Communiqué de presse,

F-Secure met en garde contre un nouveau ver affectant les réseaux d'entreprise

Helsinki, Finlande, le 7 Janvier 2009 : F-Secure Corporation lance une alerte concernant les nouvelles versions du ver "Downadup". Ce ver infecte les postes de travail et serveurs Windows, provoquant divers problèmes importants. Depuis le début de l'année, plusieurs infections par des variantes de ce ver ayant touché des réseaux d'entreprise ont été signalées à F-Secure dans plusieurs pays.

Pour lutter contre la diffusion de ce ver, F-Secure travaille de concert avec les entreprises ayant été affectées et différents centres d'alertes.

Downadup (également connu sous le nom de Conficker) fait partie d'une grande famille de vers ciblant le réseau. Ils sont particulièrement difficiles à éliminer, surtout s'ils infectent le réseau interne d'une entreprise.

Que faire pour éviter la contamination :

- Assurez-vous que les derniers correctifs de Microsoft ont été appliqués

- Assurez-vous que l'antivirus de votre entreprise est bien à jour
- Vérifiez que l'antivirus a bien téléchargé les dernières mises à jour
- Désactivez les modes AUTORUN et AUTOPLAY pour les clés USB
- Assurez-vous que les mots de passe de domaine des utilisateurs sont suffisamment complexes

Que faire si votre réseau est déjà infecté :

- Vérifiez le site Internet de votre éditeur d'antivirus pour en savoir plus sur le processus de désinfection
- La désinfection de ce ver est complexe et vous pourriez avoir besoin de fermer certaines parties de votre réseau
- Restreignez l'utilisation des clé USB et bloquez le trafic inutile au niveau du pare-feu

Comment le ver agit-il ?

Downadup utilise plusieurs moyens de propagation, notamment via la vulnérabilité tout récemment corrigée dans Windows Server Service, en devinant les mots de passe réseau

et infectant les clés USB. Par conséquent, une fois que le malware accède au réseau interne de l'entreprise, il peut être particulièrement difficile à éradiquer.

Les problèmes les plus souvent rencontrés à la suite de l'infection par ce ver sont, notamment, le verrouillage des comptes utilisateurs réseau. En tentant de connaître les mots de passe réseau, le ver déclenche le verrouillage automatique comme un utilisateur ayant tapé un mot de passe erroné plusieurs fois.

Une fois que ce ver infecte une machine, il se protège de façon très agressive. Il se paramètre pour s'exécuter très tôt dans le processus de redémarrage de la machine. Il s'arrange également pour donner les droits d'accès aux fichiers et clés de registre du ver de sorte que l'utilisateur ne puisse ni les supprimer, ni les changer.

Le ver télécharge, à partir de nombreux sites web, des versions modifiées de lui-même. Les noms de ces sites sont générés par un algorithme en fonction de la date et de l'heure actuelle. Parce qu'il existe des centaines de noms de domaines sur lesquels peut s'appuyer le malware, il est difficile pour les éditeurs de sécurité de tous les localiser et les fermer à temps.

Pour plus d'informations sur les logiciels malveillants sur le blog de F-Secure, connectez-vous à: http://www.f-secure.com/weblog/

F-Secure met également à votre disposition un nouvel outil permettant de supprimer les versions connues de Downadup. Cet outil est disponible sur le blog de F-Secure.

A propos de F-Secure Corporation

F-Secure Corporation protège les particuliers et les entreprises contre les virus informatiques et autres menaces qui se répandent via Internet et les réseaux de téléphonie mobile. Les solutions de F-Secure sont disponibles à l'abonnement auprès de plus de 170 partenaires fournisseurs d'accès Internet et opérateurs mobiles dans le monde entier, faisant ainsi de F-Secure le leader mondial de ce marché. Elles sont également disponibles sous forme de licence auprès de milliers de revendeurs dans le monde entier. La société a pour but de devenir le fournisseur le plus fiable de solutions de sécurisation et de rendre le mode de vie connecté des utilisateurs de PC et de smartphones aussi simple et sécurisé que possible. Mesurés par des organismes indépendants, les temps de réponse de la société aux menaces informatiques, plus courts que ceux de ces concurrents, sont une bonne preuve de cette politique. Fondée en 1988, la société F-Secure est cotée sur le marché boursier d'Helsinki depuis 1999, et sa croissance a toujours été plus rapide que celle de ses concurrents également côtés en bourse. Des informations en temps réel sur les toutes dernières menaces virales sont disponibles sur le blog du laboratoire de recherche antivirus de F-Secure à l'adresse http://www.f-secure.com/weblog/.