サイバーセキュリティ通信 Vol.13

令和４年11月

サイバァちゃん

【注意】Emotetの活動再開を確認！

１１月２日から、Emotetへの感染を狙うメールの送信が再開されたことが確認されています。

Emotetとは？

メールの添付ファイルなどから感染し、メールアドレスやログイン情報などを盗み出すマルウェアです。
盗み出したメールアドレスやメールの内容などを元に、メールの返信や関係者を装った攻撃メールを送信し、さらに感染を広めようとします。

※自組織の端末が感染していなくても、他社からメール情報等が流出し、なりすまされてしまうこともあります。

Emotetの攻撃の手口

攻撃の手口に大きな変更はありません。

悪意のあるマクロを仕込んだWordやExcelファイル又はWordやExcelファイルを圧縮したパスワード付ZIPファイルを添付した攻撃メールが送りつけられています。

ただし、これまでとは違う新しい手口として、

Officeの設定で「信頼できる場所」に登録されているフォルダ（「Templates」フォルダなど）にコピーして開くように指示し、マクロを実行させようとする

ものも発見されています。

【注意事項】

関係者からのメールであっても、不用意にファイルを開き、マクロを実行しないでください。

従業員に対し、添付ファイル付きのメールには特に注意するよう、繰り返し注意喚起をお願いします。

自組織がなりすまされてしまった場合に備えて、関係者への注意喚起のほか、プレスへのお知らせについても、日頃から検討しておきましょう。

長崎県警察本部サイバー犯罪対策課
095-820-0110（3451・3452）

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！

@387ojopi