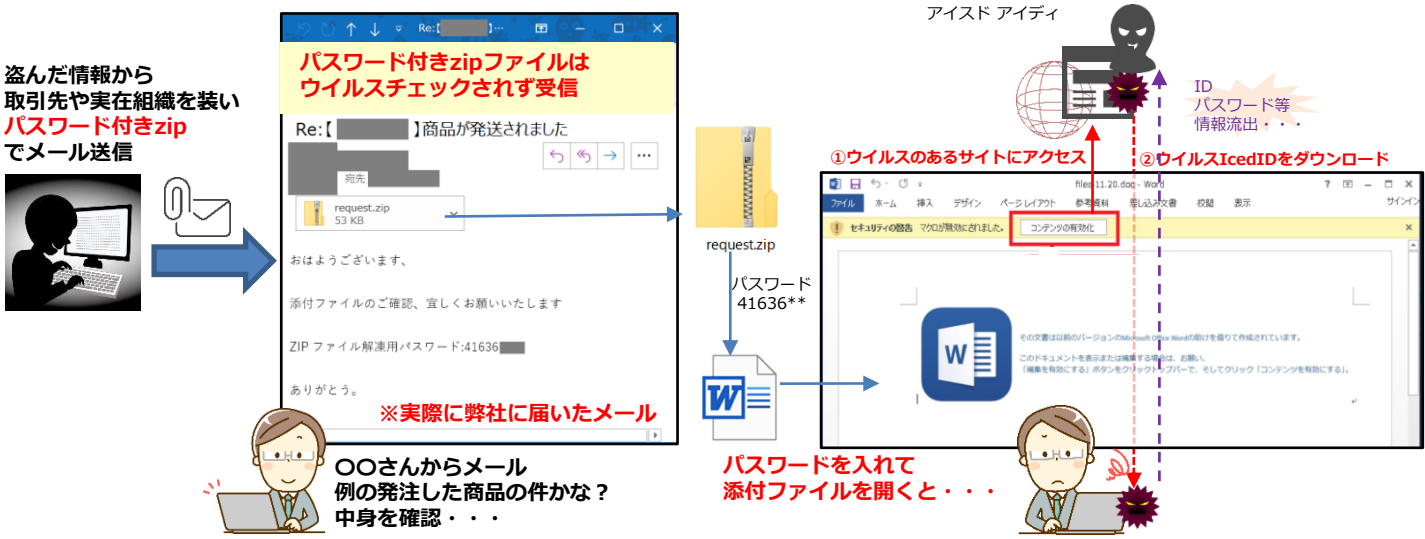
回　覧　印　印　印　印　印　印　印　印　印　印　印　印

ASAMA Security News Letter Vol.67

あさまセキュリティニュースレター

パスワード付き添付ファイルに再注意！　「EMOTET」に続き「IcedID」出現　（2020年12月9日）



攻撃のパターン

不正なプログラムを組み込んだWordファイルを、暗号化しメールで送信

→暗号化ファイルはウイルスチェックされず、相手に届く可能性が高い

取引先、過去にやり取した相手先、実在する企業を装っている、本文もWordファイル内の文も日本語

→メールを開かせる、添付ファイルを開く可能性を上げる

（Wordを開くと、コンテンツの有効化するような指示が書かれてますが、コンテンツの有効化は絶対にしないように！！）

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、その情報を悪用し感染を広げるメールが送信される
IcedIDが他のウイルスをダウンロードし、二次被害の恐れもあり！！

対策

- Wordのマクロの設定が、『警告を表示してすべてのマクロを無効にする』（デフォルト設定）になっているか確認
- 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！

以前のニュースレターで紹介している「EmoCheck」というツールでは、今回の「IcedID」の感染有無のチェックができません。感染が疑われる場合、ウイルス対策ソフトでウイルスチェックを実施ください

情報源

JPCERT/CC 分析センター(Analysis Center)の公式アカウント　https://twitter.com/jpcert_ac/status/1324561915738091522

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