Devolutions

Logiciels espions : Ce que c'est, ce qu'ils font, et quoi faire pour les éviter

DES LOGICIELS MALVEILLANTS CONÇUS POUR S'INFILTRER SECRÈTEMENT

Dans les films de James Bond, les espions sont élégants et sophistiqués. Ils sont capables d'escalader des montagnes dangereuses, de nager avec des requins tueurs et même de vaincre leurs ennemis à l'aide d'un lance-flammes. Dans le monde de la cybercriminalité, toutefois, les espions ne font pas partie de la même catégorie que 007! En fait, parfois, ils ne sont même pas humains du tout. Ce sont des logiciels espions.

Qu'est-ce qu'un logiciel espion?

Les logiciels espions sont des logiciels malveillants conçus pour s'infiltrer secrètement dans l'ordinateur de la victime, recueillir des données et les transmettre à des tiers. Il fonctionne en permanence en arrière-plan et peut persister pendant des années. Si les pirates qui se cachent derrière les logiciels espions sont capables d'exploiter à peu près tout ce qui leur tombe sous la main (y compris des éléments que de nombreuses victimes considèrent comme inoffensifs, comme les informations relatives à l'utilisation d'Internet), ils sont particulièrement intéressés par les données confidentielles et privées, comme les informations relatives aux cartes de crédit et aux comptes bancaires, de même que les informations d'identification.

Comme les logiciels espions existent depuis longtemps (le terme a été introduit en 1995, ils n'attirent pas autant l'attention et ne suscitent pas autant d'inquiétude que d'autres cybermenaces comme les rançongiciels, l'hameçonnage ou les attaques de la chaîne d'approvisionnement. Pourtant, les logiciels espions constituent une menace sérieuse, omniprésente et imminente, et pas seulement pour les utilisateurs d'ordinateurs de bureau et d'ordinateurs portables : les utilisateurs mobiles sont également exposés.

En effet, les logiciels espions mobiles sont conçus pour se cacher en arrière-plan d'un appareil et voler des données comme des SMS, des journaux d'appels, des listes de contacts, des courriels, des photos, l'historique des navigateurs, etc. Certains types de logiciels espions mobiles peuvent même prendre secrètement des photos, suivre des emplacements et contrôler des appareils par le biais de commandes envoyées par des serveurs ou des SMS distants. En juillet 2021, un groupe de journaux et de médias, assisté par le Security Lab d'Amnesty International et le groupe de recherche Citizen Lab, a révélé que l'un des logiciels espions les plus sophistiqués et les plus envahissants au monde – appelé Pegasus – avait été utilisé pour pirater (et tenter de pirater) des dizaines de téléphones portables appartenant à des militants des droits de l'homme, des journalistes, des dissidents politiques et des dirigeants d'entreprise.

Comment les logiciels espions se propagent-ils?

Pour les **PC et les ordinateurs portables**, voici les quatre points d'accès les plus courants :

- Se faire passer pour un logiciel que les victimes croient utile, comme un gestionnaire de téléchargement, un nettoyeur de disque, un moteur de recherche Web, un accélérateur Internet, etc.
- Caché sous la forme d'un logiciel complémentaire, d'une extension ou d'un module d'extension dans un logiciel plus important.
- Les téléchargements passifs qui infectent les victimes cliquant sur des liens reçus par courriel ou par SMS ou, dans certains cas, qui visitent simplement un site Web malveillant ou regardent une bannière publicitaire malveillante (ce qu'on appelle aussi les « téléchargements furtifs »).

- Par le biais de portes dérobées, de vers et de chevaux de Troie.

Pour les **appareils mobiles**, les points d'accès aux logiciels espions les plus courants sont les suivants :

- Le wi-fi gratuit non sécurisé offert dans les cafés, les aéroports, etc.
- Les défauts du système d'exploitation, qui entraînent des vulnérabilités que les pirates peuvent exploiter.
- Les programmes malveillants qui se cachent dans des applications qui semblent sûres et légitimes.

Les types de logiciels espions

Il existe de nombreux types de logiciels espions et chacun a ses propres caractéristiques. Voici un aperçu :

Logiciel publicitaire : Surveille l'activité et vend des données à des annonceurs et à des acteurs malveillants, ou diffuse des publicités sournoises.

Infostealer : Récolte des informations et les scannent pour trouver des données spécifiques et des conversations par messagerie instantanée.

Enregistreur de frappes : Enregistre les frappes au clavier, puis sauvegarde les données comme les noms d'utilisateur, les mots de passe, les messages texte, les courriels et tout le reste dans un fichier journal chiffré.

Outils de dissimulation d'activité : Permet aux pirates de s'infiltrer dans les appareils en exploitant les failles de sécurité ou en se connectant aux machines en tant qu'administrateur. Ils sont très difficiles et dans certains cas impossibles à détecter.

Red Shell : Infiltre un appareil pendant que les victimes installent des jeux PC compromis, puis suit leur activité en ligne (généralement utilisé par les développeurs pour améliorer les jeux et les campagnes de marketing).

Témoin de pistage : Injecté sur un appareil par un site Web et utilisé pour suivre l'activité en ligne.

Cheval de Troie : Infiltre un appareil par le biais d'un cheval de Troie, qui diffuse finalement le logiciel espion.

Les symptômes liés aux logiciels espions

Si vous vous plaignez à votre médecin que vos jambes sont rouges, gonflées et qu'elles vous démangent incroyablement après une promenade dans une zone boisée, il vous dira probablement que vous présentez les

symptômes d'une éruption liée à l'herbe à puce (désolé de l'apprendre).

