

Les outils antivirus, une porte ouverte aux malwares ?

Selon N.runs, un cabinet allemand de conseils en informatique, les logiciels antivirus pourraient en réalité ouvrir la porte aux pirates et leur permettre de pénétrer sur les réseaux d'une entreprise et de charger du code de destruction. Les experts en sécurité de la société auraient découvert environ 800 vulnérabilités dans les produits antivirus au cours de ces derniers mois.

A en croire N.runs, chaque analyseur de virus actuellement sur le marché comprend plusieurs failles extrêmement critiques qui pourraient ouvrir la voie à des attaques par déni de service et favoriser l'infiltration de code destructif dans le réseau.

L'analyse serait l'une des principales causes du problème. Dans ce cas, les analyseurs de virus doivent reconnaître le plus d'applications malveillantes possibles, ce qui signifie qu'ils doivent comprendre et traiter un grand nombre de formats de fichiers.

Pour pouvoir interpréter les formats, une application doit partitionner le fichier correspondant en blocs et structures. Mais selon N.runs, les mauvaises hypothèses lors de la programmation du code d'analyse créent des constellations qui permettent l'infiltration et l'exécution de code programme.

« En bref, plus il y a d'analyse, plus le taux de reconnaissance et le degré de protection seront élevés, ce qui augmente parallèlement la surface d'attaque et fait du produit antivirus lui-même une cible potentielle », expliquent les experts de N.runs. « Unespionnage industriel systématique, avec l'interruption de toutes les communications par e-mail, en sont deux conséquences possibles. »

La société a mis au point son Application Protection System AntiVirus afin de compléter l'infrastructure de sécurité informatique des entreprises en utilisant plusieurs moteurs pour combler les brèches de sécurité.