回　覧　印　印　印　印　印　印　印　印　印　印　印　印

ASAMA Security Newsletter Vol.98

あさまセキュリティニュースレター

メールからの脅威を知りましょう！　（2023年7月13日）

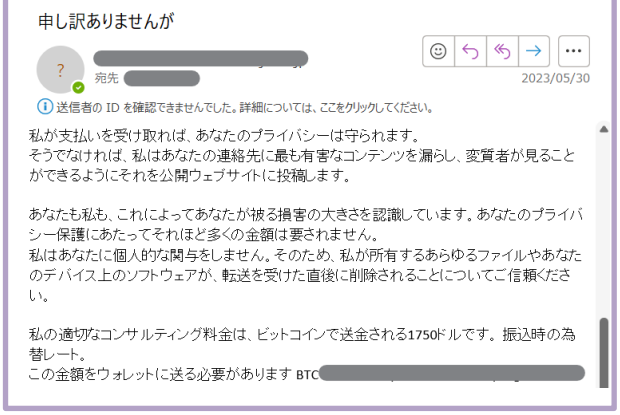
迷惑メール、不審な添付メールが毎日届く、メールの振り分けで時間を取っている方も多いのでは？
メールはビジネスに欠かせないツールですが、悪意のある者にとっても様々な攻撃が可能です
ウイルス感染被害を防ぐにも、最近の脅威をご紹介します

偽の警告や偽のログイン画面が開く
メールやMicrosoft365のパスワード
を盗む攻撃も増えてます

圧縮ファイル形式の攻撃も増えてます。検知を回避するパスワード付きZIPも増えたため、
脱PPAP対策が広まりました

↑zipの中には、invoice.exeという
不審な実行ファイル（おそらくランサムウェア）
が含まれてました

パソコンをウイルス感染させ中身を盗み見たと脅迫（セクストーション）、仮想通貨で支払要求



Office系の文書ファイルを開くと、不正なファイルをダウンロードし、マルウェア感染させる　昨今は**Emotet感染**を狙った攻撃が多い

上記は今年脅威として検知した添付ファイルや、実際に届いたメールです。
上記のようなメールや添付ファイルの他に、フィッシングメールも急増中！迷惑メール相談センター等でご確認を
https://www.dekyo.or.jp/soudan/index.html

メールによる攻撃パターン

ウイルスを添付して送る攻撃は検知されやすいため、
・暗号化ZIP（パスワード付きZIP）ファイルで送る→ファイルの中身が検査できない
・差出人を詐称、偽サイトのURLを送り、ログインさせ、ID・パスワードを盗む
・メールサーバに直接アクセスし、やり取りをのぞき見し、本人になりすまし相手に不正なメールを送る
・・・等様々な攻撃を仕掛けてきます

被害

マルウェアに感染させて情報漏洩、ファイルを暗号化して金銭要求するパターン（ランサムウェア）、偽サイトへ誘導しIDパスワードを盗むフィッシング、直接金銭を要求など、金銭要求のための攻撃です

メールサーバが乗っ取られるとやり取りしているメールなどが盗み見され、**悪用され取引先へ攻撃を行います**
メールのリンクから、メールのパスワードや、社内のデータが入っているクラウドサービスのパスワードを入力する際は要注意！

対策

・不審なメールは社内で共有・確認をしましょう
・自身が送信したメールへの返信メールであっても、不自然な点があれば相手に確認してから開きましょう
・メールに添付されたファイルで、マクロやセキュリティに関する警告が表示された場合、安易に開かない
・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対策の確認・更新を忘れずに

一度でも不審なメールが届いてしまうと、メールアドレス変更する以外に、攻撃者からのメールを来なくするのは困難です。受信トレイに届かない仕組み（迷惑メール対策・ウイルス対策）や、メール本文の不正なURLへのアクセスをブロックする、不正なサーバとの通信をブロックする仕組みなど、侵入から万が一を想定した対策が求められています

参考URL
迷惑メール相談センター　https://www.dekyo.or.jp/soudan/index.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