

Netsky-Q : la 17ème variante attaque et parle

Netsky-Q ne changera rien à la routine qui semble s'installer autour des attaques par emails des Bagle et autres vers. La nouvelle variante, la 17ème, se présente sous la forme d'un retour d'email erroné, avec en objet un message d'erreur »

Delivery Error , « *Error* » ou « *Server Error* ». Le message « *Mail Delivery ? This email couldn't be displayed* » invite le destinataire à ouvrir le message rejeté proposé en « *binary attachment* ». C'est donc à l'ouverture du fichier attaché en extension .pif ou .zip que le ver s'attaque aux systèmes non protégés. **Des attaques programmées** Le virus s'installe lui-même sur les machines Windows à l'ouverture du fichier attaché. Il se répand sur le disque dur de la machine infectée et récupère les adresses email afin de pouvoir les exploiter à certaines dates. Netsky-Q est programmé pour s'auto diffuser sur les adresses repérées le 31 mars et les 5, 12, 19 et 26 avril. De plus, il lancera des attaques par déni de services sur des sites de '*peer to peer*', dont Kazaa et eDonkey, ainsi que sur des sites pirates comme Cracks.am, les 7 et 12 avril. **Netsky-Q parle !** Dans le message caché qui accompagne le ver, les auteurs de Netsky, qui se disent être un groupe de bénévoles basé en Russie et dénommé SkyNet Antivirus, affirment qu'ils distinguent leur création des autres vers par le fait qu'ils n'ouvrent pas de '*back doors*' sur les sites qu'ils infectent, et que donc leurs attaques ne permettent pas de servir de relais pour des messages spammés, ni pour faciliter l'intrusion sur les postes. « *We don't have any criminal inspiration* », 'nous n'avons pas d'inspiration criminelle'? Etonnant discours qui voudrait faire croire qu'il pourrait y avoir de bons et de mauvais auteurs de virus ! En tous cas, les auteurs de Netsky-Q confirment une nouvelle fois leur opposition aux auteurs des « *intrusions, qui partagent des substances et du contenu illégaux* ». Autant le dire plus directement : la guerre entre Netsky et Bagle continue ! Quoi qu'il en soit, il est peu probable que les victimes de vers et virus apprécient la démarche de Netsky, car quel que soit l'origine de l'attaque, les résultats sont les mêmes et les victimes aussi désemparées...