Mebroot : un dur à cuire pour les éditeurs

Selon l'éditeur ce rootkit qui se cache dans les couches profondes du boot de la machine, est en phase RTM.

Un terme généralement utilisé par les éditeurs de solutions légitimes pour annoncer l'entrée en production de l'application (Release to Manufacturing).

Dans les faits, ce rootkit est très difficile à détecter, car il se superpose à la zone Master Boot Record du disque dur. Se détection est donc impossible pour les logiciels antivirus.

La zone MBR est le premier secteur, que va utiliser le disque dur maître d'une machine pour lancer le système d'exploitation.

Mebroot se charge donc avant tout les autres programmes. A la rédaction de cette nouvelle aucun antivirus n'est ne mesure de détecter ce rootkit.

Mikko Hypponen chef de la sécurité chez F-Secure précise : *"On ne peut rien exécuter plus tôt que cela. »*

Hypponen suggère de booter à partir du CD d'installation de F-Secure afin de détecter le rootkit.