Les virus de la semaine : chevaux de Troie en ordre de bataille

La palme revient cette semaine au ver/virus **Alanchum.VL**. Il représente à lui seul 62% des attaques repérées par l'éditeur de sécurité. Selon Luis Corrons, le directeur technique de PandaLabs,*« les malwares de cette famille utilisent l'ingénierie sociale pour se propager. Ils se servent de thèmes d'actualité ou attractifs afin d'inciter les utilisateurs à ouvrir le fichier infecté. »* Niché dans l'ordinateur, Alanchum.VL télécharge un autre cheval de Troie, Cimuz.BE **.** Ce dernier pille les informations confidentielles dès que l'internaute se connecte sur des sites bancaires ou des webmails. Bien sûr, les informations soutirées sont envoyées au créateur du logiciel malveillant. La deuxième place du podium revient à Cimuz.FH, une variante de Cimuz. Il dérobe les identifiants et autres adresses IP. Le troisième cheval de Troie brocardé est Downloader.OHC **.** Ce « trois en un » infecte un ordinateur en téléchargeant directement deux autres malwares. Le premier, AdClicker modifie la base de registre Windows. Grum.D.drp, grâce à son serveur, inonde l'utilisateur de spam. En guise d'ultime avertissement dans leur bulletin, les équipes de Panda Software montrent du doigt MSNDiablo.A. Ce ver se propage via MSN Messenger. Il envoie à tous les contacts de l'utilisateur contaminé un commentaire et une vidéo Si l'internaute clique sur le lien, il installe sans le savoir MSNDiablo.A. Il se propage de manière similaire en utilisant les contacts des usagers contaminés. Une incitation à la prudence supplémentaire.