



【注意】Emotetの活動再開！

3月上旬から、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が、今回は以下のような特徴があります。

- ・圧縮ファイル（zipファイル）付きのメールが送信される。
- ・解凍するとファイルサイズが500MBを超えるマクロ付きWordファイルが含まれている。
- ・同Wordファイルを開き、マクロを実行することで感染させる。

Officeのアップデートにより、インターネットから入手したOfficeファイルはマクロを直接実行できなくなっています。

しかし、一部のソフトウェアを利用して解凍した場合や、自社のOfficeのアップデートが行われていない場合、以前のようにマクロの実行ができてしまう危険があります。

【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、広報をどのように行うかについても、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！
友だち登録をお願いします！

@387ojopi

