2022/3/1

株式会社マキテック

弊社社員を装った不審メール発生に関するお詫びとお知らせ

拝啓 時下ますますご健勝のこととお慶び申し上げます。

2022 年 2 月 25 日、弊社内のパソコンがコンピュータウイルス（マルウェア）「Emotet」に感染していることを確認し、それを発端にして、弊社とは無関係な外部のメールサーバから不審メールが、社内外に送信されるようになりました。関係者の皆様に多大なご迷惑とご心配をおかけしておりますことを深くお詫び申し上げます。本件の経緯等について、下記のとおりご報告いたします。

記

1. 経緯

2 月 25 日（金）始業後、弊社社員より弊社情報システム課へ不審メールが届いたとの連絡があり、当該メールを調査した結果、「Emotet（エモテット）」感染の可能性が高いと判断しました。

25 日の問合せ以降、弊社社員の名前を騙る不審メールが、弊社とは無関係な外部のメールサーバより、過去にメール送受信をした宛先に送信されるようになりました。

コンピュータウイルス感染による弊社業務への影響はございません。

また、弊社がお客様に提供しております、EC サイト（マキテックオンライン）及び、マキテックサービスが運営しております、シルバーカーファクトリー、LED ファクトリー、台車ファクトリー、車いすファクトリーには、コンピュータウイルスに感染していないことを確認しておりますので、通常どおりご利用いただけます。

今回の事故に対し事実関係の調査をもとに再発防止に向けた具体的改善策を講じてまいります。

2. 弊社の関係者からメールを受信された皆様へのお願い

弊社社員を名乗るメールを受信し、かつ添付ファイルが付いている場合、送信者名だけではなくメールアドレスをご確認ください。

弊社社員が業務用に使っているメールは、「****@makitech.co.jp」を利用しております。

「@makitech.co.jp」以外のドメインのメールにつきましては、メールを開封せず、また開封した場合でも添付ファイルを開かずに、メールごと削除いただけますよう、宜しくお願い申し上げます。

又、弊社社員以外の関連業者等を名乗っているケースもありますので、添付ファイルを開封する前にメールアドレスが正しいものであるかご確認をお願いいたします。

不審メールには、Excel、Word ファイルやパスワード付き zip ファイルが添付されるパターンが多く見受けられます。

パスワード付 zip ファイルの場合、一般的なメールサーバ上のウイルス対策では防げないためご注意下さい。

「Emotet」の詳細につきましては、下記サイトをご覧ください。

◆マルウェア Emotet の感染拡大および新たな攻撃手法について
https://www.jpcert.or.jp/newsflash/2020090401.html

◆「マルウエア Emotet への対応 FAQ」
※Emotet に感染する Word ファイルの表示例の紹介と共に、
チェックツールの説明があり、ダウンロードできるようになっています。
https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html

◆「Emotet 」と呼ばれるウイルスへの感染を狙うメールについて
情報処理推進機構（IPA）
https://www.ipa.go.jp/security/announce/20191202.html

今回の件につきまして社内の感染経路は判明しておりますが引き続き調査を行い、
新たな事実が判明しましたらご報告いたします。
関係者の皆様に多大なるご迷惑をおかけしましたことを重ねてお詫び申し上げます。

以上