Alerte au ‘Ver’: Bugbear.B est très virulent

Ce ver Bugbear, aussi nommé Tanatos, est une résurgence: il est du type polymorphe (il échappe à la détection en changeant d’aspect), très gourmand, et potentiellement dangereux. Sa nouvelle version, Bugbear.B (Tanatos.B) a sans doute été développée par des ‘hackers’ qui cherchent à pénétrer les systèmes bancaires.

L’augmentation considérable du nombre de postes infectés en quelques heures en fait une menace suffisamment sérieuse pour que F-Secure, Trend ou Sophos relèvent leur niveau d’alerte. Il se propage à travers le Web à l’aide d’un moteur SMTP, et se cache derrière les fichiers attachés aux emails. Il s’attaque aux serveurs de réseaux des systèmes bancaires. Parfois, il déclenche des paiements automatiques. Et il peut aussi s’étendre en ouvrant des fichiers partagés de Windows. Particulièrement vicieux, Bugbear.B sait contourner certains antivirus, ainsi que des pare-feux (*firewalls*). Il peut donc ouvrir une ‘*back door*‘ sur les PC, et donner accès aux contenus des disques durs. Plus d’infos sur Bugbear/Tanatos sur les sites de F-Secure, Trend Micro ou Sophos. http://www.sophos.fr/virusinfo/analyses/w32bugbearb.html http://www.f-secure.com/v-descs/bugbear_b.shtml **Les conseils de Sophos**

Dans un communiqué de presse, Sophos France a confirmé l’alerte sur le virus Bugbear.B, et rapelé les quelques mesures qui s’imposent, et que tous les internautee devraient connaitre :

– Mettre à jour la protection antivirale. Cette opération doit anticiper le retour des salariés. Annie Gay, directeur général de Sophos France rappelle que « *les vers de messageries suivent souvent le soleil*« . L’explosion de la propagation de Bugbear-B a accompagné l’arrivée des utilisateurs américains en début de journée. L’ouverture des entreprises ce vendredi dans la matinée pourrait signifier le même mouvement sur l’Europe. – Bloquer systématiquement les transfertse de programmes Windows au niveau de la passerelle de messagerie. – S’assurer des dernières mises à jour d’Internet Explorer et d’Outlook. Nous l’évoquons régulièrement, mais la plupart des virus exploitent des failles connues et corrigées. – Respecter attentivement les règles de sécurité, inciter les usagers à adopter un comportement responsable, les pousser à la prudence.