サイバー防犯通信 No.49

令和元年12月25日
兵庫県警察本部
サイバー犯罪対策課

Emotet 感染拡大中!!
コンピュータウイルス感染を狙うメール攻撃に注意!

「Emotet」（エモテット）とはコンピュータウイルスの一種です。
Emotetへの感染を狙う攻撃メールの中には、**正規のメールへの返信を装う**手口が使われている場合があります。

攻撃メールの例（メールへの返信を装うもの）

差出人: ○○会社○○○○ <○○○@xxx.xx.xx>
↑実在の企業名等 ↑正規のメールアドレス
添付： ○○○○○○○.doc
↑数字の羅列.doc（ワード文書）
件名: Re: ○○○○○○○ ←注意！！
↑自分が送ったメールへの返信
本文:
○○です。
取り急ぎご連絡いたします。
↑犯人が書き加えた文章
＞○○○○○○○
↑自分が過去に送ったメール本文の引用
＿＿＿＿＿＿＿＿＿＿

○○会社○○○○ 実在の企業名等
直通メールアドレス:○○○@ xxx.xx.xx
↑正規のメールアドレス
＿＿＿＿＿＿＿＿＿＿

攻撃メールの例（業務メールを装うもの）

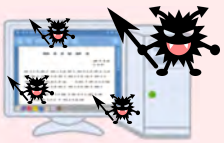
差出人: ○○会社○○○○ <○○○@xxx.xx.xx>
↑実在の企業名等 ↑正規のメールアドレス
添付： 請求書の送付のお願い○○○○.doc
↑請求書○○数字の羅列.doc（ワード文書）
件名: 請求書送付のお願い
↑業務に関係ありそうなタイトル
本文:
お世話になっております。
請求書をお送りいたしましたので
どうぞ宜しくお願いいたします。

添付ファイルが無く、https://***.**.**といったURLリンクの場合があります。

＿＿＿＿＿＿＿＿＿＿

○○会社○○○○ 実在の企業名等
直通メールアドレス:○○○@ xxx.xx.xx
↑正規のメールアドレス
＿＿＿＿＿＿＿＿＿＿

感染すると



・情報が盗まれる
　メールアカウント、メール本文、アドレス帳等の情報が盗まれる
・感染が広がる
　自分のメールアカウントやメール本文が悪用され、攻撃メールが送信される
　アドレス帳に登録されている他人の名前で、攻撃メールが送信される
等の危険性があります。

対 策

Check!

○身に覚えのないメールの添付ファイルは開かない。メール文中のURLリンクはクリックしない。
○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ず、送信元に電話等で確認する。
○OSやアプリケーション、セキュリティソフトは最新の状態にする。
○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部門等へ連絡する。