# Les cyberpirates peuvent exploiter une faille en 24h

Les cyberpirates sont devenus très rapides. Présenté dans colonnes de *Wired*, le dernier rapport publié par Internet Security Systems X-Force, la brigade de sécurité d'IBM, a le mérite de mettre les choses au clair. Selon les chercheurs, les cyberdélinquents sont aujourd'hui capables de détecter une faille de sécurité et de la rendre exploitable en **24 heures**.

En se penchant sur les six premier mois de l'année, les équipes d'IBM ont réalisé que les cyberpirates se servaient de nouveaux programmes capables de détecter un trou de sécurité et de le leur offrir sur un plateau des codes d'exploitation. Cette possibilité ne s'offrait pas à eux auparavant.

En second lieu, le rapport met en évidences le manque de cohésion inhérent au milieu des laboratoires de sécurité. Les pirates peuvent compter sur les querelles de chapelle autour des découvertes de failles de sécurité. Si certains chercheurs penchent pour une information postérieure à la sortie d'un correctifs, d'autres préfèrent exhiber leur découverte avant le patch, avec parfois, la preuve de concept (*proof of concept*) à la clef. Ce qui revient paradoxalement à donner le bâton pour se faire battre. Cette dernière approche, utilisée lors de la dernière faille DNS de taille détectée sur le Web par **Dan Kaminsky**, aurait pu provoquer une catastrophe mondiale.

Quant aux vulnérabilités constatées sur PC, **pour plus de 80%**, un code malveillant était produit le même jour. Pour l'équipe Internet Security Systems X-Force, ce chiffre a progressé de 70% en un an.