Pour contrer les menaces comme Locky, Microsoft bloque les macros d'Office 2016

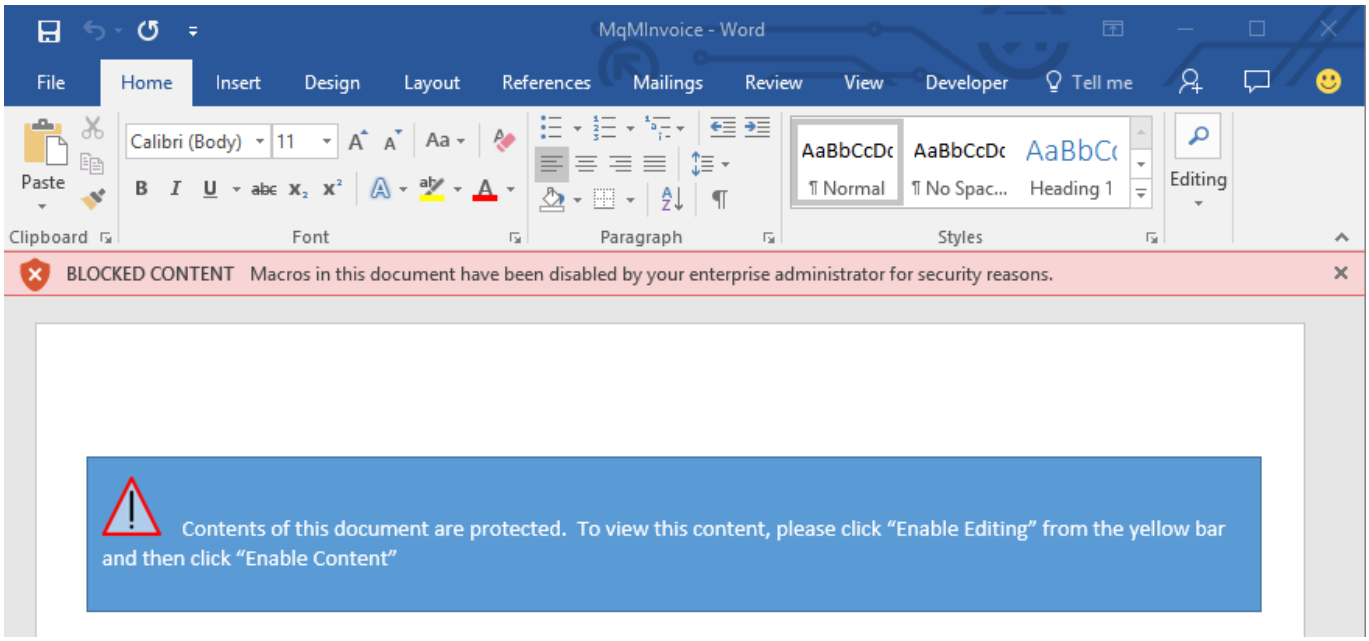
Microsoft dote Office 2016 d'une fonctionnalité permettant de neutraliser les menaces arrivant par les macros de sa suite bureautique. Par défaut, celles-ci sont désactivées dans Word, Excel et PowerPoint, mais les assaillants rivalisent d'ingéniosité pour pousser les utilisateurs à les activer, permettant ainsi l'installation de malwares via des macros malicieuses embarquées très souvent dans des documents arrivant en pièce jointe des e-mails. Une technique notamment employée par le malware bancaire Dridex ou le ransomware Locky.

Le problème ? Comme le relevait Microsoft lui-même dans un rapport de 2015, les utilisateurs ont tendance à passer outre les messages d'avertissement, surtout quand le contenu auquel ils s'apprêtent à avoir accès est alléchant. « *Cette fatigue est caractérisée par des utilisateurs qui se sentent bombardés d'avertissements ou de demandes de consentement* ». Une 'fatigue' que ne manquent pas d'exploiter les cybercriminels.

Utilisateur confiné au bac à sable

C'est pour dépasser un système manifestement à bout de souffle que Microsoft propose donc dans Office 2016 une fonctionnalité permettant aux administrateurs de bâtir des scénarios basés sur des règles qui bloquent les macros et **empêchent les utilisateurs de les réactiver** dans des situations à haut risque. En particulier quand le document renfermant la macro arrive d'Internet. Ces fonctionnalités sont **accessibles dans les politiques de groupe** de la suite bureautique, et permettent de prévenir toute réactivation des macros pour les documents téléchargés de services Cloud comme Microsoft One, Google Drive ou Dropbox, de sites de partage de fichiers ou issus de la messagerie (pour les mails externes à l'organisation et uniquement si cette dernière utilise le client Outlook et le serveur Exchange).

Si l'administrateur choisit d'activer ces options, un utilisateur ne pourra plus sortir du bac à sable (Protected View) pour exécuter la macro. Il verra s'afficher un bandeau rouge lui signalant que ce contenu a été bloqué pour des questions de sécurité (ci-dessous).



Selon Microsoft, 98 % des menaces ciblant Office passe par les macros. Dommage toutefois que l'option développée par le premier éditeur mondial soit réservée à la dernière version de sa suite, une très large majorité des entreprises employant des moutures plus anciennes.

Par ailleurs, l'observation d'une menace récente comme Locky montre que les assaillants ont **diversifié les vecteurs d'infection**. En plus des macros, ce ransomware se diffuse ainsi par des fichiers PDF renfermant un code Javascript malicieux ou encore via des sites infectés par les cybercriminels.

A lire aussi :

Le ransomware Locky mute pour multiplier ses victimes en France

Ransomware Locky : l'AFP touchée, son RSSI témoigne

Office 2016 incompatible avec les composants d'Office 2013

Crédit photo : igor.stevanovic / shutterstock