Hack du Firmware DVD XBOX360 - Suite

Soumis par redrum
20-03-2006

Quelques infos supplémentaires suite à la news précédente sur le hack du firmware du lecteur DVD Hitachi-LG GDR-3120L.
SeventhSon sur les forums de xboxhacker.net a travaillé sur le fonctionnement du lecteur sous Linux/Windows ces dernières semaines.

Sur le site de SeventhSon est expliqué comment connecter et le faire reconnaître sous les 2 OS. Il a même programmé des utilitaires en ligne de commande (dispo sur Linux/Ws) qui vous permettent de récupérer la mémoire (incluant "l'espace interdit"), le firmware et la clé unique du lecteur DVD sur le PC, ainsi que d'autres outils pour écrire sur la mémoire (pas le firmware) et exécuter du code arbitraire MN103 (ce lecteur utilise un chipset DVD MN103) depuis le PC sur le lecteur.

Maintenant pour flasher le firmware il faudra tout de même ouvrir le lecteur et utiliser un programmateur de puce (pour le moment du moins, d'autres personnes recherchent comment réussir le flash depuis le PC), mais avec ces outils il est déjà possible de récupérer le firmware sans programmateur (intéressant pour les personnes ayant les connaissances en assembleur et désireuses d'en savoir plus).

Les détails techniques très poussés sont disponibles ici: http://www.kev.nu/360/dvd.html

*Les commentaires de la Team Xecuter sur ce hack:
(Quasiment) toutes les informations nécessaires sont réparties dans ces sujets:
The Challenge Response Protocol
Hacking DVD firmware AGAIN
Dumping Security Sector with H-943A
Getting XBOX drives to work in windows

De ce que nous pouvons en dire l'image devra être elle aussi patchée, nous pouvons présumer d'une nouvelle fonction pour Qwix (un utilitaire de gestion d'ISO)
Les utilisateurs peuvent espérer un hack pour tous les lecteurs bientôt, vous pouvez être certain de sa sortie, bien que les puces ne seront pas de la partie (c'est du simple piratage, aucun logiciel homebrew n'est possible).

*Enfin le site Xlife.nl a posté une interview avec TheSpecialist (en néerlandais, traduit en anglais pour X-S, puis français^^)
Voilà un petit résumé de ses propos:
"Il y avait 6 hackers dans l'équipe, bien que sans les nombreuses contributions d'autres personnes sur XBH, le temps nécessaire aurait été bien plus grand.
(...)
Le travail sur ce hack a commencé l'année dernière avec l'analyse de la sécurité du Firmware DVD de la XBOX car peu de choses étaient connues à ce sujet.
Nous espérions que la sécurité de la xbox360 était basée sur celle-ci et qu'une bonne connaissance nous donnerait des infos utiles (il semble que nous ayons eu raison).
La raison pour laquelle nous avons commencé avec la xbox était du à la facilité de "ripper" le kernel, ce qui a aidé pour savoir si elle était "ok" pour la lecture du disque.
(...)
Je pense pour commencer que le hack n'est pas intéressant pour l'utilisateur "de base" dans cette forme, car il faut du matériel sophistiqué et les connaissances pour flasher le firmware.
Le hack est également facile à patcher pour Microsoft car une copie diffère sur de nombreux points de l'original, ce qui serait facile à vérifier. Un émulateur "parfait", qui reporte une copie dans toutes les formes possibles comme un original est hors de notre portée et demanderait un long travail.
Il est possible que celà entraîne un jeu du chat et de la souris, avec de nouveaux hacks suivant les patchs...Ce qui veut donc dire que tant qu'il n'y aura pas d'émulateur parfait, aller sur le Live sera un risque de ban potentiel. (Le hack permet actuellement de s'y rendre, mais un patch de Microsoft est bien évidemment attendu)
(...)
La preuve du hack ne réside pas dans la vidéo (voir news précédente), mais sur les détails techniques contenus dans le forum de XBH. Je pense également que si vous regardez avec attention le mouvement du laser, vous comprendrez que ce n'est pas un fake. Si vous placez une copie dans une xbox360 normale, il ne se déplacera pas de la même façon (voir par exemple les mouvements vers le bord extérieur du disque), où il lit les données de sécurité.
Seul un matériel très coûteux, ainsi que beaucoup de travail et d'argent une vidéo (fake) telle que celle-ci serait réalisable.
(...)
Pour finir, comme le disaient les groupes de release du temps de l'Amiga: "A game worth playing is a game worth buying" (=un jeu valant le coup d'être joué mérite son achat), je ne veux pas sonner trop "moraliste", mais j'ai toujours

adhéré à cette idéologie et j'espère que d'autres aussi.
J'ai également apprécié le fait de voir les Pays-Bas bien représentés sur les forums de XBH et j'espère voir plus de néerlandais intéressés dans ce petit monde.""

source - xbox-scene