Emotet（エモテット）という脅威

Emotet（エモテット）

・巧妙なメールの標的型攻撃で、ばらまき攻撃もある
・本体には不正なコードをあまり含まない
・強い感染力と拡散力
・ランサムウェアなど、マルウェアに感染する
・感染するとばらまきの踏み台にされる

重要な情報を盗まれる
他のウィルスへの感染に悪用される
日本語のメールでも攻撃
攻撃対象者の実在の相手を装う
ネットワーク全体への感染
PowerShell が利用される

IPA や、JPCERT/CC などから、非常に恐ろしいマルウェア Emotet（エモテット）の感染に関する注意喚起が行われています。
Emotet は、2014 年にバンキングのトロイの木馬として特定され、特に 2019 年後半より日本でも猛威を振るっています。
Emotet は、主にスパムメールを通して拡散されるトロイの木馬のマルウェアです。
正当なメールに見えるように巧妙に作られており、名が通った会社からの請求書や支払明細書など、ひっかかりやすい言葉をうまく使用して、悪意のあるスクリプトやマクロ付きのドキュメント、リンクなどをクリックさせようと仕向けます。
Emotet の初期バージョンは、悪意のある JavaScript ファイルとして届きましたが、その後のバージョンでは、マクロが埋め込まれたドキュメントが使用され、C&C サーバより、ウィルスを取得するように進化しました。
また、仮想マシン内で検知ツールが実行されているかどうかも認識して、サンドボックス内で休止状態になったりできます。Emotet は、ソフトウェアが一部のマルウェア対策製品の検出を回避するのに役立つ機能を持っていたりするからです。
ワームのような機能を使用して、接続されている他のコンピュータへの拡散を可能にし、マルウェアの配布を行います。
さらに恐ろしいことに、Emotet は、C&C サーバを利用して、攻撃者のソフトウェアを更新したりできます。これにより、ユーザ ID やパスワード、メールアドレスなどを盗んだりします。
実際、日本でも実在の組織や人物になりすましたメールは、攻撃対象者が過去にメールのやり取りをしたことがある相手の氏名やメールアドレス、メール内容の一部を引用し、あたかも正規のメールの返信かのように装っているとのことです。
元にした情報も、Emotet の感染によって盗まれたものであるため、被害が悪循環してしまう恐れがあります。
IPA の注意喚起によれば、Emotet の攻撃メールは、件名や本文等が変化しながら断続的にばらまかれているとのことで、「新型コロナウィルス」に関する情報を装う攻撃メールなどは、一見して不審と判断できるほどの不自然な点は少なく、悪意のあるマクロが仕組まれた Word 文書だったそうです。
Emotet は、単体で感染することはあまりありませんが、ランサムウェアなど様々なマルウェアを感染させるプラットフォームとして機能してしまっているため、結果的に非常に強い感染力と拡散力を持った、恐ろしいマルウェアです。
企業は、こうした攻撃が実際どのような形で行われているのかを把握し、社内はもちろん、関係するグループ企業や取引先に迷惑がかからないよう、しっかりとしたセキュリティ対策が必要です。