2022年3月29日
株式会社アシスト

弊社を装った不審メールに関するお詫びとご報告

この度、弊社従業員の使用するパソコン1台（以下：当該端末）がマルウェア「Emotet（エモテット）」に感染し、メール情報が窃取され、弊社従業員を装った第三者から不審なメールが複数の方へ発信されていることを確認いたしました。
本件につきまして、外部の調査会社に委託した調査を含めて、当該端末の詳細調査が完了しましたので、これまでの経緯と再発防止策を含めて下記の通りご報告いたします。

お客様ならびに関係者の皆様に多大なご迷惑とご心配をおかけいたしておりますことを、深くお詫び申し上げます。

1. 感染状況について

弊社従業員の使用していたパソコン1台がEmotetに感染し、委託先の調査会社によるログならびに端末に対する詳細調査の結果から、当該端末に保存されていたメールアドレス、メール件名、メール署名の情報が流出したことを確認しました。

また、調査会社の調査では特定できなかったものの、お客様ならびに関係者の皆様からの情報提供により、メール本文についても当該端末から流出したものと判断しております。

なお、当該端末はマルウェアへの感染疑いの時点で速やかにネットワークから遮断しました。その後は、C2サーバなどを含めた不審サイトへのアクセス状況の監視および、エンドポイントセキュリティツールによるマルウェア監視状況から、当該端末以外へのマルウェアの伝播は行われていないと判断しております。

2. これまでの経緯

2/28	・弊社内でマルウェア感染の発生が疑われる事象を確認、内部調査を開始
3/1	・弊社Webサイトにて注意喚起のお知らせを掲示
3/2	・感染が疑われるパソコンを特定し、当該端末をネットワークから遮断、外部委託先の調査会社へログを提供し調査開始 ※その後の外部委託先での調査により、2/26に感染していたこと、感染から5分後にEPP（※）によりマルウェアが隔離されたことを確認
3/3	・調査対象の端末のEmotet感染を確認 ・弊社Webサイトにて感染報告を掲示
3/7	・外部委託先にて当該端末のフォレンジック調査を開始
3/25	・当該端末の詳細調査（フォレンジック調査）が完了 ・再発防止策を策定

※EPP：エンドポイントセキュリティツール

3. Emotetについて

当該端末が感染したEmotetについては、その振る舞いに関して、次のような特徴が確認され、いわゆる「ばらまき型」と呼ばれる挙動を示しております。

弊社を装った不審メールの特徴として、メール本文中の引用部分に「Subject: Re: AW: xxxxxxx.....」のように「AW:」が入ったものがあります。外部の調査会社での調査も踏まえて、これらの特徴から、弊社の端末が感染したEmotetのタイプは「標的型攻撃」ではなく、「ばらまき型攻撃」のものと推定しております。

また、このタイプのEmotetはメールアドレス、件名に加えて、メール本文の内容がその後の不審メールにおいて引用されることが判明しています。このため、調査会社の解析ではメール本文の流出についてはっきりとした形跡は確認できておりませんが、これまでお寄せいただいた情報から、メール本文を含めて流出していると想定して対策を検討しております。

4. 弊社の情報セキュリティ対策について

弊社においては、下記4段階の防御を行っております。

1. スパムフィルターによる検疫
2. エンドポイント保護プラットフォーム（EPP）による検疫
3. FireWallによる制御
4. セキュアWebゲートウェイ（SWG）による制御

※今回弊社の所有端末が感染したマルウェアEmotetは、残念ながら上記全ての防御壁をすり抜けておりました。ただし、感染同日にはEPPツールでマルウェア判定され、その後は隔離されていることを確認しております。

5. 再発防止策

本件の発生を重く受け止め、下記の対策を実施して再発防止に努めてまいります。

1. より強固なセキュリティ対策が見込まれるWebメールへ移行
2. クラウドストレージへ移行しPPAP運用（暗号化圧縮ファイルのメールへの添付）を廃止
3. 弊社従業員への情報セキュリティ教育を強化し、不審メールの見分け方など周知徹底

今回の事象を受け、今後、より一層の情報セキュリティ対策の強化に取り組んでまいります。ご理解、ご協力を賜りますよう、何卒よろしくお願い申し上げます。

■本件に関してのお問い合わせ窓口

株式会社アシスト 情報セキュリティ委員会
メール：kka_sec2022@ashisuto.co.jp
フォーム：https://www.ashisuto.co.jp/pa/contact/attention.html