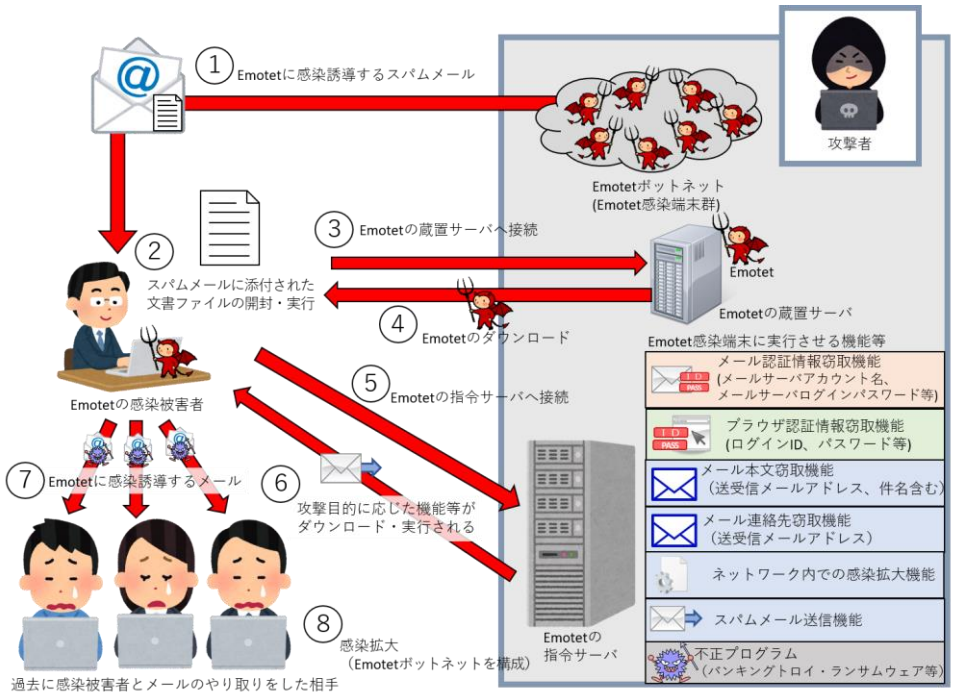
回覧 印 印 印 印 印 印 印 印 印 印 印 印

ASAMA Security Newsletter Vol.79

あさまセキュリティニュースレター

Emotet活動再開　被害にあったら取引先にも！

（2021年12月9日）



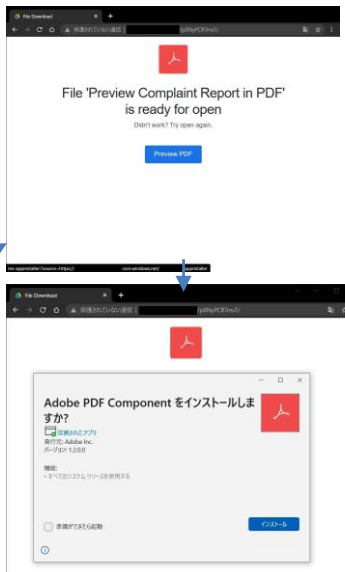
出典：警察庁 @police　https://www.npa.go.jp/cyberpolice/important/2020/202012111.html

お客様先でも、11月中旬からWordやExcelの添付ファイルでの検知が確認されています
また、パスワード付きzipファイル、PDF閲覧ソフトをダウンロードさせる手法も感染されているようです

知っている相手からのメールを装い攻撃してきますので、メールのやり取り、特に添付ファイルは確認してから開きましょう
また年末年始にたまったメールの確認も細心のご注意を！

攻撃のパターン

PDF閲覧ソフトを装った不正プログラムをダウンロードさせるパターン
Wordやエクセルファイルを添付したメールを開かせ、コンテンツの有効化をすることで、不正なプログラムをダウンロード、実行させる→Emotetに感染



PDF閲覧ソフトをダウンロードするように見せかけ、不正プログラムをインストールさせる手口
引用元: JPCERTコーディネーションセンター
マルウエアEmotetへの対応FAQ
https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html

被害

- **メールソフトやウェブブラウザーに記録したパスワードなどが窃取**される
- **過去にやり取りしたメールの本文、メールアドレスなどが窃取**される
- **窃取されたメール関連の情報が悪用され、感染拡大を目的としたメールが送信**される
- **ネットワーク内のほかのPCに感染が拡大**する
- **ほかのマルウェアに感染（インターネットバンキングの情報の窃取を目的としたものなど）**

対策

- 不審なメールだけではなく、**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。メール本文中のURLリンクはクリックしない**
- **メールに添付された文書ファイルを開いたとき**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、**
- **マクロの有効化や、警告を無視する操作は行わない**
- マクロの自動実行機能を備えたソフトは、当該の機能を無効化する
- ソフトウェアアップデート、ウイルス対策ソフト、インターネット出入り口のセキュリティ対策の確認・更新

メールの添付を開きコンテンツの有効化をした、取引先からEmotetと思われる内容の連絡を受けた場合、
下記サイトの感染確認ツール『EmoCheck』で確認を行い、手順従い対処しましょう
https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html（JPCERT/CC　マルウエアEmotetへの対応FAQ）

情報源
IPA　https://www.ipa.go.jp/security/announce/20191202.html#L16　**警察庁**　https://www.npa.go.jp/cyberpolice/important/2020/202012111.html

浅間商事株式会社　〒110-0005　東京都台東区上野7-15-70 浅間第一ビル　0120-830-414