2007, l'année du piratage industriel

- Informatique - Sécurité Informatique -

Date de mise en ligne : lundi 21 janvier 2008

Spyworld Actu

Le Clusif a présenté la nouvelle édition de son « Panorama de la cybercriminalité », qui met en particulier l'accent sur la commercialisation par des pirates de « kits prêt à infecter ».

La lecture du « Panorama de la cybercriminalité » du Clusif (Club de la sécurité des systèmes d'information français) incite à la nostalgie et à la parano. La nostalgie pour l'époque où les pirates se contentaient de balancer des virus sur la Toile. La nouvelle génération préfère utiliser des kits « prêt à infecter » pour lancer des attaques sophistiquées. Quant à la parano, elle s'explique par la multiplication des affaires d'espionnage industriel dont les auteurs sont des employés.

Le phénomène MPack

Pour ne pas éveiller les soupçons des internautes et ne pas être repérés par les logiciels de sécurité, les pirates ont donc mis au point des attaques très pointues grâce à des « kits de piratage ». L'un des plus connus est Mpack.

Il a été développé par un groupe russe qui le vend autour de 1000 euros, SAV compris ! L'exploitation la plus connue de MPack a eu lieu entre la mi-avril et la mi-juin 2007 avec l'attaque baptisée « Italian Job/Mpack ». Des dizaines de serveurs Web ont été corrompus via des failles visant Apache.

Plus de 10 000 sites ont été touchés dont 80 % en Italie. Dès qu'un utilisateur visitait un site piégé, il était redirigé à son insu vers un autre site, contenant MPack. Le pirate pouvait ensuite installer tous les codes malveillants qu'il souhaitait sur l'ordinateur. Depuis, d'autres variantes de Mpack sont proposées à 400 euros.

Vol de secrets de fabrication

Le second point marquant de l'an passé est donc l'espionnage industriel. Le Clusif présente quatre grandes affaires qui confirment que le ver est souvent dans le fruit. Et en particulier le cas d'un ancien employé de Duracell, qui a été condamné à 5 ans de prison avec sursis, 7 500 dollars d'amende et 200 heures de travail d'intérêt général. Motif : il avait téléchargé et copié sur son ordinateur des documents de recherche sur les piles AA de l'industriel. Il a ensuite tenté de les revendre à deux concurrents qui ont contacté... Duracell.

Dans son rapport, le Clusif pointe aussi du doigt les fraudes à la carte bancaire, les arnaques sur les sites d'enchères et l'exploitation de la naïveté des utilisateurs des réseaux sociaux et des mondes virtuels.

Post-scriptum :

http://www.01net.com/editorial/3697...