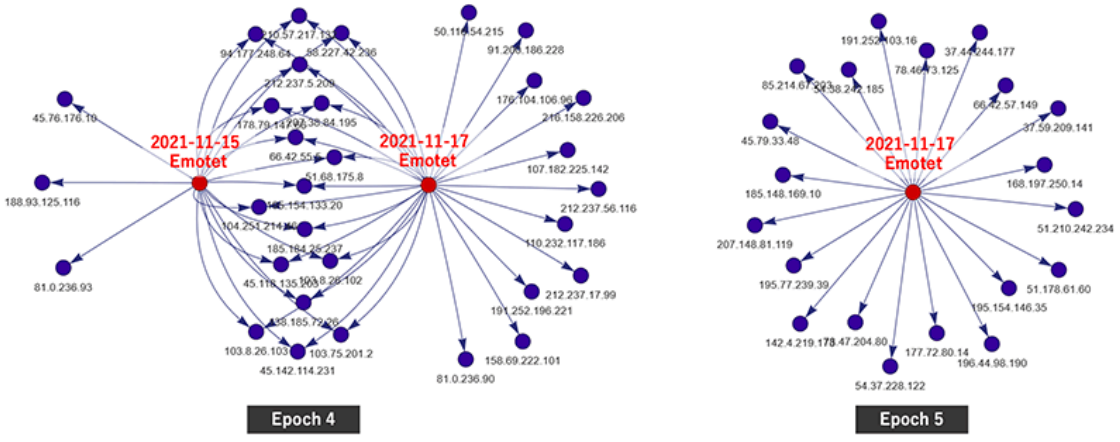


図6 EmotetのC2通信先の全体像

対策

メールに添付されているOffice文書ファイルは安易に開かない、本文内にあるメールのリンクにはアクセスしないことが重要です。また、Office文書ファイルを開いてしまった場合でも、「コンテンツの有効化」ボタンをクリックしなければ、マクロは実行されず、Emotetへ感染はしません（図7）。このようなOffice文書ファイルを開いてしまった際は、ボタンをクリックせずに、ファイルを閉じてください。

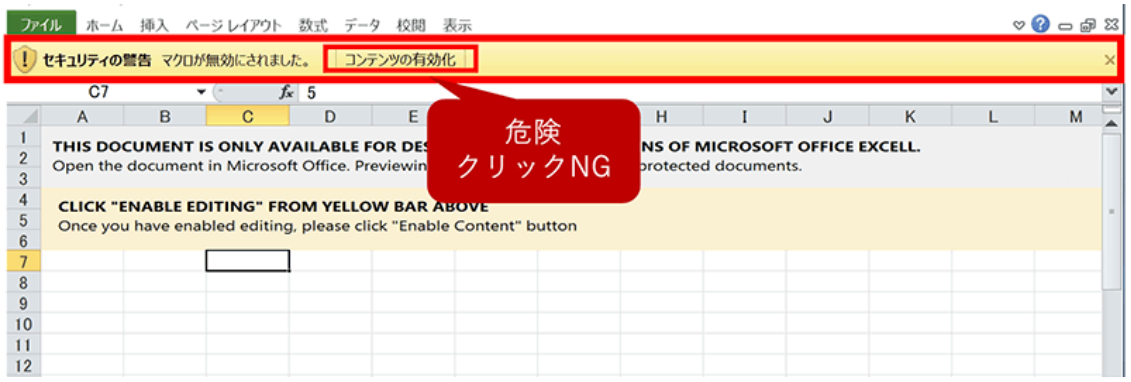


図7 感染を引き起こさないために注意すべき操作

また、Office製品のマクロ実行を強制的に無効に設定することも可能です。自組織内の業務でマクロ実行が不要という場合には、以下のMicrosoft社やIIJ社のサイトを参考に設定を変更することもご検討ください※。

※ Office ドキュメントのマクロを有効または無効にする

※ マルウェア感染対策を目的としたVBAマクロ実行の無効化

攻撃メールの内容や添付ファイル、Emotetの機能などは、今後変わっていく可能性がありますので、各組織のセキュリティご担当者様におかれましては、当社を含めたセキュリティ企業および組織の情報発信にて、定期的にEmotetの動向とその対策をご確認ください。

感染時の対応や対策方法について、不安な点がありましたらサイバー救急センターまでご相談ください。

サイバー救急センター　脅威分析チーム
（松本 拓馬、武田 貴寛、髙源 武彦、石川 芳浩）
