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

I. 概要

JPCERT/CC では、2021 年 11 月後半より活動の再開が確認されているマルウェア Emotet の感染に関して相談を多数受けています。特に 2022 年 2 月の第一週より Emotet の感染が急速に拡大していることを確認しています。

Emotet に感染しメール送信に悪用される可能性のある.jp メールアドレス数は、Emotet の感染が大幅に拡大した 2020 年に迫る勢いとなっています。感染や被害の拡大を防ぐためにも、改めて適切な対策や対処ができているかの確認や点検を推奨します。

https://www.jpcert.or.jp/at/2022/at220006_fig1.png
［図 1： Emotet に感染しメール送信に悪用される可能性のある.jp メールアドレス数の新規観測の推移（外部からの提供観測情報)］

II. 確認している Emotet の特徴/動向

2021 年 11 月後半より観測されている Emotet は、主にマクロ付きの Excel や Word ファイル、あるいはこれらをパスワード付き Zip ファイルとしてメールに添付する形式で配信されており、ファイルを開封後にマクロを有効化する操作を実行することで Emotet の感染に繋がります。
このような手法の他にも、メール本文中のリンクをクリックすることで悪性な Excel や Word ファイルがダウンロードされたり、アプリケーションのインストールを装い Emotet 感染を狙うケースも観測しています。

メールの本文には添付ファイルの開封を、Excel や Word ファイルにはマクロの実行を促す内容が記述されています。JPCERT/CC で確認しているメールのサンプルは次のとおりです。
https://www.jpcert.or.jp/at/2022/at220006_fig2.png
[図 2：Emotet メールサンプル]

https://www.jpcert.or.jp/at/2022/at220006_fig3.png
[図 3：添付ファイルを開いた際に表示されるマクロ実行を促すメッセージ例]

一見すると業務に関係がありそうな内容で、取引先や知り合いから送付されているようにみえる添付ファイルであっても、Emotet の感染につながるメールや添付ファイルである可能性があるため、信頼できるものと判断できない限りは添付ファイルやリンクは開かず、確実な手段で送信元へ確認するといった対応を行うようご注意ください。

III. 対策、対応

Emotet 感染時の対応については次の資料を参照してください。

マルウエア 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

また、国内メールサーバーからの感染につながるメールの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、ご確認ください。
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。

IV. 参考情報

JPCERT/CC Analysis Center
https://twitter.com/jpcert_ac/status/1491259846616023044

情報処理推進機構（IPA）
Emotet の攻撃活動の急増　（2022 年 2 月 9 日　追記）
https://www.ipa.go.jp/security/announce/20191202.html#L18

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