

弊社を装ったなりすましメールについて

2022年6月23日

お客さま・関係先さま各位

平素より格別のお引き立てを賜りまして誠にありがとうございます。

2022年6月15日夕方頃より送信されております「なりすましメール」に関しまして、皆さまには多大なるご迷惑とご心配をおかけしておりますことを、心よりお詫び申し上げます。以下、このような事態に至りました経緯や対策等についてご説明させていただきます。

<1. 事態の経緯>

・弊社では、受注担当者が、オンラインご注文の詳細確認のために必要に応じてお客さまとメールのやり取りをさせていただくことがございます。また、弊社にメールで直接ご注文をくださるお客さまもいらっしゃいます。そのような過程でお客さまや関係先さまとメールのやり取りを行なっているパソコン端末のうち一つの端末で、2022年6月15日夕方頃、誤って、「なりすましメール」のファイルを開封してしまいました。

・悪意あるファイルを開封してしまったことに気づき、すぐに端末をネットワークから遮断いたしました。すでに「Emotet(エモテット)」というマルウェア(コンピュータウイルス)に侵食されており、当該端末のメールソフト内の情報(メールアドレスなど)を窃取されてしまったと推察されます。

・その後、弊社を装った「なりすましメール」が届いた皆さまからのご連絡内容や、他社がEmotet(エモテット)の被害を受けた事例等を踏まえ、窃取された情報は「直近1年以内に弊社の受注担当者からメールを送信したことのある宛先のメールアドレスと、メールの題名、宛先氏名、メール本文の一部」であることと推定しております。

・なお、お客さまが弊社オンラインショップやお電話などを通じてご注文された際のご登録情報、お届け先の情報、お客さまのクレジットカード情報などを含むその他ご注文情報の詳細は、セキュリティで保護された自社および委託先のサーバー内に格納されております。また、今回の事態の前後で、それらのサーバー内の情報に外部アクセスの形跡がないことも確認済みでございます。従いまして、今回窃取された情報としては、上記の1台のパソコン端末のメールソフト内の情報のみと認識しております。

<2. お客さま及び関係先さまへのお願い>

・Emotet を仕掛けている攻撃者は、窃取したメールアドレス宛に、弊社のドメインとは異なるアドレスから、弊社になりすましてメールを送付しています。

これらの「なりすましメール」は、弊社社名、社員名をかたり送信されたメールであり、弊社とは一切関係がありません。弊社からパスワード付きの圧縮ファイルやエクセルファイルを送付することはございませんので、メールに添付されているファイルの開封やメール本文中の URL のクリックをせず、メールごと削除していただきますよう、よろしく願いいたします。

<3. なりすましメールへの対策>

・Emotet による「なりすましメール」の量は、攻撃者の活動状況に応じて増減するとされており、現時点では、一度開始されてしまった「なりすましメール」の送信を止める手立てがないのが実情です。誠にお手数ではございますが、弊社の名前の含まれたメールを迷惑メールとして分類していただくのが最善策かと存じます。

<4. 再発防止策>

・発生直後、当該のパソコン端末をネットワークから切り離し、初期化するとともに使用を停止しました。また、同じネットワーク内にあった全ての端末およびサーバーのウイルスチェックを実施し、脅威が存在しないことは確認済みです。

・各端末で、Emotet 侵入のきっかけとなった Word/Excel ファイルのマクロ自動実行の無効化を行いました。

・再発防止に向けたさらなるセキュリティ強化策として、メールソフトの変更、メールアドレスの変更、メール使用者の制限、メール使用端末の限定、各端末でのメール履歴の削除頻度を増やすことなどを検討しております。

・今後はこのようなことを引き起こさぬよう、システム面でのセキュリティ強化はもちろんのこと、社員のセキュリティ意識を高める施策も合わせて行って参る所存です。

この度、皆さまのメールアドレスやメール本文の一部を窃取されるという事態を引き起こすに至り、多大なるご迷惑とご心配をお掛けしておりますこと、重ねてお詫び申し上げます。また、皆さまへのご連絡や原因究明に時間を要しました点につきましても、合わせてお詫びを申し上げます。誠に申し訳ございませんでした。

お問い合わせやご質問等ございました際には、お問い合わせページからご連絡いただくか、03-3400-0871 へお気軽にお電話ください。

どうか引き続きのご愛顧を賜りますよう、心よりお願い申し上げます。

株式会社青山花茂本店
代表取締役社長 北野雅史