Protection d'un organisme contre les macros malveillantes

Janvier 2024

ITSAP.00.200

Les macros sont des séquences écrites qui permettent d'automatiser les processus, les flux de données et les tâches répétitives dans les applications, par exemple dans certains documents de la suite Microsoft Office. Ces séquences écrites, parfois appelées « code intégré », permettent aux utilisatrices et utilisateurs de créer des raccourcis pour des tâches précises, comme trier les feuilles de calcul par ordre alphabétique, annuler la fusion de cellules ou afficher toutes les rangées et les colonnes. Il est possible de se servir de certificats signés sur les macros afin de confirmer leur origine. Les organisations peuvent également vérifier la fiabilité des macros afin de les fournir aux utilisatrices et utilisateurs au besoin.

Si les utilisatrices ou utilisateurs, administratrices ou administrateurs et fournisseurs de services peuvent écrire des macros, **il en va de même pour les auteures et auteurs de menace**. Ces auteures et auteurs de menace peuvent créer des macros malveillantes et les intégrer dans des documents qui sont ensuite transmis via les réseaux organisationnels, comme par l'entremise d'une attaque par hameçonnage. Les macros malveillantes peuvent compromettre les applications et affecter les programmes informatiques dans les systèmes organisationnels. Lors de l'ouverture d'un fichier, une invite s'affiche parfois pour demander à la personne si elle souhaite activer ou désactiver les macros. Dans certaines versions récentes des applications Micrrosoft Office, les macros provenant d'Internet, comme celles contenues dans les pièces jointes de courriels, sont bloquées par défaut. Ce document décrit les risques liés à l'utilisation de macros et certaines des mesures à prendre pour protéger les systèmes organisationnels contre les intrusions malveillantes

Menaces possibles

Même si une application semble sécuritaire, des auteures et auteurs de menace peuvent avoir intégré des macros dans le script de l'application qui s'activeront lors de l'ouverture. Il se peut également qu'une ou un auteur de menace envoie un courriel avec des pièces jointes ou des fichiers contenant des macros malveillantes. Les systèmes et les renseignements organisationnels sont possiblement exposés aux 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. 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 auteures et 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 aux 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 utilisent des macros malveillantes contenues dans des pièces jointes qui semblent légitimes. Une ou un auteur de menace pourrait convaincre une utilisatrice ou un utilisateur d'activer les macros d'une pièce jointe, permettant au contenu malveillant de se propager dans les systèmes et les réseaux.

Menaces internes

Toute personne ayant des connaissances sur l'infrastructure organisationnelle ou ayant accès à l'infrastructure ou à l'information peut causer des dommages, de façon volontaire ou non. Pour qu'il y ait menace interne, il suffit qu'une personne soit en mesure d'exécuter les tâches suivantes :

- Créer des macros contenant de l'information sensible, comme des mots de passe ou du code copié à partir d'une source externe non vérifiée.
- Propager les macros au sein de l'organisme en transmettant des documents.
- Transmettre des documents externes non vérifiés dans le cadre de procédures organisationnelles.
- Diffuser des documents contenant des macros malveillantes via des composants du nuage.

SÉRIE SENSIBILISATION

No de cat. D97-1/00-200-2023F-PDF
ISBN 978-0-660-68428-4

Mesure 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.
- Ne pas donner le droit aux utilisatrices et utilisateurs de réactiver les macros désactivées.
- Appliquer le principe de droit d'accès minimal dans l'attribution de privilèges d'administrateur et d'accès aux comptes.
- 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, comme des justificatifs d'identité personnels.
- Vérifier les actions des personnes qui développent des macros au sein de l'organisme, comme les changements administratifs apportés).
- Donner de la formation aux utilisatrices et utilisateurs de l'organisme et leur fournir des renseignements sur la sécurité des macros et l'hameçonnage afin d'accroître la sensibilisation.
- Effectuer fréquemment la mise à jour des applications et des systèmes et appliquer les correctifs requis.
- Analysez régulièrement vos appareils au moyen d'un antivirus provenant d'un fournisseur reconnu.

Macros fiables

L'utilisation de macros est souvent sûre lorsque :

- l'organisation a développé la macro à l'interne et en est propriétaire, de même que si elle effectue la maintenance à l'interne;
- l'organisation a établi des politiques d'activation de macros signées et vérifiées seulement, comme les macros développées à l'interne;
- les documents proviennent de personnes connues, ont été produits à l'interne et n'ont pas été transmis de l'externe.

Solutions de rechange 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'application commerciales de suites bureautiques;
- 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'application sur mesure pour appuyer les processus organisationnels.

Rappel

Nous vous recommandons de désactiver 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.

Pour en savoir plus :

Ne mordez pas à l'hameçon : Reconnaître et prévenir les attaques par hameçonnage (ITSAP.00.101)

Listes d'applications autorisées (ITSAP.10.095)

Comment protéger votre organisation contre les menaces internes (ITSAP.10.003)

Gestion et contrôle des privilèges administratifs (ITSAP.10.094)

Vérification de la sécurité des réseaux (ITSAP.80.086)

Offrir aux employés une formation sur mesure en cybersécurité (ITSAP.10.093)

Application des mises à jour sur les dispositifs (ITSAP.10.096)