Le ‘pare-feu mémoire’, nouvelle étape dans la protection virale

Là où les systèmes traditionnels de protection se contentent de surveiller ce qui entre et sort d’une banque, notre technologie revient à placer un surveillant devant chaque transaction afin de détecter immédiatement toute opération anormale. C’est par cette image que Nand Mulchandani a présenté le logiciel SecureCore développé par sa société Determina Inc.. Cette start-up, qui a levé 19 millions de dollars afin de développer des recherches initiées par le MIT, a adopté une approche originale pour protéger les postes des risques d’intrusion par attaque de la mémoire du type Blaster ou Slammer. Les produits et technologies concurrents assurent une surveillance externe, et à ce titre recherchent essentiellement à repérer les signatures des attaques virales à partir d’une base de données intégrée qui doit être constamment actualisée. SecureCore quant à lui n’a besoin ni de signature, ni de règles à définir ou d’intervention humaine. L’application protège les applications et les données directement au niveau de la mémoire. Les activités traditionnelles des ordinateurs sont identifiées et toutes les applications sont suivies en permanence. Dès qu’une application exécute quelque chose qui n’entre pas dans les conventions de base, elle est immédiatement détectée, arrêtée, et l’utilisateur ou les administrateurs sont avertis. La protection se place dont au niveau stratégique des *process* de la machine, ce qui participe à son efficacité, d’autant que l’utilisateur de systèmes de protection classique n’a aucune visibilité sur ce qui se passe à l’intérieur de son système. La technologie SecureCore se décline en deux composants : un agent à installer sur les serveurs et qui veille sur le système d’exploitation, les bases de données, les serveurs Web et de messagerie. Et une console d’administration qui gère de manière centralisée le déploiement, les entrée/sortie et les évènements. Pour ambitieuse que soit la technologie développée par Determina, en particulier par son indépendance vis-à-vis des contraintes de mise à jour imposées par les systèmes de protection, il reste cependant à valider le fonctionnement de SecureCore en parallèle avec les autres systèmes de protection, car comme chacun sait la prudence impose d’adopter plusieurs niveaux de protection.