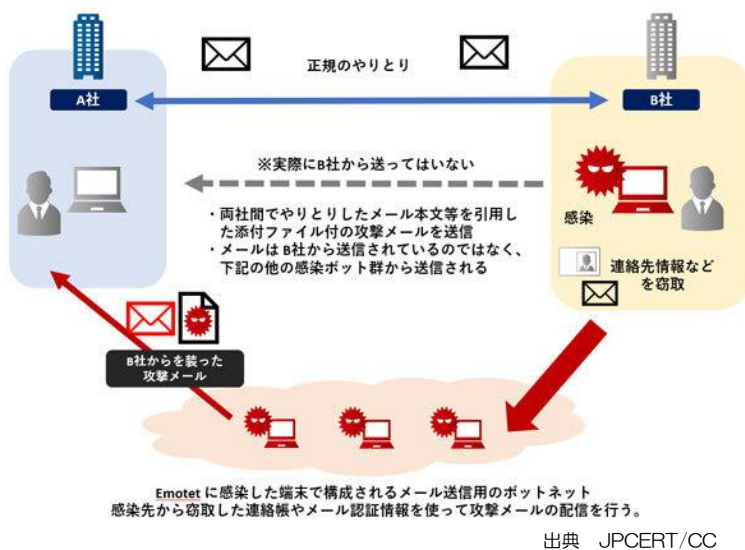


マルウェアEmotetの感染に注意!

実在の組織や人物になりすましたメールに添付された悪質なWord文書ファイルによる感染被害が増加しています。

影響

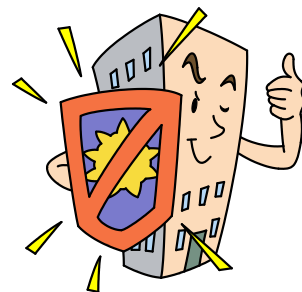
- 端末やブラウザに保存されたパスワード等の認証情報が窃取される
- 窃取されたパスワードを悪用されSMB※によりネットワーク内に感染が広がる
- メールアカウントとパスワードが窃取される
- メール本文とアドレス帳の情報が窃取される
- 窃取されたメールアカウントや本文などが悪用されEmotetの感染を広げるメールが送信される



※ Windowsを中心とした環境でLANを通じてファイル共有などに使用される通信プロトコルの総称

対策

- 組織内への注意喚起の実施
 - Wordマクロの自動実行の無効化 ※
 - メールの監査ログの有効化
 - 定期的なOSのアップデート
 - 定期的なオンラインバックアップの取得
 - メールセキュリティ製品の導入によるマルウェア付きメールの検知
- ※ Microsoft Office Wordのセキュリティセンターのマクロの設定で、「警告を表示してすべてのマクロを無効にする」を選択してください



万が一感染したら・・・まずは、

- 感染端末のネットワークからの隔離
- 感染端末が利用していたアカウントのパスワード変更

その後、セキュリティ専門ベンダと相談のうえ、

- 組織内の全端末のウイルス対策ソフトによるフルスキャン
- ネットワークトラフィックログの監視
- 調査後の感染端末の初期化

等を行ってください

詳細については、下記ウェブサイト(JPCERT/CC)からご確認ください。

<https://www.jpcert.or.jp/at/2019/at190044.html>