H.D Moore publie le code source d'un moteur de recherche de malwares

Pour mener à bien cette mission, l'éditeur avait développé un outil exploitant l'API de Google et les fonctionnalités de recherche de fichiers binaires. H.D Moore diffuse aujourd'hui le code source de son propre outil, similaire à celui de Websense.

H.D Moore aura certainement été agacé par l'attitude ? plus ou moins bien justifiée ? de Websense qui n'avait pas souhaité diffuser au grand public le code source de son application. Cette dernière permet de rechercher sur la toile les sites Internet qui hébergent des codes malicieux. *« C'est un outil précieux pour les chercheurs, mais il peut être dangereux entre les mains d'un auteur de virus »*, explique Websense dans un communiqué. Qu'à cela ne tienne, le Texan a offert aujourd'hui à la communauté quelques bouts de scripts développés en « Ruby » permettant d'en faire autant. Le principe est simple. Il combine la puissante API de Google et les fonctionnalités de recherche dans les signatures des binaires référencées. En effet, Google « parse » et comprend parfaitement le format PE des exécutables Windows et références les informations contenues dans les en-têtes des fichiers. Il est ainsi possible à partir des signatures de fichiers, de les retrouver sur la toile. De là à développer un moteur de recherche de virus, il n'y avait qu'un pas que Websense et H.D Moore ont franchi. D'autres pourront donc désormais expérimenter l'outil de Moore, voire même l'améliorer. D'ailleurs, le chercheur compte sur la communauté pour continuer l'exploration dans ce sens. Moore confie à eWeek.com qu'il ne passera pas plus de temps sur ce nouveau procédé, à moins que Google ne se mette à référencer encore plus de malwares …