OUCH ! Juin 2025

La lettre d'information mensuelle de sensibilisation à la sécurité pour vous

Se défendre contre les maliciels : l'ennemi invisible

Un email innocent aux conséquences dévastatrices

Sarah est une graphiste indépendante talentueuse dont la créativité et le gagne-pain dépendent de son fidèle ordinateur portable. Une après-midi, alors qu'elle était débordée par les échéances de ses projets, elle a reçu un email d'un client potentiel. L'objet de l'email était le suivant : "Opportunité pour un projet passionnant" Le nom de l'expéditeur lui semblait familier. Il s'agissait peut-être d'une recommandation d'un ancien client. Désireuse d'obtenir un nouveau projet, Sarah a ouvert l'email pour y trouver un message poli décrivant un projet potentiel et une pièce jointe intitulée "Descriptionprojet.pdf". Sans hésiter, elle a cliqué sur la pièce jointe, anticipant les détails d'une nouvelle mission.

Sans le savoir, ce simple clic a déclenché une série d'événements qui allaient bientôt bouleverser la vie professionnelle et personnelle de Sarah. La pièce jointe était un logiciel malveillant habilement déguisé, conçu pour s'infiltrer silencieusement dans son système. Les jours suivants, Sarah a remarqué des changements subtils : les performances de son ordinateur portable se sont dégradées et des applications se sont bloquées de manière inattendue. Elle a qualifié ces problèmes de problèmes techniques typiques, les attribuant à l'âge de son appareil et à son utilisation intensive.

Cependant, la situation s'est rapidement envenimée. Lorsque Sarah a tenté de se connecter à sa banque en ligne pour consulter ses comptes de chèques et d'épargne, elle s'est aperçue que son mot de passe ne fonctionnait plus. Paniquée, elle a contacté sa banque et a appris que des retraits importants avaient été effectués sur trois comptes à l'étranger. Ses économies, accumulées au prix d'années de dur labeur, s'étaient envolées. Sarah s'est rapidement rendu compte qu'elle avait été victime d'une attaque de maliciels qui avaient infecté son ordinateur portable, compromis sa sécurité financière et potentiellement mis en péril sa réputation professionnelle.

Qu'est-ce qu'un maliciel ?

Les maliciels sont des programmes informatiques créés par des cybercriminels pour infiltrer, endommager ou contrôler des systèmes informatiques ou des appareils mobiles sans votre consentement ou votre connaissance. Ce terme est une combinaison des mots "*malveillant*" et "*logiciel*" Vous avez probablement entendu parler des virus, des vers, des chevaux de Troie, des rançongiciels et des logiciels espions. Il s'agit de tous les types de maliciels.

Ce qui rend les maliciels si dangereux, c'est qu'une fois que votre ordinateur ou votre appareil est infecté, le cybercriminel peut en prendre le contrôle total sans que vous le sachiez. Il peut enregistrer silencieusement vos activités, y compris les personnes avec lesquelles vous communiquez, ce que vous dites, ainsi que vos identifiants et mots de passe pour vos comptes les plus importants.

Les maliciels peuvent également récupérer silencieusement tous vos fichiers, y compris les photos, les vidéos ou les documents sensibles. Ils peuvent infecter presque tous les systèmes, les smartphones, les montres intelligentes ou même les appareils intelligents de votre maison comme votre thermostat et vos serrures de porte. Oui, même les iPhones et les ordinateurs Mac d'Apple peuvent être infectés s'ils ne sont pas correctement sécurisés.

Renforcez vos défenses : les stratégies de protection

Heureusement, il existe plusieurs mesures simples que vous pouvez prendre dès maintenant pour empêcher l'infection.

1. **Mettez à jour vos systèmes** : Mettez régulièrement à jour votre système d'exploitation, vos applications et vos applications mobiles pour vous assurer que les vulnérabilités connues sont corrigées et que vous disposez des dernières fonctions de sécurité. Le moyen le plus simple est d'activer la mise à jour automatique.
2. **Soyez prudent avec les emails et les messages** : L'un des moyens les plus courants utilisés par les cybercriminels pour infecter vos appareils consiste à vous inciter à ouvrir une pièce jointe infectée, à télécharger un logiciel infecté ou à cliquer sur un lien malveillant. Méfiez-vous des messages qui vous poussent à agir immédiatement ou qui sont trop beaux pour être vrais.
3. **Utilisez un mot de passe unique et fort** : Les mots de passe sont les clés de votre royaume. Si un cybercriminel compromet l'un d'entre eux, il peut être en mesure de prendre le contrôle de l'appareil ou du compte et de l'infecter. Protégez tous vos appareils à l'aide d'un mot de passe unique et fort ou d'une phrase de passe. La longueur du mot de passe est cruciale. Dans la mesure du possible, activez l'authentification multifactorielle (MFA).
4. **Téléchargez depuis des sources de confiance** : Ne téléchargez des logiciels, des médias ou des applications qu'à partir de sites web officiels ou réputés. Les cyberattaquants infectent souvent les appareils mobiles en vous incitant à télécharger des applications mobiles non autorisées conçues pour prendre le contrôle de votre appareil.
5. **Logiciel antivirus** : Dans la mesure du possible, installez une solution antivirus fiable et configurez-la pour qu'elle se mette à jour automatiquement. Tous les systèmes ou appareils ne peuvent pas exécuter d'antivirus, et l'antivirus ne peut pas attraper tous les maliciels, mais il peut aider.

Rédacteur invité

Sherry Peng est actuellement responsable de la protection de la vie privée chez Agora. Elle a commencé sa carrière dans l'administration locale et est passée au secteur privé après avoir obtenu une maîtrise en assurance de l'information et en cybersécurité. Sherry travaille dans le domaine de la sécurité depuis près de dix ans et est l'actuelle présidente de WiCyS Colorado.

Ressources

Le pouvoir de la phrase de passe : https://www.sans.org/newsletters/ouch/power-passphrase/
La puissance des gestionnaires de mots de passe : https://www.sans.org/newsletters/ouch/power-password-managers/
Le pouvoir de la mise à jour : https://www.sans.org/newsletters/ouch/power-updating/
Les dangers du téléchargement : comment déjouer les applications mobiles malveillantes : https://www.sans.org/newsletters/ouch/download-danger-how-to-outwit-malicious-mobile-apps/

Traduit pour la communauté par : Juliette Busson