Sécurité : l'efficacité des antivirus remise en cause

Entre 2 et 40 minutes, voilà le temps qu'ont résisté les solutions de sécurité passées au crible par l'école d'ingénieurs ESIEA à Laval pour la première édition du congrès iAWACS (International Alternative Workshop on Aggressive Computing and Security). Des experts de la sécurité informatique n'ont pas ménagé leurs efforts pour **contourner les barrières de 6 antivirus parmi les plus vendus dans le monde.**

Lors du concours, organisé en marge des réunions, les experts avaient à disposition des **ordinateurs fonctionnant sous Windows**, identiques à ceux des particuliers. L'objectif donné était alors d'arriver à désactiver l'antivirus protégeant le système en moins d'une heure. La tâche était alors accomplie si l' antivirus ne parvenait pas à détecter une attaque virale conventionnelle.

Selon les organisateurs, **tous sont donc tombés à l'exception de Dr Web** : «*le plus dur à contourner, cependant suffisamment affaibli pour conclure qu'avec un peu plus de temps (plus d'une heure), les candidats seraient parvenus à désactiver un septième antivirus.* »

Robert Erra, un des responsables du congrès iAWACS donne une explication à ces tests grandeur nature. Selon lui : «*L'objet du concours n'est pas de* ***donner aux hackers les dernières astuces pour pénétrer de façon frauduleuse des systèmes informatiques***. » Pour autant, certains spécialistes n'hésitent pas à tacler sévèrement les éditeurs de sécurité jugeant les antivirus « *totalement inutiles et dépassés technologiquement*». Des propos notamment repris sur *France Inter.*

Toujours est-il qu' Eric Filiol, expert en sécurité et invité au congrès explique que les manques ne sont pas tant au niveau des éditeurs que réglementaire. Il explique : « *La loi de 2004 sur la confiance dans l'économie numérique est trop floue sur ce point… Une* ***personne peut être potentiellement poursuivie si elle parvient à désactiver un antivirus***».

Si la conférence a mis le doigt sur une réalité, reste à savoir comment un utilisateur lambda peut-il éviter les menaces sans antivirus ou solution appropriée ? Vaste question.