

令和3年11月



サイバァちゃん

Emotet攻擊活動再開办!?

IPA(独立行政法人情報処理推進機構)などによると、マルウェア「Emotet」の攻撃活 動再開の兆候が確認され、Emotetへの感染を狙う攻撃メールを受信しているという情報 も複数観測されているとのことです。

「Emotet」については、本年1月にEuropolが中心となった国際共同捜査によって壊 滅していました。

しかし、本年11月14日ころから、Emotetのボットネットインフラを急速に再構築し ており、海外のメディアは、『既に「Microsoft Office」の更新を装うEmotetの新たな スパムメッセージが生成され、複数のボットネットから拡散が開始された』として警告し ています。

なお、IPAで確認したファイルは、悪意のあ るマクロ(プログラム)が仕込まれたもので、 今年1月までの攻撃と同様の手口となっている そうです。

今後、日本でも攻撃メールの大規模なばらま きに発展する可能性もあります。

Emotet 感染対策

- ・企業内で注意喚起を行う
- ・メールに添付された、ファイルを不用意に 開かない
- ・Microsoft Office Word のマクロ設定で、 「警告を表示してすべてのマクロを無効にする」 を選択する
- ・定期的にオフラインバックアップを取得 する

偽A社 **Emotet** メール情報等を窃取 B社を名乗るメールから Emotet に感染する

実在の組織や人物になりすました偽メールの 添付ファイル(Wordの文書ファイル)を開けば ウイルスに感染し、感染を広げるメールの配信 元として利用されてしまいます

メールを経由して入手したOffice文書フ アイルについては、信用できると判断でき る場合でなければ、「編集を有効にする」「コ ンテンツの有効化」というボタンはクリッ クしないなど、感染対策を今一度徹底して ください。

前号で、偽メール対策訓練の紹介をいた しましたが、自社でも実施してみたいとい う方は、下記メール宛てでも結構ですので、 お気軽に御連絡ください。

長崎県警察本部サイバー犯罪対策課 095-820-0110 (3451 • 3452) メールアド レス e103107@police.pref.nagasaki.jp サイバー犯罪対策課 公式LINEアカウントで

情報配信中! 友だち登録お願いします! @3870iopi



