‘Des sous! sinon je crypte tes fichiers’, suite

Dans les temps très reculés de l’informatique, au début des années 90! les premiers virus informatiques s’en prenaient aux disques durs et menaçaient de les formater. Certains créateurs de ces sales bêtes avaient de l’humour: ainsi le virus ‘Casino’ présentait à l’écran une machine à sous: le malheureux utilisateur avait trois chances pour sauver ses données.

Par la suite, avec Internet, les virus ont changé d’objectif. La plupart d’entre-eux cherchent en effet à inonder les messageries ou à générer des machines à spam et à déni de service. Mais depuis quelques temps, les vers destructeurs reviennent à la une. Nous évoquions ici le cas de Nopir qui cherche à effacer les mp3 pirates ou non présents dans le PC. Le 25 mai dernier, nous évoquions également le cas de ce virus qui cryptait des fichiers et demandait une rançon pour les décoder. Désormais, on en sait plus sur cette affaire. Symantec et WebSense ont détécté ce nouveau ver/cheval de Trois qui crypte les fichiers et menace d’effacer le disque dur. Il se désactive si l’utilisateur accepte de payer une rançon de 200 dollars. « Pgpcoder » est donc un Cheval de Troie qui renvoie au très connu « Pretty Good Privacy » (PGP), un logiciel sûr et légal de cryptage. Selon le site spécialisé VirusTraq.com, cette escroquerie inédite a pu être réalisée via une faille d’Internet Explorer connue et corrigée par Microsoft en Juillet 2004. Websense précise que le code de chiffrement utilisé n’est pas excessivement complexe et qu’il n’est pas difficile de le casser pour récupérer les fichiers verrouillés. Par ailleurs, le racketteur donne une adresse internet et un compte bancaire électronique pour se faire payer, permettant éventuellement de le retrouver. Cependant, *« le risque maintenant est que de puissants systèmes militaires de cryptage soient utilisés »* obligeant les victimes à payer la rançon pour en être libérés, avertit le magazine *New Scientist*. Ce système de chantage est déjà utilisé par de nombreux pirates qui menacent de paralyser des systèmes informatiques de grandes entreprises ou de sites Internet (casinos, paris en ligne). Mais jusqu’à présent, les particuliers n’avaient pas été visés.