マルウェア Emotet の影響と対策について

はじめに

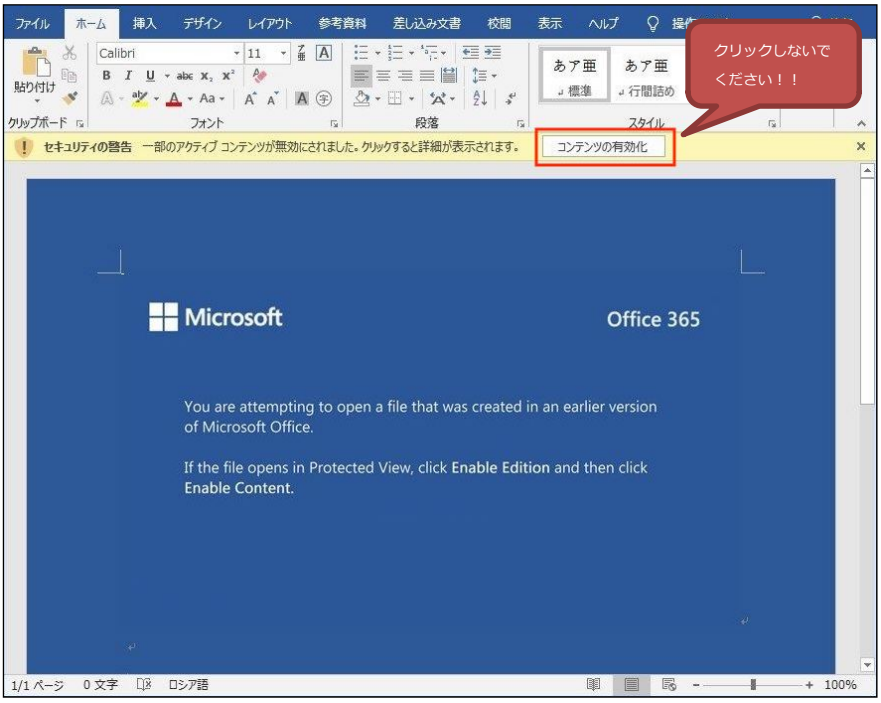
日本国内での被害が報告されているマルウェア Emotet(エモテット)について、影響と対策をご説明します。

Emotet に感染してしまうと、感染端末から情報が搾取され、攻撃者によって取引先や顧客に対して感染拡大を狙ったメールが大量に送信される可能性があります。

Emotet について

Emotet 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クリックすることで感染することが報告されています。

<添付ファイル例>



上記、添付ファイルには赤枠のコンテンツの有効化を促す内容が記載されており、クリックしてしまうと Emotet がダウンロードされることが報告されています。

※Word の設定によっては、有効化の警告が表示されず、添付ファイルを開いた際に Emotet がダウンロードされる場合があります。
(設定の確認は 4 ページ目をご参照ください)

Emotet に感染した場合、下記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しているパスワード等の認証情報が搾取される
- 搾取されたパスワードが悪用され、SMB によりネットワーク内に感染拡大する
- メールアカウントとパスワードが搾取される
- メール本文とアドレス帳の情報が搾取される
- 搾取されたメールアカウントや本文などが悪用され、Emotet の感染拡大を狙ったメールが送信される

感染したままウイルスが端末に残っていると感染拡大を狙った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してしまう可能性があります。

感染拡大を狙ったメールの大量送信だけでなく、感染した端末が別のマルウェアをダウンロードし、最終的にはランサムウェ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可能性があります。

NetStable での検知

NetStable のシグネチャで、Emotet に関連する通信を検出することが出来ます。

1. Emotet のダウンロード通信の検知

- 2001354 – 2001360 Emotet HTTP Request 1 ~ 7
- 2001362 – 2001379 Emotet HTTP Request 8 ~ 25
- 2001354 – 2001360 Emotet HTTP Request 26 ~ 34
- 2500001 – 2500103 Emotet Black-IP List 1 ~ 103

Emotet をダウンロードする際の通信を遮断するシグネチャです。
送信元 IP アドレスの端末が、添付ファイルを開き、コンテンツの有効化を行った可能性があります。

2. 感染後の通信・感染拡大通信・外部からの攻撃通信の検知

- 2000587 Eternalblue echo request

感染拡大を目的とした、Windows の脆弱性を悪用する通信を遮断するシグネチャです。
このシグネチャが検出された場合、送信元 IP アドレスの端末がマルウェアに感染している可能性があります。また、受信先 IP アドレスが自社の IP アドレスである場合、脆弱性を狙った攻撃を受けている可能性があります。

