２０２２年7月１１日
GT ソリューション株式会社

弊社 PC のウイルス感染について

この度、弊社の社員のパソコンがマルウェア（Emotet）に感染し、弊社の社員を装った第三者からの不審なメールが複数の方へ発信されている事実を確認いたしました。現在、二次被害や拡散の防止に努めております。

上記メールを受信された皆さまには多大なご迷惑、ご心配をおかけしたことを心より深くお詫び申し上げます。

なお、メールに記載された送信者をご存じであっても、不審なメールを受信された場合は、添付されたファイルやメール文中に記載の URL は開かずに、そのまま削除していただきますよう、宜しくお願い致します。

【弊社にて確認した不審なメールの一例】
※下記以外にも類似したパターンで発信されている可能性がありますので、十分にご注意ください。

差出人(表示名)：GT ソリューション株式会社の社員名
差出人(アドレス)：攻撃者のメールアドレス
件名：RE:（過去にやり取りしたメールの件名）
添付ファイル：Excel（.xls）や圧縮（.zip）ファイル

メール本文の一例：
・過去にやり取りがあったメールと関係を連想させる簡単な文章
・弊社の社員の名前が入っている
・過去にあった実際のメールのやり取りが文末に挿入

1.　これまでの経緯と対応

2022 年 5 月 19 日（火）

弊社の社員が、取引先を騙る不審メールの添付ファイルを開封し、当該社員のパソコン端末がマルウェア（Emotet）に感染。

弊社従業員宛にメールが不審な届くようになり、メールの表示名、件名から該当 PC を特定、隔離を実施。

お客様より、弊社社員を装った第三者からの不審なメールが送信されていると連絡あり。

2.　流出したと考えられる情報

当該社員とメール送受信を行った一部のメールアドレスおよび件名

3.　ウイルス感染による影響範囲

当該社員の端末に保存されていたメール情報（330 件 ※うち、お客様のメールアドレス件数 210 件）が流出した可能性があります。

現時点では、それ以外の情報が流出した事実は確認されていません。

4.　再発防止

今後、本件と同様の事象が発生しないよう、引き続き情報セキュリティ対策を強化してまいります。

以上