Les ‘blogs’ menaceraient la sûreté du Web

Le dispositif de sécurité multi-couches de Websence permet de détecter les menaces liées à Internet, et pas seulement les virus. Ainsi le Websence Security Labs a découvert qu’un nombre croissant de ‘blogs’ sont corrompus.

Ces sites personnels et fédérés de publication gratuite d’information, qui permettent aux internautes de s’afficher en ligne constituent, l’un des phénomènes les plus spectaculaires d’Internet. Mais Websense a répertorié des centaines de cas de ‘blogs’ utilisés comme dispositifs de stockage ou de diffusion de codes malveillants. Pour l’éditeur, les ‘blogs’ sont des vecteurs d’action extrêmement prisés des hackers, pour trois raisons principales : – ils offrent gratuitement de grandes quantités d’espace de stockage ; – ils ne requièrent aucune vérification de l’identité lors de la mise en ligne des informations ; – la plupart des systèmes d’hébergement de ‘blogs’ n’appliquent aucune protection antivirus aux contenus mis en ligne. Dans certains cas, les hackers créent des ‘blogs’ sur des sites d’hébergement tout à fait légitimes, puis ajoutent à leurs pages un code de virus ou un logiciel de ‘*keylogging*‘ (espion qui enregistre et transmet les mots de passe), puis cherchent à générer du trafic vers le ‘blog’ toxique en envoyant un lien à un grand nombre de destinataires, par l’intermédiaire d’e-mails ‘spammés’ ou via les messageries instantanées. Dans d’autres cas, le ‘blog’ peut être utilisé comme un système de stockage de codes malicieux accessibles par un cheval de Troie préalablement installé sur l’ordinateur de l’utilisateur. « *Il ne s’agit pas de sites de ‘blogs’ sur lesquels tout un chacun peut tomber par hasard, et voir sa machine infectée accidentellement. Si ce type d’attaques connaît un réel succès, c’est parce qu’elles s’appuient sur un certain niveau de ‘social engineering’ pour inciter les utilisateurs à cliquer sur le lien*« , a indiqué Dan Hubbard, directeur de la sécurité et de la recherche technologique chez Websense, Inc. « *J’ajouterai que les blogs sont utilisés comme première étape d’une attaque à plusieurs niveaux qui peut également faire intervenir un e-mail frauduleux, un cheval de Troie ou un ‘keylogger’…*« . En réponse à ces horribles menaces, Websense a -évidemment- l’arme défensive: son Master Database, une base de donnée d’URL et d’applications formellement associées à ces nouvelles escroqueries, ou à celles qui ont été infectées par un code de ‘keylogging’, lequel vient se placer au niveau de la passerelle Internet et du poste de travail. Cette solution de protection par indexation des menaces est une technique répandue, mais qui doit être complétée par l’artillerie sécuritaire des « pare-feu », des antivirus et autres antispams…