Alerte : un nouveau rootkit se cache au coeur du disque dur

Les éditeurs de sécurité Symantec et Verisign viennent de découvrir une nouvelle menace incarnée par un rootkit qui se cache dans le premier secteur d'un disque, la fameuse zone MBR (Master Boot Record Security) qui permet d'amorcer le démarrage d'un poste et de son système d'exploitation.

Les attaques MBR ne sont pas vraiment nouvelles. Les premières affaires remontent à l'époque de MS-DOS, ou les virus comme Brain, Stoned, ou bien encore Tequila, se dissimulaient dans la partition du disque « maître ».

Ce rootkit, qui à l'instar des autres trojans à la particularité de jouer la carte de l'invisibilité est donc particulièrement difficile à détecter. Pourquoi ? tout simplement parce que ce code malveillant dissimulé au cœur du disque dur est activé avec le système d'exploitation… Selon plusieurs sources il y aurait déjà près de 5.000 infections répertoriées entre le 12 décembre et le 7 janvier.

« Un rootkit MBR est capable de compromettre le kernel de Windows avant son démarrage. Cela lui apporte une plus grande invisibilité par rapport aux autres rootkit. Ces rootkits sont même capables de survivre à une réinstallation complète et un formatage du disque dur » explique Matthew Richard, directeur des recherches du laboratoire iDefense (un fournisseur de services de sécurité qui appartient à Verisign).

Pour l'instant, Symantec est le seul éditeur à détecter ce rootkit, un trojan baptisé Mebroot. Dans une note publiée sur le Web, un chercheur explique que ce rootkit est le symbole de la nouvelle tournure que prend la guerre qui oppose les éditeurs de solutions de sécurité et les cybercriminels auteurs de codes malveillants.

D'ailleurs, ce constat est le même partout. Les nouvelles menaces qui pèsent sur l'informatique sont très sérieuses. Et comme l'illustre cette affaire, les malfaiteurs de la Toile cherchent à cibler des failles très profondes dans le matériel informatique… Toutes les versions de Windows, y compris Vista sont vulnérables.

Notons que selon nos informations, près de 30.000 sites Web européens essayent de propager le rootkit. Le gang derrière ce rootkit est le même que celui qui a diffusé massivement le trojan de phishing Torpig.

Pour conclure, l'on ne peut que s'inquiéter de l'émergence de ces nouvelles menaces, qui sont très bien ficelées, et orchestrées par des hackers professionnels au service d'organisations mafieuses. Les particuliers, et certains éditeurs sont désarmés face à une telle sophistication des attaques. La seule solution pour lutter contre les rootkits est d'envisager une refonte totale des OS présents sur le marché, autant dire que cela risque de prendre du temps…