サイバーセキュリティ通信 Vol.16

令和４年２月

サイバァちゃん

Emotetによる感染が再拡大中！

JPCERT/CCなどによると、２月現在、Emotetの感染が再拡大しています。
ただし、現在のところ、新しい感染手法がとられている訳ではありません。
今後、新しい手法が出てくる可能性はありますが、現時点では、Officeソフトのマクロを有効にしなければ感染しないようです。
従業員の皆さんに再度、Emotetの感染が再拡大中であるため、メール、特に添付ファイルには十分注意するよう、注意喚起をお願いします。
また、自組織のメールアドレスを装ったEmotetメールが送信されることも懸念されます。

１　Emotetとは？

・非常に高い感染力と拡散力を持つマルウェア（コンピュータウイルス）
・メールの添付ファイルから感染させる手法が主流
・感染したパソコンからメールアドレスやログイン情報などを盗み出す。
・ほかの様々なマルウェアにも感染させる役割を持っている。（ランサムウェアに感染してデータが暗号化され、業務が停止してしまうおそれもある。）

２　再流行したEmotetにはどんな特徴がある？

・日本語による本文、パスワード付きzipファイル添付のパターンが多く確認されている。
・xlsmファイルやパスワード無しのzipファイルが添付されるパターンもある。
・返信メールを装った件名、文字化けした引用文などの特徴がある。
※手口は変わっていきますので、これだけに注意していれば万全、ということはありません。

３　なりすましメールに利用される場合は、どんなケースがある？

JPCERT/CCによると、
・自組織がEmotetに感染し、なりすましメールが配信されるケース
・取引先がEmotetに感染し、なりすましメールが配信されるケース
があるようです。ほかにも、
・国内メールサーバーからの感染につながるメール配信の増加傾向
が確認されているそうです。次ページに図解入りの記事を許可を得て引用しています。

４　感染したら？

警察や保守管理を委託しているベンダーなどへ早急に通報してください。感染端末の隔離や証拠保全、調査などを行う必要がありますが、早期に対応しなければ、時間経過とともに証拠が失われてしまう可能性が高まります。

５　日頃の備えは？

従業員に対し、添付ファイル付きのメールには特に注意するよう、繰り返し注意喚起をお願いします。ExcelやWordなどのOfficeソフトのファイルを送受信する場合は、あらかじめ電話で連絡するという取り決めをしていてもいいかもしれません。
その他、自組織がなりすまされてしまった場合に対する備えも必要です。関係者への注意喚起のほか、プレスへのお知らせも検討しておく必要があります。

長崎県警察本部サイバー犯罪対策課
095-820-0110（3451・3452）
ﾒｰﾙｱﾄﾞﾚｽ e103107@police.pref.nagasaki.jp

