

FICHE CYBER

Fuites de données (*data leaks*) et cybercriminalité

Statut : **En cours**

Secteurs affectés : **Tous**

Zones géographiques touchées : **Monde**

Objectif : **Lucratif, Hacktivisme, Challenge, Espionnage**

Met en vente ou divulgue
les informations sur Internet

Exploite les données afin de mener
d'autres actions malveillantes



Attquant A

Données fuitées

Attquant B

SYNTHÈSE

L'exploitation des fuites de données (ou *data leak* en anglais) par des cybercriminels consiste à pirater ou récupérer, puis diffuser ou vendre des bases de données massives sur Internet. Ces informations sont généralement utilisées comme premier point d'accès pour de nouvelles actions malveillantes (escroqueries, cyberattaques, usurpation d'identité, etc.). Ce phénomène, particulièrement lucratif pour les malfaiteurs, génère un préjudice de plusieurs millions d'euros chaque année en France.

EN QUOI CONSISTE CE PHÉNOMÈNE CYBERCRIMINEL ?

Une fuite de données peut se produire de manière intentionnelle ou non, avec ou sans intention malveillante. Elle peut contenir toute sorte d'informations confidentielles (**commerciales, médicales, identifiants de connexions, etc.**). Ces données sont ensuite téléchargées et exploitées par des acteurs malveillants, qui **les vendent ou les diffusent principalement** sur des forums ou des messageries dédiés à la cybercriminalité.



Les motivations des acteurs malveillants sont variées : **gains financiers, revendications idéologiques, challenge personnel, espionnage ou encore vengeance**. Plusieurs groupes cybercriminels ou individus se sont spécialisés dans la vente de ce type de données. Cependant, certaines fuites ne sont pas systématiquement dues à des acteurs malveillants : **l'erreur humaine** peut aussi en être à l'origine (négligence, mauvaise configuration, etc.).



Les usages criminels de ces fuites peuvent être multiples : **escroqueries, atteintes aux personnes, atteintes aux systèmes d'information, intelligence économique, atteinte à la réputation d'une entreprise, etc.** Autant de préjudices qui peuvent devenir **l'élément déclencheur d'autres attaques « opportunistes » par rebond** et qui peuvent toucher directement les particuliers, les entreprises ou les administrations.

En France, de 2019 à 2023, 18 898 violations de données ont été recensées (CNIL).

