

# Hacktivisme et exploitation de la crise... les tendances du malware, saison 2009

En matière de menaces informatiques, on pourrait croire que tout a déjà été fait ou vu en 2008. Des attaques, principalement du phishing, via des sites comme Facebook ou LinkedIn, des spams taxés de nigériens, des sites Web piégés ou encore des offensives bien réelles contre des installations d'Etats ou institutions publiques.

Toute cette panoplie de malwares devrait se retrouver fatalement dans nos colonnes puisque la tendance devrait être la même en 2009 selon la plupart des prévisions des éditeurs de sécurité.

Pire la tendance du « **Hacktivisme** » devrait se développer à en croire François Paget, ingénieur-chercheur en menaces chez l'éditeur américain **McAfee**. Il explique, « *certaines groupes sont soutenus indirectement par des gouvernements. Sur certains d'entre eux comme la Russie et la Chine planent de forts soupçons. Ces pays attaquent toujours de manière détournée. Par exemple, certains membres du Russian Business Network, un FAI basé à St Petersburg, ont été montrés du doigt. Il a été établi qu'ils avaient des liens avec certains membres du gouvernement russe en place. Son chef, un certain « FlyMan » n'a jamais été inquiété, son père étant un proche du pouvoir...* ». Autant d'interrogations qui viennent se nicher dans des sphères de pouvoir difficilement accessibles à des opérations de police d'envergure.

Une position que partage l'éditeur **Sophos**. Son directeur Marketing, Michel Lanespèze s'explique : « *L'analyse de l'année 2008 prouve sans le moindre doute que les groupes de pirates agissant sur Internet sont plus organisés que jamais, se jouant des frontières pour dérober argent et données. Nous ne pensons pas que ces attaques diminueront en 2009. Avec l'entrée en récession des économies, il est plus important que jamais que les particuliers aussi bien que les entreprises s'assurent qu'ils sont protégés contre les attaques via Internet* ». Sophos cible alors plutôt les Etats-Unis comme l'Etat hébergeant le plus de malwares. Si en 2007, la Chine hébergeait plus de 50% du code malveillant présent sur le Web, en 2008, les Etats-Unis recensent 37% de cette menace. Loin devant la Chine (27%) et la Russie avec 9,1%.

Face à ces dangers, McAfee stigmatise un manque patent de cyberpolice. « *Les forces de police en première ligne manquent souvent des compétences spécialisées pour lutter efficacement contre le cybercrime. Face au manque de formation dédiée et continue, à une rémunération insuffisante ou à l'absence d'un plan de carrière bien défini, les cyberspécialistes sont récupérés par le secteur privé ou séduits par l'économie clandestine* ».

2009 sera donc l'année des arnaques en tous genres, un phénomène qui sera amplifié par la crise économique. Faux organismes de prêts, sites de faux juristes, travaux de « mules ». La crise risque fort de servir les plus mal-intentionnés. La mode pour l'année à venir sera donc aux malwares qui vont jouer sur les peurs et attentes des internautes, elles devraient se faire moins visibles... en apparence.