2019年12月23日

株式会社 エム・シー・フーズ

わが社 社員名等を騙った不審メール(なりすましメール)に関する件

11月下旬、わが社 社員名を騙った不審なメールが送信される事象が確認されました。

今般の不審メールはEmotetと呼ばれるマルウエアが仕込まれた標的型メールです。
メールをお受け取りの皆様には多大なご迷惑をおかけして申し訳ございませんが、これらのメールはわが社社員になりすまして送信された悪質なメールであり、わが社とは一切関係がございません。

Emotet自体は2014年頃からオンライン銀行の認証情報窃取を目的としたバンキングマルウエアとして確認されていますが、現在においては全く異なる挙動、目的を持ったマルウエアとなっており、特に10月後半から流行しているタイプは受信者が過去にメールのやり取りをしたことのある実在の相手の氏名、メールアドレスで正規のメールへの返信を装う文面による攻撃メールの場合もあり注意が必要です。
メールに添付されているWORD文書を開封すると、情報を搾取されたり、ウイルス感染する可能性がございます。Emotetはウイルス対策ソフトで検知が可能ですが、Emotetに限らず、出回り始めたばかりのものについてはSPAM判定されずに届いてしまう可能性があります。これらのメールには、決して返信を行わず、また文面に添付されているURLのリンク、添付ファイル等を開くことなく削除されますようお願いいたします。

わが社におきまして、不審メールが収まるまではお手数ですが、メールの本文等でご連絡申し上げていた内容等も、重要事項は全て添付ファイルにしてパスワードを設定し、パスワードは別メールで送付させて戴くことと致します。今後もセキュリティ向上に日々努め、スパム・ウイルスメール対策及びファイヤーウォール機能強化等の対応を全力をあげて強化してまいりますのでご理解とご協力頂きますよう、宜しくお願い致します。

以　上