BusyBotNet, le BusyBox des routeurs piratés ?

BusyBox est un logiciel qui combine de multiples outils du monde UNIX au sein d'un unique exécutable de petite taille. Une offre regroupant des dizaines d'utilitaires pour **moins d'un mégaoctet** et qui se montre très populaire dans les systèmes embarqués.

Il lui manque toutefois des outils de sécurité. C'est ce que propose le projet BusyBotNet 1.0, un dérivé de BusyBox axé sur **le chiffrement et la sécurité**. Divers outils de chiffrement et de scan réseau sont présents, mais aussi de quoi mener des tests d'attaque. L'outil d'attaque par force brute **THC Hydra** est ainsi présent dans BusyBotNet.

Pour des botnets à base de routeurs ?

Comme souvent, ce type d'outil servira aussi bien les besoins des experts en sécurité que des pirates. Ces derniers pourront remplacer le BusyBox **présent dans les routeurs** par cette version, capable de mener des attaques contre des réseaux informatiques (une fonctionnalité à peine cachée, le nom de BusyBotNet étant relativement explicite).

Compilé avec toutes les options, BusyBotNet se montrera toutefois trois fois plus gros que l'original et ne pourra donc être installé sur toutes les machines initialement pourvues de BusyBox. Pour des usages traditionnels, BusyBox devrait donc garder la préférence des administrateurs système, en conjonction avec d'autres outils, comme **Dropbear**, qui apporte la connectivité **SSL**, cliente et serveur, pour environ 110 ko.

À lire aussi :
Le navigateur web embarqué NetSurf se met au JavaScript
DMP étoffe sa gamme de machines x86 embarquées
Minix3 : mises à jour à chaud et sécurité renforcée pour l'OS embarqué