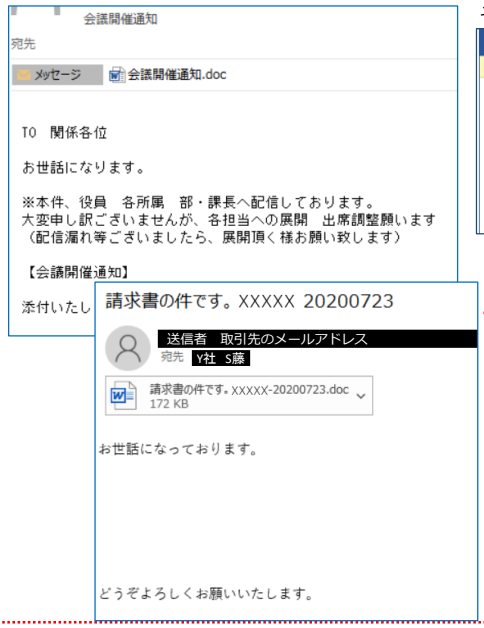
回覧 印 印 印 印 印 印 印 印 印 印 印 印

ASAMA Security News Letter Vol.63

あさまセキュリティニュースレター

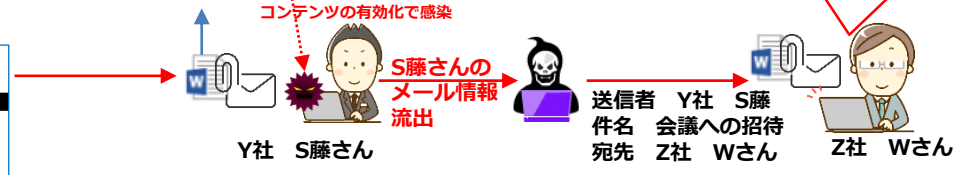
活動再開！取引先からの請求書・会議招待メールに要注意！！ （2020年08月12日）

取引先や実在する企業を装ったメール



添付ファイルの中身の一例

コンテンツの有効化で、ウイルスがダウンロードされ
Emotetと呼ばれる**ウイルスに感染**
メール本文、メールパスワード、アドレス情報等搾取、
その情報を元に同様の手口で攻撃



取引先 Y社 S藤さんからだ！

会議への招待.doc(0.17 MB)
Z社 Yさん
お世話になっております。
8月24日金曜日10:00の作業会議への招待。会議の質問をご覧ください。

添付を開き、コンテンツの有効化で感染→取引先へ拡散・・・

添付ファイルは主に**Word形式（.doc）**
件名・ファイル名は**請求書・会議招待といった内容**が多い！
送信者は、**実在する会社・取引先を装い、以前やり取りしたメールの返信・転送で送ってくる**こともあり
信用して開いてしまうケースがほとんどです！！

攻撃のパターン

- **取引先からのメールと思わせ、WordやExcelファイルを開かせる**
- **コンテンツの有効化をするように誘導し、裏でウイルスをダウンロード・感染させる**
- **メール、ネットバンキング、カード情報、WEBサービスのID・パスワードを窃取し、不正利用**
- **盗んだメールの内容・パスワード、アドレス情報を元に、他社へ感染を広げる**

被害

メール・パスワード・アドレス帳情報搾取、不正利用
ネットバンキング不正利用・ランサムウェア被害
社外に同様のメール配信

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は開かない、相手先に確認する**
- **添付ファイルを開き、Office製品の警告が表示されても、安易にコンテンツの有効化をしない**
- **社員全員で最新の情報を得る、最新の脅威を知る、手口を知る、セキュリティに対し常に意識をもつ**

情報源

IPA https://www.ipa.go.jp/security/announce/20191202.html **JPCERT/CC** https://www.jpcert.or.jp/newsflash/2019112701.html
マルウエア Emotet の感染に繋がるメールの配布活動の再開について（追加情報） https://www.jpcert.or.jp/newsflash/2020072001.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