２０２２年１０月４日
有限会社 東海ホケン事務所

1. 概要
このたび弊社役員の使用するパソコンがマルウェア「Emotet」に感染したことを確認いたしました。 お客様ならびに関係者の皆様にご迷惑をおかけておりますことを、深くお詫び申し上げます。

2.経緯
6 月 11 日に、弊社役員が利用しているメールアカウントに取引業者を装うメールを受信し、添付ファイルを誤って開封してしまいました。 翌日 6 月 12 日にパソコン内のセキュリティソフトが作動しており、ウイルス感染を確認しました。調査の結果、当該メールアドレス利用 PC にてマルウェア「Emotet」への感染を確認いたしました。

3. 発生原因
ただちに外部の専門家による調査を開始、アンチウィルスソフトによる検出履歴より、6 月 11 日にメールに添付されたマルウェア「Emotet」の暗号圧縮ファイルを当該 PC にて解凍・実行しウイルス感染したものと推測しています。 また、その際メールアカウントに 登録されているメールアドレス情報が窃取された可能性があります。

4. 被害
ウイルス感染した当該 PC で保有していたメールアドレス情報 392 件(氏名、メールアドレス)の流出の可能性があります。幸いウイルス感染に気付くまでに時間を要さなかった為、当該 PC 以外への感染は無く、現在のところ機密情報流出は確認できておりません。また、感染日以後の不審なアクセスログは確認できず、その他の情報の流出は無かったと判断しております。

5. 対応状況
① 該当 PC の使用停止、感染 PC の隔離
事象確認後すぐに当該 PC を使用停止。社内の全 PC・ネットワーク機器に「Emotet」、およびその他マルウェアがないかアンチウィルスソフトと Emocheck にて感染有無確認し、感染 PC が当該 1 台のみであることを確認し感染 PC を社内ネットワークから隔離いたしました。

② パスワード変更
被疑メールアカウント含む全メール、ネットワークのパスワードを変更いたしました。

③ お客様へのお詫びと通知
感染 PC にて保持していたメールアドレスのお客様、関係者へは個別に電話連絡いたしました。

④調査方法
第三者機関に依頼し、フォレンジック調査を実施しました。この調査は、PC を調査・分析し被害範囲や影響範囲を特定するためのものです。感染日以降の不審なアクセスログは確認できず、その他の情報の流出は無かったと判断しております。

6. 再発防止対応
外部の専門家に相談、 指導のもと、不審メール開封リスク低減策および万一開封してしまった際の迅速な対応体制整備を検討、実施してまいります。

7. 本件に対するお問合せ先
（所在地）愛知県知多市にしの台 4 丁目 13-8
（名称）有限会社 東海ホケン事務所
（代表者）代表取締役 竹内良光
（電話番号）0562-55-8118
（メールアドレス） y.take@t-hoken.co.jp
（受付時間）09:00～17:00
（定休日）日曜・祝日・土曜午後

参考情報: 独立行政法人情報処理推進機構
「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
https://www.ipa.go.jp/security/announce/20191202.html