Alerte au virus Wallon: ne pas ouvrir un faux lien Yahoo!

Sasser n'est pas encore mort que déjà, les éditeurs de sécurité nous signalent la prolifération préoccupante du ver Wallon, apparu ce mardi 11 mai sur les réseaux. F-Secure le classe en 'Level 2', soit le deuxième niveau d'alerte le plus élevé.

Le virus se propage via les e-mails. Contrairement à d'autres virus 'mass-mailer', Wallon ne contient pas un fichier attaché. Son astuce est qu'il contient un faux lien Yahoo qui prend la forme suivante: https://drs.yahoo.com/nom de domaine connu/NEWS (cf. copie d'écran). En cliquant sur le lien, un script est téléchargé (« terra.html ») qui permet d'aspirer et d'exécuter un autre élément du virus (« sys.chm »). L'exécution de ce fichier télécharge « sys.exe » qui écrase le fichier Windows Media Player (« wmplayer.exe »). A chaque ouverture du lecteur multimédia de Microsoft, ce module « sys.exe » est exécuté sur le système. Ce programme a pour objectif de télécharger un fichier appellé « NOT.EXE » qui remplace dans la racine du répertoire 'C:/' le programme « ALPHA.EXE ». Ce « sys.exe » modifie également la page de démarrage d'Internet Explorer pour la faire pointer vers Google.com ou un autre moteur, « Super-fast-search.apsua.com. » (A suivre)