CITL : Un hacker évalue gratuitement la sécurité des logiciels

Un nouveau coup d'éclat pour l'un des initiateurs de L0pht Heavy Industries ? Ce groupe de hackers de Boston qui, en 1998, déclarait aux parlementaires américains pouvoir paralyser Internet en 30 minutes ? L'homme, Peiter Zatko, est surnommé Mudge. Il a développé, conjointement avec son épouse Sarah, mathématicienne, un système d'évaluation de vulnérabilité des logiciels. Le but : identifier les logiciels robustes sur le plan de la sécurité ou trop coûteux à pirater.

Les Zatko ont obtenu le soutien (à hauteur de 600 000 dollars) de la Darpa américaine, de la Fondation Ford et de la Consumers Union. La méthode est inspirée de la traditionnelle certification de sécurité de produits. Leur « Cyber Independent Testing Lab » (CITL, une organisation à but non lucratif) se propose donc de tester et évaluer la sécurité de logiciels (navigateurs, comparateurs, antivirus, etc.). Sans faire payer les évaluations. Mais dans l'idée de pousser les éditeurs et les développeurs à en améliorer le code, pour que leurs programmes restent performants et bien notés.

« Il y a des applications qui font vraiment preuve d'un bon [niveau de sécurité]. Mais la grande majorité se situe ailleurs, entre un niveau modéré et catastrophique de sécurité », a expliqué Mudge dans les colonnes de *The Intercept*. *« La bonne nouvelle c'est que vous pouvez maintenant savoir où se situe un logiciel sur cette échelle »*, a-t-il ajouté quelques jours avant la conférence Black Hat 2016.

Logiciels robustes ou trop chers à pirater

Le projet a été présenté cette semaine à Las Vegas. La technique consiste à analyser les fichiers binaires en utilisant des algorithmes (créés par Sarah Zatko) pour mesurer le niveau de sécurité du code. 300 critères sont étudiés. Le nombre de branches dans un programme est quantifié. Plus les branches sont nombreuses, plus le risque d'erreurs est elevé. Ils étudient, enfin, la possibilité d'utiliser des entrées valides potentiellement sensibles aux attaques par complexité algorithmique.

Ainsi sur les ordinateurs Mac d'Apple, le navigateur web Chrome de Google serait plus résistant aux attaques que Safari d'Apple. Safari serait lui-même plus sûr que Firefox de Mozilla. Les solutions de Microsoft testées jusqu'ici ne sont pas mal notées, sauf la suite Office pour OS X qui n'a pas convaincu le CITL. Il n'est pas sûr que les éditeurs apprécient. Ils pourraient rejeter la méthode utilisée ou l'idée d'un indicateur de risque (les compilateurs vieillissants, les binaires risqués…).

Les éditeurs ne paient pas l'évaluation, selon *The Intercept*. Le couple Zatko choisit les solutions propriétaires ou Open Source à évaluer, et en obtient copie (légalement). Une fois les tests effectués, trois rapports seront produits par logiciel testé (une note comprise entre 0 et 100, une étude détaillée en accès libre, et des données brutes de recherche que le couple prévoit de vendre). Jusqu'ici 12 000 programmes auraient été analysés et les premiers rapports devraient être remis début 2017.

Lire aussi :

Direction, frein : les hackers de Jeep récidivent à la Black Hat

Navigateurs web : Mozilla Servo en test sous Linux et OS X

Apple prépare le retour en force de Safari