Emotetマルウェアが猛威をふるっています

～ SS5000対応状況について

オフィス営業本部中部支社

2019年11月27日 20:36 Yahooトップページニュースでも取り上げられた

「最強ウイルス、感染拡大　メアド盗んでなりすましメール」

ですが、Emotet(エモテット)と呼ばれるマルウェアが猛威をふるっています。

Emotetとは

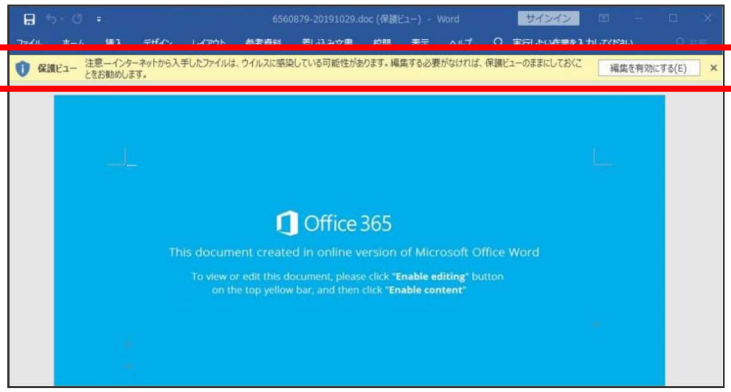
2014年６月に銀行情報を盗むマルウェアとして初めて確認されました。
今年(2019年)8月末より再び活動を開始し、亜種のEmotetや返信型・ばらまき型など攻撃者によって様々な型のものも増殖しています。

感染経路に関して

①メールの添付ファイルまたはリンク先URLをクリックしてファイルをダウンロードして、そのファイルを開く。
②ファイルを開くとパソコン内のパスワードやメールアドレス、さらにメール本文を盗み、
外部サーバ(C&Cサーバ)に送る。
③外部サーバから、盗み取った連絡先へEmotetに感染した添付ファイルを送信する。
①へ戻る。という具合に増殖を繰り返します。

実際の動きについて

例えばWindowsの場合、マルウェアによるマクロを実行しようとすると、初期状態で警告を発します。



このように警告が表示されます。

しかしながら、この警告を無視して開いてしまうと感染してしまいます。

SS5000の対応は？

見える化サイト

カスペルスキーでは既にEmotetには対応済みです。

しかしながら・・・裏へつづく

Emotetマルウェアが猛威をふるっています

～ 対応策について

オフィス営業本部中部支社

saxa

前頁にも記載されている通り、様々な亜種が確認されており、SS5000やαScan Ⅱであっても現時点では「Emotetについては100%対応済み」とは言い切れません。

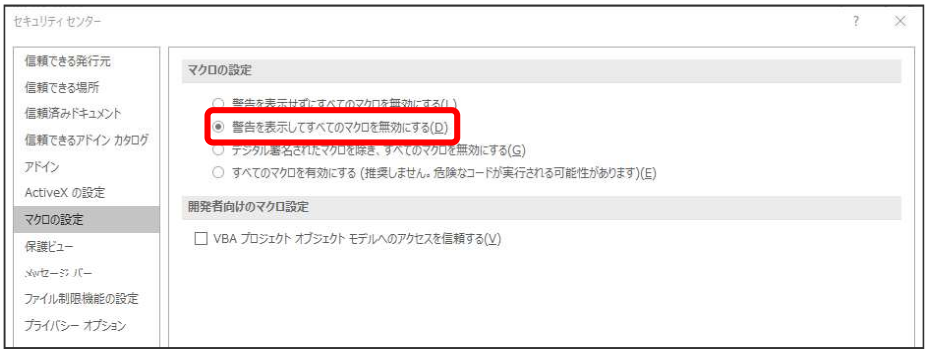
また、今後ランサムウェアなどと組み合わせた新たなウイルスの登場も懸念されます。

すり抜けた場合を想定しEmotet対策を実施して頂くようお願いします。

対策

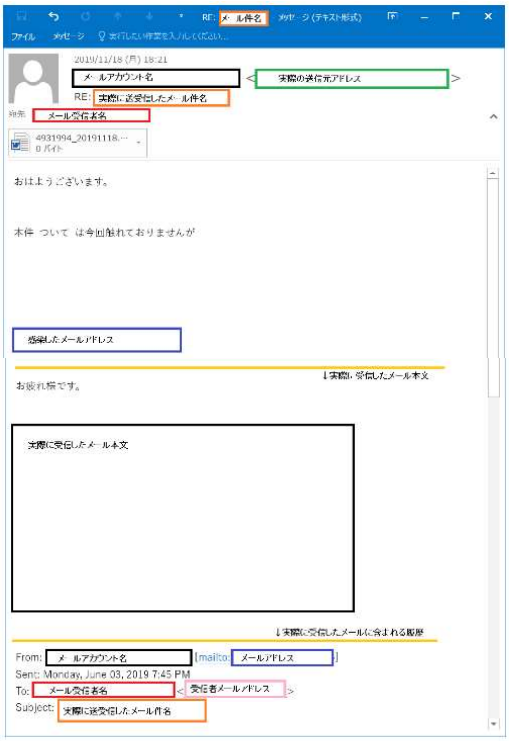
① SS5000やαScan Ⅱのシグネイチャーは最新に更新されるようにしてください。
(電源が入っていれば通常は自動的に更新されます)

② Microsoft Wordのマクロ自動実行の無効化
(初期では無効に設定されていると思われますが、念のため確認してください)



Wordのファイルメニュー → オプション → セキュリティセンター → セキュリティセンターの設定をクリック

③ 怪しいメールは開かない／添付ファイルは実行しない
右図参考→
・メール本文に記載のメールアドレスと送信元アドレスが異なる。
・身に覚えのないメール等・・・



④ OSのセキュリティパッチは最新に保つ

⑤ 大事なデータファイルはオフラインによるデータバックアップの実施