USBDumper

rstack.org

valgasu@rstack.org

+ La clé USB est un support privilégié pour l'échange de données
+ Les données en question sont parfois sensibles
+ Le propriétaire fait confiance aux données sur sa clé
+ Problème bien connu des clés USB malicieuses (autorun)
+ A l'inverse l'utilisateur est moins vigilant quand il connecte sa clé sur un autre ordinateur

⇨ **USBDumper**

Comment ça marche ?

+ Détection de l’évènement de connexion
+ Récupérer la lettre assignée au disque
+ Agir sur les fichiers

Suggestions

+ Copier tout ou partie des données de la clé
+ Copier un programme malveillant sur la clé
+ Copier du contenu illégal sur la clé
+ Infecter un exécutable
+ Ajouter une macro aux documents Office

⇨ **Chiffrer ses données**