Lancer XBox Media Player (ou autre) sur une XBox non modifiée (sans puce)

Soumis par leo
03-07-2003

Oui, il est possible de lancer XBMP sur sa XBox (ou toute autre application) sans puce. Mais ne vous réjouissez pas trop vite, la maniputation a effectuer est assez ardue...
En voici un cours résumé, d'après ce que j'ai lu et (peut être) compris:

La technique se base en fait sur une faille découverte dans le jeux 007 Agent. Cette faille correspond à un buffer overflow (en gros c'est allouer à une variable une valeur non prévue initialement et qui permet l'execution de code). Ce buffer overflow est réalisable via les fichiers de sauvegarde des parties du jeux en question. Il faudra donc vous procurer une sauvegarde hackée que vous tranférerez sur une carte mémoire XBox via votre PC.
Il faut ensuite charger cette sauvegarde dans le jeux pour lancer l'exploit. Il ne reste ensuite plus qu'à enlever le DVD de votre jeux pour y mettre un CDRW contenant XBMP par exemple...

Attention: Je tiens à signaler que je n'ai pas testé cette manipulation. Je poste cette news dans un but informatif, pour montrer qu'il est maintenant possible de booter des applications non-signées sans puces. A vous de faire vos recherches si vous voulez expérimenter la méthode. Je compte également tester la manip, mais je manque de temps pour l'instant.
Notez enfin que des modifications du programme XBMP et de la sauvegarde hackée semblent être necessaire pour réaliser le buffer overflow d'une manière correcte...

Allez faire un tour sur XBox Hacker si vous souhaitez vous procurer ces sauvegardes hackées ainsi que d'autres informations sur cette méthode.