緊急情報を確認する

- 注意喚起
- インターネット定点観測
- JVN
- 脆弱性対策情報
- インターネットリスク可視化サービス—Mejiro—（実証実験）

おすすめ情報

- JPCERT/CC Eyes「攻撃グループBlackTechが使うダウンローダ IconDown」
- JPCERT/CC Eyes「攻撃グループBlackTechが侵入後に使用するマルウエア」
- JPCERT/CC Eyes「マルウエアの設定情報を自動で取得するプラグイン ~MalConfScan with Cuckoo~」
- JPCERT/CC Eyes「マルウエアの設定情報を抽出する ~ MalConfScan ~」

マルウエア Emotet の感染に関する注意喚起

最終更新: 2019-11-27

JPCERT-AT-2019-0044
JPCERT/CC
2019-11-27

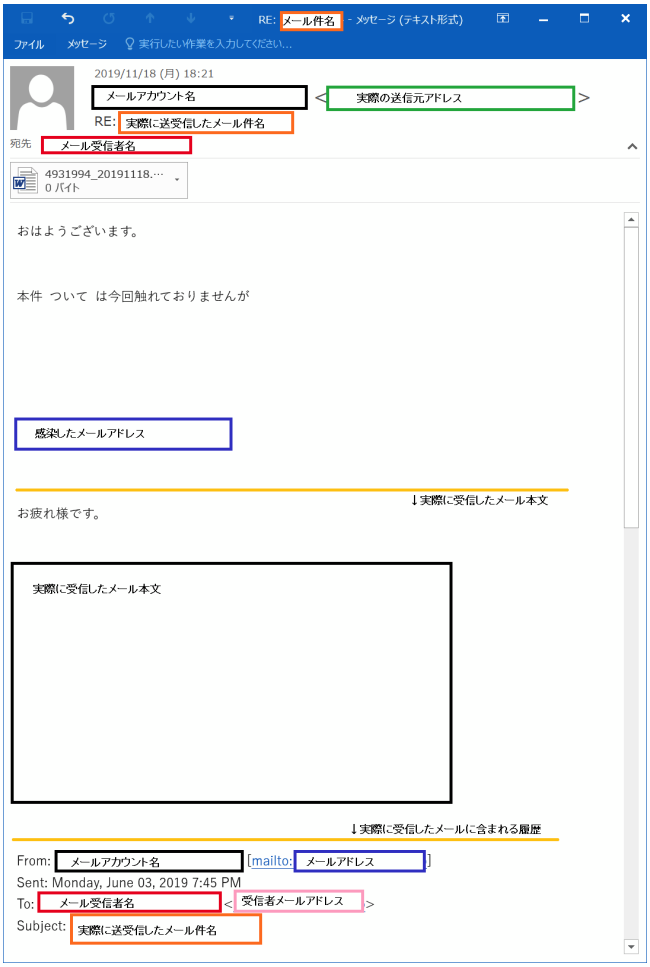
I. 概要

JPCERT/CC では、2019年10月後半より、マルウエア Emotet の感染に関する相談を多数受けています。特に実在の組織や人物になりすましたメールに添付された悪性な Word 文書ファイルによる感染被害の報告を多数受けています。

こうした状況から、Emotet の感染拡大を防ぐため、JPCERT/CC は本注意喚起を発行し、Emotet の主な感染経路、Emotet に感染した場合の影響を紹介した後、感染を防ぐための対策や、感染に気付くためにできること、感染後の対応方法などに関する情報を紹介します。

II. 感染経路

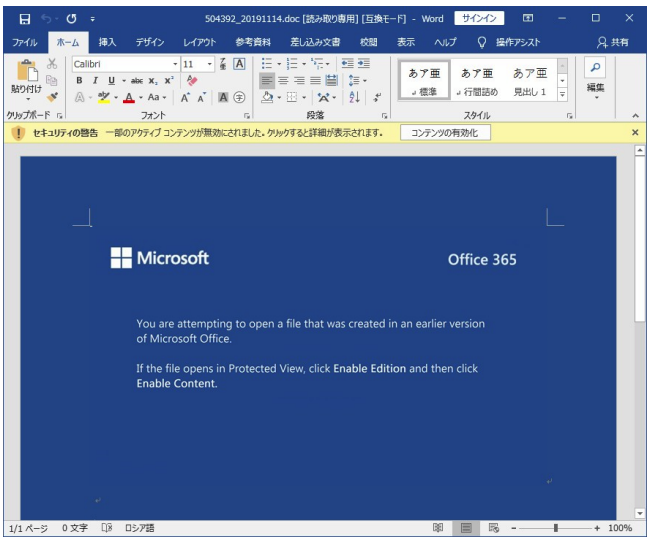
JPCERT/CC が確認している事案では、主にメールに添付された Word 形式のファイルを実行し、コンテンツの有効化を実行することで Emotet の感染に繋がることが分かっています。Emotet の感染に繋がる可能性のあるメールの例は次のとおりです。



[画像1: メール例]