Il s'agit du même principe avec les logiciels espions. Il existe aussi des symptômes communs qui suggèrent que votre ordinateur ou votre appareil mobile a été infiltré. Voici ce à quoi vous devez faire attention :

- Votre ordinateur/appareil fonctionne plus lentement que d'habitude.
- Votre ordinateur/appareil se bloque ou tombe en panne fréquemment.
- Des fenêtres publicitaires apparaissent de manière répétée dans vos navigateurs.
- Vous voyez des messages d'erreur inhabituels.
- Vous constatez des changements inattendus dans le navigateur.
- De nouvelles icônes apparaissent soudainement dans votre barre des tâches.
- Le dossier des favoris de votre navigateur a été modifié.
- Vous ne pouvez pas modifier les paramètres de votre navigateur.
- Après avoir effectué une recherche à l'aide d'un navigateur, un autre navigateur la complète pour vous.

Si vous utilisez un appareil mobile, voici quelques symptômes supplémentaires :

- Vous utilisez beaucoup plus de données pour une raison inexplicable.
- Votre batterie se vide rapidement et vous ne savez pas pourquoi (rappelez-vous que les logiciels espions fonctionnent en arrière-plan sans interruption).
- Votre appareil surchauffe (encore une fois, parce que les logiciels espions utilisent une quantité importante de batteries/données).
- Vous entendez des sons étranges pendant les appels - il peut s'agir d'une application qui enregistre ce que vous dites et entendez.
- Vous découvrez des applications étranges que vous ne vous souvenez pas avoir téléchargées.
- Vous constatez des facturations surprenantes dans vos comptes App Store ou Google Play.
- Votre appareil montre des signes d'activité en mode veille (par exemple, l'appareil photo s'ouvre, des messages sont envoyés, etc.)
- L'arrêt de votre appareil prend un temps anormalement long.

Avant de voir comment se débarrasser d'un logiciel espion, il est important d'ajouter deux choses importantes : une bonne et une mauvaise.

La bonne nouvelle, c'est que les indications ci-dessus ne sont que des symptômes d'une infection potentielle par un logiciel espion. Ce ne sont pas des preuves irréfutables de l'existence d'un logiciel espion. Par exemple, un

ordinateur ou un téléphone peuvent commencer à devenir lents pour diverses raisons qui n'ont rien à voir avec un logiciel espion (par exemple, il est en fin de vie, il n'a pas assez de mémoire, etc.)

La mauvaise nouvelle, c'est que d'autres types de logiciels malveillants partagent bon nombre de ces symptômes. Ainsi, si vous n'avez pas de logiciel espion (ouf!), vous avez peut-être quelque chose d'encore plus insidieux et menaçant (oups!).

Comment se débarrasser d'un logiciel espion

Nous présentons ci-dessous quelques étapes de base pour se débarrasser d'un logiciel malveillant sur un ordinateur de bureau ou portable fonctionnant sous Windows, qui sont les types de machines les plus ciblés. Qu'en est-il si vous utilisez un Mac, un iPhone ou un téléphone Android ? Ne vous inquiétez pas : après ces étapes, nous partagerons également des liens qui fournissent des instructions pour supprimer les logiciels espions de votre machine ou appareil.

1. Déconnectez-vous d'Internet.
2. Utilisez l'option Ajout/Suppression de programmes pour essayer de désinstaller le ou les programmes indésirables ou douteux.
3. Redémarrez toujours après avoir désinstallé le(s) programme(s), même si vous n'êtes pas invité à le faire.
4. Effectuez une analyse complète du système avec un programme antivirus à jour. Idéalement, cela mettra en évidence tout autre programme suspect que vous pourrez nettoyer, mettre en quarantaine ou supprimer si nécessaire. Il existe de nombreux bons programmes antivirus, dont certains sont gratuits, comme Norton Power Eraser.
5. Si le logiciel espion (ou les symptômes du logiciel espion) persiste, accédez au disque dur de votre système en mode sans échec, afin que le logiciel espion ne se charge pas. Ensuite, accédez manuellement aux dossiers des logiciels espions et supprimez-les. Si vous n'êtes pas compétent dans ce domaine, demandez l'aide d'un expert.

Avec un peu de chance, cela éliminera tous les logiciels espions de votre vie. Mais comment empêcher les logiciels espions de revenir hanter votre machine ? Voici quelques conseils pratiques :

- N'ouvrez pas les courriels provenant d'expéditeurs inconnus.
- Ne téléchargez pas de documents provenant de sources non fiables.
- Ne cliquez pas sur les publicités pop-up.
- N'utilisez que des logiciels antivirus réputés et assurez-vous qu'ils sont à jour.
- Faites des recherches avant de télécharger/installer des programmes, surtout s'ils sont gratuits.

Instructions pour Mac/iOS/Android

Comme promis, si vous pensez que votre Mac, votre iPhone ou votre téléphone Android est infecté par un logiciel espion, cliquez sur les liens ci-dessous pour obtenir des instructions détaillées qui, nous l'espérons, résoudront le problème rapidement et définitivement :

- Pour Mac
- Pour iPhone
- Pour Android

Les logiciels espions ne font pas les gros titres ces jours-ci, contrairement aux rançongiciels, mais c'est certainement un type de menace qui doit être pris au sérieux. N'oubliez pas que 80 % des failles de sécurité commencent par des informations d'identification compromises et que les logiciels espions peuvent permettre aux pirates de dérober des données hautement confidentielles. En restant vigilant, en effectuant des analyses régulières et en faisant preuve de prudence lorsque vous naviguez sur le Web, vous pouvez garder une longueur d'avance sur les méchants !