令和４年１１月２２日　第４１号

ＣＹＳＥＰ通信

サイバー　セキュリティ　パートナーシップ

～ CYBER SECURITY PARTNERSHIP ～

マルウェア Emotet（エモテット）の活動再開

Emotet と呼ばれるマルウェアの感染を狙う攻撃メールが令和４年７月中旬頃から活動を停止していましたが、今般警察庁において、Emotet メールを複数確認するなど国内で活動が再開したとみられる事象を確認しております。

１　Emotet に感染すると

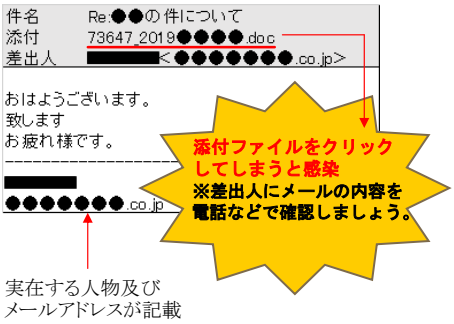
Emotet は感染すると情報を盗まれる、ランサムウェア等の他のマルウェアにも感染するといった被害に遭うおそれがあります。

２　最近の手口

最近の手口では、添付ファイルを指定されたフォルダにコピーするよう指示され、マクロを実行可能とさせ Emotet に感染させるといった特徴があります。

この手口は、「Word ファイル」を直接送りつけたり、同ファイルをパスワードが設定された「zip ファイル」にして送りつけ、ファイルを開くと「指定したフォルダ」にファイルをコピーし再度開くように求める警告文に見せかけた文章が記載されております。

【不審メールの例】



※　指定したフォルダとは

「Office」では、開くと警告無しにマクロが実行できる「信頼できる場所」を設定でき、その一部は Office のインストール時にデフォルトで作成されております。

本来「信頼できる場所」は、自身で作成したファイルや、安全で信頼できるファイルをスムーズに開くために用意した機能となります。

Emotet の感染を狙った不審メールの特徴

- 実在する企業等のメールを装う
  （差出人に実際にやりとりのある担当者の名前やメールアドレスを使用するなど）
- 件名に「Re：」をつけ返信メールを装ったり、「実際の件名を流用する」などし、正規のメール装う
- Word ファイル等を添付する
- ファイルをダウンロードする web リンクを記載する
- ショートカットファイル（LNK ファイル）を添付する
- 指定されたフォルダにコピーするように指示する
  （指定されたフォルダで開くと自動でマクロ実行）

対策

- 不用意に添付ファイルを開かない
- Word マクロの自動実行の無効化
- 組織内での注意喚起
- セキュリティソフトで保護する
- OS やセキュリティソフトを常に最新の状態にする

【協定参画機関】千葉県警察・千葉県産業振興センター・千葉県商工会議所連合会・千葉県商工会連合会・千葉県中小企業団体中央会・千葉大学・千葉工業大学・東京情報大学・木更津工業高等専門学校・日本大学理工学部・東京理科大学・東邦大学・日本大学生産工学部・ＮＴＴ東日本 千葉事業部・ｷﾔﾉﾝｼｽﾃﾑｱﾝﾄﾞｻﾎﾟｰﾄ株式会社・ＫＤＤＩ株式会社・ﾄﾚﾝﾄﾞﾏｲｸﾛ株式会社・富士通 Japan 株式会社・あいおいニッセイ同和損害保険株式会社・損害保険ジャパン株式会社・東京海上日動火災保険株式会社・三井住友海上火災保険株式会社

【警察窓口】
サイバー犯罪対策課対策係
℡043-201-0110（内線 3497）