Un nouveau ver Sober déferle, toujours aussi virulent

Depuis ce dimanche, les messageries professionnelles sont inondées de mails rédigés en langue allemande. Leur contenu? Les bombardements de la Seconde guerre mondiale, le génocide arménien, l'entrée de la Turquie en Europe… Leur objectif: véhiculer la énième version de Sober, en l'occurrence la variante Q.

Sober.Q est un Cheval de Troie qui utilise la porte laissée grande ouverte par son prédécesseur déjà très virulent, qui promettait aux internautes des billets pour la prochaine coupe du monde de football. Sober.Q a littéralement inondé les messageries allemandes, suisses et autrichiennes pendant ce week-end de Pentecôte. Il se propage désormais dans le reste de l'Europe et notamment en France. Lorsqu'il est exécuté, Sober.Q envoie massivement des mails de propagande politique en allemand aux adresses présentes dans le carnet d'adresses et divers autres fichiers, en utilisant une adresse d'expéditeur falsifiée et sans attacher de fichier. Il utilise son propre serveur SMTP pour se répandre, supprime certains fichiers d'antivirus notamment ceux de la fonction LiveUpdate de Norton. Selon une étude de l'équipe CSRT de l'éditeur Aladdin, 30% des e-mails reçus sur les réseaux d'entreprise sont contaminés essentiellement par les variantes de la souche Sober.