情報セキュリティ対策で
お客様の会社を守る運動

6月頃からEMOTET再熱！クレジットカード情報も盗み出せるように･･･

2022年6月頃から再度EMOTETによるサイバー攻撃が急増しています。
警察庁は、マルウェア「EMOTET」の最新の解析結果として、「Google Chrome」に保存されたクレジットカード番号や氏名、有効期限を盗み、外部に送信する機能の追加を確認したことを公表しました。暗号化されたデータを復号するための鍵も同時に盗み出すため、保存したカード情報が第三者に知られるおそれがあるとし、注意を呼び掛けています。
企業にとっては、もちろん対策が必要になりますが、個人の方々も、より一層EMOTETへの感染に注意する必要が出てきています。添付ファイルとして次のファイルが確認されています。

・zip（パスワード付き）→　解凍するとlnk、xls、doc形式のファイルが入っている
・xls

もし感染被害にあってしまったら

個人の方の場合
まずは下記の対応をしておくと安心です。

・Chromeブラウザに登録しているクレジットカード情報、パスワード情報の変更

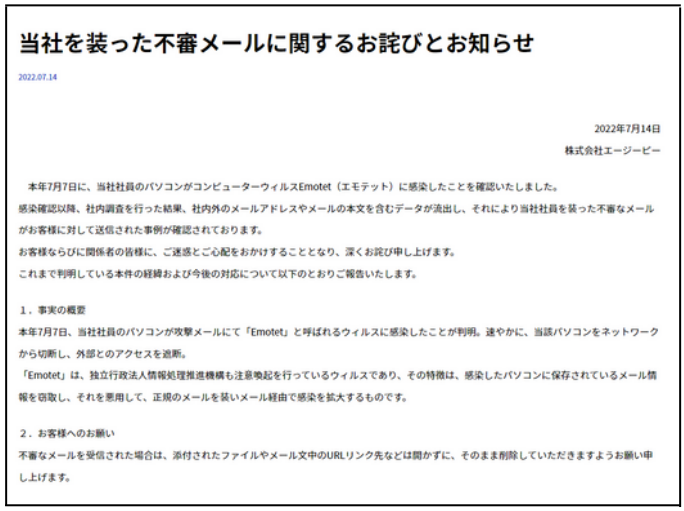
企業の場合
・Emocheckによる感染調査（感染が見つからなくても感染していないとは言い切れないのでご注意ください）
・社内への注意喚起（社員同士でも怪しいメールがあれば報告するように）
・メールサーバーのパスワード変更
・取引先等への注意喚起
・個人情報保護委員会への報告
・感染状況の調査＆解析

被害事例

航空機への電力供給を行う東証スタンダード上場企業の株式会社エージーピーは7月14日、EMOTET感染による不審メールについて発表しました。
2022年7月7日、社員のパソコンが攻撃メールにて「EMOTET」と呼ばれるウィルスに感染したことが判明し、速やかに、当該パソコンをネットワークから切断し､外部とのアクセスを遮断。

感染確認以降、社内調査を行った結果、社内外のメールアドレスやメールの本文を含むデータが流出し、それにより当社社員を装った不審なメールがお客様に対して送信された事例が確認さたそうです。

また今後の対応について、外部専門機関の協力を得ながら事実関係についての更なる調査を実施し、二次被害の防止や拡散防止に努め、再発防止の徹底と一層の情報セキュリティ対策の強化に取り組むと報告しています。



当社を装った不審メールに関するお詫びとお知らせ

2022.07.14

2022年7月14日
株式会社エージーピー

本年7月7日に、当社社員のパソコンがコンピューターウィルスEmotet（エモテット）に感染したことを確認いたしました。
感染確認以降、社内調査を行った結果、社内外のメールアドレスやメールの本文を含むデータが流出し、それにより当社社員を装った不審なメールがお客様に対して送信された事例が確認されております。
お客様ならびに関係者の皆様に、ご迷惑とご心配をおかけすることとなり、深くお詫び申し上げます。
これまで判明している本件の経緯および今後の対応について以下のとおりご報告いたします。

1．事実の概要
本年7月7日、当社社員のパソコンが攻撃メールにて「Emotet」と呼ばれるウィルスに感染したことが判明。速やかに、当該パソコンをネットワークから切断し、外部とのアクセスを遮断。
「Emotet」は、独立行政法人情報処理推進機構も注意喚起を行っているウィルスであり、その特徴は、感染したパソコンに保存されているメール情報を窃取し、それを悪用して、正規のメールを装いメール経由で感染を拡大するものです。

2．お客様へのお願い
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のURLリンク先などは開かずに、そのまま削除していただきますようお願い申し上げます。

出典:https://www.agpgroup.co.jp/

EMOTETに感染してしまった場合
最初にすべきことは、感染した端末、感染が疑われる端末のネットワークを遮断することが重要です。

MAGMAX マグマックス株式会社

5分でできる！マルウェア対策チェックシート

サイバー攻撃を防ぐためには、適切にセキュリティ対策を行うことが重要です。
そこで以下のチェック項目で自社の状況を振り返ってみましょう。

対策

- ☐ **①ウイルス対策ソフトを導入していないパソコンがある**
- ☐ **②社員がどういったWebサイトにアクセスしているのか分からない**
- ☐ **③HDDを暗号化していない**
- ☐ **④業務で利用するパソコンの設定や管理は社員に任せている**
- ☐ **⑤社内にIT担当者がいないため、どのようにセキュリティ対策を行えばよいのか分からない**

このチェックシートの項目に1つでも当てはまるものがあれば、自社のセキュリティ対策を考え直すべきでしょう。
各項目には以下のようなリスクがあるためです。

①ウイルス対策ソフトを導入していないパソコンがある

ウイルス対策ソフトの導入は、セキュリティ対策の基本です。必ずすべてのパソコンで利用するようにすべきです。

②社員がどういったWebサイトにアクセスしているのか分からない

昨今ではWebサイトにアクセスするだけでマルウェアに感染する攻撃手法が広まっているため、
不必要なWebサイトへのアクセスは遮断することを考えましょう。

③HDDを暗号化していない

特に社外に持ち出す、あるいはリモートワークで利用するパソコンは、
盗難や紛失によって第三者の手に渡ることが考えられるため、情報漏えい対策としての暗号化は重要です。

④業務で利用するパソコンの設定や管理は社員に任せている

業務で利用するパソコンを社員任せにした場合、セキュリティ上危険な状態である可能性が十分に考えられます。
適切にセキュリティ対策を施したパソコンを社員に提供すべきでしょう。

⑤社内にIT担当者がいないため、どのようにセキュリティ対策を行えばよいのか分からない

サイバー攻撃は企業規模や業種などを問わずに行われており、たとえIT担当者がいなかったとしても
適切に対策を講じなければなりません。

出典：https://www.ntt.com/bizon/web-separate.html#section02

皆様がよりセキュリティに興味を持ち、日々の対策にご活用いただくきっかけとなれば幸いです。

MAGMAX マグマックス株式会社