2022 年 5 月 25 日
セーフティ＆セキュリティ株式会社

弊社を装った不審なメールに関するお詫びとお知らせ

この度、弊社従業員を装った不審なメールが複数の方へ発信されている事を確認致しました。
お客様、並びに関係者の皆様に多大なご心配とご迷惑をおかけしておりますことを、深くお詫び申しあげます。
現在、原因の調査、並びに二次被害や拡散の防止に努めておりますが、不審なメールを受信した際には添付ファイルは開かず、メールを削除いただきますようお願い致します。
メールを受信した場合や、開封してしまった場合の対応を以下のとおりまとめましたので、対策・対応のご参考になれば幸いです。

※本情報は独立行政法人 情報処理推進機構（IPA）のサイトや IPA への問い合わせから得た情報より出展しています。
※詳細情報は本ページ下部のリンクよりご参照ください。

《この度の不審なメールについて》
複数の特徴より、「Emotet（エモテット）」と呼ばれるマルウェアであると認識しています。

《Emotet（エモテット）の特徴①》
差出人表示と実際の送信元のメールアドレスが異なります。
弊社従業員のメールアドレスは「****@saf-sec.co.jp」のアドレスです。
不審なメールの特徴は、差出人の表示は「セーフティ＆セキュリティ株式会社」や、「（従業員名）〇〇」等と表示されております。
また、件名の冒頭には「Re:」や「FW:」が記載され、受信した方のお名前や、「ご確認ください」などの文言が記載されるなど、弊社従業員から送信しているかのような表示になっておりますが、送信元のアドレスは弊社とは全く関係のないアドレスになっています。

《Emotet（エモテット）の特徴②》
Zip（圧縮）ファイルやエクセル、ワードなどのファイルが添付されています。

《不審なメールを受信したら》
メールごと削除してください。

メール本文を閲覧しただけでは感染しませんが、添付ファイルを開封したり、メールに記載されている URL にアクセスした場合はウイルスに感染するおそれがあり、PC に保存されている個人情報などを不正に取得されてしまう場合があります。

《添付ファイルを開いてしまったら》

①インターネットに接続しないよう、Wi-Fi 接続を切る、LAN ケーブルを抜くなど、PC を物理的に**ネットワークから切り離してください**。

②パソコンにインストールされている**ウイルス対策ソフトウェアを起動し、ウイルススキャンを実施してください**。不正なファイルがある場合はそのファイルが隔離・削除されます。なお、ウイルス対策ソフトのセキュリティ更新プログラムは最新バージョンであることを確認してください。

（定期的なウイルススキャンでもファイルの隔離・削除が行われています）

《Emotet（エモテット）の被害範囲》

本ウイルスは Windows OS に対する脅威であることから、iPhone（iOS）や Android のスマートフォンでの被害は確認されておりません。

※独立行政法人 情報処理推進機構（IPA）による情報（2022.03.01）

弊社では今回の事態を受け、被害拡大の防止に努めるとともに、より一層の情報セキュリティ対策の強化を推進してまいります。何卒、ご理解とご協力を賜りますようお願い申しあげます。

■このウイルスの詳細について

・独立行政法人情報処理推進機構セキュリティセンター

(「Emotet（エモテット）」と呼ばれるウイルスへの感染を狙うメールについて）をご参照ください。

https://www.ipa.go.jp/security/announce/20191202.html

（最終更新日：2022.04.26)

・警視庁

https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/joho/emotet.html

なお、迷惑メールによるコンピュータウイルス・不正アクセスに関する被害の届出につきましては、経済産業省が所管する独立行政法人 情報処理推進機構（IPA）のサイトをご参照いただければ幸いです。

・独立行政法人 情報処理推進機構（IPA）コンピュータウイルス・不正アクセスに関する届出について

https://www.ipa.go.jp/security/outline/todokede-j.html

― 以上 ―