ISS : l'analyse comportementale représente l'avenir de l'antivirus

Baptisée 'VPS', la technologie d'ISS consiste dans un premier temps à piéger le code malveillant dans un environnement virtuel où il peut s'exécuter sans causer de dommages aux ressources réelles. Dans un second temps, VPS analyse en profondeur le code malveillant.

La technologie VPS dispose d'une base de données de scénarios d'attaques (il n'en existe pas plus de 600) à laquelle elle peut comparer le code malveillant qui est en train de s'exécuter. Cela permet de créer une signature dynamique du code. La seconde fois que le code malveillant ou l'une de ses variantes se présentera, l'empreinte MD5 de ses caractéristiques sera comparée à celles des codes malicieux précédemment découverts. Si le code est détecté comme dangereux, il sera éliminé d'office sans que VPS ait à répéter l'analyse. Vous avez dit 'Sand Box' ? Ne vous y trompez pas. Ce procédé, qui peut s'apparenter à la technique du 'bac à sable' (Sand Box), n'est en rien comparable à la technologie d'ISS. VPS diffère en effet dans la façon de traiter les informations recueillies. La « sandbox » fournit en général un fichier de logs que l'expert en sécurité devra analyser manuellement. À la différence du 'Sand Box', qui est avant toute chose un piège passif, la technologie d'ISS est capable d'apprendre de manière autonome. *« Cette technologie est révolutionnaire. De nos jours, la technologie la plus commune se base sur le 'pattern matching'. Il n'est pas rare également de rencontrer des IPS exploitant le 'sandboxing'. Cependant, les utilisateurs de ces deux technologies ne sont pas à l'abri d'éventuels dommages (virus, piratage?). La première technologie étant purement réactive, elle arrive toujours trop tard. Quant à la seconde, elle permet au virus d'être actif dans l'environnement de l'utilisateur? Par souci de réelle prévention, VPS crée un système d'exploitation virtuel dans lequel le virus ne pourra en aucun cas causer de dommages et protégera totalement l'utilisateur »*. Dixit Jean-Paul Ballerini. Bien que cette solution ne nécessite pas de mise à jour, elle permettrait de détecter et contrer plus de 90% des nouveaux virus et nouvelles menaces qui foisonnent sur la toile. *« Après une année de sa mise en fonction dans une ambiance de test, la technologie VPS sans mise à jour est toujours capable de détecter et contrer plus de 90% des nouveaux virus et nouvelles menaces qui foisonnent sur la toile, contre le 30%-40% des technologies traditionnelles »*, ajoute Jean-Paul Ballerini. ISS décline sa technologie 'VPS' sur plusieurs niveaux. Afin de protéger les postes de travail, la solution 'Proventia Desktop' en est équipée. Prochainement, 'VPS' sera intégré aux appliances 'Proventia M' pour la protection au niveau réseau. **Aurélien Cabezon** pour **Vulnerabilite.com.**