Virus: un faux mail du FBI utilise le ver Sober

Le fameux et tristement célèbre ver Sober fait son retour (un de plus !) dans nos PC. Pour s'incruster, le virus tente de duper l'utilisateur en se dissimulant derrière un faux mail du FBI, la police fédérale américaine, ou de la CIA, service de contre-espionnage.

Repérés entre autres par Sophos, ces mails *« disent à la personne qui les reçoit que leur compte internet a été surveillé par le FBI et qu'ils ont visité des sites illégaux. Ces courriels demandent à leurs destinataires d'ouvrir un dossier attaché et de répondre à des questions »*, indique le FBI dans un communiqué. Voici le texte en anglais: *« Dear Sir/Madam, We have logged your IP-address on more than 30 illegal Websites. Important: Please answer our questions! The list of questions are attached. Yours faithfully, Steven Allison, Federal Bureau of Investigation-FBI- 935 Pennsylvania Avenue, NW , Room 3220 Washington , DC 20535 Phone: (202) 324-30000 »* Observons le souci du détail des créateurs de cette attaque: adresse, numéro de téléphone, et même numéro de bureau. Evidemment, en ouvrant le dit fichier joint, le ver collecte d'autres adresses électroniques sur le disque dur, à la recherche de nouveaux ordinateurs à infecter. Et il ouvre une « back door » (ou porte arrière) permettant une prise de contrôle du PC à distance. *« Cette variante du ver Sober tente de piéger les utilisateurs en jouant sur deux tableaux : le désir d'aider la police dans ses recherches, et la crainte d'être faussement accusé de fréquenter des sites illégaux »*, commente Annie Gay, dg de Sophos France et Europe du Sud. L'éditeur de sécurité précise: *« Au cours des dernières heures, le ver a représenté plus de 65% des virus signalés à Sophos, ce qui en fait actuellement le virus le plus répandu dans le monde »*. Un constat partagé par F-Secure qui estime quee ver est le plus répandu de l'année. De son côté, le FBI déclare qu'il « *prend cette affaire très au sérieux et a ouvert une enquête »*. Notons enfin que des attaques similaires ont été rapportées en Allemagne, où les courriels portaient l'adresse du BKA, la police criminelle fédérale allemande.