

R&D : DAVFI, un projet d'antivirus français

open source

Le projet est ambitieux : créer un antivirus français et européen, et « *permettre à la France et à l'Europe d'acquérir leur souveraineté numérique dans le domaine des antivirus* ». DAVFI (Démonstrateurs d'antivirus français et internationaux) devra être capable de dépasser les solutions existantes, avec une double capacité de détecter les variantes inconnues de codes identifiés et de prévenir l'action de codes inconnus, grâce en particulier à l'intégration de différentes technologies de protection selon le concept de défense en profondeur.

DAVFI est porté par un consortium d'experts, avec comme chef de file la société Nov'IT, opérateur de services de sécurité; le laboratoire de cryptologie et de virologie opérationnelles de l'école d'ingénieurs de l'EISA (*Ecole supérieure d'informatique, électronique et automatique*); Init SYS pour la R&D; l'éditeur de solution de Network Intelligence Qosmos; l'expert en développement et intégration d'outils d'inventaire et gestion de parc Teclib; et DCNS Research, géant mondial de la défense navale.

5,5 millions d'euros pour développer un antivirus

Coté financement, DAVFI est soutenu par le FSN (*Fond national pour la Société Numérique*) dans le cadre des Investissements d'Avenir (Grand Emprunt), et l'appel à projet Sécurité et Résilience des réseaux. Le projet se base sur les travaux du Laboratoire de virologie et cryptologie de l'ESIEA, dirigé par **Éric Filiol**, Docteur en mathématiques appliquées et en informatique, ingénieur en cryptologie. Il bénéficie d'un budget de 5,5 millions d'euros.

Le projet démarrera en septembre 2012, avec pour échéance une disponibilité en 2014. DAVFI sera-t-il proposé au format open source ? Le consortium se contente pour le moment d'évoquer une « *confiance garantie par l'ouverture du code* »... afin dans un premier temps d'attirer une communauté apte à assurer le succès du produit. Plusieurs versions seront proposées, poste de travail et réseau, ainsi qu'une version gratuite pour le grand public.

Détecter des variantes inconnues

« *Les modèles technologiques de détection des antivirus actuels ont montré leurs limites et ne répondent plus aujourd'hui aux menaces, note **Éric Filiol**. L'approche technique innovante de DAVFI le rendra capable de détecter les variantes inconnues de codes identifiés et de prévenir l'action de codes inconnus. Basé sur une décennie de travaux de recherche, DAVFI assure d'ores et déjà une rupture technologique dans la lutte antivirale.* »

« *La confiance que l'on pourra lui accorder en tant qu'outil de sécurité sera notamment garantie par l'ouverture du code, précise **Jérôme Notin**, président de la société Nov'IT. Un fondamental pour ce type de solution est en effet de pouvoir valider que son comportement réel est bien le comportement attendu.* »