PRÉJUDICES

Financiers



Atteinte à l'image



Données personnelles



Espionnage

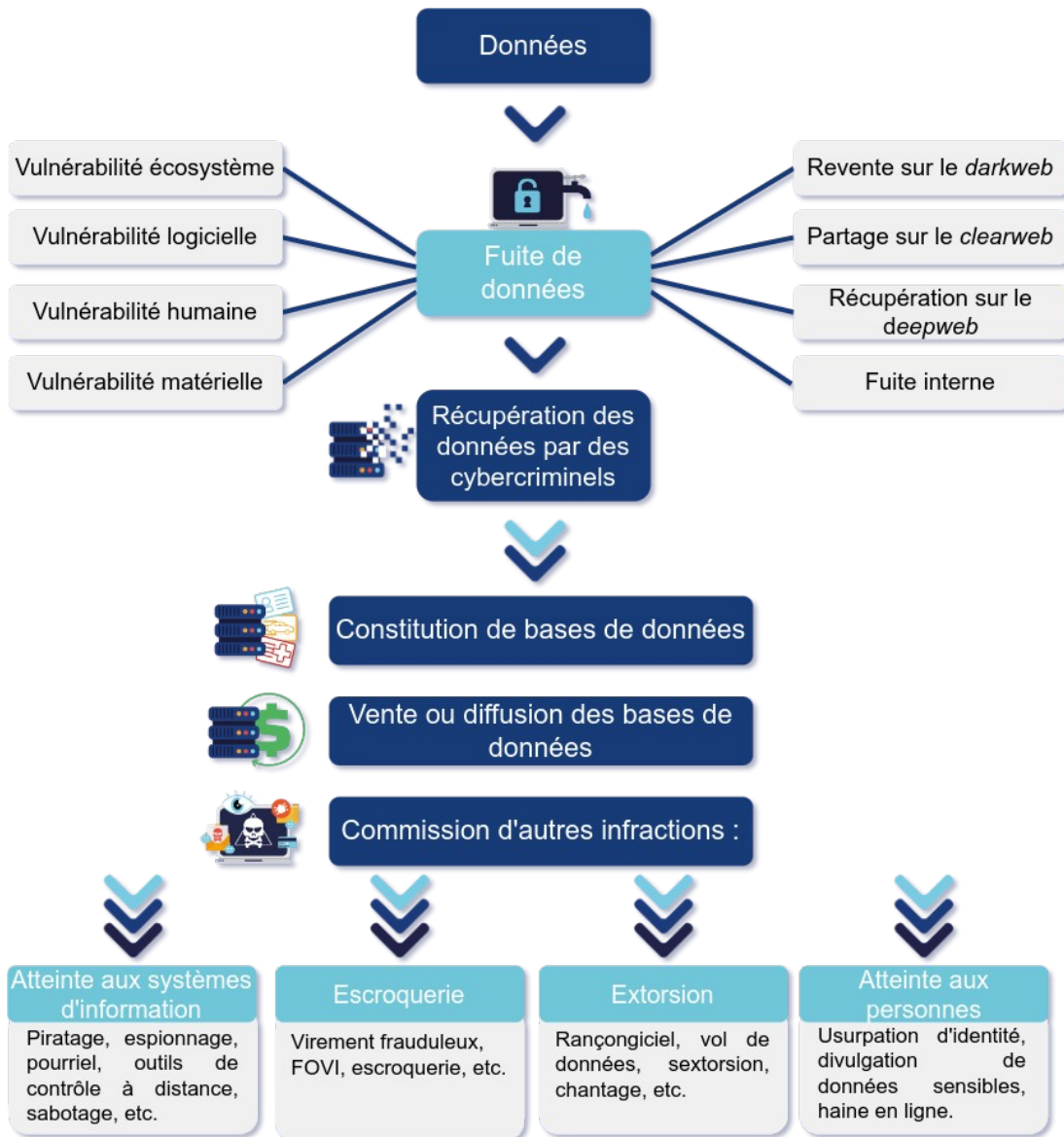


QUE DIT LA LOI ?

- ✓ Accès frauduleux et extraction de données d'un système informatique (STAD) : art. 323-1 et 323-3 du Code pénal
- ✓ Participation à une association de malfaiteurs : art. 450-1 à 450-5 du Code pénal
- ✓ Service de cyberdélinquance ou complicité : art. 323-3-2 et art. 121-7 du Code pénal
- ✓ Atteintes résultant des fichiers ou des traitements informatiques : art. 226-16 à 226-24 du Code pénal
- ✓ Vente illicite de données personnelles (recel) : art. 321-1 du Code pénal
Les peines encourues peuvent être portées jusqu'à dix ans d'emprisonnement et un million d'euros d'amende.
- ✓ Par ailleurs, le règlement européen n°2016/679 « RGPD » impose aux entreprises responsables d'un traitement de données personnelles de notifier à la CNIL toute violation de données, sous peine d'une sanction administrative.

MODÉLISATION DE L'ÉCOSYSTÈME CRIMINEL CONCERNANT LES FUITES DE DONNÉES

Certains cybercriminels sont spécialisés dans le piratage, la récupération, la consolidation et la revente de bases de données. D'autres se contentent d'exploiter ces bases pour commettre d'autres méfaits qui recoupent un champ important de la cybercriminalité.



COMMENT S'EN PRÉMUNIR ?

- ✔ Limitez le partage de vos informations au minimum et uniquement sur des sites de confiance. Réduire votre empreinte numérique permet de réduire le risque de voir vos données fuir.
- ✔ Tenez-vous à jour sur l'actualité et les fuites de données depuis nos réseaux sociaux. Anticiper et réagir au plus tôt est essentiel afin de réduire l'impact en cas de fuite avérée.
- ✔ Soyez prudent lorsque vous recevez des courriels venant d'un expéditeur inconnu. Si vos informations ont fuité, il est probable que vous soyez une cible pour les attaquants opportunistes.
- ❗ Ne réutilisez pas le même mot de passe afin de ne pas donner accès à vos comptes aux acteurs malveillants. Il suffit qu'un seul mot de passe fuite pour que chacune de vos informations fuite également.

SOURCES

<https://cnil.fr/fr/fuite-ou-vol-de-donnees-comment-savoir-si-cela-vous-concerne-et-que-pouvez-vous-faire>
<https://cnil.fr/fr/violations-de-donnees-personnelles-bilan-de-5-annees-de-rgpd>
<https://www.portail-ie.fr/univers/droit-et-intelligence-juridique/2023/la-reutilisation-dune-fuite-de-donnees-un-risque-juridique/>