PROTECTION D'UN ORGANISME CONTRE LES MACROS MALVEILLANTES

SEPTEMBRE 2020 **ITSAP.00.200**

Les macros sont des séquences d'instructions écrites qui permettent de remplacer les commandes qu'un utilisateur communique normalement au moyen du clavier et de la souris et qui permettent également, par le fait même, de répéter automatiquement des tâches dans une application. Les macros sont utilisées dans de nombreux documents de la suite Office pour automatiser les processus et les flux de données. Elles sont intégrées dans le code des fichiers, ce qui permet aux utilisateurs de créer des raccourcis afin d'effectuer certaines tâches précises (par exemple, trier les feuilles de travail par ordre alphabétique, défusionner toutes les cellules fusionnées, masquer toutes les rangées et les colonnes). Lors de l'ouverture d'un fichier, une invite s'affiche parfois pour demander à l'utilisateur s'il souhaite activer ou désactiver les macros. L'utilisateur peut se servir d'un certificat signé sur les macros qu'il crée pour confirmer leur origine. Afin d'assurer une utilisation pratique et sûre des macros dans les applications, l'organisme peut aussi vérifier leur fiabilité.

Si les utilisateurs, les administrateurs et les fournisseurs de services peuvent écrire des macros, **il en va de même pour les auteurs de menaces**. Ces derniers peuvent créer des macros malveillantes et les intégrer dans des documents qui sont ensuite transmis via les réseaux organisationnels. Les macros malveillantes peuvent compromettre les applications et affecter les programmes informatiques dans les systèmes organisationnels. C'est dans ce contexte que s'inscrit le présent document : il décrit les risques liés à l'utilisation des macros et présente certaines mesures de protection des systèmes informatiques contre les intrusions malveillantes.

MENACES POTENTIELLES

Même si un fichier semble sûr, il est possible qu'un auteur de menaces ait intégré des macros malveillantes dans le script de l'application qui seront activées lors de l'ouverture du fichier. Un auteur de menaces peut aussi envoyer un courriel avec une pièce jointe contenant des macros malveillantes. Les systèmes et renseignements organisationnels sont possiblement exposés à certaines des menaces décrites ci-dessous lorsque sont utilisées des macros provenant de sources internes et externes.

VIRUS MACROS

Le virus macros est un code malveillant qui a l'apparence d'une macro légitime et qui est intégré dans une application. Un virus macro s'exécute automatiquement lors de l'ouverture du document et infecte ainsi les fichiers de l'utilisateur. Les fichiers infectés peuvent endommager le contenu des documents et se propager à d'autres logiciels et fichiers avec lesquels ils entrent en contact (par exemple, les fichiers sur disque, les fichiers de réseau, les pièces jointes aux courriers électroniques), et même infecter l'ensemble du système.

ACCÈS NON AUTORISÉ

Les auteurs de menaces utilisent des macros malveillantes pour contourner les contrôles de sécurité (p. ex., liste des applications approuvées) et obtenir l'accès aux systèmes et réseaux. Ces macros peuvent servir à exécuter du contenu malveillant et à dérober ou à détruire de l'information sensible. Souvent, les tentatives d'hameçonnage sont perpétrées au moyen de pièces jointes dans un courrier électronique et dont l'apparence semble légitime.

MENACES INTERNES

Toute personne ayant des connaissances sur l'infrastructure organisationnelle ou ayant accès à cette infrastructure peut causer des dommages, de façon volontaire ou non. Les menaces liées à l'utilisation de macros malveillantes peuvent également provenir de l'interne. Il suffit qu'une personne soit en mesure d'exécuter les tâches suivantes :

- Créer des macros (p. ex., copier le code à partir d'une source externe non vérifiée), y compris les macros contenant de l'information sensible (p. ex., les mots de passe).
- Propager les macros au sein de l'organisme (p. ex., en transmettant des documents à d'autres destinataires).
- Transmettre des documents provenant de l'externe (p. ex., des documents non vérifiés dans le cadre de procédures organisationnelles).
- Diffuser des documents contenant des macros malveillantes via des composants en nuage.

Pour de plus amples détails sur les menaces internes, prière de consulter sur **cyber.gc.ca** le document ITSAP.10.003, *Comment protéger votre organisation contre les menaces internes*.

SÉRIE SENSIBILISATION

MESURES DE SÉCURITÉ

Pour protéger les systèmes organisationnels contre les macros malveillantes, il est impératif de mettre en œuvre des mesures de sécurité comme celles qui sont énoncées ci-dessous :

- Désactiver les macros par défaut qui ne sont pas nécessaires.
- Appliquer le principe du privilège minimum au moment de l'attribution des privilèges administratifs et des accès aux comptes.
- Ne pas donner le droit aux utilisateurs de réactiver les macros désactivées.
- Utiliser des macros signées ou développées par l'organisme qui ont été vérifiées par les autorités techniques.
- Veiller à ce que les macros ne contiennent pas d'informations sensibles (p. ex., les justificatifs d'identité d'une personne).
- Vérifier les actions des utilisateurs qui développent des macros au sein de l'organisme (p. ex., les changements administratifs qu'ils apportent).
- Donner de la formation aux utilisateurs de l'organisme et leur fournir des renseignements sur la sécurité des macros afin de les sensibiliser.
- Effectuer fréquemment la mise à jour des applications et des systèmes et appliquer les correctifs requis.

SOLUTIONS DE REHARGE AUX MACROS

Dans le cas où est désactivée l'utilisation des macros, il existe d'autres moyens d'automatiser les tâches, notamment :

- l'utilisation d'applications commerciales de suites bureautiques (c'est-à-dire un produit commercial qui n'a pas été personnalisé);
- l'utilisation d'un logiciel en tant que service (SaaS, de l'anglais « software as a service ») pour automatiser le flux de données;
- le développement d'applications sur mesure pour appuyer les processus organisationnels.

MACROS FIABLES

L'utilisation de macros est souvent sûre et peut être permise au sein d'un organisme lorsque :

- la macro a été développée en interne (c'est-à-dire que l'organisme qui l'a créée et la détient peut, entre autres, en faire la maintenance en interne);
- des politiques permettent l'activation des macros signées et vérifiées (c'est-à-dire, les macros développées par l'organisme);
- les documents proviennent d'expéditeurs connus et ont été produits en interne (p. ex., aucun transfert de l'extérieur).

RAPPEL

Nous recommandons que vous désactiviez les macros qui proviennent de sources externes.

Bien qu'il soit possible d'utiliser des macros tout en protégeant les systèmes contre les macros malveillantes, certains risques demeurent. Les macros de l'externe exposent votre organisation à des répercussions inattendues.

Vous avez des questions ou vous avez besoin d'aide? Vous voulez en savoir plus sur les questions de cybersécurité? Consultez le site Web du Centre canadien pour la cybersécurité (Centre pour la cybersécurité) à **cyber.gc.ca**.