Benoit Grunemwald, ESET France : « Nous bloquons les failles zero day »

Courant octobre, ESET a lancé la **nouvelle génération de ses offres de sécurité** : NOD32 Antivirus 7 et Smart Security 7. **Benoit Grunemwald**, directeur commercial d'ESET France, revient avec nous sur ce lancement, et l'activité de l'éditeur slovaque.

Silicon.fr : Quelles sont les nouveautés les plus importantes de cette v7 ?

Benoit Grunemwald : L'Advanced Memory Scanner propose une meilleure détection des applications malveillantes présentes en mémoire vive. C'est un élément essentiel. En effet, des méthodes de camouflage permettent de cacher les menaces sur le disque. Le seul moyen de les détecter, c'est lorsqu'elles sont chargées en mémoire vive. Grâce à une analyse avancée de la mémoire, nous détectons la menace au moment où elle est visible.

Autre nouveauté, l'Exploit Blocker, qui bloque les failles zero day. Pour cela on fait communiquer les modules de l'antivirus entre eux. Par exemple, lorsque le module chargé de protéger la base de registres de Windows empêche l'installation d'un virus et la corruption du système, nous pouvons faire remonter cette information et détecter un éventuel comportement lié à l'exploitation d'une faille zero day.

Votre moteur a la réputation d'être massivement optimisé. Est-ce toujours le cas ?

Oui. Malgré l'ajout de nouvelles fonctions, la consommation mémoire et CPU bouge très peu, car le cœur est continuellement optimisé. Il a été refondu pour la v6, mais reste écrit majoritairement en assembleur. Depuis la v4, le module d'autoprotection est très évolué. Il évite la désinstallation, désactivation ou corruption de l'antivirus.

Des mises à jour sont envoyées au minimum 4 fois dans la journée, en fonction de l'actualité de nos laboratoires. Notez que – grâce à sa compacité – le moteur est mis à jour aussi souvent que la base de signatures, ce qui permet d'améliorer les détections.

Notre offre s'est élargie avec un pare-feu (solution maison), une technique innovante d'authentification à deux facteurs (solution maison) et l'intégration prochaine d'une brique de chiffrement (solution tierce). Il est à noter toutefois que ces produits sont (éventuellement) packagés, mais pas intégrés avec l'offre d'origine, afin de ne pas l'alourdir.

Qui sont vos clients et comment collaborez-vous avec eux ?

Notre cheval de bataille reste l'entreprise, même si cette nouvelle offre est grand public. Notre clientèle se répartit comme suit : 60% d'entreprises et 40% de particuliers. De par sa légèreté, notre

offre est très populaire dans les environnements industriels SCADA. Nous disposons également de gros déploiements chez les ISP. Le service 'dl.free.fr' est ainsi protégé par nos solutions de sécurité dédiées à Linux.

La qualité de la détection ne peut se faire sans l'aide de nos utilisateurs et partenaires. Notre force réside dans notre base d'utilisateurs geeks et passionnés, qui participent à cet effort. Nous pouvons également compter sur notre réseau de 2500 partenaires en France. Ces professionnels de l'informatique disposent de licences pour leur usage interne et font ainsi remonter des alertes.

Enfin, nous travaillons à la mise en place de partenariats avec certains grands acteurs, comme des ISP ou la Phishing Initiative.

Crédit photos : © ESET France

Voir aussi : l**es autres améliorations d'ESET Smart Security 7**