Un labo français pour évaluer l'efficacité des logiciels antivirus

- Informatique - Sécurité Informatique -

Date de mise en ligne : jeudi 27 dÃ©cembre 2007

Spyworld Actu

Installé à Nancy, ce laboratoire analysera les virus et le comportement des antivirus. Il devrait être opérationnel au début de 2008.

Le 2 novembre 1988, le ver Morris contamine quelque 6 000 ordinateurs, soit 10 % des PC connectés à l'époque au Web. C'était la première grande infection informatique. Aujourd'hui, les virus font partie du quotidien des internautes. Et la menace est toujours réelle. « Un code malveillant correctement programmé pourrait paralyser Internet en une poignée de secondes », rappellent Olivier Festor, chercheur à l'Inria, et Jean-Yves Marion, professeur à l'Ecole nationale supérieure des Mines de Nancy.

Une première en France

C'est pour étudier de façon scientifique et indépendante les virus et les différentes techniques employées par les pirates que ces chercheurs mettent sur pied un laboratoire dédié. Une première française dans le domaine civil, car les autres unités de ce genre dépendent du ministère de la Défense, comme le Laboratoire de virologie et de cryptologie créé en 2001.

N'ayant pas encore de statut officiel, ni de budget complet, cette nouvelle unité s'appelle pour l'instant Laboratoire de haute sécurité civile. Elle dépend du ministère de l'Enseignement supérieur et de la Recherche via trois entités officielles que sont le CNRS (Centre national de la recherche scientifique), l'Inria (Institut national de recherche en informatique et en automatique) et Nancy-Université.

Traquer les rétrovirus

Comprenant actuellement cinq personnes (deux enseignants-chercheurs et trois thésards et ingénieurs), ce laboratoire visera deux grands objectifs. Le premier « ne sera pas le plus intéressant scientifiquement puisqu'il s'agira de récolter les codes malveillants qui traînent sur le Web ».

Les captures se feront notamment sur un ensemble de réseaux de fournisseurs d'accès (Orange, Free, Alice, Neuf, etc.). Dans ce cas, des microsondes seront connectées chacune à un fournisseur sur la base d'un abonnement ADSL de particulier. Le deuxième objectif risque de faire du bruit puisqu'il s'agit de créer un audit des antivirus qui soit réellement indépendant des éditeurs. Ces logiciels seront soumis à de multiples codes malveillants.

« Les antivirus actuels n'agissent que sur des codes malveillants dont on connaît déjà la signature. Or, nous avons en tête les travaux du lieutenant-colonel Eric Filiol, du Laboratoire de virologie, sur notamment les rétrovirus, c'est-à-dire les codes malveillants qui se servent des failles des antivirus pour attaquer, indique Jean-Yves Marion. En détectant de nouveaux virus, nous espérons mettre au point des méthodes d'analyses heuristiques bien plus puissantes que celles utilisées par les antivirus actuels. »

S'il obtient le feu vert de son ministère de tutelle, ce laboratoire pourrait vendre les résultats de ses audits et de ses avancées en matière de défense informatique.

Post-scriptum :

http://www.01net.com/editorial/3681...