サイバーニュース

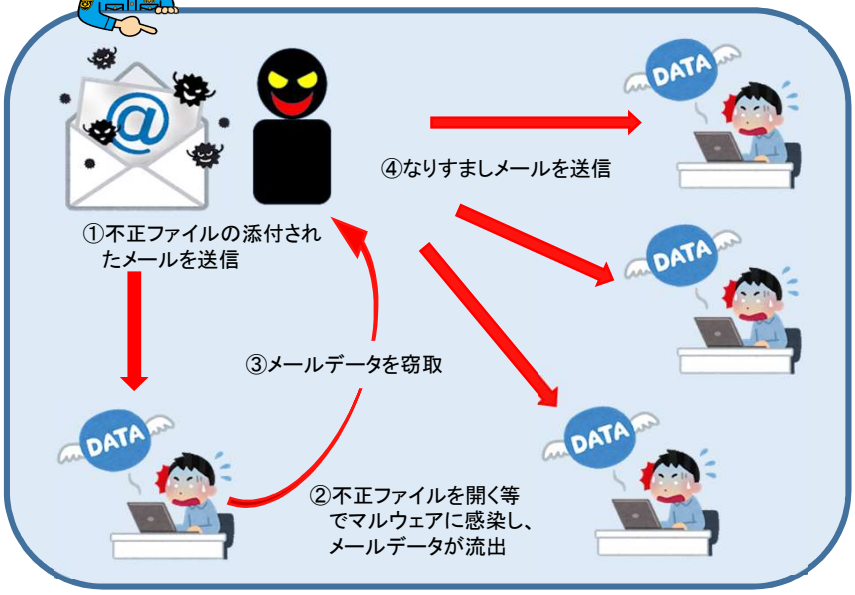
R 2 年 第 2 号
奈良県警察本部
サイバー犯罪対策課

「Emotet」への感染を狙うメールに注意!!
新型コロナウイルスに乗じた偽メールが確認!!

これまでにもマルウェアとして世界で確認されていた[Emotet」(エモテット）が、昨年９月後半から国内で活発化をはじめ、感染する状況が確認されていました。

この「Emotet」の攻撃の手口は、メールを主な感染経路としており、感染環境から窃取したメールデータを元に、「なりすましメール」を送信します。受信者は、なりすましに気付かずにメールに添付された不正なファイルを開いたり、メール内に記載のURLをクリックして不正なファイルをダウンロードし、マルウェアに感染してしまいます。

Emotetの活動概要図



注意

新型コロナウイルスに関連したフィッシングメールをばらまく手口が確認されています！！

例：新型コロナウイルスに乗じたフィッシングメール

感染を防ぐ対策

「Emotet」をはじめとしたマルウェアへの感染を防ぐためには、一般的なウイルス対策が重要となり次のような対応をすることを勧めます。

- 身に覚えのないメールの添付ファイルは開かない。メール本文中のURLリンクはクリックしない。
- 自分が送信したメールへの返信に見えるメールであっても、不自然な点があれば添付ファイルは開かない。
- OSやアプリケーション、セキュリティソフトを常に最新の状態にする。
- 信頼できないメールに添付されたWord文書やExcelファイルを開いた時に、マクロやセキュリティに関する警告が表示された場合、「マクロを有効にする」「コンテンツの有効化」というボタンはクリックしない。
- メールや文書の閲覧中、身に覚えのない警告ウインドウが表示された際、その警告の意味がわらない場合は、操作を中断する。
- 身に覚えのないメールや添付ファイルを開いてしまった場合は、すぐにシステム管理部門等へ連絡する。

【参考】独立行政法人情報処理推進機構IPA「Emotet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
日本サイバー犯罪対策センター（JC3）「新型コロナウイルスに乗じた犯罪」
https://www.jc3.or.jp/topics/newmodel_coronavirus.html