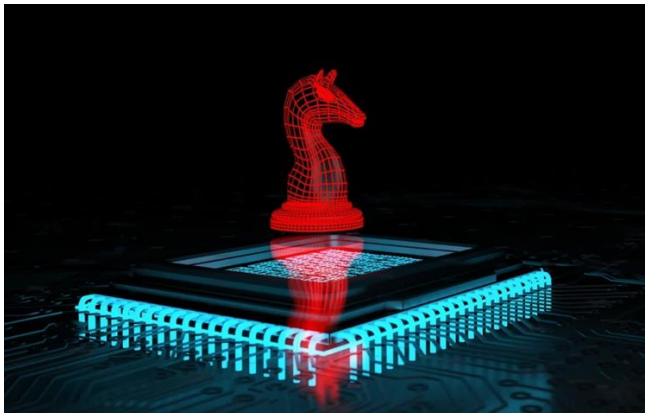
猛威を振るうマルウェア「Emotet」
サイバー攻撃の 91%はメールから始まります
企業規模を問わず、いますぐメールセキュリティ対策を！



蔓延する Emotet、1 週間の診断を行なったすべての企業で Emotet を受信しています

食料品　A 社	970 件
サービス業　B 社	15 件
製造業　C 社	17 件
電気機械　D 社	230 件
金融機関　E 社	25 件
製造業　F 社	105 件

※企業規模は数百名から数千名。測定期間は 2022 年 3 月第 1 週のわずか 1 週間。

メールセキュリティ無料診断実施中（2022 年 6 月末まで）

Emotet の感染拡大にともない、Vade/高千穂交易　では無料でメールセキュリティ診断を実施します。

Vade for M365 を「監視モード」で使用し、お客様の Emotet 受信状況をレポートします（サービス詳細はこちら）

・利用条件：Microsoft 365（Office 365)を利用している

・診断期間：2 週間（Emotet を受信次第、直ちにわかります。Emotet 以外の脅威の確認も可）

既存の環境変更は不要で、10 分ほどで導入、ご利用の Microsoft 365 メールの送受信に一切影響を与えません。

詳しくは、高千穂交易　Vade 担当：（tk_vadesecure@takachiho-kk.co.jp）までお問い合わせください。

Emotet と呼ばれるウィルスへの感染を狙うメールについて

2021 年下旬から再開が確認された、Emotet と呼ばれるウィルスメールは 2022 年 3 月現在では残念ながら日本国内は既に大流行しています。

主にマクロ付きの Excel や Word ファイル、あるいはこれらをパスワード付き Zip ファイルとしてメールに添付する形式で配信されており、ファイルを開封後にマクロを有効化する操作を実行することで Emotet の感染に繋がります。このような手法の他にも、メール本文中のリンクをクリックすることで悪性な Excel や Word ファイルがダウンロードされたり、アプリケーションのインストールを装い Emotet 感染をねらったりするケースも観測しています。日頃取引をしているメールの送信者になりすましてメールが着信するケースも確認されており正しいメールかどうかの判断が困難で、メールフィルタなどで検知されないケースも多く、最悪のケースではアカウントを乗っ取られて社内のデータを暗号化され、復帰するための身代金要求などの、企業を狙った犯罪が拡がっています。

ランサムウェアの感染による被害の報道を見る限り、大企業がターゲットと思われがちですが、実際には企業の大小を問わず攻撃を受けています。

VadeSecure 社とは、

Vade は、AI（人工知能）を用いた脅威検出とその対応技術の開発に特化したグローバルなサイバーセキュリティ企業です。サイバーセキュリティの向上と IT 効率の最大化をサポートする評価の高い製品とソリューションを、ISP、MSP および企業に提供しています。Vade の製品とソリューションは、マルウェア、ランサムウェア、スピアフィッシング、ビジネスメール詐欺、フィッシングなどのメールを介したサイバー攻撃から消費者、企業、組織を保護します。2009 年に設立され、現在 10 億個以上のメールボックスを保護しています。2016 年には、日本法人の Vade Secure 株式会社を東京都港区に立ち上げ、日本市場に本格参入しました。日本国内大手キャリアすべてのメールセキュリティとして採用され、個人および企業を未知の攻撃から守るための予測型防御を実践しています。

本製品のお問い合わせ先： tk_vadesecure@takachiho-kk.co.jp

高千穂交易製品サイト：https://www.takachiho-kk.co.jp/prod/network/vade-for-m365/

https://www.takachiho-kk.co.jp/prod/network/vadesecure/