

# Trend Micro veut démembrer les réseaux

## Botnet

L'éditeur de logiciels de sécurité va équiper ses clients avec des protections contre les botnets automatisés. Trend présente « Micro Behavioral Analysis Security Engine » intégrée à la suite InterCloud Security Service. Rappelons qu'un botnet est un réseau de machines compromises pouvant être contrôlées à distance par un pirate pour par exemple envoyer des spams ou des malwares.

InterCloud Security Service, permet notamment à l'administrateur réseau de placer en quarantaine les ordinateurs infectés et éventuellement de les nettoyer. Cette solution a été conçue pour les réseaux de grandes tailles, par exemple ceux des universités. L'application intègre également une plate-forme de services de façon à ce que les ingénieurs de l'éditeur puissent régler les contaminations au cas pas cas. La principale innovation apportée par cette suite est qu'elle est capable de traiter les menaces générées par les réseaux de machines zombies. Les menaces généralement associées à ces réseaux sont la fraude aux clics, les attaques DDoS (Deni de service), les pourriels ou spam, le vol d'identité via le phishing ou les techniques dites de pharming, bref presque tout le panel des cyber-attaques. Généralement les machines d'un botnet sont configurées pour éviter la détection par les antivirus. Mais cette fois Trend Micro a innové en utilisant un système d'analyse comportementale (BASE : Behavioral Analysis Security Engine) qui cherche les traces laissées par les codes malveillants, par exemple en analysant les processus en cours d'exécution, les requêtes DNS, le protocole d'échange de route Border gateway protocol (BGP). Trend Micro's InterCloud Security Service peut donc identifier et isoler les botnets en temps réels et annihiler les risques d'infection, affirme l'éditeur. Les clients de Trend peuvent également profiter du savoir-faire du groupe de spécialistes de la sécurité qui surveillent en permanence les activités des robots et leurs mécanismes de propagation. Pour Dave Rand, chef technologique, Trend Micro : *« avec le lancement de ce service et les capacités de nos experts, il s'agit de la première solution véritablement efficace pour lutter contre les botnets qui ciblent plus particulièrement les FAI et les grandes institutions. »* **A** vérifier sur pièces...