Un hacker s'apprêterait à dévoiler le code source de VMware

Dans une information transmise à l'agence Reuters, le *hacker* Hardcore Charlie, un homme de 40 ans, de langue espagnole et qui vivrait dans un pays proche des États-Unis, a annoncé qu'il dévoilera le code source du noyau (*kernel*) de la plateforme de virtualisation de VMware, le 5 mai prochain.

Il aurait dérobé ce code en mars dernier, à la suite d'une attaque orchestrée contre des entreprises chinoises et vietnamiennes. Il aurait tout d'abord volé et piraté des comptes *email* cryptés sur Sina.com, qu'il aurait ensuite *'crackés'* avec l'aide d'autres *hackers*. Il aurait ensuite piraté les données sur des serveurs ainsi identifiés. Enfin il aurait réalisé une *'sneak preview'* de 300 Mo du code source de VMware piraté.

Une information confirmée

VMware n'a pas contredit l'information. **Iain Mulholland**, directeur du VMware Security Response Center, l'a même confirmée sur un blogue. En revanche, il affirme que la publication et le partage du code ne vont pas nécessairement se traduire par une augmentation des risques liés à la plateforme VMware. Et de rappeler que l'éditeur partage déjà proactivement ce code et les interfaces avec ses partenaires industriels afin d'élargir l'écosystème de la virtualisation. De même que les API fournies par VMware qui sont destinées à permettre l'exécution d'autres systèmes d'exploitation sur des instances virtuelles.

Si l'information se révèle juste, ce pourrait bien être une bien mauvaise publicité pour l'éditeur. VMware doit depuis longtemps affronter certaines rumeurs selon lesquelles sa plateforme de virtualisation n'est pas aussi sécurisée qu'il l'affirme. D'autres éditeurs ont d'ailleurs plus ou moins confirmé cette vision. Reuters cite IBM qui dans un rapport publié en 2010 a affirmé qu'un tiers des failles dans les environnements virtualisés seraient tracées jusqu'à l'hyperviseur de VMware.

Nous pouvons légitimement nous interroger quant à la menace que pourrait représenter cette publication. Quelle est tout d'abord sa réalité ? N'est-ce pas vantardise de *hacker* qui ne cacherait qu'une baudruche à dégonfler ? Par ailleurs, il n'y a pas automatiquement corrélation entre des lignes de code dérobées et une hypothétique menace sur les plateformes VMware. Notons enfin que l'exploitation du code d'un *kernel* nécessite des compétences qui manquent certainement à ceux qui le dérobent.