Firmware DVD de la XBOX 360 hacké

Soumis par redrum
19-03-2006

Et oui, ils l'ont fait!
The Specialist, ainsi que son équipe ont réussi à lancer une copie d'un jeu grâce à un firmware modifié pour le DVD-ROM Hitachi-LG GDR-3120L. La sécurité du Toshiba/Samsung TS-H943 semble similaire, mais celà nécessitera un autre firmware bien entendu

"Months of hard work have come to an end. The 360 FW security details were posted a few days ago already, so why not make it official :-) It's been done.

Respect to all the people on this board who made it possible with their brilliant contributions:
Anita999, Geremia, Nayr, Bluecop, Interestedhacker, MacDennis, Phantasm, Marvin, Tiros, SpenzerX, Team Modfreakz, Fuzzylogic, Takires, loser, jasper, SMO, Groepaz, Zobyone, Jumba, Amadeus, Tser, DjHuevo, oz_paulb, DaveX, darkfly, evestu, Robinsod, Dark_Neo, Gael360, Seventhson, probutus."

Une vidéo est alors sortie pour confirmer, d'ailleurs TheSpecialist vient de distribuer la vidéo originale (100Mo) disponible sur rapidshare. La qualité est bien meilleure
TheSpecialist a confirmé qu'il ne sortirait pas le firmware pour le grand public, mais il encourage les intéressés à reproduire ce hack grâce à toutes les discussions effectuées sur le forum de xboxhacker depuis des mois sur le sujet. Nul doute que ce hack sera "leaké" ou bien refait par une autre équipe...

Beaucoup de questions se posent désormais: homebrew, linux, live360...Qu'est-il possible de faire?

Les executables xbox360 sont signés par Microsoft, ce qui veut dire qu'il est impossible de modifier quoique ce soit sur le fichier .xex ou le fichier ne sera pas lancé.
Maintenant, pour empêcher le fait de lancer une copie du jeu sur un disque gravé, Microsoft attribue à chaque fichier .xex un "mediaflag".
Ce mediaflag dit à la xbox sur quel media le .xex est autorisé à se lancer (on se rappelle l'épisode du kiosk disk).
Changer ce mediaflag n'est pas une option car celà casserait la signature du fichier xex. Ce qui est fait dans ce firmware "casse" la détection du disque et le reporte comme étant un DVDXBOX360 (les disque xbox360 originaux ont des mauvais secteurs spécifiques ainsi que des infos spéciales dans le lead-in/lead-out qui ne sont pas reproductibles par un graveur standard).

Celà veut donc dire que ce hack n'est pour l'instant utile qu'à l'utilisation de copies, lancer linux ou tout autre programme homebrew reste impossible!
Pour le live, seules des suppositions existent, mais puisque la xbox fonctionne dans son état "normal", on peut supposer que celà marcherait (néanmoins une maj de Microsoft pourrait surement bloquer celà, mais vu le fait que le firmware est désormais dans le mains des hackeurs, une "réponse" serait très probable).
La réponse de Microsoft sera peut-être au niveau matériel, l'avenir nous le dira...

Pour finir, dans l'éventualité d'une sortie pour ce hack, l'utilisateur "lambda" serait bien incapable de flasher son firmware, bien sur des programmes pour flasher son lecteur DVD xbox360 pouraient être écrits mais rien n'est encore sorti. (du moins pas pour le grand public).

sources - XboxHacker.net - xbox-scene