Les toolkit à l'origine de la majorité des attaques détectées

Parmi les virus, ver, chevaux de Troie, et autres *malwares* qui prolifèrent sur la toile, on oublie trop souvent la part des toolkit. Rappelons que ces «boîtes à outils» ne sont pas des applications malveillantes à l'origine mais des outils d'administration des couches basses du système. C'est donc un outil détourné par les pirates qui le classe aujourd'hui dans la catégorie des solutions à maintenir loin des ordinateurs. L'occasion pour Symantec de faire un point sur les menaces liées aux toolkit sur Internet, en s'appuyant sur son grand rapport annuel *Norton by Symantec* et que nous présente *ITespresso.fr*.

Si la vente en ligne de toolkits, mis au point par des développeurs qui y insèrent des « exploits » pour tirer parti des failles de sécurité des systèmes, a débuté en 1992, *« c'est véritablement au milieu des années 2000 que les ventes de kits d'attaques en ligne ont décollé, avec l'arrivée de MPack en 2007, qui a par exemple réussi à compromettre des milliers de sites italiens »*, a expliqué Laurent Heslault, directeur des technologies de sécurité pour Symantec Europe de l'Ouest, lors d'une conférence de presse. Les kits d'attaques Eleonore, Tornado ou Zeus ont ainsi fait beaucoup parler d'eux ces derniers mois…

Au fil des ans, les toolkits ont évolué pour se rendre plus attractifs et plus « vendeurs ». Ainsi, souligne l'éditeur, leur particularité est d'être simple d'emploi et facilement accessible. Selon Symantec, rien de plus facile que d'acheter un toolkit. Il suffit de se rendre sur son moteur de recherche préféré, de taper les mots-clés appropriés (comme le nom d'un kit), et c'est parti ! Qui plus est, *« ces kits d'attaques sur Internet sont aussi modernes : ils offrent désormais des supports en ligne, via le tchat, et de la maintenance »* pour les apprentis cyber-criminels, note Laurent Heslault.

Rapides, efficaces, les kits d'attaques sur Internet ont indéniablement la cote. Sur la base des rapports de son réseau de surveillances des menaces en ligne, Global Intelligence Network, Symantec affirme que *« 61 %des attaques détectées proviennent de toolkits, comme MPack, Zeus, Nukesploit, Phoenix »*.

Ces kits d'attaques en ligne sont aussi protéiformes et s'adaptent facilement aux nouveaux usages informatiques. Symantec note ainsi l'émergence de ce que Laurent Heslault qualifie de « Crimeware-as-a-Service » sur le modèle du SaaS (Software-as-a-Service), ce qui permet à des internautes de louer pendant quelques heures ou quelques jours un toolkit à la demande… Les pirates sont décidément très à la pointe des nouvelles tendances.