Alerte : le virus Mitglieder fera-t-il pire que Sober ?

Nouvelle variante d'une famille de chevaux de Troie déjà riche de menaces,

Mitglieder.GB est la dernière version en date à se propager massivement sur la toile. S'il est présent mondialement, il se diffuse rapidement en Europe, et plus particulièrement en Pologne, Belgique et France. C'est la seconde vague d'attaques enregistrée ce mois de novembre, et comme la première, le PandaLabs la qualifie d'**alerte orange**. Comme tout cheval de Troie, Mitglieder.GB se cache derrière un mail, en l'occurrence un fichier attaché compressé. En revanche, à la différence de ses nombreux confrères qui évoluent cachés, ses symptômes d'affections sont visibles : lorsque l'internaute lance l'ouverture du fichier vérolé, il ouvre le lecteur d'images dans Windows et affiche le logo d'un système d'exploitation avec un fond blanc légèrement flouté. Une fois installé, Mitglieder.GB insère des clés dans la base de registre pour s'assurer de son exécution à chaque démarrage de l'ordinateur et essaie aléatoirement de se connecter à une série de 50 adresses URLs inscrites dans son code, afin d'accéder au fichier z.php, utilisé notamment pour télécharger d'autres malwares dans le système ou être lui-même un malware. ?*Nous vivons une période de très forte activité pour certaines familles de malware, comme Bagle, Mitglieder ou Sober, avec un grand nombre de variantes diffusées dans un laps de temps très court*?, confirme Luis Corrons, directeur de PandaLabs de Panda Software. ?*L'objectif principal est de sortir un grand nombre de variantes simultanément de sorte que le nombre d'emails infectés en circulation soit extrêmement élevé, provoquant une confusion totale auprès des utilisateurs*?.