F-Secure constate de nouvelles attaques contre les réseaux d'entreprise

F-Secure Corporation vient de lancer une alerte concernant la circulation d'une **nouvelle version d'un ver informatique** appelé « **Downadup**« . Ce malware dont la terminologie complète est W32.Downadup à la vocation de s **'i**

ntroduire dans les postes de travail et serveurs Windows.

F-Secure établit alors un constat : « *Depuis le début de l'année, plusieurs infections par des variantes de ce ver ayant touché des* ***réseaux d'entreprise*** *nous ont été signalées dans plusieurs pays*« . Le malware aussi appelé **Conficker** fait partie de la famille des vers s'attaquant principalement aux réseaux plutôt qu'aux données propres. « ***Une catégorie particulièrement difficile à éliminer*** » nous confie l'éditeur d'Helsinki.

D'autant que le ver utilise divers moyens de propagation, notamment grâce à une vulnérabilité récemment corrigée dans **Windows Server Service**. **W32.Downadup** devine alors les mots de passe réseau et infecte les supports externes. Un motif contre lequel il est nécessaire de **désactiver les fonctions Autorun ou Autoplay des clés USB,** histoire de ne pas encourager la propagation du virus.

Les effets du virus sont dès lors bien connus. La première conséquence de l'infection est le **verrouillage des comptes nécessitant des codes d'accès**. Un peu comme si un utilisateur avait tapé un mot de passe erroné plusieurs fois. De même, ce ver malotru s'arrange pour **se donner les droits d'accès aux fichiers et clés de registre.** Ainsi, l'utilisateur ne peut ni les supprimer, ni les changer.

Dès lors, les préconisations traditionnelles existent pour éviter d'être contaminé. Chacun doit s'assurer de la **correcte installation des dernières mises à jour Microsoft.** Mais aussi d'avoir un **antivirus à jour** et des mots de passe et identifiants suffisamment complexes pour ne pas être piratés.

En cas d'infection, la solution est différente. F-Secure prévient : « *La* ***désinfection de ce ver est complexe*** *et vous pourriez avoir besoin de fermer certaines parties de votre réseau. Il va donc vous falloir bloquer le trafic inutile au niveau du pare-feu*« . D'autant que le **ver vit sa propre existence en téléchargeant des versions modifiées de lui-même**. Un malware des plus malins donc. A prendre très au sérieux.