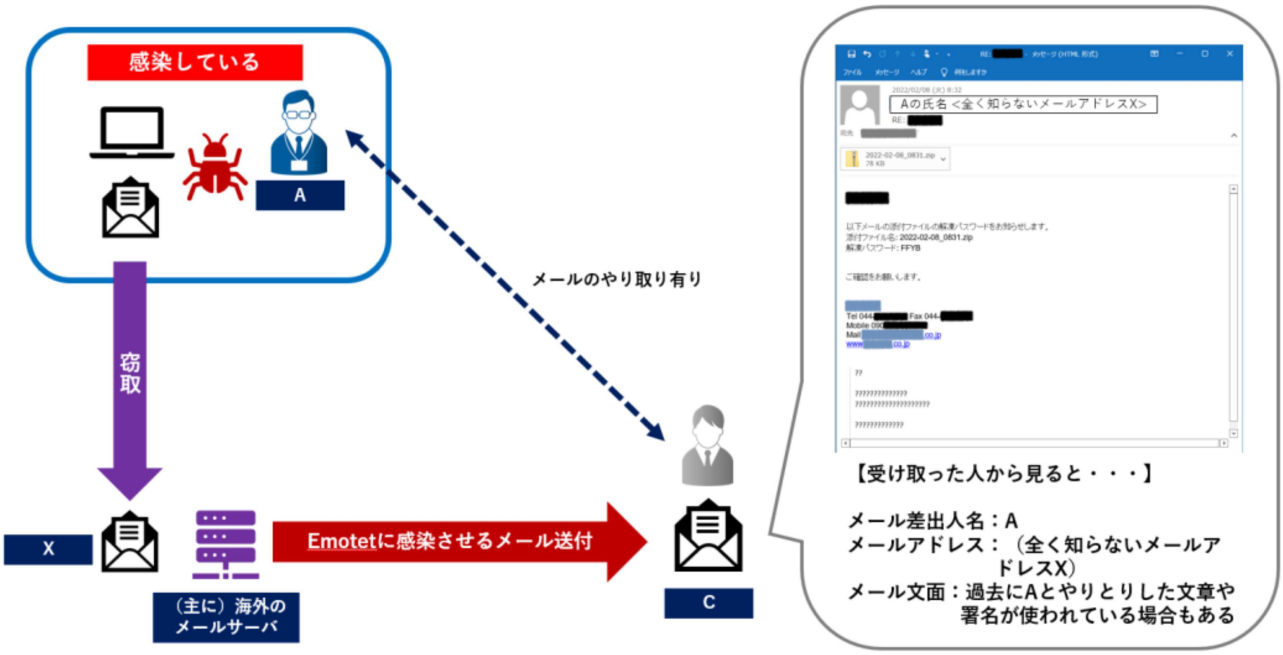
サイバー犯罪対策課
公式LINEアカウントで
情報配信中！
友だち登録お願いします！

@387ojopi

＜Emotet感染によってメールが送信されるケース＞

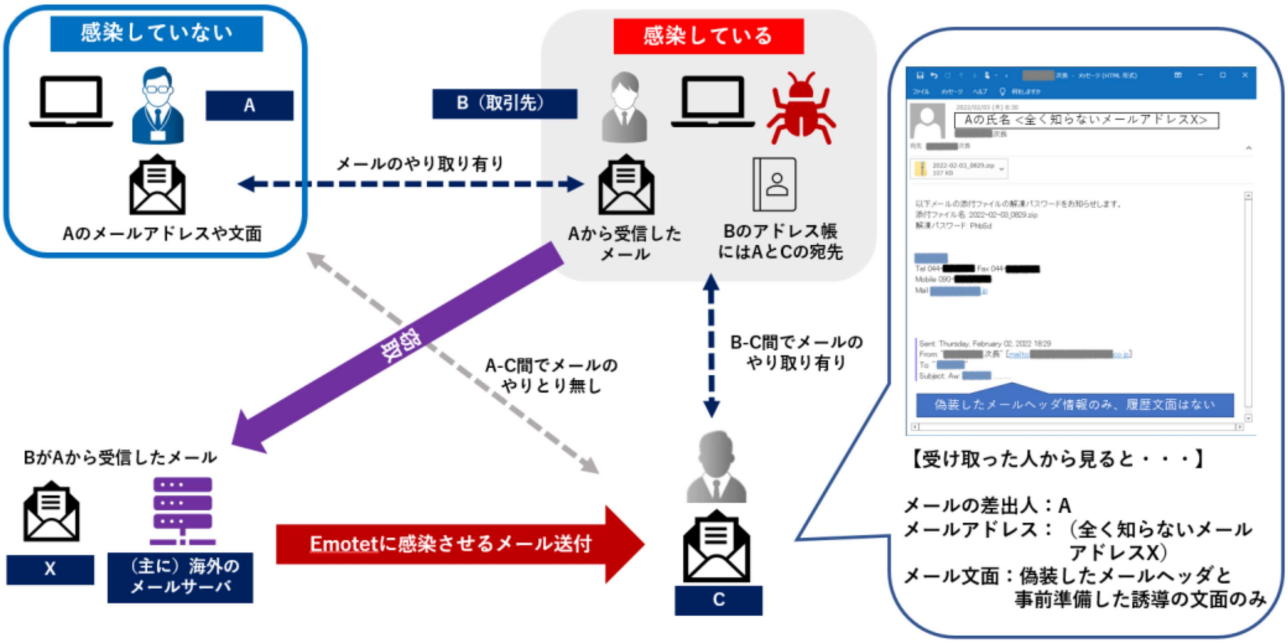
1　自組織がEmotetに感染し、なりすましメールが配信されるケース

Emotetに感染すると、感染端末に保存されていたメールの情報やアドレス帳に登録されていた担当者名などの情報が窃取されます。窃取された情報は、その後のEmotet感染につながる「なりすましメール」で悪用されることがあります。

