サイバーセキュリティ通信 Vol.21

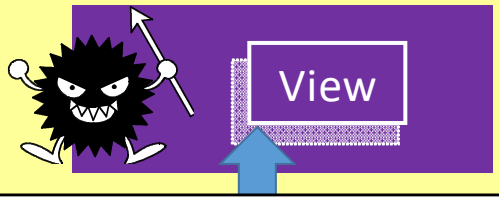
令和５年３月

サイバァちゃん

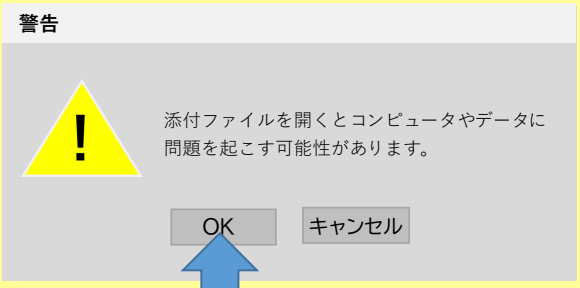
Emotetの新たな手口

Emotetへ感染させる新たな手段に Onenote が使われています。

添付ファイルを開くと「View」ボタンを押すように求められますが、これは偽物です。



「View」の画像ファイルの後ろに、スクリプトファイルが隠されています。



OKボタンを押すとスクリプトファイルが実行され、Emotetに感染します。

※信頼できないスクリプトファイルを実行すると、悪質なマルウェアがインストールされるおそれがあります。

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。

【注意事項】

関係者からのメールであっても、警告表示などが出た際は、不用意にOKボタンを押さないでください。

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！
友だち登録お願いします！

@387ojopi