回　覧　印　印　印　印　印　印　印　印　印　印　印　印

ASAMA Security Newsletter Vol.94

あさまセキュリティニュースレター

Emotet（エモテット）2023年攻撃活動開始　（2023年3月10日）

差出人や署名は、実在組織や
取引先を装うケースがあります

ZIPファイルの中は500MBを超えるWord文書
552MB

2023年3月7日からEmotetの攻撃活動が再開！
今回、**ファイルサイズを大きくしウイルス検知を回避**する手法のため、**メールが届きやすい→被害増が考えられます**
圧縮ファイルの中身が、**古いOffice形式**（拡張子『.doc』『.xls』のもの）の場合、Emotetの可能性があります
差出人や署名も実在する組織や、取引先を装うのもEmotetの特徴です。**知っている方からのメールでも必ず確認**をとりましょう

参考
今までの攻撃は、**1Mを超えないファイルでの攻撃**がほとんどのため、インターネットの出入口でセキュリティ対策をするUTMや、パソコンにインストールするウイルス対策ソフトも、容量の大きいファイルをスキャンをしない、一部だけスキャンするという設定になっていることが多い
（ファイルの大きいものまで検査すると、ネットワークの遅延等の影響があるため）

Emotetメールが届くケース

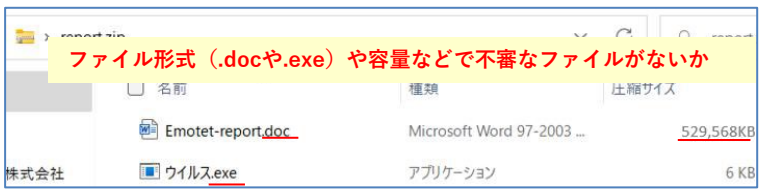
Emotetのメールが送信されるケースは、感染者とその関係者を巻き込む形で複数のパターンが考えられます

- **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**
- **攻撃者が事前に入手したメール・パスワード等で、メールサーバーに直接アクセスされ悪用されているケース**
- **以前、Emotetのメールを受け取ったことがあるメールアドレス（ランダムで配信されるケース）**

Emotetは様々なパターンで配信されますので、メールが届いた場合の報告、確認、対策をまとめておきましょう

開く必要のあるZIPファイルは念のためチェックを

ダブルクリックで開かず、右クリックでウイルス検査や、エクスプローラー表示でどんなファイルが入っているか確認を



対策

- **不審なメールだけではなく、自分が送信したメールへの返信に見えるメールであっても、不自然な点があれば添付ファイルは開かない。メール本文中のURLリンクはクリックしない　相手に確認する**
- **メールに添付されたファイルを開き、マクロやセキュリティに関する警告が表示された場合、安易に開かない**
- **ソフトウェアアップデート、ウイルス対策ソフトの導入、インターネット出入り口のセキュリティ対策の確認・更新**

情報源
JPCERT https://www.jpcert.or.jp/at/2022/at220006.html　**IPA** https://www.ipa.go.jp/security/announce/20191202.html

浅間商事株式会社　〒110-0005　東京都台東区上野7-15-70 浅間第一ビル　0120-830-414