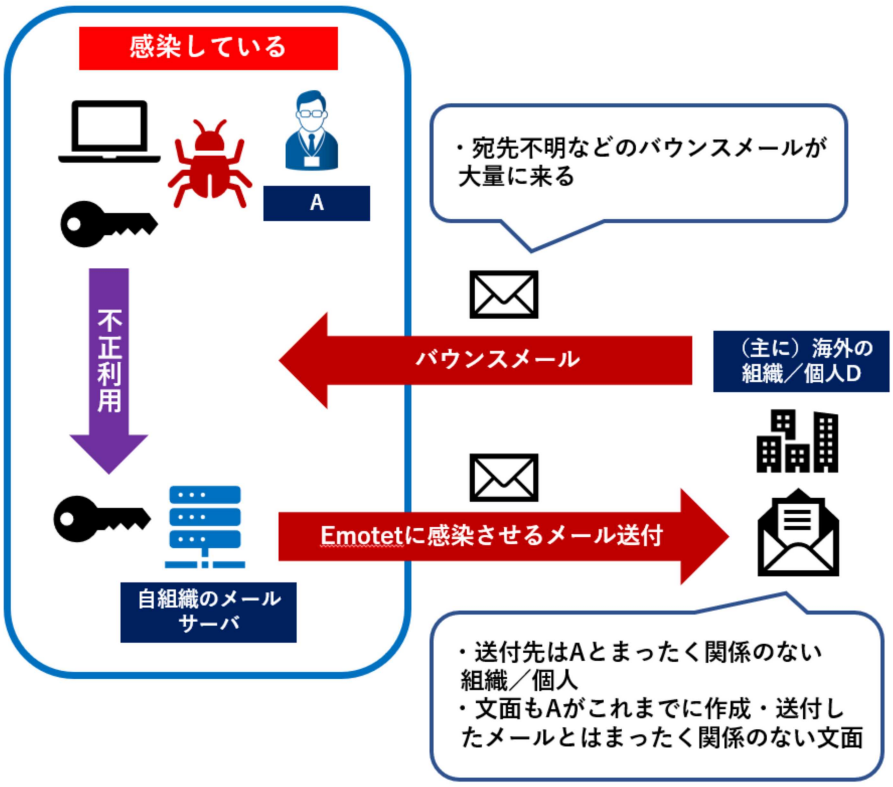


2　取引先がEmotetに感染し、なりすましメールが配信されるケース

自組織の職員になりすましたメールが飛んでいるからといって、その職員の端末がEmotetに感染しているとは限りません。職員が過去にメールのやりとりを行った取引先の端末がEmotetに感染し、その端末から窃取された情報に含まれていた当該職員の情報が悪用されているというケースの可能性があります。



また、国内メールサーバからの感染につながるメール配信の増加傾向も確認されています。自組織で管理するメールサーバーなどのインフラが悪用されていないか、御確認ください。もし自組織のインフラが悪用されていた場合、Emotet感染につながるメールの配信先が存在しないなどの理由で、大量のバウンスメールを受信している可能性があります。



自組織の職員になりすましたメールが送られているという場合でも、送られているメールの内容や状況を関係者間で確認及び整理の上、次に示すEmoCheckやFAQの内容などを参考に自組織の感染の有無を御確認いただくことを推奨します。

マルウェアEmotetへの対応FAQ
https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html

Emotet感染有無確認ツールEmoCheck
https://github.com/JPCERTCC/EmoCheck/releases

EmoCheckをお使いいただく場合、Emotet感染につながる可能性が考えられるメールを開いたパソコンのアカウントで端末にログインした状態で、EmoCheckを実行してください。別のアカウントでログインした場合では正しく検知できない可能性があります。

出典：JPCERT/CC「マルウェアEmotetの感染再拡大に関する注意喚起」
https://www.jpcert.or.jp/at/2022/at220006.html