Emotet の感染に繋がる添付ファイル付きのメールは、Emotet が窃取した情報などを元に独自に作成されているものに加え、実際の組織間のメールのやりとりの内容を転用することで、感染元から送信先への返信を装うものがあります。そのため、取引先の担当者から送られているようにみえるメールでも、実際はEmotet が窃取した情報を元に攻撃者側から送られている「なりすましメール」である可能性があるため、注意が必要です。

添付されたファイルには、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ます。Word の設定によっては、有効化の警告が表示されずに Emotet がダウンロードされる場合があります。



[画像2: 添付ファイル例]

III. 影響

Emotet に感染した場合、次のような影響が発生する可能性があります。

- 端末やブラウザに保存されたパスワード等の認証情報が窃取される
- 窃取されたパスワードを悪用され SMB によりネットワーク内に感染が広がる
- メールアカウントとパスワードが窃取される
- メール本文とアドレス帳の情報が窃取される
- 窃取されたメールアカウントや本文などが悪用され、Emotet の感染を広げるメールが送信される

このように、Emotet に感染してしまうと、感染端末から情報が窃取された後、攻撃者側から取引先や顧客に対して感染を広げるメールが配信されてしまう恐れがあります。また、感染したままの端末が組織内に残留すると、感染を広げるメールの配信元として攻撃者に利用され、外部に大量の不審メールを送信することになります。

また、Emotet に感染した端末が、Trickbot などの別のマルウエアをダウンロードし、結果としてランサムウエアに感染してデータが暗号化されるなどの被害に繋がるケースに関する情報も公開されています。

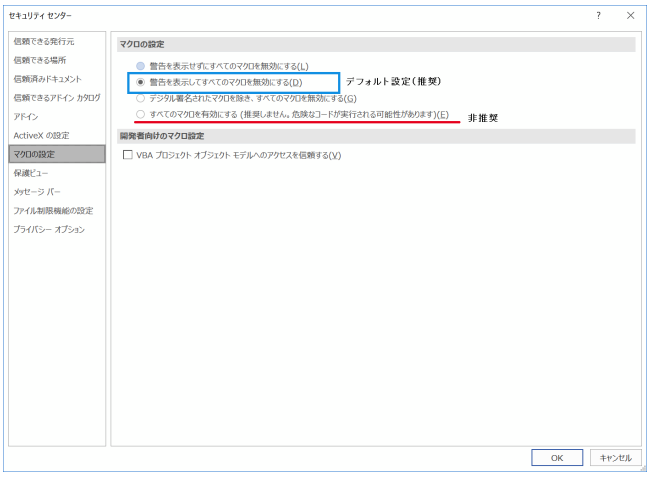
情報の窃取や感染拡大を防ぐためにも、ランサムウエアなどによる業務への影響を防ぐためにも、下記の対策や対処の実施を検討することを推奨いたします。

IV. 対策

Emotet の感染を予防し、感染の被害を最小化するため、次のような対応を実施することを検討してください。

- 組織内への注意喚起の実施
- Word マクロの自動実行の無効化 ※
- メールセキュリティ製品の導入によるマルウエア付きメールの検知
- メールの監査ログの有効化
- OS に定期的にパッチを適用（SMBの脆弱性をついた感染拡大に対する対策）
- 定期的なオフラインバックアップの取得（標的型ランサムウエア攻撃に対する対策）

※ Microsoft Office Word のセキュリティセンターのマクロの設定で、
「警告を表示してすべてのマクロを無効にする」を選択してください。



[画像3: Microsoft Office のセキュリティセンターのマクロの設定]

V. 事後対応

自組織で使用するウイルス対策ソフトが検知して Emotet の感染を発見する場合に加え、次のような状況を確認

した場合は、自組織の端末が Emotet に感染している可能性があります。

- 自組織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外部組織から連絡を受けた場合
- 自組織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

自組織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次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、次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

また、Emotet の感染が疑われる場合など、本件についてご相談が必要でしたら、次の「JPCERT/CC インシデント報告窓口」までご連絡ください。

JPCERT/CC インシデント報告窓口
メール：info@jpcert.or.jp
電話 ：03-6271-8901

VI. 参考情報

US-CERT
Alert (TA18-201A) Emotet Malware
https://www.us-cert.gov/ncas/alerts/TA18-201A

Australian Cyber Security Centre (ACSC)
Advisory 2019-131a: Emotet malware campaign
https://www.cyber.gov.au/threats/advisory-2019-131a-emotet-malware-campaign

今回の件につきまして提供いただける情報がございましたら、JPCERT/CC までご連絡ください。

一般社団法人 JPCERT コーディネーションセンター (JPCERT/CC)
MAIL: ew-info@jpcert.or.jp
TEL: 03-6271-0610 FAX: 03-6271-8908
https://www.jpcert.or.jp/

一般社団法人 JPCERT コーディネーションセンター
〒103-0023
東京都中央区日本橋本町4-4-2 東山ビルディング8階
TEL: 03-6271-8901 FAX 03-6271-8908
JPCERT/CCは移転のため、住所、電話番号、FAX番号が変わりました。