3. マルウェアによる不審な通信を発見する

- 3000105 Global SMB Session
- 2000368 Global SMB Connect

外部の IP アドレス(グローバル IP アドレス)宛に Windows の共有アクセスを試みようとした通信を検知するシグネチャです。
受信先 IP アドレスにアクセスした記憶がない場合、のマルウェアに感染している可能性があります。

- 2000586 SMB IPC Access

Windows の共有をパスワード無しの匿名でアクセスしようとした通信を検知するシグネチャです。
社内間のファイル共有ではパスワード無しでの共有がされていることがありますが、受信先 IP アドレスが共有サーバ以外である場合や、外部の IP アドレスである場合、マルウェアに感染している可能性があります。

4. マクロ機能が含まれた添付ファイルの検知

- 2000874 Office Macro file download from Global-IP
- 2000875 Office Macro file receive e-mail 1
- 2000876 Office Macro file receive e-mail 2
- 2000877 Office Macro file receive e-mail 3

従来の Word 形式である.doc ファイルにマクロが含まれているものを受信またはファイルのダウンロードを検出するシグネチャです。
受信先 IP アドレスの端末が、マクロ機能が含まれた.doc ファイルを受け取った可能性があります。

感染時の対処・予防策

1. 感染時の対処

- 一般社団法人 JPCERT コーディネーションセンター社がリリースしている Emotet 感染チェックツール「EmoCheck」を実行し、感染の有無を確認してください
  感染が確認された場合は、該当ファイルの削除を実施してください

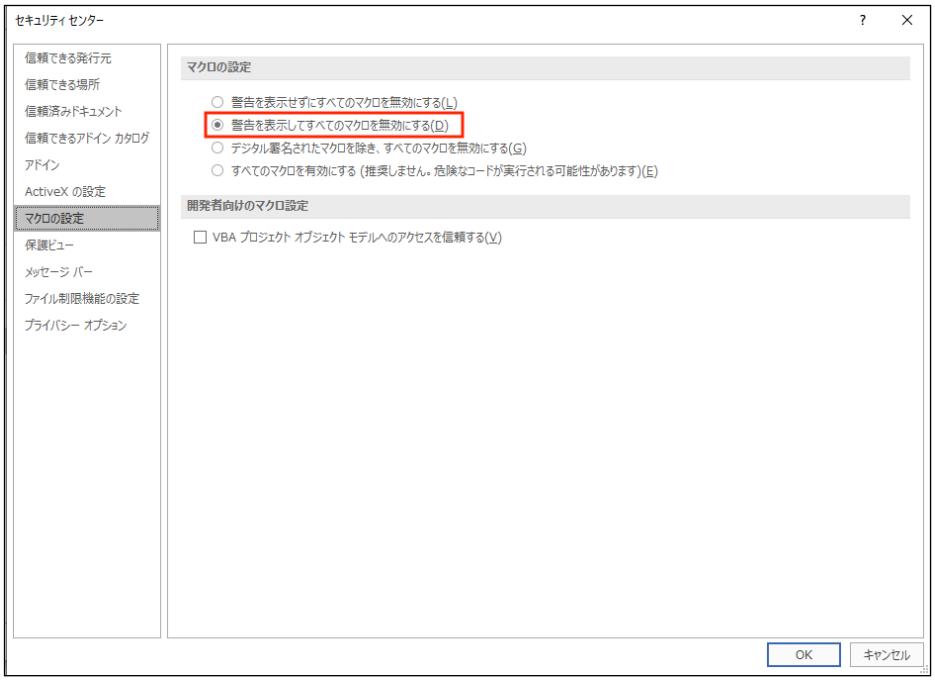
  JPCERTCC/EmoCheck - github:
  https://github.com/JPCERTCC/EmoCheck/releases

- 感染端末にてセキュリティソフトを使用したスキャンを行い、マルウェアを駆除してください
- 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を変更してください

2. 予防策

- Windows Update を行い、最新の更新プログラムを適用してください
- セキュリティソフトを最新の状態に更新し、定期的なチェックを行ってください
- 不審なメールに添付してあるファイルは開かないようにしてください
- Word マクロの自動実行の無効化　※

※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



<参考 URL>

・マルウェア Emotet の感染に関する注意喚起 – JPCERT/CC
https://www.jpcert.or.jp/at/2019/at190044.html