

250.000 nouveaux PC zombies par jour!

CipherTrust, le fabricant des appliances de sécurisation des messageries d'entreprise IronMail, recueille quotidiennement des informations en provenance de ses 4.000 appliances en place dans les entreprises.

De quoi être en prise directe avec l'évolution des menaces qui se diffusent via les courriels et faire un constat alarmant. L'été avait pourtant laissé planer l'espoir d'une inversion de la tendance, avec un repli des volumes de spams. Mais c'était sans compter sur la recrudescence du ver Sober, bien décidé à rappeler que la menace demeure et à faire exploser les statistiques. Ainsi, selon CipherTrust, la nouvelle variante de Sober comptabiliserait à elle seule plus de 500.000 infections de machines depuis son introduction. Et Sober n'est pas seul? Le 3 novembre, l'introduction de nouvelles variantes de Mytob et Bagle a augmenté en une nuit de 8% le volume global des courriels. Le 21 novembre, Sober seul a augmenté de 15% le volume du spam. *« Alors que nous avons constaté l'été dernier une légère baisse du volume des spams, le mois de novembre indique une toute autre tendance. La propagation de ces menaces prouve bien que les 'spammeurs' et les pirates sont plus actifs que jamais »*, a déclaré Paul Judge, CTO de CipherTrust. Plus inquiétant encore. TrustedSource, le moteur global de corrélations de menaces de CipherTrust, identifiait une moyenne de 170.000 nouvelles machines zombies infectées chaque jour. Depuis la diffusion de la variante Sober, le nombre total des machines transférant le message spammé et le virus qui l'accompagne a augmenté de presque 50%, portant la moyenne journalière de nouvelles adresses IP infectées à plus de 250.000. *« Ceci est particulièrement significatif, dans la mesure où cette recrudescence en messages non sollicités a un coût, qu'il s'agisse de consommation de bande passante, de stockage, ou encore de consommation de ressources internes »*. Constat d'autant plus alarmant, à l'heure où les outils de lutte contre le spam et les antivirus se multiplient, qu'en théorie la conscience de l'internaute progresse et que les fournisseurs d'accès affirment bloquer la majorité des messages spammés. Mais alors comment lutter contre le phénomène ? Les entreprises ont aujourd'hui l'obligation d'implémenter de nouvelles stratégies de sécurité évolutives, englobant les passerelles et l'ensemble du périmètre réseau, afin de se protéger contre l'augmentation croissante des messages non sollicités et l'augmentation des machines zombies diffusant les spams, les virus et les attaques par usurpation d'identité. CipherTrust ne nous contredira pas !