RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

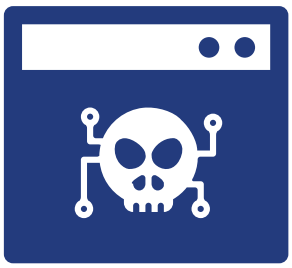
CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

PIRATAGE DE COMPTES ENT / PRONOTE
Mise en garde face aux virus *stealers*

En partenariat avec
POLICE NATIONALE
le ministère de l'Éducation nationale et de la Jeunesse
et le ministère de la Justice

Les établissements scolaires ont connu une vague importante de fausses alertes à la bombe, diffusées via les Espaces Numériques de Travail (ENT) ou des applications de suivis scolaires telles que Pronote. Si ces faits ont faibli depuis l'interpellation de plusieurs individus, **des comptes d'élèves, dont les identifiants ont été volés, sont encore utilisés pour poster des messages sur ces applications à leur insu**.

Lors des investigations, plusieurs logiciels malveillants de type *stealer* ont été retrouvés sur des ordinateurs personnels d'élèves.



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

Les virus informatiques de type *stealer* sont spécialisés dans le vol d'identifiants (mots de passe…), 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.

MÉTHODES D'INFECTION

Les *stealers* sont des logiciels malveillants souvent disponibles à la vente ou gratuitement. Leurs détenteurs peuvent ensuite diffuser le virus, notamment par des messages d'hameçonnage (*phishing*). Dans le cadre du dossier des fausses alertes à la bombe, le virus a été diffusé *via* des liens postés sur différentes plates-formes, telles que Youtube ou Discord. Les utilisateurs ont été invités à installer des extensions pour des jeux vidéo, des logiciels de triche, etc. La promesse étant d'améliorer leurs performances en jeu. Parfois, les messages indiquent de désactiver l'antivirus avant de télécharger et d'installer le programme, ce qui permet au *stealer* d'éviter une détection par l'antivirus. Des jeux très prisés des adolescents et jeunes adultes sont ciblés, permettant une diffusion large dans cette catégorie de public.

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, etc.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

En partenariat avec
POLICE NATIONALE
le ministère de l'Éducation nationale et de la Jeunesse
et le ministère de la Justice

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