Le hack de la PS3 par la Team NDT

Soumis par robocop
25-09-2008

Du nouveau sur le hack de cette satanée PS3 qui résiste si bien aux hackers. StreetSkaterFU a réussi à duper partiellement la mémoire de la PS3 sur une machine du commerce! L'air de rien ce qui permettra de pouvoir lire des clefs privées, des certificats...etc...et le hack vient de faire un grand pas. Ceci est à rapprocher des avancées de la Team NDT qui ont réussi a recréer le CRC de la mémoire flash de la PS3 et même à réparer une PS3 brickée par un mauvais flashage. En termes non techniques, le bios de la PS3 est protégé de la modification par une fonction mathématique (contrôle de redondance cyclique ou CRC (Cyclic Redundancy Check)) qui évite toute modification. C'est cet algorithme qui a été craqué par la Team NDT. On peut donc désormais faire un dump de la ram, le modifier et regénérer un CRC pour ensuite la flasher dans la PS3. Il y aura pour cela un programme nommé FlowRebuilder qui sera releasé bientôt mais nul doute qu'un bios hacké va voir le jour d'ici peu!

Dernière précision, à ce jour seule la puce INFECTUS 2 permet de flasher le bios mais la porte est ouverte aux autres fabricants et puis à 43 euros la puce...