情報セキュリティ対策で

# お客様の会社を守る運動

# マルウェアエモテット　対策方法

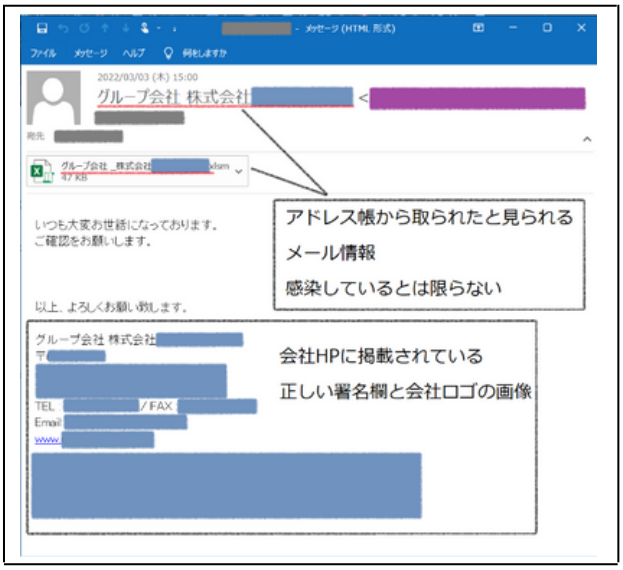
EMOTET　注意喚起

## EMOTET攻撃メールの例

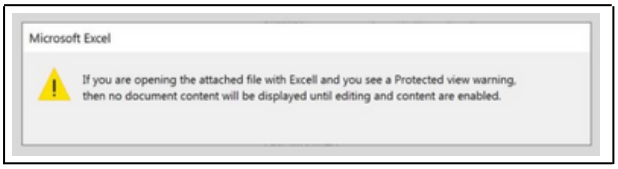
- WordやExcelの添付ファイルでマクロを有効させる攻撃
- URLリンクを悪用した攻撃
- PDF閲覧ソフトを偽装する手口
- パスワード付きZIPファイルを使った攻撃

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サンプル(図1.2.3参照)

画像引用元：JPCERT Coordination Center

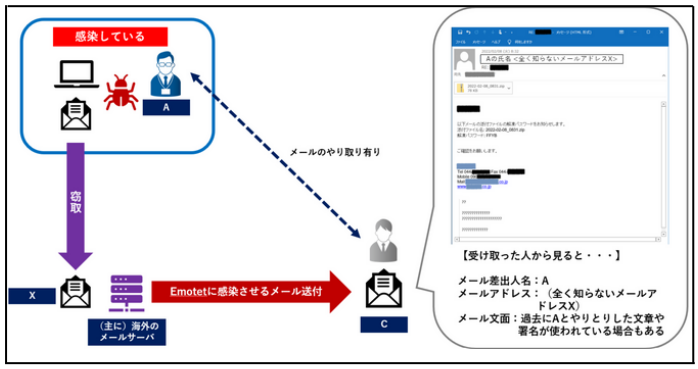



[図1：Emotetメールサンプル]




[図2：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]

[画像2: 添付ファイル例]




[図3：自組織がEmotetに感染、なりすましメールが配信されるケース]

このようなメールは、*EMOTET*に感染してしまった組織から窃取された、正規のメール文面やメールアドレス等の情報が使われていると考えられます。
すなわち、*EMOTET*への感染被害による情報窃取が、他者に対する新たな攻撃メールの材料とされてしまう悪循環が発生している恐れがあります。

**本文中に URL が記載されたメールも、安易にURL に接続しないようご注意ください**

また、Emotet を配布する活動は、これまでも感染経路が変化しており、今後も変化する可能性があります。
そのため、これまで観測されている手法に限らず、不審なメールの添付ファイルの実行やリンクの押下をしないよう注意を高めるとともに、万が一に備えてシステム管理部門への連絡体制などの確認を推奨します。



MAGMAX マグマックス株式会社

# マルウェアエモテット　対策方法

EMOTET　注意喚起

## EMOTET に感染した場合、次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されたパスワード等の認証情報が窃取される
- 窃取されたパスワードを悪用され SMB によりネットワーク内に感染が広がる
- メールアカウントとパスワードが窃取される
- メール本文とアドレス帳の情報が窃取される
- 窃取されたメールアカウントや本文などが悪用され、Emotet の感染を広げるメールが送信される

## 自分が加害者にならないために、セキュリティ対策3原則を知り、対策を打ちましょう

**情報被害が多発する中、少なくともこれら3原則は押さえましょう！**

1.情報被害のメカニズムや手口、その対策方法を知ること
2.できる限りOSやパターンファイル、ソフトのバージョン等を最新化すること
3.ウイルスや詐欺メール、怪しいサイト等を会社の中に持ち込まないこと

## EMOTETに感染しないために、対策はどうしたらいいの？

**EMOTETの対策としては、一般的なウイルス対策が有効です。**

今できる対策方法

- 身に覚えのないメール、添付ファイルは開かない
- メール本文中のURLはクリックしない
- 自分が送信したメールの返信に見えても不自然に感じたら添付ファイルは開かない
- OSやアプリケーション、セキュリティソフトを最新にする
- 身に覚えのないメールや添付ファイルを開いた場合は、すぐにシステム管理者に連絡する

上記対策で予防することはできますが、完全には防ぐことはできません。知人や取引先と今後も良好な関係を築いていくために、脅威を最小化する対策とは･･･

## より具体的、有効な対策方法

**上記を前提として、JPCERTコーディネーションセンターでも以下の対策も推奨しています。**

- マクロの自動実行の無効化
-メールセキュリティ製品導入によるマルウェア付きメールの検知
（事前に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」を選択しておく）
-メールの監査ログの有効化
-OSに定期的にパッチを適用
（SMBの脆弱性を突く感染拡大に対する対策）

## 対策の基本として、情報を得るだけではなく、社内での共有注意喚起も重要です！

脅威を知ったところで、社内全員が意識をして対策をしないと、社内感染が広がってしまい被害が拡大してしまう恐れがあります。ぜひこのチラシも社内回覧などにご活用いただき、社内の警護活動またはＩＴリテラシーを高めるきっかけになりましたら幸いです。



MAGMAX マグマックス株式会社