Antivirus DAVFI : l'autre grand gâchis de l'informatique souveraine ?

Décidément, la souveraineté a du mal à démontrer sa pertinence dans le domaine des nouvelles technologies. Après l'échec des Cloud souverains, Numergy et CloudWatt réintégrés chez leurs actionnaires respectifs Orange et SFR, c'est au tour de l'antivirus à la française de connaître des tiraillements. Le projet est connu sous le nom DAVFI (Démonstrateurs d'antivirus français et internationaux) et a vu le jour en juillet 2012. A l'origine, il est porté par un consortium d'experts, avec comme chef de file la société spécialisée en sécurité Nov'IT, le laboratoire de cryptologie et de virologie opérationnelles de l'ESIEA (École supérieure d'informatique, électronique et automatique), Init SYS pour la R&D, l'éditeur de solutions d'analyse du trafic réseau Qosmos, l'expert en développement et intégration d'outils d'inventaire et gestion de parc Teclib et DCNS Research, la branche recherche du géant mondial de la défense navale.

Ce projet bénéficie d'un budget de près de 6 millions d'euros, dont 40% provenant du FSN (Fonds national pour la Société Numérique). Donc l'argent du contribuable. Eric Filiol, docteur en mathématiques appliquées et en informatique, ingénieur en cryptologie, était alors en charge de fournir le code du projet DAVFI ainsi qu'une équipe d'ingénieurs « *pour aller plus vite dans l'industrialisation* », précise-t-il dans un entretien. Ce code est livré en septembre 2014, avec la validation de la DGA (Direction Générale de l'Armement), à la société Nov'IT, dirigée par Jérôme Notin, chargée d'industrialiser le produit. Précisons que le rapport de la DGA n'a jamais été rendu public.

Il n'a pas fallu 6 mois pour que de premières anicroches commencent à ternir les relations entre la société Nov'IT et Eric Filiol. La première se plaint de la qualité des livrables et le second constate la démission de la moitié des ingénieurs de l'équipe mise à disposition pour le projet, notamment ceux en charge de la R&D et du développement Windows et Linux. Entre-temps, une première livraison a lieu avec le lancement d'Uhuru, nom commercial du projet DAVFI pour la plateforme Android. Elle a été dévoilée lors du Mobile World Congress de 2014, à Barcelone.

Armadito : un résultat « *pitoyable et consternant* »

Mais la semaine dernière, la tension est montée d'un cran avec la publication sur GitHub de la version finale de l'antivirus souverain, qui a, au passage, hérité d'un nouveau nom, Armadito. Et le moins que l'on puisse dire est que cette version ne fait pas l'unanimité. Eric Filiol n'y va pas par quatre chemins : « *cela n'a aucun rapport avec le projet que nous avions livré. Le résultat est pitoyable et consternant. Le code est devenu un fatras mêlant développements Linux et Windows, fichiers json, scripts… Aucune analyse statique de code n'a été menée* », poursuit le spécialiste. « *Et la qualité du code n'est pas digne d'un étudiant en programmation* », lâche Eric Filiol. Enfin, pire que tout, il relève « *la présence de ce que l'on pourrait qualifier de backdoor, mais qui a été très vite retirée. Cela en dit long sur le sérieux et la crédibilité de l'équipe en charge de l'industrialisation de DAVFI* ».

Et la communauté des spécialistes de sécurité semble rejoindre la critique au vitriol de l'initiateur du projet. Une lecture du blog de Nicolas Ruff, membre de la Google Security Team, résume bien la

perception qui entoure le cas DAVFI : « *le gâchis* ». Et de pointer les faiblesses techniques du logiciel livre : « *le projet Armadito échoue à innover dans le domaine de la virologie opérationnelle* », peut-on lire sur le blog. La conclusion de Nicolas Ruff ne fait pas dans la demi mesure : « *Confier le développement d'un logiciel – qui plus est de sécurité – à une armée mexicaine en partie composée de stagiaires et de thésards, n'ayant aucune expérience antérieure ni dans l'édition logicielle, ni dans la sécurité, ni aucune connaissance opérationnelle du monde de l'entreprise, sur la base de quelques travaux académiques à l'applicabilité douteuse : quelqu'un y croyait-il sérieusement ?* ».

Des contributeurs pas des trollers

Nous avons sollicité un entretien à Jérôme Notin, le responsable de Nov'IT, pour connaître son point de vue. Il nous a indiqué dans un message qu'il ne gérait plus le projet. Ce dernier a été repris en main par François Déchelle, polytechnicien et doctorant en informatique, qui a bien voulu répondre à nos questions. Sur les critiques techniques portées par Nicolas Ruff, il admet « *qu'elles sont sensées, car Armadito est un projet encore très jeune* ». Il rappelle qu'en reprenant le projet, il y a apporté beaucoup de modifications : « *refonte de l'interface graphique, du noyau, du moteur heuristique, etc. Il y a des choses réclamées par Nicolas Ruff, comme les notions de sandboxing, qui figurent dans notre roadmap* ».

La discussion sur la position d'Eric Filiol est par contre d'une toute autre nature : « *je préfère que le projet Open Source dispose de contributeurs et non de trollers* », tranche le responsable. Sur les mises en cause de la qualité du code, il renvoie le chercheur à ses propres contradictions : « *le code de DAVFI n'a jamais été publié et je suis sur la même position que Linus Torvalds en la matière : avant de donner des leçons, 'show me the code'* ». Ne souhaitant pas polémiquer plus avant, François Déchelle préfère miser sur les potentialités du projet disponible sur GitHub. « *Il y a encore du travail à faire, des fonctionnalités à ajouter* », dit-il.

Nous avons aussi contacté l'ANSSI pour connaître son opinion sur cette affaire, mais sans réponse pour le moment. Rappelons qu'Eric Filiol a, de son côté, lancé en 2015 un fork du projet nommé « OpenDAVFI ». Objectif du chercheur : montrer que le travail accompli ne l'a pas été en vain. Mais, il lui faudra surmonter un obstacle juridique, en revenant sur le transfert de propriété intellectuelle à Nov'IT réalisé aux débuts du projet. « *Nous sommes en train de regarder comment juridiquement nous pouvons valoriser nous-même notre travail* », souligne Eric Filiol, qui précise avoir déjà finalisé un module opérationnel pour bloquer les ransomwares.

A lire aussi :

L'antivirus bleu-blanc-rouge Uhuru sécurise Windows et Linux

Jérôme Notin (Nov'IT) : « DAVFI : l'outil antivirus souverain marquera une rupture technologique »

Crédit Photo : Ollyy-Shutterstock