情報セキュリティ対策で

お客様の会社を守る運動

EMOTET

感染拡大中マルウェアエモテット

2022年4月頃より、新たな手口が確認されています。

EMOTETとは攻撃メールの受信者が過去にメールのやり取りをしたことのある、実在の相手の氏名、メールアドレス、メールの内容等の一部が、攻撃メールに流用され、「正規のメールへの返信を装う」内容となっている場合や、業務上開封してしまいそうな巧妙な文面となっている場合があり、開封してしまう可能性が非常に高いです。IPA(情報処理推進機構)はショートカットファイル（LNKファイル）を悪用した攻撃を確認した為注意を呼び掛けています。

EMOTETに感染すると

- 重要な情報を盗み取られる
- ランサムウェアなど強力なマルウェアに感染する
- 社内の他の端末にEMOTETが感染する
- 社外へのEMOTETばら撒きの踏み台にされる

感染後のリスク

・信用失墜　・損害賠償請求　・全データ暗号化
・取引停止　・業務停止　・身代金要求

重要な情報を盗み取られる

不正侵入したEMOTETがもたらす被害

端末内の情個人情報や、メール関連だけではなくIDやパスワードといった、認証情報も盗み取ります。社内ネットワークやクラウドサービスに不正ログインされ、重要情報の流出へと繋がります。

社内ネットワークに感染が広がる

EMOTETには自己増殖が可能な「ワーム」機能がある

ワームは、自分自身を複製して増殖するプログラムです。自己複製と単独活動により、社内ネットワークを介して他の端末へと感染を広げます。

ランサムウェアなどの強力なマルウェアに感染する

EMOTETがプラットフォームとなる

強力なマルウェアをダウンロード・実行し、マルウェアの1つ「ランサムウェア（身代金要求型ウイルス）」に感染すると、PCや重要ファイルが暗号化され、攻撃者から元の状態に戻す代わりに金銭を要求されます。EMOTETは、様々なマルウェアを呼び込んで企業・組織に深刻な被害をもたらします。

社外へのばら撒きの踏み台にされる

新たな被害を生み出す可能性があります。

EMOTETは、侵入した端末からメール情報を盗みます。メールアドレスや企業・個人名を悪用し、取引先などへEmotetを添付した偽装メールをばら撒きます。自社の感染が原因で取引先などに被害が生じた場合、注意喚起や補償の対応に追われるでしょう。企業の信用も損なわれ、機会損失に繋がる可能性もあります。

MAGMAX マグマックス株式会社

EMOTET

感染拡大中マルウェアエモテット

対策をしていなかったために、知らぬ間に自分が加害者に･･･？

インターネット社会では、被害者になるだけではなく、知らない間に加害者になってしまうこともあります。自社のシステムやパソコンが第三者に乗っ取られてしまい、不正アクセスやスパムメール等の中継サイトとして知らぬ間に攻撃に加担してしまうのです。これを『踏み台にされる』と言います。

なぜ自分が加害者に？

なぜ悪くない自分が加害者のように見えるのか･･･
踏み台にされた自社のサーバがもともとの被害者であるにも関わらず、実際に攻撃を受けた側からは、踏み台にされたサーバからの攻撃のように見えてしまうのです。つまり、きちんと情報セキュリティ対策を行わないと、被害者になると同時に加害者になってしまうこともあるのです。

通常、自分のパソコンが踏み台にされている、ということを知るすべがありません。知らぬ間に他国や大手企業に攻撃を仕掛けて、いきなり冤罪事件に巻き込まれる･･･あなたの会社は大丈夫ですか？

EMOTET攻撃手法

WordやExcelの添付ファイルでマクロを有効化させる

基本的な攻撃手法

不正なメールに添付された主に上記ファイルに仕込まれています。添付ファイルには、マクロの実行を促す文面が記載されており、受信者がそれに気づかず「コンテンツの有効化」をクリックすることでマクロが起動しEmotetに感染します。

パスワード付きZIPファイルを使う攻撃

ZIPファイルの中に悪意のあるマクロを仕掛けている

この手口では、添付ファイルが暗号化されていることから、メール配送経路上でのセキュリティ製品の検知・検疫をすり抜け、受信者の手元に攻撃メールが届いてしまう確率が高いのです。悪意のあるマクロが仕掛けられているZipファイルの「コンテンツの有効化」ボタンをクリックすると、ウイルスに感染させられてしまいます。

URLリンクを悪用した攻撃

メールの本文中のリンクをクリックすると･･･

このリンクをクリックすると、外部ウェブサイトから不正なファイルがダウンロードされる手口です。メールの本文は複数のパターンが存在し、今後、件名・本文ともに更に巧妙化していく可能性があります。

PDF閲覧ソフトを偽装する手口

攻撃者の用意した偽のウェブサイト）へ誘導される

メール本文中のURLリンクをクリックすると、閲覧可能なPDFファイルが存在するかのような画面に誘導し、そこでPDFファイルの閲覧ソフトを装ったウイルスファイルをダウンロードさせ、利用者の手で実行させるという手口です。
リアルなメールの文面、PDF閲覧のために必要だと促しファイルをダウンロードさせる、次々と手段を変えて攻撃してきます。

MAGMAX マグマックス株式会社