DAVFI : voici venir l'antivirus souverain

Après le smartphone estampillé Bull, la sécurité IT « souveraine » poursuit son déploiement avec le consortium **DAVFI**, réunissant des organisations ou sociétés françaises engagées dans le développement d'un **antivirus national**. Le consortium pilotant ce projet regroupe Nov'IT (services de sécurité), l'ESIEA (plus spécifiquement le laboratoire de cryptologie et de virologie opérationnelles de l'école d'ingénieurs), Qosmos (éditeur de solution de Network Intelligence), Teclib (développement et intégration d'outils d'inventaire et gestion de parc) et DCNS Research (défense navale).

Démarré en 2010 sous l'ombrelle des « investissements d'avenir », le projet a abouti au développement d'un démonstrateur (POC en anglais) pour les terminaux Android (smartphones, tablettes et PC).

Ce matin, le consortium a annoncé la livraison d'une **première version** de cet antivirus souverain, qui sera dévoilée **le 15 novembre** à l'occasion de la conférence Ground Zero Summit se déroulant en Inde.

L'occasion de mettre au défi la communauté des développeurs qui pourra tester l'antivirus Android et contribuer à son enrichissement avant un lancement commercial prévu dans le courant du premier trimestre 2014.

Linux et Windows en ligne de mire

Il sera possible de télécharger une version sur le site Davfi.fr pour tester le nouveau produit en attendant sa disponibilité générale

La priorité est accordée aux marchés des **entreprises et des administrations publiques** (et aux opérateurs d'intérêt vital en France). Parmi le comité des utilisateurs, on retrouve ainsi le ministère de la Défense, les services du Premier ministre, le ministère de l'Education nationale, mais aussi le Crédit Agricole.

DAVFI (acronyme de Démonstrateur Antivirus Français et Internationaux) est considéré comme *« un projet stratégique, majoritairement open source, intégrant des technologies de rupture et qui fera l'objet d'une évaluation auprès de l'ANSSI »*, explique Jérôme Notin, Président de Nov'IT qui pilote ce projet de sécurité (voir à ce sujet son interview chez nos confrères de ITespresso).

Au-delà d'Android, des versions DAVFI pour environnements GNU/Linux (livrée d'ici mars 2014) et MS-Windows (échéance octobre 2014) sont prévues. Cette dernière sera toutefois moins complète, Microsoft ne donnant pas accès à son code source.

Un **budget de R&D de 5,5 millions d'euros sur deux ans** a été consenti pour mener à bien les travaux avant de passer à la phase industrielle et commerciale.

La version Android (livrée plus tôt que prévu si l'on tient compte du calendrier initial), doit encore connaître quelques ajustements techniques (notamment sur le volet de la console MDM pour la

gestion des terminaux mobiles) et marketing avant sa mise sur le marché… sous une marque encore inconnue (DAVFI n'étant que le nom du projet).

« Faire corps avec le système d'exploitation »

L'outil sera intégré dans certains modèles de terminaux Android (smartphones et tablettes) issus de la **gamme Galaxy S de Samsung ou Nexus de Google**.

En attendant de monter une véritable chaîne de distribution DAVFI (intégrateurs, grossistes…), Nov'IT sera le principal interlocuteur pour se procurer ces terminaux.

« On va revendre le téléphone sur lequel, on aura préalablement installé l'OS. On fournit le logiciel et le matériel. Le prix tournera autour de quelques centaines d'euros », précise Jérôme Notin.

Bien moins cher que le smartphone Hoox de Bull présenté comme « *le premier smartphone Android 100% sécurisé en Europe* ».

La solution DAVFI se déploie selon trois axes : **sécurité antimalware**, **chiffrement bas niveau** du système et des données, **chiffrement VoIP et SMS**.

Pour élaborer la version Android estampillé DAVFI, le consortium s'appuie sur une base ROM Cyanogen (système d'exploitation Android modifié) et sur Android Open Source Project (AOSP).

« Il faut travailler au plus bas pour pénétrer au cœur du système et faire corps avec lui », explique Eric Filiol, Directeur du laboratoire de cryptologie et de virologie opérationnelles de l'école d'ingénieurs ESIEA. DAVFI est présenté comme un « OS antiviral » (le système d'exploitation et l'antivirus ne font qu'un). Un « *système immunitaire complet* » censé favoriser la lutte contre les attaques inconnues (notamment zero day).

Une place de marché… et seulement celle-là

La fonction de sécurité IT rattachée au terminal est même déportée en amont sur un serveur antivirus dédié, censé garantir une « autoprotection » du système global.

L'architecture retenue permet l'exploitation d'une place de marché d'applications : 450 apps sont ainsi disponibles sur la **DAVFI Market** (comme un navigateur Firefox ou un client de messagerie), sachant que des outils spécifiques « métiers » peuvent être développés.

« Aucune app ne peut être exécutée sur le téléphone si elle ne provient pas de la DAVFI Market », précise Eric Filiol, qui se veut rassurant en cette période post-PRISM. *« DAVFI intègre ni trapdoor, ni backdoor. Je veux bien admettre que c'est une problématique d'Etat mais pas celle d'un laboratoire de recherche. »*

Voir aussi
Silicon.fr en direct sur les smartphones et tablettes