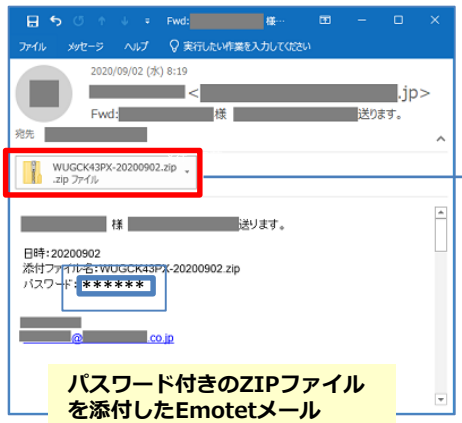
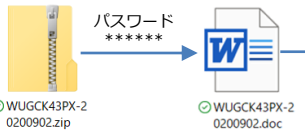
回覧 印 印 印 印 印 印 印 印 印 印 印 印

ASAMA Security News Letter Vol.64

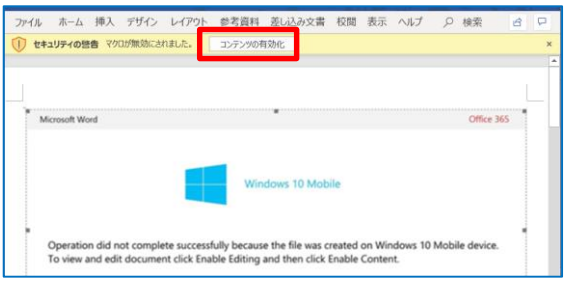
あさまセキュリティニュースレター

被害急増中！パスワード付き添付ファイルにも要注意！！　（2020年09月15日）





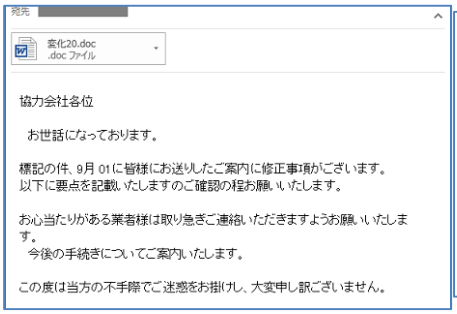
ファイルを開いてしまっても、
コンテンツの有効化は絶対にしないように！！

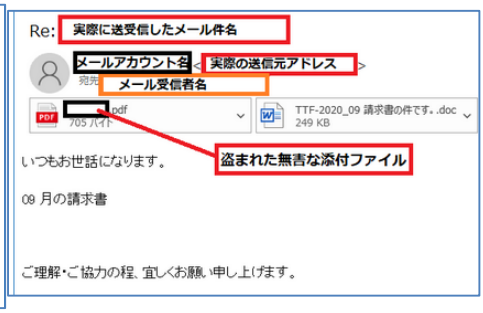


パスワード付きのZIPファイル
を添付したEmotetメール
通常、ウイルスチェックを
すり抜けて受信されます！！

攻撃が高度化し、被害相談も急増中です！
添付ファイルがパスワード付きのフォルダで送られてきた場合、**セキュリティ製品では中のファイルを検査できません。**安易に記載のパスワードで、開かないように！
取引先からのメールでも、必ず確認しましょう。

攻撃のパターン事例





お客様先で実際に検知した添付ファイル名

コンテンツ名
からの変更2020.09.doc
からの変更2020.09.doc
に修 2020_09.doc
からの変更09-04.doc
からの変更9月.doc
からの変更09_03.doc
請求書送付のお願い 13527089-20209月03.doc
トレンドマイクロ・カスタマー満足度アンケー.doc

このような添付ファイル名は開かず削除！

被害

端末やブラウザに保存されたパスワード等の認証情報が窃取される
窃取されたパスワードを悪用され、社内ネットワーク内に感染が広がる
メールアカウントとパスワードが窃取される→メールサーバに直接アクセスされ、大量送信にも使われる
メール本文とアドレス帳の情報が窃取され、その情報を悪用しEmotet の感染を広げるメールが送信される

対策

- **知っているメール送信者からでも不審な添付ファイル、URLリンクは開かない、相手先に確認する**
- **添付ファイルを開き、コンテンツの有効化を求める画面が出ても、有効化をせず、ファイルを閉じ削除**
- **社員全員で最新の情報、脅威、手口を知る、ネット利用には社内外問わず、常に脅威が存在すると考える！**

情報源

IPA https://www.ipa.go.jp/security/announce/20191202.html#L13
JPCERT/CC https://www.jpcert.or.jp/newsflash/2020090401.html
マルウエアEmotetへの対応FAQ https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html ←感染有無の確認方法も記載あり

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