マルウェア Emotet に関するお詫びとお知らせ

2022 年 2 月から Emotet の感染が急速に拡大しているとの情報が確認されています。

また、弊社関係者を装った不審なメールが、社内・外の方を問わず複数発信されているという事実を確認しております。

弊社をご利用いただいたお客さま及び関係者の皆さまには、多大なご迷惑とご心配をおかけいたしますこと、深くお詫び申し上げます。本件の経緯及び今後の対応について、下記のとおりご報告いたします。

1. 事実の概要

弊社パソコンが「Emotet」(ｴﾓﾃｯﾄ)と想定されるマルウェアに感染し、弊社社員を装うメールが送信されました。

Emotet は、実在の組織や人物になりすまして発信されたメールの添付ファイルによるマルウェアです。
主にマクロ付きの Excel や Word ファイル、またはこれらをパスワード付き Zip ファイルとして添付されたメールで配信されており、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。
感染するとアドレス帳やメールの窃取または転送設定などが行われ、情報を窃取される恐れがあります。また、窃取された情報を利用され、さらにフィッシングメールやマルウェア添付メールを送信されるなど、被害の拡大に繋がります。

2. 弊社を名乗る不正メールを受取られたお客さまへのお願い

実在の組織や人物から送信（返信）されたように見えるメールでも、「身に覚えがないメール」や「不審な点があるメール」につきましては、メールに記載された URL のクリックや添付ファイルの開封は行わないようにしてください。

また、エクセル、ワードなどのオフィスソフトのマクロを実行しないよう、設定をよろしくお願いいたします。

3. 現時点での被害状況

弊社関係者を詐称する不正なメールの添付ファイルを開封された方がいらっしゃいますが、現時点では本件を悪用したフィッシングメールや詐欺等の被害は報告されておりません。

4. 発生したおそれがある個人データ

弊社社員のアドレス帳データが読み取られた可能性があります。お名前とメールアドレ

スが 300 件程度流出した可能性があります

5. 今後の対応

弊社では、今後この様な事態が発生しないよう、セキュリティソフトの見直し、ファイヤーウォールなどの対策を行っておりますが引き続きさらなるセキュリティの強化を実施いたします。

再発防止に向けて個人情報の管理強化・徹底に努め、信頼回復に全力を尽くして参ります。

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

令和 5 年 1 月
株式会社三春情報センター