Test anti-Rootkit : les solutions sont loin d'être parfaites…

Même si les menaces ne sont pas nouvelles, elles deviennent de plus en plus difficiles à détecter. Les différents échecs rencontrés lors des tests menés par l'Epitech (groupe d'écoles d'études supérieures en informatique) rappellent la situation des vers et des virus, il y a quelques années.

Bilan de cette étude indépendante: les produits du marché sont imparfaits, perfectibles et parfois défectueux dans leur conception. Les ingénieurs de l'Epitech rapportent que les meilleurs taux de détection sont attribués à SafetyCheck et Sysprot anti-rootkit, ainsi qu'à Rootkit Unhooker.

Dans son communiqué, l'Epitech détaille la méthodologie mise en oeuvre pour ce test:

« Les tests ont été réalisés en compromettant des machines Windows, par l'exécution des rootkits Fu, Futo, Phide, RkU (1.2), BadRK (demo), et Unreal. Par ailleurs, parmi tous les anti-rootkits collectés, nous avons choisi de retirer de la liste de tests les outils qui ne sont plus maintenus, ou qui ne correspondent plus aux critères de détection actuels des technologies de furtivité. Aussi, nous avons choisi d'étendre le test au-delà des anti-rootkits "classiques". En plus des outils de détection des grandes firmes (Symantec, FSecure, Sophos, etc.), nous avons décidé d'évaluer des outils moins connus, moins maniables, et nécessitant quelquefois des connaissances techniques assez pointues. »

Critique des résultats

Ce test est surprenant à plusieurs égards. D'une part, on constate que des menaces facilement détectables posent encore problème à certains anti-rootkits.

Comme pour les virus, une simple modification des '*patterns*' recherchés par l'outil le laissent complètement à l'écart, affirmant que la machine est saine.

Les anti-rootkits qui ne procèdent qu'à un scan sont de facto voués à l'échec. Il est absurde de détecter un rootkit comme on le fait d'un virus. Déjà, dans ce domaine, cela a posé de nombreux problèmes. Les limites de l'exercice ont été rapidement atteintes. Ce qui a donné naissance aux approches 'heuristiques', l'analyse d'un comportement suspicieux avec des niveaux pour lesquels alerter l'utilisateur.

Les produits des grandes sociétés ne se révèlent pas des plus efficaces. Malgré tout, certains arrivent à se trouver une place, comme AVG, SysProt, Sophos, ou encore le moteur Tucan. Ces produits trouvent les processus cachés, et même s'ils ne décèlent pas l'ensemble des codes furtifs, ils peuvent donner quelques indices. Nous pensons que ces produits peuvent (et devraient) servir de base à une analyse plus fine. Il est impératif de ne pas se conformer aux dires d'un seul de ces outils de protection.

Dixit l'Epitech: les meilleurs taux de détection vont à **SafetyCheck** et **Sysprot anti-rootkit**, ainsi que **Rootkit Unhooker**. Ce logiciel est idéal à coupler avec un autre produit, puisque – de façon très technique il est vrai – il pointe la plupart des crochetages, et met l'accent sur nombre d'intrusions.

Même pour des utilisateurs confirmés, la prise en main de Rootkit Unhooker est difficile, mais il s'agit là d'un outil efficace, qui est un très bon renfort dans la chaîne de sécurité. Il peut surtout corroborer ou infirmer les résultats d'un outil tiers, plus facile à prendre en main, mais aussi moins efficace.

« On sent les produits imparfaits, perfectibles, et quelquefois défectueux dans leur conception. Actuellement, la plupart de ces logiciels ne peuvent pas être considérés comme dignes de confiance » , conclue l'Epitech.

Le site de l'Epitech est disponible sur ce lien.