RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

En partenariat avec
POLICE NATIONALE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE
Liberté Égalité Fraternité

PIRATAGE DE COMPTES ETUDIANTS ET D'ACCÈS À DES PLATEFORMES PÉDAGOGIQUES

Mise en garde face aux virus dérobeurs («*stealers*»)

Les universités et établissements d'enseignement supérieur constatent depuis fin 2022 de nombreuses intrusions sur des accès distants. Les enquêtes ont montré que les faits sont liés à des **usurpations de comptes d'étudiants, dont les identifiants ont été volés.**
Lors des investigations, des **logiciels malveillants dérobeurs de mots de passe («stealers»)** ont été retrouvés sur des ordinateurs personnels d'étudiants.

QU'EST-CE QU'UN *STEALER* ?

Les virus informatiques de type « *stealer* » sont spécialisés dans le vol d'identifiants (mots de passe d'applications, de VPN, ...), de portefeuilles de cryptomonnaies, de cookies de session et autres données stockées notamment dans les navigateurs Internet. Une fois exfiltrées, ces données sont utilisées par les cybercriminels à des fins frauduleuses ou malveillantes.

EXEMPLE DE MÉTHODES D'INFECTION

À titre d'illustration, les investigations ont montré que des *stealers* ont été introduits intentionnellement dans des logiciels contrefaits (versions non validées par les éditeurs légitimes). La version du logiciel disposant du virus est ensuite diffusée via des liens sur différentes plates-formes grand public comme les réseaux sociaux ou les messageries instantanées. Certains liens sont parfois même proposés dans les premiers résultats des moteurs de recherche. Les utilisateurs sont invités à installer des extensions promettant d'améliorer les performances d'un jeux vidéo ou de l'ordinateur, ou parfois de bénéficier gratuitement de logiciels habituellement payant. Dans certains cas, le site web ou le programme d'installation demande la désactivation de l'antivirus avant le téléchargement et l'installation du programme infecté, ce qui a permet au *stealer* de ne pas être détecté.

LE RISQUE DES MOTS DE PASSE STOCKÉS DANS LES NAVIGATEURS

Il est très simple d'enregistrer dans son navigateur Internet ses mots de passe, ses adresses de messagerie, ses coordonnées de cartes bancaires, etc.
Ils présentent cependant des risques importants face aux *stealers* qui cherchent à dérober ces informations.

De manière générale, les cybercriminels exploitent l'intérêt des internautes à obtenir des fichiers vidéo (films, séries), des logiciels piratés (« crackés ») ou encore des programmes permettant d'améliorer les performances dans les jeux vidéo, de l'ordinateur, etc.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

En partenariat avec
POLICE NATIONALE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE

LES BONNES PRATIQUES
POUR SE PROTÉGER DES *STEALERS*

1. Ne **pas télécharger**, ni utiliser de logiciels, d'applications et de vidéos piratés ou **d'origine douteuse** qui peuvent souvent contenir un virus.

2. Ne **jamais désactiver votre antivirus** à la demande d'un logiciel.

3. Face à un **message suspect** (inattendu, alarmiste, aguicheur...), **ne pas ouvrir les pièces jointes** ou cliquer sur les liens.

4. **Mettre régulièrement à jour** vos appareils, logiciels et applications.

5. **Utiliser des mots de passe forts** qui ne disent rien sur vous et différents pour chaque accès afin d'éviter des piratages en cascade.

6. Deux sécurités valent mieux qu'une : **activer la double authentification** lorsque cela vous est proposé.

7. **Ne pas stocker vos mots de passe de manière non sécurisée** : post-it, fichiers textes, messages brouillons, notes sur votre smartphone...

8. Utiliser un **gestionnaire de mots de passe** ou un trousseau d'accès sécurisés, stockés de préférence en local, pour conserver vos mots de passe en sécurité. Vous n'aurez ainsi à retenir qu'un mot de passe pour accéder à l'ensemble de vos comptes.

9. Ne **jamais sauvegarder vos mots de passe dans le navigateur** d'un ordinateur partagé.

10. **Se déconnecter systématiquement de votre compte** après utilisation, pour éviter que quelqu'un puisse y accéder après vous.

RETROUVEZ TOUTES NOS PUBLICATIONS SUR :
www.cybermalveillance.gouv.fr

Version 1.0