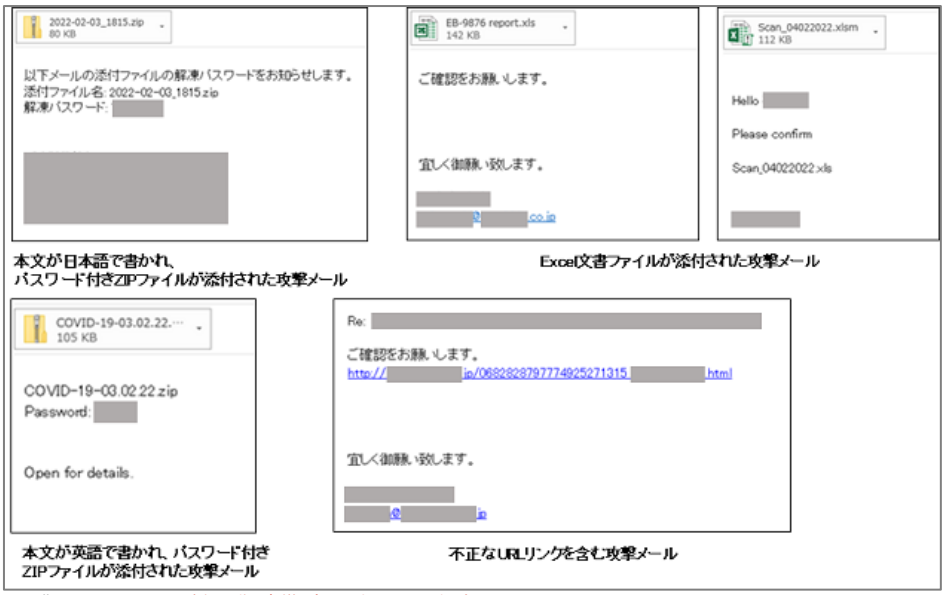
回覧 印 印 印 印 印 印 印 印 印 印 印 印

ASAMA Security Newsletter Vol.81

あさまセキュリティニュースレター

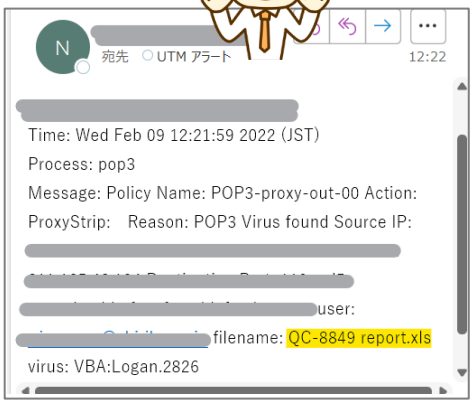
Emotet（エモテット）被害急増！　取引先からのメールでも要注意 （2022年2月9日）

2021年11月から2022年2月までにIPAで確認した、Emotetの攻撃メールの一例です。
これら以外にも様々なパターンのメールは存在し、いずれも添付ファイルの開封やURLリンクのクリックを誘導する内容となっています。



出典：IPA　Emotetの攻撃活動の急増 （2022年2月9日 追記）
https://www.ipa.go.jp/security/announce/20191202.html#L18

お客様先でも、2月初旬からExcelやzip形式の添付ファイルでの検知が確認されています
差出人は、取引先のみならず、社内の方を装った攻撃も確認しました
社内メールのやり取りでも注意が必要です



検知履歴を確認すると、XX-数字4桁report.xls
というファイル名でメール添付してくる
攻撃を多く検知してます

攻撃のパターン

WordやExcelファイル、ダウンロードリンクを開かせ、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

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（ランサムウェア、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　相手に確認する**
- **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、**
- **コンテンツの有効化や、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の導入、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、手順に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#L18　**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