回　覧　印　印　印　印　印　印　印　印　印　印　印　印

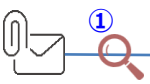
ASAMA Security Newsletter Vol.82

あさまセキュリティニュースレター

Emotet（エモテット）とセキュリティ対策について

（2022年3月14日）

メール受信時



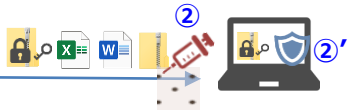
①スパムチェック

メールの件名確認
（SPAM判定の付与の有無）

迷惑メールフォルダに振分

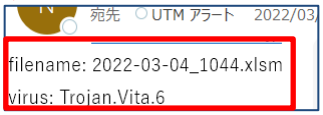
差出人が、社内・取引先からでもSPAMの疑いがある場合は要注意！相手に確認を！！

メール受信時、受信後



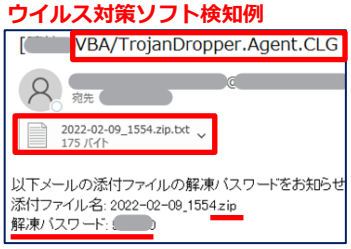
②アンチウイルスやサンドボックス

社内に入る際にチェック
検知例



暗号化メールやファイルは、解凍後
②'ウイルス対策ソフトでチェック可能！

ウイルス対策ソフト検知例

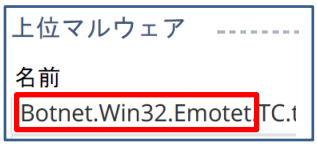


ファイルを開き不正なプログラムを実行サイトへ誘導、ウイルスダウンロード時

③　アンチボット・WBEブロッカー
ウイルスをダウンロードするサイトへのアクセスをブロック

②②'　アンチウイルス、サンドボックス
ダウンロードされるウイルスをブロック

アンチボットでの検知例



Emotet（エモテット）の攻撃パターン

①Word、Excel、zipの添付ファイル、ダウンロードリンクがあるメールを受信　対策①・②・②'
②添付ファイルやURLリンクから不正なプログラムを実行させ、ウイルスをダウンロードさせる　対策②・②'・③
③Emotetをダウンロードさせるサイトへ接続、ダウンロード・感染　対策　③・②・②'
④感染後は、ボットネットと通信し指令通りに操作、情報搾取・踏み台として利用　対策②・②'・③

対策

・Emotetに感染するまでに、セキュリティ対策の機能で防げるシーンがいくつもあるため、社内や利用しているパソコンのセキュリティ対策の環境がどうなっているか確認しましょう
（社内と自宅、外出先のインターネットは環境も異なるため、社内で防げても外出先や自宅で防げないこともあり）
・迷惑メールと判断されているメールは知っている相手でも、不審なメールは確認しましょう
・添付ファイルや、URLを安易に開かず、脅威があることを知りましょう（知っていれば防げる）
・メールの添付を開きコンテンツの有効化をした、取引先から変なメールが来てますと連絡を受けた場合、インターネットを遮断し、下記サイトの感染確認ツール『EmoCheck』で確認、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
警察庁　Emotet（エモテット）感染を疑ったら　https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/joho/emotet.html
JPCERT　マルウエアEmotetの感染再拡大に関する注意喚起　https://www.jpcert.or.jp/at/2022/at220006.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